UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

PROPUESTA DE POLÍTICAS, BASADAS EN BUENAS PRÁCTICAS, PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE PAITA; 2016.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

BACH. RONALD EDUARDO DE LA CRUZ VARGAS

ASESOR:

MGTR. ING. CIP. VÍCTOR ÁNGEL ANCAJIMA MIÑÁN

PIURA – PERÚ

2016

JURADO EVALUADOR DE TESIS

ING. CIP. RICARDO EDWIN MORE REAÑO

PRESIDENTE

ING. CIP. JENNIFER DENISSE SULLÓN CHINGA

SECRETARIA

ING. CIP. MARIO ENRIQUE NIZAMA REYES MSc.

MIEMBRO

DEDICATORIA

A mi amada esposa Isabel por su apoyo y motivación incondicional al estar siempre a mi lado liberándome incluso de los quehaceres y preocupaciones cotidianas, permitiéndome así, dedicar y centrar mi esfuerzo en la consecución de mis metas profesionales.

A mis queridos hijos Gabrielita y Santiaguito esperando que el esfuerzo plasmado en la realización de esta tesis, se constituya en estímulo y ejemplo en el futuro a seguir para la realización de sus metas profesionales.

A mis queridos padres Melva y Eduardo por ser quienes estuvieron apoyándome a lo largo de mis estudios que con sus consejos y sacrificio me inspiran para seguir siempre adelante para alcanzar la meta de ser un profesional.

Los amo con todo mi corazón.

AGRADECIMIENTO

Mis más infinitas gracias a Dios por brindarme la oportunidad y la dicha de vivir, por la salud de mis seres queridos y por proveer los medios necesarios para continuar mi formación a lo largo de mi carrera universitaria.

A nuestro Asesor MGTR. ING. CIP. Víctor Ángel Ancajima Miñán, por su valioso aporte tanto en lo profesional como en lo personal, nos ha permitido lograr la tesis.

Al Subgerente de Sistemas e Informática de la Municipalidad Provincial de Paita y a todos los servidores municipales quienes decidieron confiar en mí, por brindarme las facilidades para la realización de la tesis.

A mis hermanos, personas que llegaron a mi vida y al compañero de proyectos porque guardo las enseñanzas y consejos que alguna vez me dio.

RESUMEN

La investigación tuvo como objetivo general, realizar la propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; en el año 2016. El tipo y diseño de la investigación es no experimental, descriptiva, de corte transversal y cuantitativa, para el recojo de información se escogió una muestra seleccionada de 152 trabajadores constituidos de la siguiente manera para la dimensión: Evaluación del estado actual de la seguridad de la información estuvo conformada por 152 trabajadores municipales, para la dimensión: Factibilidad técnica, económica y operativa de la propuesta se escogió a 08 trabajadores municipales y para la dimensión: Propuesta de Políticas del Plan de Gestión de Seguridad de la Información se aplicó a 02 trabajadores municipales, a quienes se les aplicó un cuestionario de 10 preguntas cerradas, aplicando la técnica de la encuesta. Obteniéndose los siguientes resultados: el 72.37% de los empleados municipales opinan que SI se encuentran expuestos a riesgos y amenazas, el 100.00% de los empleados municipales encuestados opinan que SI existe factibilidad técnica, económica y operativa de la propuesta, el 100.00% de los empleados municipales encuestados opinaron que NO existen controles pertinentes en cuanto a la seguridad de la información. Finalmente, las conclusiones y recomendaciones son: la Municipalidad Provincial de Paita carece de políticas y controles eficientes por lo tanto queda demostrado que es necesario la elaboración de una propuesta el mismo que permitirá minimizar la pérdida de información.

Palabras clave: Información, Activo, Seguridad de la Información.

ABSTRACT

The research was general objective, the proposal make policies based on best practices for managing information security in the Provincial Municipality of Paita; in 2016. The type and design of the research is not experimental, descriptive, cross-sectional and quantitative information gathering for a selected sample of 152 workers constituted as follows was chosen for the dimension: Assessment of current status security information consisted of 152 municipal workers, for the dimension: technical, economic and operational feasibility of the proposed 08 municipal workers were chosen and dimension: proposed Policy Plan Management information security is he applied until 02 municipal workers, who were applied a questionnaire 10 closed questions, using the survey technique. Obtaining the following results: 72.37% of municipal employees believe that if they are exposed to risks and threats, 100.00% of municipal employees surveyed say that if there is technical, economic and operational feasibility of the proposal, 100.00% of the municipal employees surveyed felt that there are no relevant controls regarding security of information. Finally, conclusions and recommendations are: the Provincial Municipality of Paita lacks efficient policies and controls therefore demonstrated that the development of a proposal required the same which will minimize the loss of information.

Keywords: Information, Active, Information Security

ÍNDICE DE CONTENIDO

JURADO EVALUADOR DE TESIS ii
DEDICATORIA iii
AGRADECIMIENTO iv
RESUMEN v
ABSTRACT vi
ÍNDICE DE CONTENIDO vii
ÍNDICE DE TABLAS ix
ÍNDICE DE GRÁFICOS xi
I. INTRODUCCIÓN 1
II. REVISIÓN DE LA LITERATURA 13
2.1. Antecedentes 13
2.1.1. Antecedentes a nivel internacional 13
2.1.2. Antecedentes a nivel nacional 18
2.1.3. Antecedentes a nivel regional 21
2.2. Bases teóricas 22
2.2.1. El Sector Público en Perú 22
2.2.2. Las Municipalidades en Perú 25
2.2.3. Municipalidad Provincial de Paita 33
2.2.4. Las Tecnologías de información y comunicaciones (TIC) 64
2.2.5. Norma Técnica Peruana NTP 70
2.2.6. ISO/IEC 76
2.2.7. ISO/IEC 27000 76
2.2.8. Norma Técnica de Gestión de Seguridad de la Información 27001 y su uso obligatorio 79
2.3. Sistema de hipótesis 90
2.3.1. Hipótesis principal 90
2.3.1. Hipótesis especificas 90
III. METODOLOGÍA 91
3.1. Diseño de la investigación 91

3.2. Población y Muestra 93
3.3. Técnicas e instrumentos. 95
3.3.1. Técnica 95
3.3.2. Instrumentos 95
3.4. Procedimiento de recolección de datos. 96
3.5. Definición operacional de las variables en estudio 97
3.6. Plan de análisis 98
IV. . RESULTADOS 99
4.1. Resultados 99
4.2. Análisis de resultados 137
4.3. Diseño de Propuesta de Seguridad de la Información 140
4.3.1. Propuesta de mejora 140
4.3.2. Diagrama de Gantt para el diseño de la propuesta 319
4.3.3. Presupuesto del diseño de la propuesta 320
V. CONCLUSIONES 321
VI. . RECOMENDACIONES 323
REFERENCIAS BIBLIOGRÁFICAS 325
ANEXOS 331
ANEXO Nº 1: CRONOGRAMA DE ACTIVIDADES 332
ANEXO Nº 2: PRESUPUESTO 334
ANEXO Nº 3: CUESTIONARIO 335
ANEXO Nº 4: COSTO DEL PROYECTO EN EL MERCADO: SISTEMA NACIONAL DE INVERSIÓN PÚBLICA (CODIGO SNIP: 268985) 338

ÍNDICE DE TABLAS

Tabla Nº 1: Número de Municipalidades, Población total proyectada 2015. 32
Tabla Nº 2: Provincia de Paita, Dispositivo Legal de Creación. 35
Tabla Nº 3: Provincia de Paita, Municipalidades de Centros Poblados..... 35
Tabla Nº 4: Hardware – Equipos Informáticos del Palacio Municipal. 57
Tabla Nº 5: Hardware – Equipos Informáticos de la GAT 58
Tabla Nº 6: Sistemas Operativos de la Municipalidad de Paita..... 58
Tabla Nº 7: Equipos de Comunicación y Transmisión de datos..... 59
Tabla Nº 8: Servidores 59
Tabla Nº 9: Estaciones de Trabajo 60
Tabla Nº 10: Sistemas Operativos 60
Tabla Nº 11: Software – Inventario software - Licencias 61
Tabla Nº 12: Población 93
Tabla Nº 13: Conocimiento de un plan de seguridad de información 99
Tabla Nº 14: Aprobación del diseño de un plan de seguridad de información..... 100
Tabla Nº 15: Aceptación de la aplicación del plan de seguridad de la información 101
Tabla Nº 16: Aceptación de implementación del plan de seguridad de información 102
Tabla Nº 17: Aprobación de programas de sensibilización 103
Tabla Nº 18: Colaboración con la implementación del plan de seguridad 104
Tabla Nº 19: Conocimiento de un plan de recuperación ante desastres 105
Tabla Nº 20: Conocimiento de evaluaciones realizadas de riesgos 106
Tabla Nº 21: Conocimiento de evaluaciones de vulnerabilidades de la red 107
Tabla Nº 22: Conocimiento sobre software antivirus actualizado..... 108
Tabla Nº 23: Conocimiento e Importancia de la Norma ISO/IEC 27001:2014..... 109
Tabla Nº 24: Capacidad de liderar el Proyecto 110
Tabla Nº 25: Capacitación o asistencia técnica brindada por la ONGEI..... 111
Tabla Nº 26: Desarrollo de la propuesta en equipamiento informático suficiente .. 112
Tabla Nº 27: Aprobación del diseño del plan de seguridad de la información..... 113
Tabla Nº 28: Disponibilidad para formarse en el desarrollo de cada fase del sistema de gestión de seguridad de la información 114

Tabla Nº 29: Disponibilidad de asumir costos de implementación de la propuesta 115
Tabla Nº 30: Conocimiento y experiencia en aspectos de seguridad tecnológica... 116
Tabla Nº 31: Conocimiento sobre incidentes de seguridad 117
Tabla Nº 32: Colaboración en el desarrollo del plan de seguridad de información 118
Tabla Nº 33: Importancia de políticas de seguridad para la plataforma tecnológica119
Tabla Nº 34: Existencia de un documentos de políticas de seguridad 120
Tabla Nº 35: Conocimiento de algún estándar de seguridad de información 121
Tabla Nº 36: Responsabilidad del personal en el manejo de la información..... 122
Tabla Nº 37: Conocimiento de programas de sensibilización 123
Tabla Nº 38: Conocimiento de la existencia de acuerdos de confidencialidad 124
Tabla Nº 39: Importancia de realización de pruebas de penetración perimetral 125
Tabla Nº 40: Existencia de un documento de responsabilidades de los empleados 126
Tabla Nº 41: Conocimiento de planes de contingencia en pérdida de información 127
Tabla Nº 42: Conocimiento de revisiones periódicas de riesgos internos 128
Tabla Nº 43: Dimensión Evaluación del estado actual de la seguridad de la información..... 129
Tabla Nº 44: Dimensión de la Factibilidad Técnica, Económica y Operativa de la Propuesta 131
Tabla Nº 45: Dimensión de la Necesidad y diseño de la propuesta de políticas del plan de gestión de seguridad de la información 133
Tabla Nº 46: Resumen general por dimensiones 135
Tabla Nº 47: Encabezado para todas las páginas..... 141
Tabla Nº 48: Cuadro de Control Documental..... 141
Tabla Nº 49: Cuadro de Control de Versiones..... 141
Tabla Nº 50: Cuadro de Historial de Revisiones 142
Tabla Nº 51: Cuadro de Aprobación..... 142
Tabla Nº 52: Cuadro de Mejora Continua 142
Tabla Nº 53: Cuadro de Responsabilidades Propuesto..... 316
Tabla Nº 54: Cuadro de conformidad y aprobación del proyecto 318

ÍNDICE DE GRÁFICOS

Gráfico Nº 1: Vulnerabilidades los sistemas de información en el 2013 2
Gráfico Nº 2: Frontis del Palacio Municipal de Paita 5
Gráfico Nº 3: Mapa de la Región Piura 34
Gráfico Nº 4: Organigrama de la Municipalidad Provincial de Paita 42
Gráfico Nº 5: Organigrama de la Subgerencia de Sistemas e Informática 44
Gráfico Nº 6: Pantalla principal del SIAF-SP 48
Gráfico Nº 7: Sistema Integrado de Gestión Administrativa 49
Gráfico Nº 8: Pantalla del Sistema de Gestión Documentaria 50
Gráfico Nº 9: Pantalla Principal del SGTM - Paita 51
Gráfico Nº 10: Pantalla Principal Sistemas de Planillas 52
Gráfico Nº 11: Pantalla Principal de SIGEDEM Paita 53
Gráfico Nº 12: Pantalla Principal de Registro Civiles 54
Gráfico Nº 13: Pantalla Principal del Portal Web - MuniPaita 56
Gráfico Nº 14: Mapa de la Red Institucional - 2016 62
Gráfico Nº 15: Área de conectividad de la red de datos 63
Gráfico Nº 16: El Proceso de la Información 64
Gráfico Nº 17: Origen y Evolución de la TIC 66
Gráfico Nº 18: Ciclo DEMING 73
Gráfico Nº 19: Relación de los estándares de la familia del SGSI 79
Gráfico Nº 20: Estructura de la Seguridad NTP ISO/IEC 27001:2008 85
Gráfico Nº 21: Plan de Continuidad del Negocio 86
Gráfico Nº 22: Razones para tener un Plan de Continuidad del Negocio 87
Gráfico Nº 23: Resultados de la dimensión 01 130
Gráfico Nº 24: Resultados de la dimensión 02 132
Gráfico Nº 25: Resultados de la dimensión 03 134
Gráfico Nº 26: Resumen general de las dimensiones 136
Gráfico Nº 27: Modelo de Carátula 140
Gráfico Nº 28: Pie de Página para todo el documento 142

I. INTRODUCCIÓN

Desde sus orígenes la informática ha revolucionado la forma de actuar de las empresas, llegando a desempeñar un papel decisivo en el éxito de éstas. La constante aparición de nuevas plataformas tecnológicas y la posibilidad de interconectarse a través de redes, reporta incrementos significativos de la productividad y permite ampliar el mercado de negocio más allá de las fronteras nacionales. Esto ha generado grandes beneficios pero también nuevos retos hasta entonces no cubiertos en su totalidad, siendo uno de los más importantes la seguridad de la información. Los sistemas informáticos son vulnerables a multitud de amenazas que pueden ocasionar daños que resulten en pérdidas significativas. Los daños pueden variar desde simples errores en el uso de aplicaciones de gestión que comprometan la integridad de los datos, hasta catástrofes que inutilicen la totalidad de los sistemas. Las pérdidas pueden aparecer por la actividad de intrusos externos a la organización, por accesos fraudulentos, por accesos no autorizados, por el uso erróneo de los sistemas por parte de empleados propios, o por la aparición de eventualidades en general destructivas. En cualquier caso una correcta gestión de los riesgos debe implicar un profundo conocimiento de las vulnerabilidades de los sistemas y de las amenazas que los pueden explotar. Las propias características de las organizaciones deben influir en las medidas de seguridad que resulten más adecuadas y más eficientes en términos de costes, para contrarrestar las amenazas o incluso para tolerarlas conociendo en todo caso sus implicaciones. Aplicar políticas de seguridad permitirá un buen manejo de riesgos pues son normas y procedimientos internos que deben seguir los integrantes de la organización. Debe describirse la criticidad de los sistemas y de la información, los roles de cada puesto de trabajo y la mecánica de acceso a los sistemas, herramientas, documentación y cualquier otra componente del sistema de información. Conviene destacar que las políticas de seguridad deben emanar de la estrategia corporativa y que se trata de documentos que deberían conocer todos los integrantes de la Organización. La protección de los sistemas y de la información delimitada en políticas no suele eliminar completamente la posibilidad de que estos bienes sufran daños. En consecuencia, los gestores deben implantar aquellas medidas de seguridad que lleven los riesgos hasta niveles aceptables, contando para ello con el coste de las

medidas a implantar, con el valor de los bienes a proteger y con la cuantificación de las pérdidas que podrían derivarse de la aparición de determinado incidente de seguridad. La aplicación de políticas de seguridad es la mejor manera de controlar los riesgos que afrontan los sistemas informáticos en las organizaciones no con más tecnología sino con mejor tecnología (1).

Gráfico Nº 1: Vulnerabilidades los sistemas de información en el 2013

Fuente: blog.mp3.es (2).

El Gobierno Colombiano, ha reconocido a la información como un activo valioso que requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Es por ello que la Administración Central del Municipio de Santiago de Cali implementó el 22 de agosto del 2014 el Sistema de Gestión de Seguridad de la Información – SGSI, según lo indicado en la directriz presidencial de Gobierno en Línea, como una herramienta de gestión que permita identificar y minimizar los riesgos a los cuales se expone la información, ayudar a la reducción de costos operativos y financieros, establecer una cultura de seguridad

y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios vigentes. La Administración Central del Municipio de Santiago de Cali, identificó que los sistemas y red de información enfrentaban amenazas de seguridad que incluían, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, posibles daños y pérdida de información por causa de código malicioso, esta situación determinó la urgente necesidad de gestionar adecuadamente una política de seguridad integral de la información a fin de clarificar las acciones para minimizar los riesgos de seguridad (3).

En el Perú, expertos de seguridad de la información participaron en la mesa interdisciplinaria en la última edición del ESET Security Day Perú, denominada "Gestión de las vulnerabilidades en entornos corporativos", realizada en el año 2015, en la que panelistas como el director general de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros (PCM), Cesar Vílchez Inga; el Subgerente de Servicios de Tecnologías de la Información del Banco Central de Reserva del Perú (BCRP), Miguel Ángel Tejada Malaspina; y el gerente general de Open-Sec, Walter Cuestas Agramonte, abordaron varios temas de interés en los que destacan: Vulnerabilidades en los entornos corporativos, el perfil de los especialistas de seguridad de la información para las empresas y finalmente el mundo móvil y las empresas. En el tema de vulnerabilidades el Sr. Cesar Vílchez Inga manifestó que la ONGEI al interior de las entidades del Estado viene realizando un trabajo constante exigiendo que se actualicen los procedimientos y políticas de seguridad de la información, por su parte el funcionario de Open-Sec Sr. Walter Cuestas Agramonte indicó que "hay cierta periodicidad que definir para hacer análisis de vulnerabilidades, pero no hay un estándar para determinar la frecuencia". En el tema del perfil de los especialistas de seguridad de la información para las empresas, el funcionario del BCRP afirmó que estos profesionales deben contar con un "background de análisis de riesgos, así como conocer de los procedimientos de la empresa donde laboran y de informática". El director general de la ONGEI, señalo que es bueno conocer los antecedentes de la persona que se contrata, el perfil y la fidelización con la organización donde labora. "El área de seguridad debe monitorear lo que se hace

en cada empresa. El reto es saber quién controla al administrador de red, al administrador de correo, o a otros responsables". En relación al empleo del smartphone del usuario como dispositivo para laborar en la empresa, Walter Cuestas dijo que existe restricciones a los equipos móviles hace años, y que el "tema es la complejidad en la administración de estos equipos". Por su parte el Subgerente de Servicios de Tecnologías de la Información del BCRP expresó: "La gente vive con el equipo móvil y el mundo laboral no puede estar ajeno a eso. Más bien, debe desarrollarse una política de acceso móvil". Finalmente el director general de la ONGEI añadió que al Estado Peruano todavía le falta trabajar en cultura digital con los ciudadanos. "Por ejemplo, todo ciudadano que tenga una computadora, tableta, smartphone, etc. debe contar mínimamente con un software antivirus instalado que sea legal y actualizado" (4).

El Ministerio de Economía y Finanzas reconoce que la información generada, procesada o administrada en el ejercicio de sus funciones constituye un recurso de valiosa importancia para el eficaz desempeño institucional, siendo necesario resguardar y proteger dicha información así como los diversos medios físicos y electrónicos de soporte, almacenamiento, tratamiento, transporte y transmisión de modo que garantice el normal desarrollo de las labores del Ministerio, la seguridad de la información es declarada de absoluta relevancia en el quehacer diario del Ministerio, ya que por medio del cual se preservan la confidencialidad a los activos críticos de información en niveles adecuados que aseguren la prosecución confiables de las operaciones, contribuyendo así al efectivo cumplimiento de la misión y objetivos estratégicos institucionales. Por ello que en cumplimiento a la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información, Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos" se conformó el Grupo de Trabajo denominado "Comité de Gestión de Seguridad de la Información" como instancia administrativa responsable de dirigir, coordinar y revisar la puesta en práctica de la seguridad de la información; teniendo como una de sus funciones, proponer políticas y normatividad de seguridad de la información para su aprobación, en ese sentido mediante Resolución Ministerial Nº 081-2014-EF/44 del 28 de febrero del 2014 fue

aprobado el documento de gestión interna denominado: “Política de Seguridad de la Información del Ministerio de Economía y Finanzas” bajo un esquema de evaluación de los riesgos pertinentes y de permanente adaptación a los cambios en las necesidades y objetivos institucionales, requisitos de seguridad identificados, los procesos empleados, el tamaño y estructura organizacional del ministerio, con el fin de establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información en concordancia con las recomendaciones contenidas en normas técnicas peruanas, estándares internacionales y mejoras prácticas de la industria en seguridad de la información (5).

La Municipalidad Provincial de Paita, es el órgano de Gobierno Local con personería jurídica de derecho público, con autonomía política, económica y administrativa en los asuntos de su competencia, aplicando las leyes y disposiciones consagradas en la Constitución Política del Perú y la Ley Orgánica de Municipalidades Nº 27972 (6).

Gráfico Nº 2: Frontis del Palacio Municipal de Paita

Fuente: Paita virtual (7).

Según el Artículo 99º del Reglamento de Organización y Funciones – ROF, la Municipalidad Provincial de Paita, cuenta con la Subgerencia de Sistemas e Informática, la cual es un órgano de apoyo técnico de la gestión municipal, tiene como objetivo, hacer uso eficiente de la información y de las nuevas Tecnologías de Información y Comunicaciones TIC como recursos para proveer servicios de calidad, accesibles, seguros y oportunos a la propia Institución, en aplicación de las directivas, lineamientos y normas emitidas por la Oficina Nacional de Gobierno Electrónico e Informática ONGEI, ente rector del Sistema Nacional Informático y depende jerárquica, funcional y administrativamente de la Gerencia Municipal, le corresponde el tercer nivel orgánico (8).

Se ha observado que la Subgerencia de Sistemas e Informática no puede afrontar con eficiencia y eficazmente la demanda de servicios, debido al poco personal asignado, llegando a contar con solo dos técnicos en informática, una secretaria y el responsable del área quien asume múltiples funciones, cabe mencionar que el espacio de trabajo asignado a esta Subgerencia es muy reducida para que pueda cumplir sus funciones, y dentro del mismo espacio se aloja una pequeña zona de dos metros cuadrados para que opere la sala de servidores, además a simple vista se puede observar que el trabajo de cableado estructurado de la red dentro de las instalaciones del Palacio Municipal se encuentra en pésimas condiciones sin tener en cuenta el detalle técnico mínimo necesario para el diseño, instalación, configuración y correcto funcionamiento, de la infraestructura informática y de seguridad perimetral de la Municipalidad Provincial de Paita, que garantice la correcta operación de los servicios de telecomunicaciones con tecnología de vanguardia.

La Municipalidad Provincial de Paita, tiene actualmente equipos de cómputo de diversas generaciones, muchas de ellas con software obsoleto y bajo el sistema operativo Microsoft Windows XP o 7 los cuales Microsoft está dejando de dar soporte técnico, exponiéndolas a ser vulnerables a riesgos de seguridad. Tampoco cuenta con políticas de Normalización para la seguridad de la Información que permita evitar fugas y eliminación de información que pertenece a la institución.

El Estado Peruano a través del D.S. Nº 066-2011-PCM aprobó el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0", en cuya Matriz de Objetivos y Estrategias, establece la necesidad de promover una Administración Pública de calidad orientada a la población (9).

La Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado, aprobada por el Congreso de la República en el año 2002, establece en su artículo 1: "Declárese al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano" (10).

Se debe considerar, que mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información, código de buenas prácticas para la gestión de la seguridad de la información. 2da. Edición", en todas las entidades del Sistema Nacional de Informática; así mismo mediante Resolución Ministerial Nº 197-2011-PCM, se estableció el plazo para determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente el 23 de Mayo del 2012, mediante Resolución Ministerial Nº 129-2012-PCM, se estableció un nuevo cronograma y la incorporación del rol oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información", cuyos controles debieron ser implementados de acuerdo a las recomendaciones establecidas, Sin embargo, por desconocimiento de estos temas por parte de los organismos públicos, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno Electrónico e Informática. En la actualidad, el 08 de enero de 2016, mediante Resolución Ministerial Nº 004-2016-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de

seguridad de la Información. Requisitos. 2da. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo. Derogándose la R.M. 129-2012-PCM (11).

La Municipalidad Provincial de Paita, a pesar de ser integrante del Sistema Nacional de Informática, no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) en el marco de la norma NTP-ISO/IEC 27001:2014, que permita establecer una adecuada gestión de seguridad de la información y cumplir la normatividad vigente; es este sentido tampoco se ha realizado un diagnóstico previo del estado actual de la gestión de la seguridad de la información, ni ha establecido un plan de trabajo para la adecuación a la misma. Finalmente, no se ha realizado ningún proceso para mejorar la seguridad, evitar la fuga de información a través de políticas de uso de la información institucional; con lo cual es evidente un alto riesgo de pérdida de información.

En búsqueda de las mejoras continuas basadas en la NTP ISO 27001, la Municipalidad de Paita, debe iniciar el proceso de mejora en la plataforma tecnológica, con la finalidad de implementar los roles respectivos para el control y administración de los diferentes procesos administrados por la Municipalidad, además de contar con los documentos normativos respectivos para una mejor administración de los procesos.

En tal sentido, en la presente investigación se plantea presentar una alternativa de solución viable al siguiente enunciado del problema: ¿se podrá realizar una propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016, para minimizar el riesgo de pérdida de información?

En consideración al problema planteado y con la finalidad de resolver este enunciado se determinó el siguiente objetivo general:

Realizar la propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; en el año 2016, de tal forma que se minimice el riesgo de pérdida de información.

Con la finalidad de poder cumplir y lograr el objetivo general indicado en el párrafo anterior se hizo necesario determinar los siguientes objetivos específicos:

1. Efectuar un diagnóstico de la situación actual de la seguridad de la información en la Municipalidad Provincial de Paita, en cumplimiento de los requisitos establecidos en la NTP-ISO/IEC 27001:2014.

2. Determinar la factibilidad técnica, económica y operativa de la propuesta de políticas basadas en buenas prácticas para la gestión de seguridad de la información de acuerdo a la NTP-ISO/IEC 27001:2014.

3. Realizar la Propuesta de políticas basadas en buenas prácticas para la gestión de seguridad de la información de acuerdo a la NTP-ISO/IEC 27001:2014.

La Justificación de esta investigación se basa en que la seguridad de la información es el elemento muy importante en cualquier organización a tal punto que no es suficiente hacer grandes inversiones en sistemas y dispositivos de seguridad, para salvaguardar la integridad, la confidencialidad y la disponibilidad que manejan las entidades, sino que es necesario implementar y poner en funcionamiento sistemas de gestión de seguridad de la información; para tal fin es pertinente disponer de una la línea de base de control, como lo establece el diseño de la propuesta de políticas basadas en buenas prácticas para la gestión de seguridad de la información en la Municipalidad Provincial de Paita, de tal forma que permita administrar y salvaguardar la seguridad de la información, así como minimizar los efectos que

prevé amenazas o eventos adversos a la continuidad del funcionamiento de la institución.

Como Justificación Académica se usó los conocimientos adquiridos a través de todos los años de estudios en la Universidad Católica Los Ángeles de Chimbote – sede Piura, lo cual nos sirvió como base para evaluar la propuesta de políticas basadas en buenas prácticas para la gestión de seguridad de la información en la Municipalidad Provincial de Paita, de tal forma que se minimice el riesgo de pérdida de información.

Como Justificación Operativa se debe tener en cuenta que el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 en todas las entidades integrantes del Sistema Nacional de Informática, permite involucrar a toda la organización que incluye a la alta dirección, en ese aspecto el Subgerente de Informática y Sistemas ha participado en el taller de capacitación sobre los lineamientos del sistema de gestión de seguridad de la información, quedando demostrado la sostenibilidad de la propuesta, ya que la aplicabilidad del modelo en definitiva está también ligada a la capacitación del personal involucrado.

Como Justificación Económica se tiene que para la implementación de un sistema de gestión de seguridad de la información, se requiere invertir tanto en capital humano, como en tecnología, para ello el Subgerente de Informática y Sistemas presentó el año pasado un requerimiento de consultoría para el análisis de brechas y plan de adecuación a la NTP-ISO/IEC 27001:2008 "Sistemas de Gestión de Seguridad de la Información e Implementación de Políticas de Buenas Prácticas de Uso de Información Municipal" logrando ser incluido en el ¨Plan Operativo Anual, quedando pendiente su ejecución en el presente año que por la situación económica limitada de gastos no ha sido posible solventar su autogestión, sin embargo el proyecto se ejecutará de todas maneras ya que se cuenta con un plazo máximo de dos años para la implementación de la norma.

Como Justificación Tecnológica, se tuvo que la propuesta de políticas basadas en buenas prácticas para la gestión de seguridad de la información en la Municipalidad Provincial de Paita, proporcionará a la entidad una herramienta de soporte de información adecuado para el manejo de sus procesos el cual ayudará a la entidad a cumplir con los objetivos de seguridad de la información tales como: Minimizar el riesgo de pérdida de información, cumplir los principios de seguridad de la información e innovación tecnológica y asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Como Justificación Institucional se debe tener en cuenta que la Municipalidad Provincial de Paita, necesita estar alineada a las normas técnicas Internacionales, considerando que mediante de la Resolución Ministerial Nº 004-2016-PCM de fecha 08 de enero de 2016 se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, en ese sentido la propuesta de políticas basadas en buenas prácticas para la gestión de seguridad de la información en la Municipalidad Provincial de Paita, surge como una herramienta organizacional para para concientizar a sus miembros sobre la importancia y sensibilidad de la información, hay que considerar que existe plazos establecidos para que las entidades públicas puedan implementar y adecuar la norma.

El presente estudio se desarrolló únicamente en la Municipalidad Provincial de Paita, cuya política de seguridad se aplicará a todos los activos de información de su propiedad, en su inicio abarcó el diagnóstico de la situación actual de la municipalidad con el objeto de recolectar información sobre la seguridad de la información que maneja actualmente y así determinar sus deficiencias; se determinó la factibilidad técnica, económica y operativa de la Propuesta y posteriormente se pudo diseñar o realizar la propuesta de políticas basadas en buenas prácticas para la gestión de seguridad de la información de acuerdo a la

NTP-ISO/IEC 27001:2014, con la finalidad de minimizar el riesgo de pérdida de información e implementar los roles respectivos de control cuyos beneficios son los siguientes:

1. Beneficios Institucionales:

   - Permitirá contribuir al cumplimiento de los Objetivos Estratégicos y las metas dentro del contexto de la modernización de la gestión municipal y la normatividad vigente.

   - Mejorará la calidad de los servicios de la Institución.

   - Asegurará la continuidad de las operaciones, integridad de los datos y garantizará el acceso seguro a los usuarios, y los Sistemas de informáticos.

   - Mejorará la cultura organizacional en aspectos de seguridad de Información.

   - Permitirá cumplir con las leyes y normas gubernamentales relacionadas a la seguridad de Información.

2. Beneficios Externos:

   - Creará una ventaja competitiva, ante las instituciones estatales.

   - Mejorará la atención de los usuarios con relación a los servicios brindados.

   - Mejorará la imagen de la institución.

3. Beneficio Global:

   - Será una fuente de soporte y consulta para la implementación de la norma ISO 27001:2014, tal como lo recomienda la Presidencia del Consejo de Ministros PCM.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

En Venezuela, una investigación realizada en el año 2011 la cual se tituló "Diseño de un Plan de Gestión de Seguridad de la Información. Caso: Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara", se pudo constatar que existían varias deficiencias en los servicios de red que ofrecía este organismo, e incidían directa o indirectamente en la seguridad de la Alcaldía, de su personal y de la infraestructura. Entre algunas de las deficiencias puntualiza las siguientes: a) Carencia de un control de acceso efectivo a las instalaciones de la Alcaldía; b) Modificación de archivos por personas ajenas a la jefaturas de servicios; c) Ausencia de un Control continuo de la administración de los sistemas de antivirus pertenecientes a la red; d) Sustracción indebida de información por parte de los empleados que ya no ejercen funciones dentro de la institución; e) Existencia de usuarios que acceden a información que no es de su competencia. Todo ello le causa problemas a la institución como: acceso de personas no autorizadas a las instalaciones de la alcaldía, falta de continuidad en los procesos administrativos, presencia de virus en las computadoras de la alcaldía, pérdida de información requerida para la continuidad de los procesos administrativos, manejo de información por usuarios no autorizados, entre otros. Esta situación determinó la urgente necesidad de gestionar adecuadamente un plan de seguridad integral a fin de clarificar las acciones a tomarse en cuenta para minimizar los incidentes de seguridad. La investigación tuvo como objetivo fundamental diseñar un Plan de Gestión de Seguridad de la Información en la Alcaldía del Municipio Jiménez del Estado Lara. La investigación se enmarcó desde el punto de vista metodológico en la modalidad de proyecto factible, apoyado en la investigación monográfica

documental y de campo, el cual se dividió en tres fases: a) una primera fase de diagnóstico de la situación actual de la Alcaldía del Municipio Jiménez en relación a la seguridad de la información; b) seguida por la evaluación de la factibilidad técnica, económica y financiera de la propuesta; c) y por último el diseño del Plan de Seguridad de la Información de acuerdo a la norma ISO/IEC 27001:2005 aprobada por la Organización Internacional de Estandarización y por la Comisión Internacional Electrotécnica de sus siglas en ingles ISO/IEC. La importancia del diseño de dicho plan permitió determinar los objetivos, procesos y procedimientos para el establecimiento de políticas de seguridad, así como de un conjunto de controles de seguridad que ayudarán a gestionar los riesgos en la Seguridad de la Información que maneja el organismo objeto de estudio, mejorando de esta forma la gestión de los incidentes de seguridad que se detecten y generando resultados en concordancia con los objetivos y políticas requeridas para optimizar la Plataforma Tecnológica de la Alcaldía. En conclusión; se pudo evidenciar que la Alcaldía del Municipio Jiménez carece de políticas y controles eficientes en cuanto a: la seguridad de la red, resguardo de la información y manejo de los riesgos a los que está expuesta; se demostró que existe la factibilidad técnica, económica y operativa para diseñar el Plan de Seguridad de la Información; el diseño propuesto, permitirá brindar un esquema de seguridad más sólido y eficiente en el uso de los Sistemas de Información una vez implantado; cabe destacar que la Seguridad de la Información no depende única y exclusivamente del Diseño del Plan de Gestión de Seguridad; faltaría la implantación, evaluación y mejoras a dicho plan. Dentro de las recomendaciones se tuvieron las siguientes: a) Designar dentro de la estructura organizativa un ente que se responsabilice por la ejecución del Plan de Seguridad de la Información diseñado en este trabajo. b) Extender el Plan de Gestión de Seguridad de la Información presentado a los dominios no estudiados en este trabajo con la finalidad de definir completamente los riesgos a los que está sometida la información de la alcaldía del Municipio Jiménez y así tratarlos

adecuadamente. y c) Se hace indispensable mantener actualizada las normas, procedimientos y políticas de acuerdo a la dinámica en que vayan surgiendo nuevas estrategias de ataque contra los sistemas y sus activos de información, en concordancia con lo planteado por la norma que establece que se debe revisar y monitorear el plan de Gestión de Seguridad de la Información (12).

En Ecuador, una investigación realizada en el año 2011 la cual se denominó "Implementación de Políticas de Seguridad Informática para la M.I. Municipalidad de Guayaquil aplicando la Norma ISO/IEC 27002", se pretende dar una adecuada solución de seguridad a la M. I. Municipalidad de Guayaquil, tomando como base estándares internacionales. El primer capítulo presenta una introducción de lo que implica un Sistema de Gestión de Seguridad de la Información, es decir conceptos básicos, permitiendo tener una visión general y clara en donde se determina objetivos y acciones necesarias para conseguir que la entidad involucrada cuente con un conjunto de reglas y políticas para la seguridad y gestión de riesgos de la información. En el segundo capítulo se presenta los antecedentes, objetivos y funciones desempeñadas dentro de la Muy Ilustre Municipalidad de Guayaquil en donde se implementaría las Políticas de Seguridad de acuerdo a las Normas ISO/IEC 27002 y descripción de los departamentos y/o áreas en que se divide y su organigrama principal. El capítulo tres del manual presenta la metodología PDCA y los conceptos por cada una de las etapas implicadas en el modelo. Se detalla el Alcance que se desea establecer, indicando los lineamientos y principios a implementar, mantener y así mejorar la gestión de la seguridad de la información dentro del Municipio de Guayaquil. Continuando con una breve descripción de las políticas generales que se deben aplicar en el área de Informática. El capítulo cuatro describe la metodología MAGERIT con el concepto y ventajas principales de su implementación. Se detalla el inventario de Activos dentro del Departamento de Informática y de acuerdo al informe se realiza un exhaustivo análisis de riesgo con sus

apropiados criterios de valorización. En el capítulo cinco se explica la implementación de las políticas, descripción y objetivos por cada una. Se especifica el plan de tratamiento de riesgos a utilizar para la gestión de riesgos que se encontró en el Área de Informática. Y por último el capítulo seis son las estrategias de difusión que se aplicara para llegar a difundir las políticas dentro del Departamento. La forma de conseguir el mayor beneficio en seguridad de la información es contar con una adecuada evaluación de riesgos, que oriente las inversiones, que minimicen el impacto en casos de incidentes. Entre las conclusiones se tienen las siguientes: 1) La seguridad de la información no es una responsabilidad únicamente del área de tecnología, debe fluir desde la alta gerencia hacia todos los procesos de negocios. 2) Un comité de seguridad de la información compuesto por cada jefe de área genera más compromiso para hacer cumplir las políticas de seguridad de la información. 3) La organización debe entender la seguridad como un proceso que nunca termina. 4) Es de gran importancia limitar la asignación de privilegios, por lo que deberán estar perfectamente identificados y asignarse en base a la necesidad de uso. Los privilegios tienen que revisarse de forma periódica para evitar la existencia de privilegios que ya no son necesarios. Entre las recomendaciones tenemos: 1) Crear un Comité de Seguridad, Un Equipo de Seguridad de Información y un Equipo de Tecnología de la Información. 2) Habilitar un Centro de Cómputo alterno en un lugar distante al edificio principal donde funciona el Centro de Cómputo actual. 3) Para los usuarios de alto riesgos (cajeros, administradores, directores etc.), adquirir equipos con reconocimiento de huellas digitales. 4) Capacitar al personal municipal en el conocimiento básico de seguridades de la información prevención de virus, ingenierita social, respaldos de información etc. 5) Evaluar la posibilidad de adquirir Forefront Client Security y Forefront Server Security Management Console para obtener mayor protección, control y gestión de la seguridad de la estructura tecnológica. 6) Efectuar un Ethical Hacking para verificar las seguridades

a nivel de la red. 7) Planificar la realización de un simulacro de incendio y evacuación del personal de informática (13).

En Colombia, una investigación realizada en el año 2014 la cual se tituló "Diseño de Políticas de Seguridad de la Información para la Alcaldía Municipal de Rio de Oro, Cesar", en donde se pretende establecer una política de seguridad de la información para la Municipalidad de Rio de Oro, Cesar; compuesta de una serie de lineamiento de implementación, que contiene una clara definición de seguridad de la información, sus objetivos y alcances generales, importancia, intención de la administración en cuanto al tema de seguridad de la información, estructuras de evaluación y gestión de riesgos, definición de responsabilidades individuales en cuanto a la seguridad, entre otras. Determinando un alto compromiso de la Alcaldía con el proceso de gestión responsable de su información; donde en un inicio se efectuó el análisis de la situación actual de la Alcaldía en materia de seguridad para esto se contó con técnicas de recolección de información como encuestas, análisis y evaluación de riesgos y auditorias. Habiendo identificado las amenazas latentes se procedió con un proceso de planificación donde se estudió las diferentes normas existentes para la gestión de la seguridad de la información y con esto poder decidir qué modelo seguir para el diseño de las políticas. Se continuó documentando el modelo elegido para poder tener las pautas que permitan dictaminar los controles y la creación de un documento formal a fin de preservar los tres elementos principales de la información. Integridad, confidencialidad y disponibilidad (14).

2.1.2. Antecedentes a nivel nacional

En Chiclayo, una investigación de grado para optar el Título de Ingeniero de Sistemas y Computación realizada en el año 2008 titulado "Elaboración y Aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad tecnológica de la USAT" de la Universidad Católica Santo Toribio de Mogrovejo, concluye que en la actualidad las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones; también ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios los cuales se están volviendo cada vez más comunes, ambiciosos y sofisticados. Pues teniendo en cuenta que la información adopta diversas formas, ya que, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación; sea cual sea la forma en la que se muestra se comparta o almacene, debería protegerse adecuadamente; ante esto se optó por elaborar y aplicar un Sistema de Gestión de la Seguridad de la Información en la Universidad Católica Santo Toribio de Mogrovejo - USAT delimitando su alcance a las áreas involucradas con las TIC: Desarrollo de Sistemas y Taller de computo, con lo cual se pretendió garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados; de tal manera de proteger la información de un amplio rango de amenazas (15).

En Lima, una investigación de grado para optar el Título de Ingeniero Informático realizada en el año 2014 denominado "Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A" de la Pontificia Universidad Católica del Perú, concluye que ante la exigencia de la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de

gestionar adecuadamente la seguridad de la información en cada una de las empresas. Sin embargo, el desconocimiento de estos temas por parte de la alta dirección, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI, entidad responsable de apoyar a las entidades públicas durante el proceso de implementación de la norma. La Resolución Ministerial Nº 129-212-PCM se emitió a finales de mayo del 2012 y se hizo efectiva 45 días después de publicada en el diario "El Peruano", en ella se mencionaban plazos máximos para cada fase según cronograma, las entidades públicas debieron haber terminado la implementación de este sistema de gestión para finales de enero del 2014; sin embargo, se maneja muy poca información de los avances de las distintas entidades públicas con respecto a estos temas, siendo la Oficina de Normalización Previsional – ONP y el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI las únicas del sector público con una certificación internacional relacionada a seguridad de la información en aquel tiempo. Una de las posibles causas de esta situación es que la norma indica que se debe hacer, más no, como se debe hacer. Debido a ello, se decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir como referencia para la implementación del mismo (16).

En Lima, una investigación de grado para optar el Título de Ingeniero Informático realizada en el año 2015 designado "Diseño de un Sistema de Gestión de Seguridad de Información para una Entidad Estatal de Salud de acuerdo a la ISO/IEC 27001:2013" de la Pontificia Universidad Católica del Perú, concluye que existe una brecha importante en cuanto a seguridad de la información en la institución sobre la que se ha realizado el presente proyecto. La principal falencia que debería ser resuelta cuanto antes es

involucrar a la dirección en las acciones del plan que se debe definir con motivo de la implementación del Sistema de Gestión de la Seguridad de la Información institucional, el cual debería ser gestionado como un proyecto institucional, de manera que se cuente con el apoyo de las distintas direcciones y áreas del Instituto Nacional Materno Perinatal – INMP – ex Maternidad de Lima. Es de vital importancia que se defina formalmente el comité de Seguridad de la Información, órgano que debería encargarse del proyecto de implementación del Sistema de Gestión de la Seguridad de la Información y que deberá contar con el apoyo de la Dirección General de modo que se facilite el acceso a la información de todas las áreas pertinentes. El factor humano que constituyen los colaboradores debe ser apropiadamente atacado en cuanto a los cambios que el proyecto. Esto deberá incluir sesiones de capacitación en las que se concientice al personal sobre la importancia de la información con la cual se realizan las labores institucionales, así como fomentar el cumplimiento de las políticas que garantice la seguridad de la misma. Es probable que la implantación de las nuevas condiciones de empleo para los colaboradores antiguos sea recibida con rechazo dado que muchos de ellos se encuentran trabajando mucho tiempo en la institución y puedan percibir este cambio como una amenaza. Este posible obstáculo deberá ser debidamente manejado en conjunto con el área de recursos humanos. El tipo de actividades que realiza a la institución, así como la normativa a la cual se encuentra sujeta en cuanto a la gestión de Historias Clínicas – MINSA del año 2005, obliga a que la información recolectada de los pacientes o generada durante la atención sea almacenada en formato físico. Este escenario al cual se adiciona la falta de definición de los procesos de negocio y la caótica presencia de personas externas a la institución, pacientes, familiares, estudiantes, entre otros que incrementa la probabilidad de pérdida o extracción de información. Es pertinente indicar que las medidas actuales de aseguramiento de estos documentos no cumplen con los mínimos necesarios tanto en acceso físico, como en protección frente a incidentes como incendios, inundaciones, daño por

humedad, etc., el Sistema de Gestión de la Seguridad de la Información se encuentra estrechamente relacionado con la gestión de riesgos de una institución, el análisis que realiza no está sesgado a los activos o controles tecnológicos que la institución pueda tener o requiera. Es por este motivo que el equipo que tenga la responsabilidad de mantener el Sistema de Gestión de la Seguridad de la Información debería trabajar en conjunto con el área de Control Interno apoyándose en el mismo durante el análisis de los riesgos de la institución dado que dicha área debería tener una visión holística de los riesgos que se presentan en la misma. De igual manera el monitoreo de los controles aplicados por el Sistema de Gestión de la Seguridad de la Información debería conformar una parte del trabajo que realiza el área de Control Interno, garantizando la aplicación de los mismos como parte del plan maestro institucional (17).

2.1.3. Antecedentes a nivel regional

No se ha encontrado citas.

2.2. Bases teóricas

2.2.1. El Sector Público en Perú

Características

De acuerdo con la Constitución, Perú es una república democrática, social, independiente y soberana. Su gobierno es unitario, representativo y descentralizado. Se rige por la Constitución de 1993 redactada por el Congreso Constituyente Democrático. La Constitución fue ratificada por referéndum popular el 31 de octubre de 1993. El Presidente de la República es el Jefe del Estado, su mandato es de cinco años no hay reelección inmediata. Transcurrido otro periodo constitucional, como mínimo, el Expresidente puede volver a postular, sujeto a las mismas condiciones Artículo 112 de la CPP modificado por Ley Nº 27365, publicada el 5 de noviembre de 2000). La dirección y la gestión de los servicios públicos están confiadas al Concejo de Ministros; y a cada ministro en los asuntos que competen a la cartera a su cargo. Corresponde al Presidente de la República presidir el Consejo de Ministros cuando lo convoca o cuando asiste a sus sesiones. El Poder Legislativo radica en el Congreso que es unicameral, constituido por 130 miembros elegidos por distrito nacional único. El Poder Judicial es ejercido por la Corte Suprema de Justicia, las Cortes Superiores y los Juzgados de Primera Instancia. El Tribunal Constitucional y el Ministerio Público son autónomos e independientes del Poder Judicial. El Perú está integrado políticamente por 24 departamentos y la provincia constitucional del Callao, siendo su capital la ciudad de Lima (18).

Constitución Política del Perú

La Constitución de 1993 fue redactada por el Congreso Constituyente Democrático-CCD y ratificada por referéndum popular en octubre de 1992 y tiene vigencia a partir del 29 de diciembre de 1992. Sustituye la anterior

Constitución sancionada por la Asamblea Constituyente en 1979. Su contenido está presentado en seis títulos, 206 artículos y 16 disposiciones finales y transitorias (18).

Administración Financiera Gubernamental

La administración gubernamental en el Perú está organizada con base a sistemas administrativos de los años 70'. Con el tiempo tales sistemas fueron fortalecidos o desactivados. Los sistemas de presupuesto, tesorería y crédito público operan en el Ministerio de Economía y Finanzas, cuyo funcionamiento no está formalmente integrado en una norma legal; sin embargo, sus órganos rectores cuentan con normas legales independientes y disposiciones normativas sobre sus áreas de competencia. El sistema de contabilidad pública está a cargo de la Contaduría Pública de la Nación que es un organismo público descentralizado dependiente del Ministerio de Economía y Finanzas-MEF. La administración financiera gubernamental se encuentra a cargo del MEF. Para el cumplimiento de sus funciones cuenta con un Viceministerio de Hacienda, responsable del funcionamiento de la Dirección Nacional del Presupuesto Público y las Direcciones Generales de Tesoro Público y Crédito Público. El Viceministerio de Economía está a cargo de las Direcciones Generales de Política Fiscal, de Asuntos Económicos y Financieros y la Secretaría General de la Comisión Nacional de Inversiones. El universo de control del Sistema Nacional de Control hasta agosto del año 1999, comprendía aproximadamente 2,600 entidades del sector público nacional El sector público en el Perú está conformado por 2,600 entidades integrantes del Estado Peruano. Divididos en Gobierno Central (Ministerios), Organismos Públicos Descentralizados conformado por 467 entidades; Gobiernos Regionales, Empresas Regionales y Municipalidades, Municipios Provinciales y Distritales (más del 70% de las entidades son gobiernos locales comprendido por 2,034); y por las empresas estatales y comités de privatización conformado por 99 entidades. En el año 1997 el

Ministerio de Economía y Finanzas-MEF inició el desarrollo del proyecto "Sistema Integrado de Administración Financiera del Sector Público- SIAF-SP", como un sistema asociado a la ejecución del presupuesto anual, con el objetivo de mejorar la gestión de las finanzas públicas, mediante el registro único de las operaciones de ingresos y gastos de las unidades ejecutoras del Sector Público y permitir la integración de los procesos presupuestarios, contables y de tesorería. El módulo SIAF-SP permite que los datos de ejecución sean ingresados adecuadamente por cada unidad ejecutora, transmitidos y registrados en el MEF. El proceso presupuestario comprende las fases de: programación, formulación, aprobación, ejecución, control y evaluación del presupuesto. Tales fases se regulan anualmente por la ley de presupuesto las directivas que emite la Dirección Nacional de Presupuesto, las que deben ser cumplidas por las Oficinas de Presupuesto de las entidades del sector público. El sistema de Tesorería en el Perú está conformado por la Dirección General del Tesoro Público del Ministerio de Economía y Finanzas, en su calidad de órgano rector y las Tesorerías de las entidades del sector público, excepto las empresas estatales. Sus atribuciones están orientadas a proponer políticas y dictar la normatividad necesaria para regular la administración de fondos en el nivel nacional, determinar las disponibilidades de caja, centralizar el proceso de pago de los fondos públicos y llevar la contabilidad del Tesoro, así como preparar el Estado de Tesorería en forma anual. Las Normas Regulatorias de las Funciones del Sistema de Tesorería, establecen que cada entidad pública en su calidad de unidad ejecutora disponga de una subcuenta de gasto dependiente de la cuenta única, para manejar la asignación de fondos aprobada mediante calendario de compromisos por la Dirección Nacional del Presupuesto Público. El endeudamiento público es administrado por el Ministerio de Economía y Finanzas a través de la Dirección General de Crédito Público. El proceso de endeudamiento se enmarca dentro de los alcances de las leyes anuales de endeudamiento externo, que fija los parámetros para la deuda externa, y de equilibrio financiero, que señala los límites y políticas para las operaciones de

endeudamiento interno que consiste en avales o garantías de contratos de préstamo y emisión de bonos del Tesoro Público. La Dirección General de Crédito Público, actúa como agente financiero del Estado, pero puede designar a otro agente financiero. Las operaciones de endeudamiento interno, directo y/o con aval del gobierno central se aprueban por Decreto Supremo, con el voto del Consejo de Ministros, refrendado por el Ministro de Economía y Finanzas y por el Ministro del sector. Las operaciones de endeudamiento externo se aprueban por Decreto Supremo, con el voto aprobatorio del Consejo de Ministros refrendado por el Ministro de Economía y Finanzas y por el Ministro del Sector. Las operaciones de endeudamiento externo que no conllevan garantía del gobierno central se aprueban por acuerdo de sus respectivos directorios u órganos equivalentes, previa autorización por Resolución Suprema refrendada por el Ministro de Economía y Finanzas y por el Ministro del Sector. La ley del Sistema Nacional de Control, Decreto Ley 26162 precisa que la Contraloría General de la República tiene autonomía técnica, funcional, administrativa y financiera. Siendo esta una entidad pública descentralizada, la Contraloría tiene acceso en cualquier momento y sin limitación a los registros documentos, e información de las entidades, aun cuando sean secretos (19).

2.2.2. Las Municipalidades en Perú

Concepto de Municipalidades

Es la institución del estado, con personería jurídica, facultada para ejercer el gobierno de un distrito o provincia, promoviendo la satisfacción de las necesidades de la población y el desarrollo de su ámbito. Las Municipalidades o Gobiernos Locales son instituciones que forman parte de la estructura orgánica del Estado. Su principal característica es la cercana relación que mantiene con la comunidad de su jurisdicción. A través de los municipios, la ciudadanía expone los problemas localizados en el desarrollo de su vida cotidiana, canalizando propuestas de solución

a favor de la integración de los vecinos para una mejor convivencia en armonía (20).

Historia de las Municipalidades

"La necesidad de que el pueblo sea defendido o representado por una autoridad se remonta a la República de Platón, donde emergió la democracia. Los Concilios Municipales se remontan a la época de la República Romana". Hubo una época en donde la autoridad estaba representada por el emperador o el rey, dejando a un lado el concepto de una igualdad de deberes y derechos. Con la revolución de 1973, las comunas sustituyeron las formaciones monárquicas y predominantes que estaban bajo custodia del poder real. En el antiguo Perú la organización administrativa se inicia formalmente con la división del Imperio Incaico en cuatro suyos conformando el Tahuantinsuyo. Esta división se realizó en el período del Inca Pachacútec. Una vez creados los suyos, estos se organizaron en Ayllus y en demás subdivisiones para un mejor control de modo de que haya una autoridad que este en permanente contacto con administraciones superiores, hasta llegar al inca. De esta forma se organizó un módulo de organización que mantenía el orden administrativo, que se consideraba la base firme del sostenimiento del imperio incaico. Esta organización, la cual le dio una época de prosperidad al imperio incaico, se interrumpió debido a la colonización del territorio por parte de Francisco Pizarro y se terminó de eliminar con las primeras disposiciones de las autoridades españolas durante la ocupación total del territorio. En la época que duró la estadía de la corona española en el Perú representada por los virreyes, el tipo de organización administrativa se daba por medio de las Ordenanzas Reales distadas para las debidas ocasiones en que se viera necesario modificar las anteriores. No existió una adecuada división regional ni zonal que sirva para un pertinente mantenimiento para el apropiado orden de la vida urbana y suburbana. En base a que su principal necesidad era la extracción de la riqueza del imperio incaico, la

administración se basaba en la existencia de un Virrey, una Audiencia para fines netamente jurídicos y religiosos, y luego se encontraban los Encomenderos y Corregidores como los más calificados en materia de la autoridad jurídica. Luego se formaron, por medio de las Ordenes Reales, los Cabildos o Ayuntamientos en base a la realizada, en la administración comunal española. Los Ayuntamientos estaban dirigidos por alcaldes ordinarios y sus funciones eran regidas estrictamente por la Ordenanza Real y supervisado siempre bajo la suprema autoridad virreinal. Pero la dirección de estas funciones no solo era administrada por los españoles o los criollos. Los indígenas formaron parte de esta administración bajo las funciones de alcaldes o también Gobernadores bajo la dependencia del Corregidor. Para que exista un claro entendimiento entre las autoridades españolas y las concentraciones aborígenes se designaban a un cacique, el cual se encargaba de organizar estos lugares. "La transformación de convertirnos en un estado, con una organización dependiente de la corona españolas, a ser un gobierno libre, caracterizado por la República, transcurrió en un largo período caracterizado por varias batallas entre los representantes de la corona española y los representantes de una doctrina libertaria de mentores intelectuales que se inspiraban en la gran Revolución Política inspirada en el Liberalismo". Al Perú le costó mucho adquirir su independencia y asumir un gobierno Republicano debido a la hostilidad de las últimas fuerzas españolas, aun cuando ya se había declarado la Independencia de la República. La designación del Gobierno Municipal, referida a un principio de autonomía administrativa fue en el momento de su creación un acierto de la expresión unánime de los pueblos del Perú. Aún antes de la Constitución de 1960, ya se reconocía la autonomía económica y administrativa de los municipios, que eran constituidos por organizaciones de agrupación de personas, para asegurar la estabilidad de las localidades y ciudades que la conforman. Desde 1980, las Municipalidades en el Perú han comenzado a recibir nuevas rentas y funciones. La Constitución y la Ley le aseguran a la municipalidad un

nuevo rol, ya no de mantenimiento de algunos servicios urbanos menores, sino de desarrollo integral de la provincia o del distrito (21).

La Constitución Política vigente otorga a las Municipalidades tres clases de autonomía que conocemos: la económica, política y Administrativa en los asuntos de su competencia. No encontramos una definición sobre lo que entiende por autonomía, sin embargo la autonomía Municipal, consiste en la capacidad de gestión independiente dentro de los asuntos atribuidos como propios de la Municipalidad. Es decir, autonomía Municipal es la capacidad de decidir y ordenar (autonormarse), dentro de sus funciones y competencias exclusivas que no pueden ser ejercidas por ninguna otra institución (18).

La Ley de Bases de la Descentralización, Ley 27783, es una norma muy importante, porque define el término "autonomía" en sus tres dimensiones, establece la definición de Municipalidades, las clases de competencias que tendrán y, además, su criterio de distribución. La autonomía, según esta norma, es el derecho y la capacidad efectiva del gobierno en sus tres niveles, de normar, regular y administrar los asuntos públicos de su competencia. Se sustenta en afianzar en las poblaciones e instituciones la responsabilidad y el derecho de promover y gestionar el desarrollo de sus circunscripciones, en el marco de la unidad de la nación. La autonomía se sujeta a la Constitución y a las leyes de desarrollo constitucional respectivas. La autonomía Municipal tiene tres dimensiones que consisten en que se le da autoridad para hacer cumplir todos los asuntos que la Ley les ha encomendado para impulsar el desarrollo local. 1) Autonomía Política.- Como elemento de la autonomía Local, pueden emitir normas con naturaleza de Ley material, como son las Ordenanzas, son las que van a decidir, que cosa se va hacer. Entonces las Municipalidades, están constitucionalmente facultadas para decidir qué cosa hacer para lograr el desarrollo Local. 2) Autonomía Administrativa.- se refleja en la posibilidad de emitir reglamentos, actos administrativos; en la

organización Interna. En la contratación y Ejecución de las decisiones; estas son varias formas de cómo se manifiesta la autonomía administrativa. 3) Autonomía Económica.- se da en dos aspectos; en la posibilidad de generar sus propios recursos y, en segundo lugar, en disponer de los recursos que tiene. Sobre el primero, uno de los medios más importantes es la Tributación Municipal en ejercicio de la potestad Tributaria y decidir sobre su presupuesto (22).

Tipos de Municipalidades

Existen tres tipos de municipalidad: 1) Municipalidades Provinciales, ejercen el gobierno local en las demarcaciones provinciales. 2) Municipalidades Distritales**,** ejercen el gobierno local en las demarcaciones distritales. 3) Municipalidades de Centro Poblados**,** se crean por ordenanza municipal provincial y ejercen funciones delegadas, las que se establecen en la ordenanza que las crea. Para el cumplimiento de sus funciones las municipalidades provinciales y distritales deben asignarles recursos económicos de manera mensual. Existen municipalidades que, por sus características particulares, se sujetan a regímenes especiales como la Municipalidad de Lima Metropolitana, las ubicadas en zonas de frontera y las Municipalidades ubicadas en zonas rurales. La Ley Orgánica de Municipalidades 27972 establece un título especial – el Título XI- , con el objeto de promover el desarrollo municipal en zonas rurales (20).

Ley Orgánica de Municipalidades – Ley 27972

La vigente LOM, Ley N° 27972, dada la influencia de la Constitución vigente, reproduce las tres autonomías ya mencionadas en los asuntos de su competencia. No obstante, la autonomía va más allá de lo señalado en la Constitución Política, de tal manera que otorga a las municipalidades la facultad de ejercer actos de gobierno y de administración, con sujeción al ordenamiento jurídico. La actual LOM aporta otra característica de la

autonomía municipal al señalar que la estructura, organización y funciones específicas de los gobiernos locales se cimientan en una visión de estado democrático, unitario, descentralizado y desconcentrado. Otra característica que podemos rescatar de la actual LOM en cuanto a definir autonomía municipal es que establece que los gobiernos locales están sujetos a las leyes y disposiciones que, de manera general y de conformidad a la Constitución Política del Perú, regulan las actividades y el funcionamiento del Sector Público; así como a las normas técnicas referidas a los servicios y bienes públicos, y a los sistemas administrativos del Estado, que por su naturaleza son de observancia y de cumplimiento obligatorio. Al analizar el Título V de la vigente LOM, referido a competencias y funciones específicas de los gobiernos locales, llegamos a la conclusión de que se confunden los conceptos de competencia y funciones, al regularse como si fueran lo mismo. Al revisar la exposición de motivos de la LOM vigente se aprecia que no hay una definición clara de lo que es "autonomía municipal". No obstante ello, se pueden rescatar algunos aspectos que permiten una delimitación en cuanto su extensión como concepto: - Se señala que la autonomía municipal se refiere a un campo de acción libre e independiente, dentro de un marco legal en la cual se desenvuelve el municipio. - El municipio forma parte de la estructura de un Estado. Ambos se encuentran vinculados de modo de ninguno de ellos puede desarrollarse aisladamente del otro existiendo una relación de dependencia mutua entre ambos. - Las municipalidades se han transformado en entes realizadores, pues los vecinos centran en ella buena parte de sus expectativas, y ello es gracias a la autonomía municipal, porque los vecinos ven en el municipio la posibilidad de solución a sus problemas para no acudir a otros niveles que, de por sí, resultarían inaccesibles. Asimismo, en la exposición de motivos se define a la autonomía política como el derecho que tienen los municipios a normarse a sí mismos en atención a sus necesidades a través de ordenanzas municipales, así como el derecho de elegir a sus autoridades. Por otro lado, se precisa que la autonomía económica es el derecho a contar con un

patrimonio para administrarlo sin intromisiones. Y, finalmente, se señala que la autonomía administrativa es el derecho a organizarse por sí mismos, de acuerdo con sus necesidades. Sin embargo hay que tener en cuenta lo siguiente: - No es absoluta. No puede entenderse como soberanía ni como autarquía. - Debe estar al servicio de la ciudadanía. Su fin es instrumental, únicamente en cuanto sirva para que cumplan cabalmente con las competencias y funciones que la Constitución y la Ley Orgánica de Municipalidades le han encomendado. - Deben ejercer sus funciones y competencias en el marco del ordenamiento jurídico estatal en su conjunto. Cabe recordar que éste último se encuentra compuesto por leyes generales de alcance nacional y leyes sectoriales que ha sido adoptadas con el fin de que las entidades del Estado realicen una buena gestión y presten servicios a la ciudadanía en forma eficiente y eficaz. - La autonomía municipal no puede ser alegada para incumplir lo dispuesto por la Constitución, la Ley Orgánica de Municipalidades, ni las leyes nacionales y sectoriales (23).

Estadísticas de Municipalidades

El Instituto Nacional de Estadística e Informática ha puesto a disposición de las autoridades, instituciones públicas, privadas y público en general el documento: "Directorio Nacional de Municipalidades Provinciales, Distritales de Centros Poblados 2015". Cuyo propósito es brindar un aporte valioso de consulta permanente, el cual contiene la relación de 196 Provincias y 1,646 Distritos actualizado al 02 de febrero del año 2015. También, incluye el directorio de 2,437 Municipalidades de Centros Poblados inscritas en el Registro Nacional de Municipalidades, creadas por Norma de la Municipalidad Provincial. Adicionalmente, se incluye información del dispositivo legal de creación de cada distrito, población total proyectada en edad electoral de 18 a 70 años, población total proyectada al 30 de junio de 2015, altitud, latitud sur, longitud oeste y mapas político administrativo a nivel provincial (24).

Tabla Nº 1: Número de Municipalidades, Población total proyectada 2015.

Departamento	Municipalidades Provinciales	Municipalidades Distritales	Municipalidades de Centros Poblados	Población Total Proyectada en Edad Electoral de 18 a 70 años al 2014	Población Total Proyectada al 30-06-2015
Total	**196**	**1,646**	**2,437**	**19,203,621**	**31,138,345**
Amazonas	**7**	**77**	**67**	**253,756**	**422,629**
Áncash	**20**	**146**	**201**	**692,488**	**1,148,634**
Apurímac	**7**	**73**	**95**	**265,744**	**458,830**
Arequipa	**8**	**101**	**23**	**831,848**	**1,287,205**
Ayacucho	**11**	**104**	**141**	**386,398**	**688,657**
Cajamarca	**13**	**114**	**327**	**909,127**	**1,529,755**
Prov. Const. del Callao	**1**	**5**	**1**	**666,968**	**1,013,935**
Cusco	**13**	**95**	**127**	**805,563**	**1,309,858**
Huancavelica	**7**	**88**	**252**	**256,649**	**488,536**
Huánuco	**11**	**66**	**258**	**498,929**	**860,537**
Ica	**5**	**38**	**4**	**492,873**	**787,170**
Junín	**9**	**114**	**108**	**786,012**	**1,350,783**
La Libertad	**12**	**71**	**96**	**1,136,870**	**1,859,640**
Lambayeque	**3**	**35**	**36**	**780,267**	**1,260,650**
Lima	**10**	**161**	**56**	**6,361,845**	**9,834,631**
Loreto	**8**	**43**	**22**	**590,718**	**1,039,372**
Madre de Dios	**3**	**8**	**10**	**85,746**	**137,316**
Moquegua	**3**	**17**	**24**	**121,549**	**180,477**
Pasco	**3**	**26**	**71**	**178,335**	**304,158**
Piura	**8**	**57**	**67**	**1,098,200**	**1,844,129**
Puno	**13**	**96**	**308**	**814,540**	**1,415,608**
San Martín	**10**	**67**	**96**	**513,696**	**840,790**
Tacna	**4**	**23**	**24**	**222,809**	**341,838**
Tumbes	**3**	**10**	**7**	**155,791**	**237,685**
Ucayali	**4**	**11**	**16**	**296,900**	**495,522**

Fuente: INEI – Directorio Nacional de Municipalidades (24).

2.2.3. Municipalidad Provincial de Paita

La Municipalidad Provincial de Paita, es el órgano de gobierno local con personería jurídica de derecho público, con autonomía política, económica y administrativa en los asuntos de su competencia, aplicando las leyes y disposiciones consagradas en la Constitución Política del Perú y de la Ley Orgánica de Municipalidades (8).

Información general

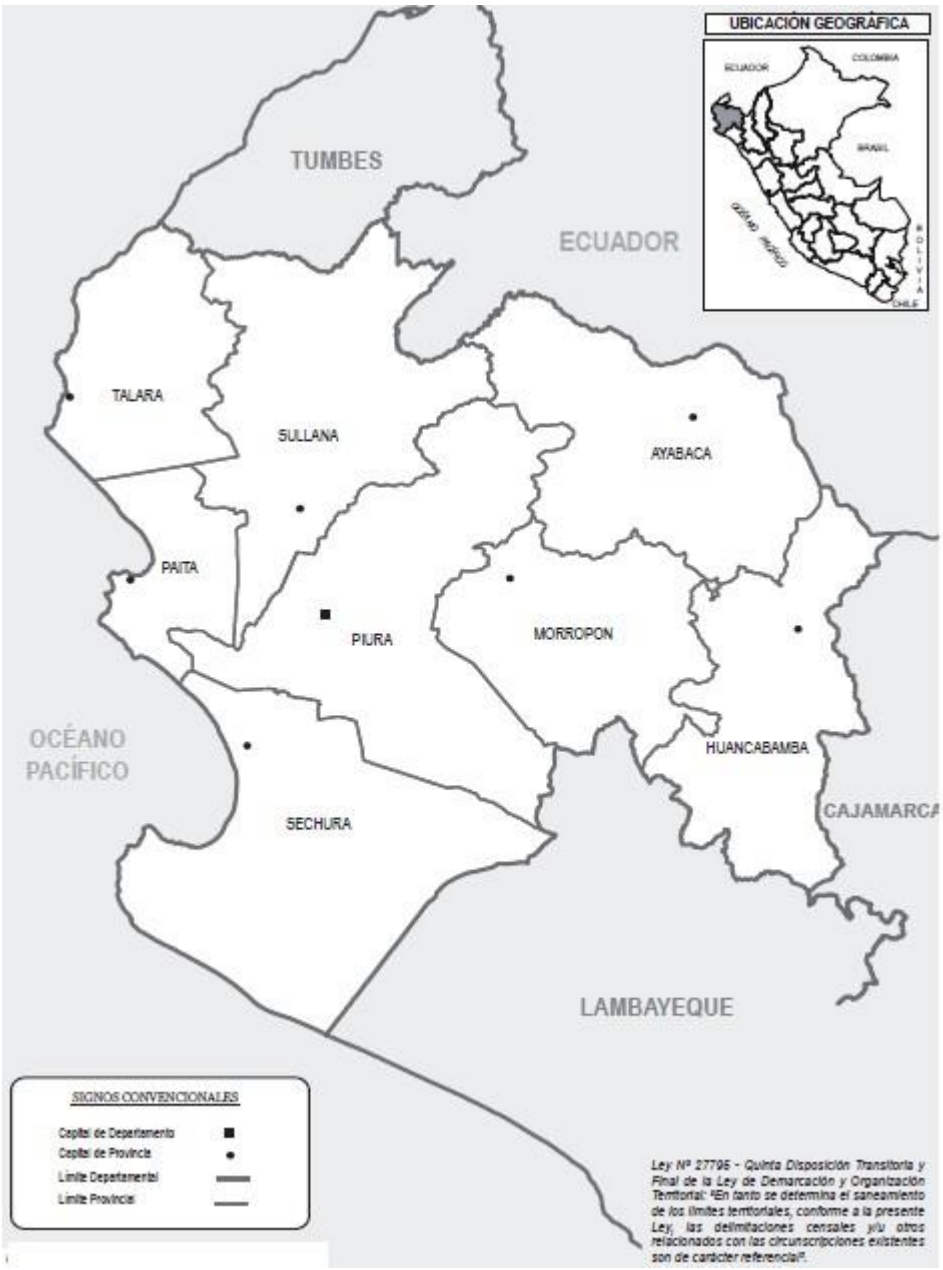
Nombre de la Entidad:		Municipalidad Provincial de Paita
Dirección	:	Cercado de Paita - Plaza de Arma S/N.
R.U.C	:	20162361440
Teléfono	:	(073)211043 ó (073)212122 Fax: 211187
Página Web	:	www.munipaita.gob.pe/
Giro del Negocio	:	Gobierno Local, cuya actividad es la Administración Pública.
Representante Legal	:	Prof. Reymundo Dioses Guzmán - Alcalde de la Municipalidad Provincial de Paita.

Información

La Provincia de Paita es una de las 8 provincias que integran la Región Piura. Cuenta con una Extensión de 1,786.16 Km². Limita por el norte, con las provincias de Talara y Sullana; por el sur, con las provincias de Piura y Sechura; por el este, con la Provincia de Sullana y por el oeste, con el mar de Grau. El distrito de Paita cuenta con una población de 72,522

habitantes. A nivel provincial cuenta con 108,535 habitantes según el Instituto Nacional de Estadísticas e Informática año 2007.

Gráfico Nº 3: Mapa de la Región Piura



Fuente: INEI – Directorio Nacional de Municipalidades (24)

La Provincia de Paita está formada por 7 distritos que son: Colán, El Arenal, Vichayal, Amotape, Tamarindo, La Huaca, y Paita.

Tabla Nº 2: Provincia de Paita, Dispositivo Legal de Creación.

Provincia y Distrito	Dispositivo Legal de Creación		
	Nombre	Número	Fecha
Paita			
Paita	**-**	**-**	**Época Indep.**
Amotape	**Decreto**	**S/N**	**08 Oct. 1840**
Arenal	**Ley**	**S/N**	**03 Nov. 1874**
Colán	**Decreto**	**S/N**	**08 Oct. 1840**
La Huaca	**-**	**-**	**Época Indep.**
Tamarindo	**Ley Regional**	**315**	**28 Ago. 1920**
Vichayal	**Ley Regional**	**316**	**28 Ago. 1920**

Fuente: INEI – Dirección Nacional de Censos y Encuestas (24).

La Municipalidad de Paita en la actualidad ha creado 06 Municipalidades de Centro Poblado que son: Viviate, San Lucas de Colán, La Islilla, La Tortuga, Miramar y Yacila.

Tabla Nº 3: Provincia de Paita, Municipalidades de Centros Poblados.

Provincia y Municipalidad de Centro Poblado	Norma Municipal	Número	Fecha
Paita			
Viviate	**Resolución Municipal**	**074**	**22 Feb. 1989**
San Lucas de Colán	**Resolución Municipal**	**218**	**23 May. 1989**
La Islilla	**Resolución Municipal**	**100**	**04 May. 1990**
La Tortuga	**Resolución Municipal**	**002**	**17 Ene. 2001**
Miramar	**Resolución Municipal**	**009**	**23 Nov. 2009**
Yacila	**Resolución Municipal**	**028**	**27 Dic. 2013**

Fuente: INEI – Registro Nacional de Municipalidades (24).

Altitud y aspectos climáticos

La Provincia de Paita se encuentra situado al occidente de la costa norte del Perú, con un clima cálido seco tropical, cuya temperatura promedio es de 25°C, siendo su máxima altitud de 3 msnm y sus coordenadas son 05°04'57" longitud oeste.

Historia

La Provincia de Paita está formada por 7 distritos que son: Colán, El Arenal, Vichayal, Amotape, Tamarindo, La Huaca, y Paita. Son pueblos netamente agrícolas, pues la mayor parte de estos distritos y caseríos tienen como actividad económica principal la agricultura, siendo productores generalmente de algodón arroz y maíz. Territorialmente Paita cuenta con 3 caletas: Yacila, La Islilla y La Tortuga; playas y caletas de pescadores, cuya actividad económica principal es naturalmente la pesca. Casi todos los distritos pertenecen a tiempos muy remotos, como los rublos antiguos de: Colán, La Huaca, Amotaxe, Vichayal, Tamarindo, y Payta. Estamos hablando desde tiempos prehispánicos, cuando los primeros grupos humanos primitivos se establecieron y/o asentaron en la desembocadura del valle del Chira (hoy provincia de Paita) y demoraron miles de años para alcanzar su desarrollo cultural. Estos antiguos pueblos, aun en las entrañas de su corteza terrestre, esconden vestigios y enigmas por descubrir, que constituyen un verdadero reto a la geología para establecer conclusiones culturales e históricas muy importantes, su pasado histórico está lleno de costumbres, tradiciones y leyendas muy arraigadas. Una característica importante es que forman parte del fértil y hermoso valle del Chira, pues están ubicados geográficamente en la margen izquierda y derecha del río Chira en donde se observan majestuosos, esplendidos y pintorescos paisajes. Sus valles son hermosos, de colorida y fresca vegetación. Sus sembríos en lontananza parecen una extensa alfombra verde, rodeada de infinidad de palmeras o cocoteros, que agitadas por el

viento, dan un agradable olor con sabor a campiña. Por los años 1870, estuvieron muy bien comunicados vía ferrocarril Paita- Sullana- Piura, en la actualidad estos distritos están unidos por una carretera asfaltada en buenas condiciones, desde Paita hasta Sullana, así como sus caseríos y centros poblados están interconectados por tramos de vías carrozables. Las personas de los caseríos aún conservan su folklor, mantiene sus creencias y supersticiones; son conservadores de sus costumbres, comidas y modo de vestir rural, celebran fiestas religiosas y patronales. Paita ha sido cuna de ilustres personajes y mujeres heroicas, que han sobresalido en distintos campos del quehacer humano, así como en la lucha reivindicativa de su pueblo; sobresaliendo: políticos, escultores, maestros, artistas y poetas (25).

La Provincia de Paita fue creada por ley dictada por el presidente Ramón Castilla y Marquezado el 30 de marzo de 1861. Siendo su capital la ciudad de Paita; esta ciudad forma parte del desarrollo del centro de la actividad económica mundial. El movimiento que predomina en las operaciones del puerto de Paita es el de exportación, principalmente el embarque de productos agrícolas y pesqueros que produce la zona norte del país. Esto lo convierte en la primera opción como puerto de partida para el Corredor Bioceánico Paita-Belem do Pará en el marco de la integración de la Región Nor-oriental del Perú con Brasil, además de contar con un Centro de Exportaciones, Transformación, Industria, Comercialización y Servicios (CETICOS) que debe constituirse en un atractivo centro de inversiones orientadas a la exportación, para lo cual existe un marco legal que otorga beneficios tributarios; no obstante, la dinámica es bastante lenta.

Uno de los problemas más importantes en la provincia sigue siendo el desempleo, tanto en el sector público como en el sector privado que adicionado con el fenómeno climático del niño, no se genera la suficiente oferta de trabajo, a pesar de que Paita es un puerto con empresas de producción y de servicios.

Objetivos organizacionales

Objetivo Estratégico Sectorial:

a) Priorizar la Promoción del Desarrollo Económico Local

Comprende los programas y proyectos que generan directa o indirectamente economías, en este eje se ubican los proyectos de infraestructura que sustentan y promueven el desarrollo productivo de la Provincia. Esta labor estará enfocada a la ejecución de acciones para el fomento de la economía local, logrando que Paita sea una ciudad a la inversión privada y generadora del empleo, Paita, tiene un gran potencial en diversos campos de la actividad económica, por lo que durante los próximos años se coadyuvara al desarrollo de éstas capacidades, procurando la incorporación de los sectores más vulnerables de la sociedad a los procesos del crecimiento sostenido de las cadenas productivas económicamente de la micro, pequeña, mediana y gran empresa Local (8).

b) Desarrollo Social

Comprende los programas y proyectos referidos a educación, saneamiento integral, entre otros, en este eje se concentran lo infraestructural y también la gestión de estos servicios. Promueve la formación de capacidades aprovechando los recursos del Municipio; fortalecer las acciones en materia educativa y cultural, destinando recursos financieros para atender sus necesidades. Este desarrollo pretende la adopción ejecución y evaluación de políticas y programas como: lucha contra la pobreza, desarrollo del potencial humano, equidad e igualdad de género, transferencias de programas sociales, ayuda a la población en riesgo en situación de

pobreza y extrema pobreza de niños, adolescentes gestantes y adulto mayor en desamparo (8).

c) Medio Ambiente y Desarrollo Urbano

Comprenden los programas y proyectos que impliquen el uso racional de los recursos naturales y de mejoramiento ambiental. Establece y mejora las condiciones de infraestructura básica en armonía con un crecimiento urbano ordenado priorizando la integración vial y aspiración de la población a vivir en un ambiente saludable, permitiendo a Paita convertirse en una Provincia sostenible y saludable que respete y consolide la identidad de la ciudad (25).

d) Desarrollo Institucional y de Capacidades

Comprende los programas y proyectos orientados a desarrollar la capacidad de los actores locales y organizacionales dirigida a fortalecer la capacidad institucional, organizativa y técnica de la Municipalidad para lograr una gestión eficiente, consolidando la capacidad de gobernabilidad del gobierno provincial de Paita, contando con el apoyo de las instituciones con mayor participación ciudadana en la toma de decisiones. Las diversas unidades de la Administración Municipal deben cumplir sus atribuciones con transparencia, honestidad y eficiencia, contando para ello con adecuadas estructuras organizacionales e instrumentos normativos que las regulan. Es así que desde este espacio, los gobernantes buscan establecer una buena gobernabilidad, donde se hace necesario modernizar los viejos estilos de gobierno municipal, orientándolo a realizar gestiones Transparentes, confiables y eficientes (8).

Objetivos Institucionales Informáticos:

Hacer uso eficiente de la información y de las nuevas Tecnologías de Información y Comunicaciones (TIC) como recursos para proveer servicios de calidad, accesibles, seguros y oportunos a la propia Institución, en aplicación de las directivas, lineamientos y normas emitidas por la Oficina Nacional de Gobierno Electrónico e Informática, ente rector del Sistema Nacional Informático (25).

Objetivos Informáticos Específicos:

a) Planear, organizar, dirigir, supervisar, ejecutar y evaluar, el diseño e implementación de la infraestructura tecnológica de voz y datos, los sistemas informáticos y los procesos digitales de la información de la municipalidad.

b) Reglamentar el uso de equipos y sistemas informáticos, desarrollando acciones en niveles de acceso, de seguridad y calidad en resguardo de la información automatizada de la municipalidad.

c) Formular el plan anual de desarrollo de proyectos tecnológicos y sistemas de información, en base a los requerimientos de información de las áreas usuarias de la municipalidad, acorde con los lineamientos institucionales.

d) Programar, ejecutar, supervisar y evaluar las actividades relacionadas con el soporte técnico, mesa de ayuda y el mantenimiento de los programas y equipos informáticos, así como de las redes y comunicaciones de voz y datos.

e) Formular, elaborar y ejecutar el plan de contingencia informático y de comunicaciones, a fin de garantizar la normal operatividad

de la red, los servicios de internet, correo electrónico y transmisión de data.

f) Mantener un inventario general de los equipos de cómputo, de sistemas, productos y programas informáticos.

g) Brindar a la Subgerencia de Imagen Institucional y Comunicaciones, el soporte técnico oportuno para mantener el portal institucional debidamente actualizado.

h) Asesorar a la Alta Dirección y demás unidades orgánicas, en concordancia con las normas técnicas y estándares municipales, sobre la adquisición de equipos, repuestos, sistemas de tecnología y sobre soluciones tecnológicas propuestas por terceros (8).

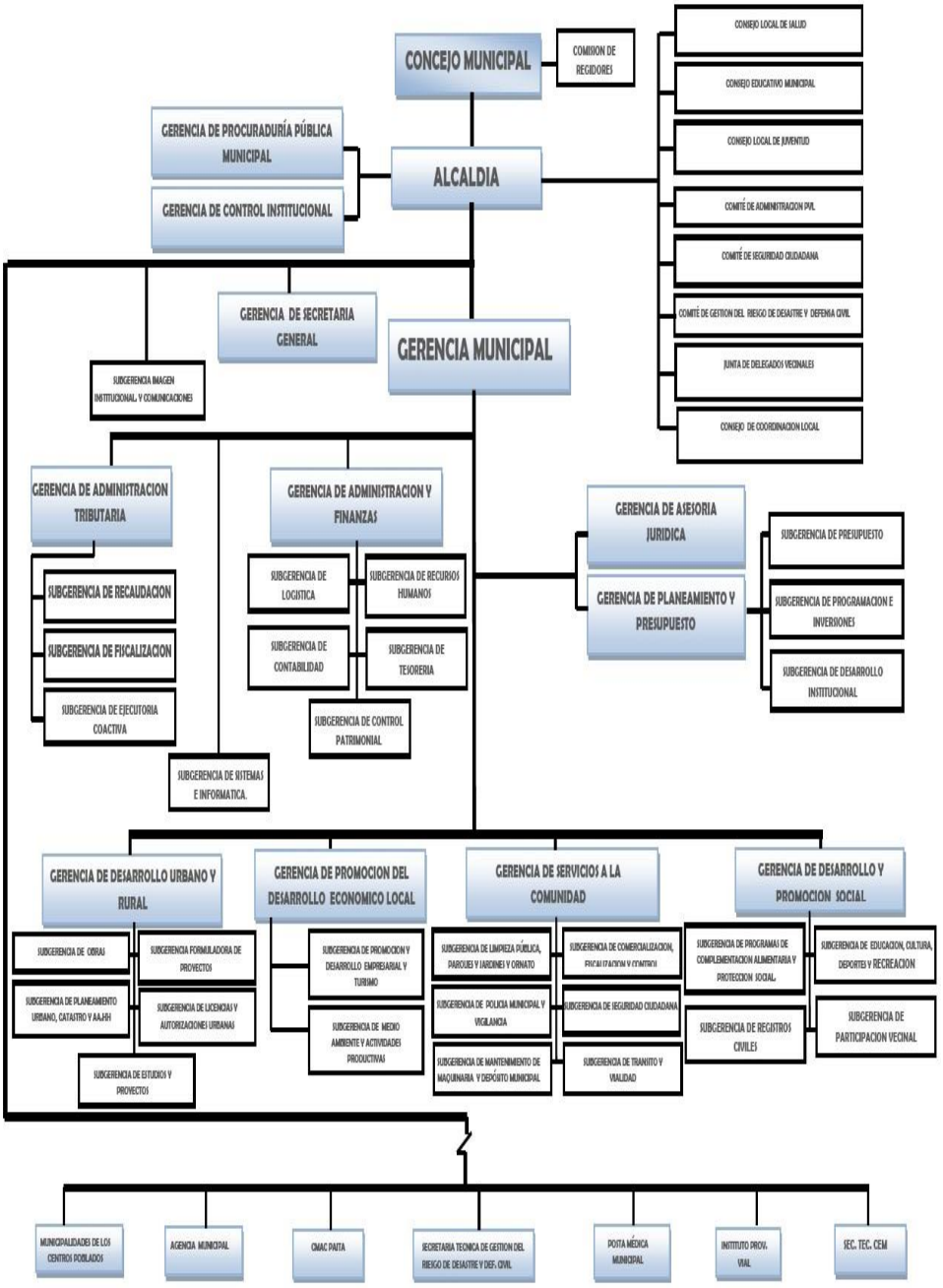
Funciones Organizacionales:

Son funciones de la Municipalidad Provincial de Paita promover el desarrollo humano, productivo y urbano sostenible y armónico del distrito, a través de las siguientes materias:

En la planificación del desarrollo local y el ordenamiento territorial a nivel provincial (Organizacional del espacio físico – Uso del suelo), servicios públicos locales, protección y conservación del medio ambiente; desarrollo económico local; participación vecinal; servicios sociales locales; además de impulsar la captación de la inversión pública, privada y de las oportunidades que brinda la cooperación técnica internacional en el marco de las políticas nacionales y regionales que permitan ejecutar proyectos y programas que incidan directamente en el mejoramiento de la calidad de vida de la población Paiteña (25).

Organigrama

Gráfico Nº 4: Organigrama de la Municipalidad Provincial de Paita



Fuente: Portal MuniPaita.gob.pe (25).

Misión

Brindar la adecuada prestación de los servicios públicos y el desarrollo local, con participación plena y organizada de la comunidad, que se constituyen en los actores sociales que intervienen, apoyan, coordinan y fiscalizan la gestión municipal (25).

Visión

Al 2021, Paita es una provincia ordenada, limpia, segura, moderna, integrada y productiva; con educación y salud de calidad. Cuenta con infraestructura básica de saneamiento y energía que garantizan el bienestar y dignidad de la población. Paita Provincia tiene como pilar fundamental la persona, con valores, identidad y conciencia ciudadana, con igualdad de oportunidades, inclusión social y equidad de género. Cuenta con un gobierno local provincial democrático, participativo y transparente. Está totalmente articulada con vías de comunicación adecuadas al interior de sus distritos, y a nivel nacional e internacional. Tiene un desarrollo sostenible, armónico e integral (Ibídem).

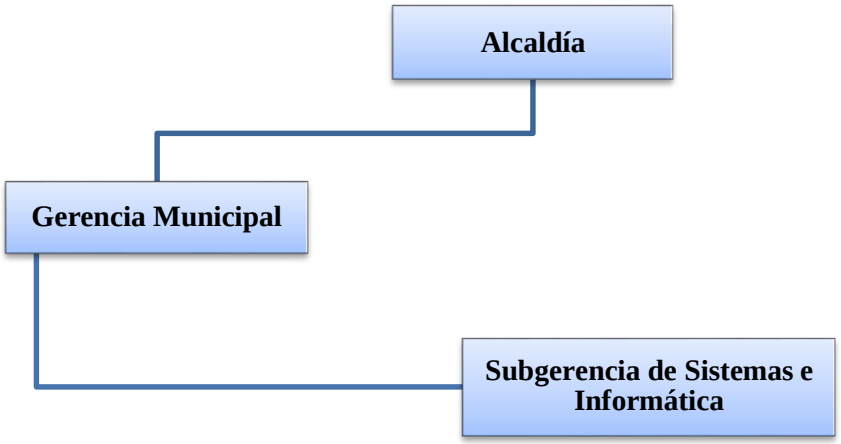
Área de Tecnologías y Sistemas de la Municipalidad de Paita

La Subgerencia de Sistemas e Informática – SSI, es el órgano de apoyo técnico de la gestión municipal, encargado de la gestión de las tecnologías de la información, procesos de comunicación interna y con la comunidad, depende jerárquica, funcional y administrativamente de la Gerencia Municipal. Le corresponde el tercer nivel organizativo (8).

En la actualidad la Subgerencia de Sistemas e Informática no se encuentra debidamente constituida dentro de la estructura orgánica municipal ya que las funciones descritas en el Reglamento de Organización y Funciones – ROF se encuentran asignadas a una sola subgerencia lo cual no permite afrontar adecuadamente la demanda de servicios, se debería contar con

oficinas especializadas tales como la Oficina de Informática y de Soporte tecnológico a las que se deben descentralizar ciertas funciones a fin de lograr un mejor servicio y una mejor funcionalidad.

Gráfico Nº 5: Organigrama de la Subgerencia de Sistemas e Informática.



Fuente: Subgerencia de Desarrollo Institucional año 2011 (26).

Análisis Estratégico de la Subgerencia de Sistemas e Informática - SSI

Fortalezas:

a. El personal cuenta con el conocimiento y experiencia necesaria para el desarrollo de las labores relacionadas a las actividades informáticas, en el marco de las funciones asignadas.

b. La edad promedio del personal de la Subgerencia es 38 años, siendo fundamental para la adopción de cambio organizacional así como en la implementación de nuevas tecnologías.

c. Existencia de un clima laboral aceptable.

Oportunidades:

a. Las tecnologías de información y comunicaciones proporcionan herramientas de gestión para una adecuada toma de decisiones.

b. Uso de Internet como herramienta de acceso a la información a nivel Estado.

c. Tecnología de redes disponible en el mercado para enlazar recursos tecnológicos, facilitando el intercambio de información.

Debilidades:

a. La Subgerencia de Sistemas e Informática cuenta con un reducido número de personal lo cual le impide atender oportunamente el requerimiento de las diversas dependencias de la Institución, relacionadas con labores de soporte técnico, mantenimiento de equipos informáticos y desarrollo de sistemas principalmente.

b. Desaprovechamiento de las bondades de la tecnología de la información por usar algunas versiones de software desactualizadas. Las acciones de capacitación son escasas, propiciando personal autodidacta.

c. La capacidad operativa de la Subgerencia Sistemas e Informática, está representada aproximadamente en un 50% por personal contratado y/o practicante.

d. Reducido espacio de trabajo asignado a la Subgerencia donde se aloja el servidor central, equipos de cómputo, el personal que realiza labores de soporte técnico y la Jefatura de área.

e. Carencia de un plan de mantenimiento rutinario y periódico de los equipos informáticos.

f. A pesar de ser integrante del Sistema Nacional de Informática, no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI).

Amenazas:

a. Rápido avance tecnológico que genera desfase de equipos informáticos.

b. Alto costo de software Licenciado.

c. Inseguridad de las instalaciones físicas de la Municipalidad susceptibles de sufrir daño parcial o con pérdida total originado por factores naturales o eventos provocados por el hombre tales como incendio, atentado, robo y otros (27).

TIC que utiliza la Municipalidad Provincial de Paita

La constante evolución de la Tecnología, junto a la aparición de nuevas y más complejas formas de utilización de las mismas, junto con la interconexión, la globalización de la economía y el uso de los sistemas, ha implicado en la actualidad que las tecnologías de la información ofrezcan extraordinarias oportunidades en el aspecto competitivo (28).

A través del uso de las TIC se logran importantes mejoras en las instituciones, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas competitivas o también permite reducir la ventaja en relación a sus rivales.

Entre los principales aplicativos con que cuenta la institución, tenemos:

a. Sistema Integrado de Administración Financiera (SIAF –SP)

De acuerdo a la descripción del Ministerio de Economía y Finanzas, el SIAF es un Sistema de Ejecución, no de Formulación Presupuestal ni de Asignaciones (Trimestral y Mensual), que es otro sistema. Sí toma como referencia estricta el Marco Presupuestal y sus Tablas.

El SIAF ha sido diseñado como una herramienta muy ligada a la Gestión Financiera del Tesoro Público en su relación con las denominadas Unidades Ejecutoras (UE). El registro a nivel de las UE, está organizado en dos partes:

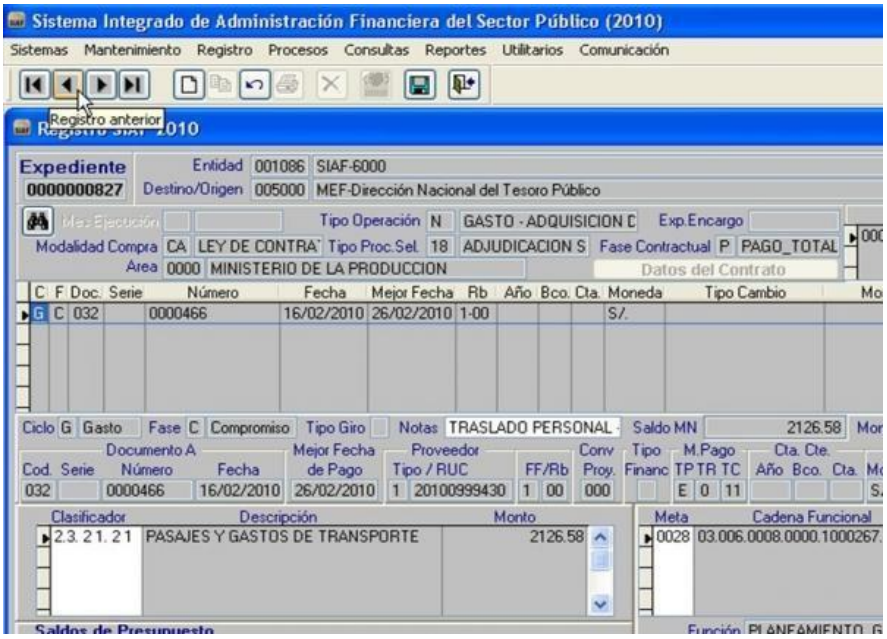
- Registro Administrativo (fases de Compromiso, Devengado, Girado) y

- Registro Contable (contabilización de las Fases así como Notas Contables).

El Registro Contable requiere que, previamente, se haya realizado el Registro Administrativo. Puede realizarse inmediatamente después de cada fase, pero no es requisito para el registro de la Fase siguiente.

A diferencia de otros sistemas, la contabilización no está completamente automatizada. Esto, que podría ser una desventaja, ha facilitado la implantación pues el Contador participa en el proceso (29).

Gráfico Nº 6: Pantalla principal del SIAF-SP



Fuente: Ministerio de Economía y Finanzas (29).

Así mismo el SIAF radica su importancia, porque permite:

- Tener un registro del presupuesto de cada institución pública de forma tal que podemos cotejar el gasto contra el presupuesto, Registrar las metas físicas de las actividades o proyectos es decir, ¿qué se quiere lograr con dichas actividades?, lo que nos da información que complementada con otras permite ver la utilidad del gasto y la efectividad del mismo.

- Registrar todos los pasos previos a la realización de cada gasto de forma tal que no se asuman compromisos que no están presupuestados o para los cuales aún no se cuenta con los recursos financieros.

- Está conectado con el Banco de la Nación y permite que los "cheques SIAF" nunca reboten pues a la hora de hacer el pago (30).

b. Sistema Integrado de Gestión Administrativa

El SIGA es un sistema informático que contribuye al ordenamiento y simplificación de los procesos administrativos en el marco de las normas establecidas por los Órganos Rectores de los Sistemas Administrativos del Estado, permitiendo: el Manejo ordenado de todo el proceso previo al registro SIAF, realiza la simplificación de los procesos administrativos, se tiene la información oportuna de calidad y permite la disponibilidad de información de costos.

El SIGA comprende los módulos de: Administrador, Logística, Patrimonio, Programación Presupuesto por Resultados, Tesorería, Bienes Corrientes, Revaluación de Edificios y Terrenos, Configuración y Utilitarios (31).

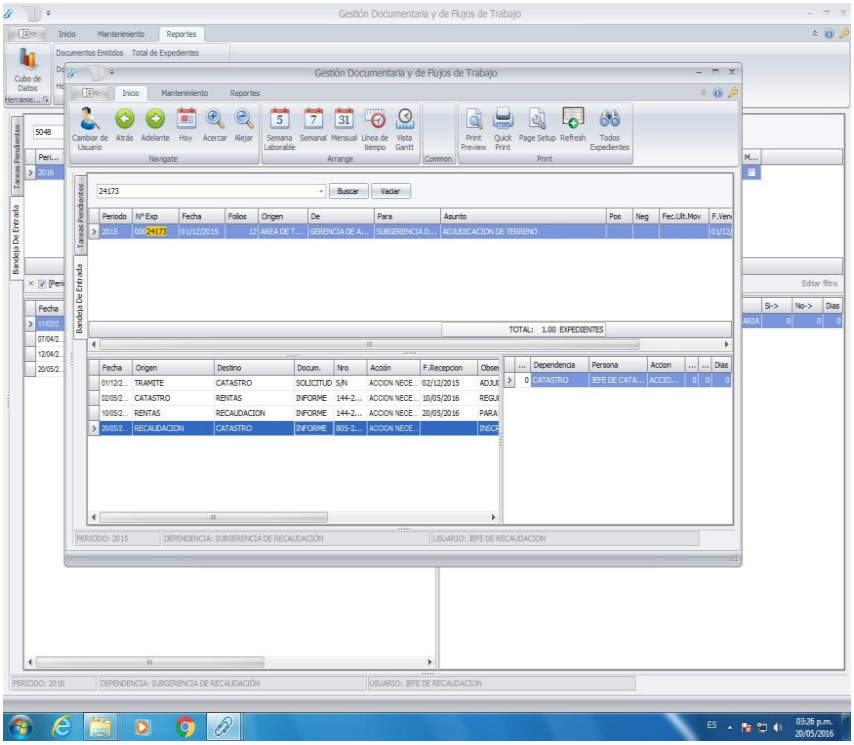
Gráfico Nº 7: Sistema Integrado de Gestión Administrativa

Fuente: Ministerio de Economía y Finanzas (29).

c. Sistema de Gestión Documentaria

Este aplicativo permite tener el control de la ubicación física y el estado actual y pasado de la documentación que llega, fluye y se genera dentro de ellas, así mismo se realiza el registro y seguimiento de la documentación interna y externa, su principal objetivo como componente del sistema de apoyo administrativo es el soporte de la información, además permite realizar la búsqueda de un expediente en forma rápida ya sea que se encuentre en trámite o con su proceso concluido y ya almacenado, ahorrando tiempos de búsquedas al no tener que sumergirse en voluminosos archivos fiscos para ubicar un documento. Este sistema no cuenta con una interface en el Portal Web institucional.

Gráfico Nº 8: Pantalla del Sistema de Gestión Documentaria



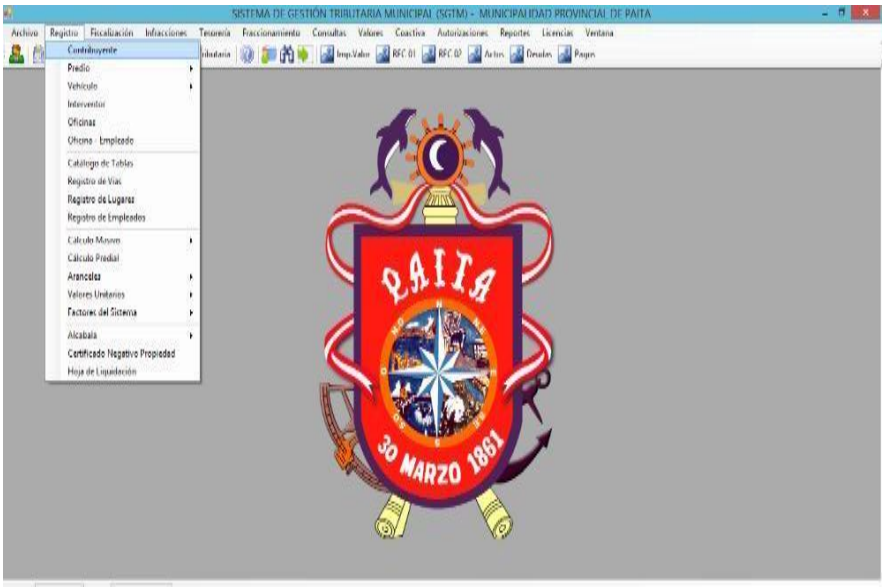
Fuente: Subgerencia de Sistemas e Informática (32).

d. Sistema de Gestión Tributaria Municipal – SGTM

Este sistema ha sido diseñado para ser la pieza central para el Área de Administración Tributaria de las Instituciones Municipales; dicha herramienta permite automatizar el registro de Contribuyentes, Predios, Vehículos y conocer su historial; también permite la determinación de las tributos municipales como Impuesto Predial, Impuesto Vehicular, Impuesto de Alcabala, Arbitrios Municipales e Imprimir los formatos de Declaración Jurada; controla la cobranza de los impuestos, arbitrios municipales, tasas y derechos así como las Infracciones de Tránsito e Infracciones Administrativas.

Para la gestión de cobranza en la etapa ordinaria el sistema SGTM permite la emisión de las Ordenes de Pago, Resoluciones de Determinación y Resoluciones Multa; para la cobranza coactiva el sistema emite la Resolución de 7 días (REC 01), Resolución N° 02, y otras, todo ello luego de generar el expediente coactivo (33).

Gráfico Nº 9: Pantalla Principal del SGTM - Paita

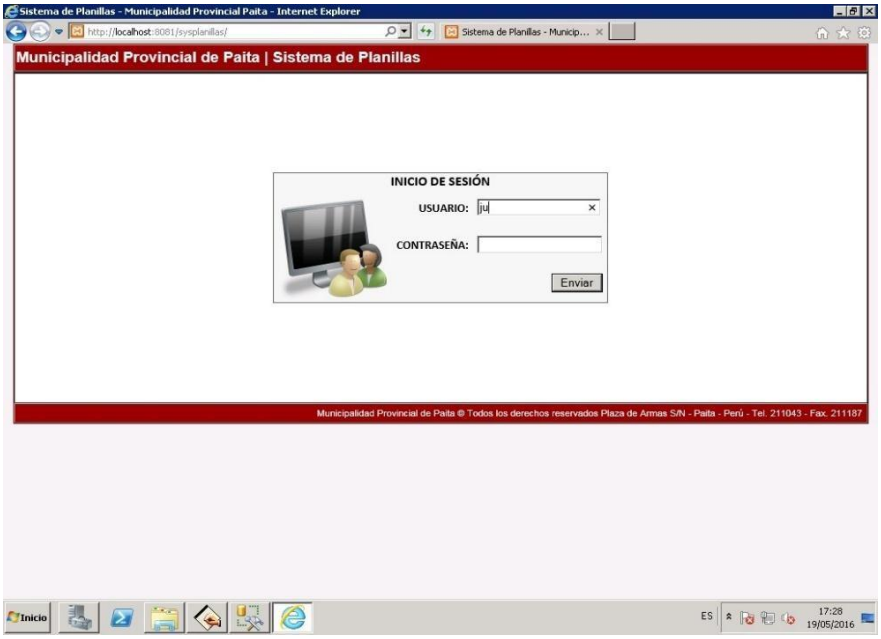


Fuente: Subgerencia de Sistemas e Informática (32).

e. Sistema de Planillas

El software de Planillas está diseñado para gestionar la información laboral del personal, efectuar los cálculos de la planilla en forma automática, emitir todos los reportes relacionados con los trabajadores. El sistema administra la base de datos de personal, familiares, control de las planillas de pagos del personal nombrado, contratado y obrero en su condición de eventuales, pensionistas, gratificaciones, bonificación vacacional, escolaridad, realiza el control de préstamos al personal, escalas de quinta categoría, descuentos judiciales, tasas de AFP´s, leyes sociales. Un conjunto de opciones que se registrarán amigablemente para determinar el cálculo final de la planilla.

Gráfico Nº 10: Pantalla Principal Sistemas de Planillas

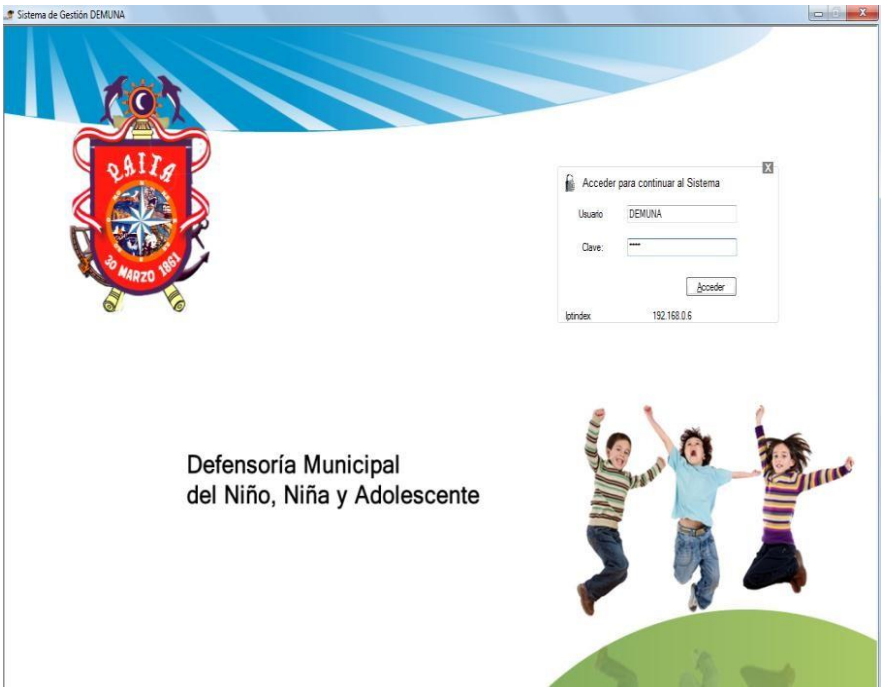


Fuente: Subgerencia de Sistemas e Informática (32).

f. Sistema Integrado de Gestión de la DEMUNA Paita - SIGEDEM

El Sistema Integral de Gestión de la DEMUNA (Defensoría Municipal de Niño y el Adolescente) de Paita, ha sido diseñado para dar soporte a una adecuada gestión de los procesos de atención de casos, de tal manera que se pueda contar con toda la información ordenada tanto del obligado como del beneficiario, así como tener el control de depósitos y retiros de dinero o alimentos. Los casos atendidos por materia son los siguientes: Alimentos, Tenencias, Régimen de Visitas, Normas de Comportamiento, Maltrato Infantil, Reconocimiento Voluntario de Filiación, Inscripciones de Nacimiento/Rectificación de partida, Matrícula Escolar, Atentado contra la libertad sexual, Abandono de Hogar, Casos Sociales, Atención Psicológica, Orientaciones y Otros (especifique) Violencia Adultos – Situación del Menor – Inscripción SIS.

Gráfico Nº 11: Pantalla Principal de SIGEDEM Paita

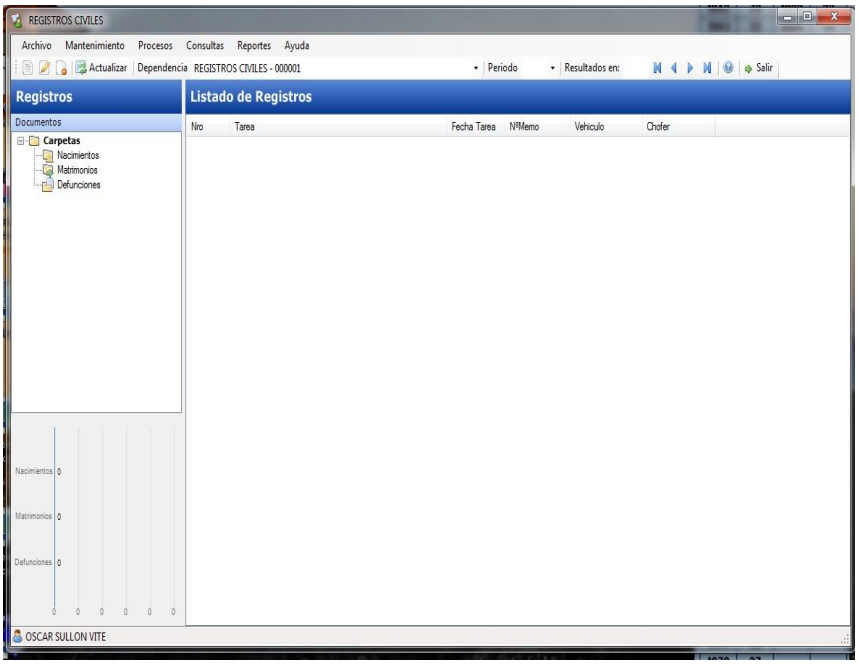


Fuente: Subgerencia de Sistemas e Informática (32).

g. Registro Civil

El Sistema de Registro Civil es un sistema de captura, digitalización, almacenamiento y reportes de los archivos de registro civil (nacimiento, matrimonio y defunción), sirve para almacenar en la computadora datos de registro civil mediante imágenes escaneadas y registros capturados en bases de datos, que de otro modo estarían expuestos a pérdidas por causas naturales. Asimismo, permite imprimir el archivo sin necesidad de buscar el documento físico, lo que genera un ahorro de tiempo y a la vez evita el deterioro del mismo. Por otro lado, con el Sistema de Registro Civil se pueden obtener estadísticas de nacimientos, matrimonios o defunciones de manera exacta y en poco tiempo.

Gráfico Nº 12: Pantalla Principal de Registro Civiles



Fuente: Subgerencia de Sistemas e Informática (32).

h. Portal Web MuniPaita.gob.pe

Mediante el Decreto Supremo N° 043-2003-PCM se aprobó el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, cuya finalidad era promover la transparencia de los actos del Estado y regular el derecho fundamental de todo ciudadano y ciudadana al acceso a la información que consagra la Constitución Política del Perú. Según la referida norma, toda información que posea el Estado se presume pública, salvo las excepciones que esta misma ley establece en su artículo 15. Señala que es obligación del Estado, entregar toda información que demanden los ciudadanos con excepción de aquella información expresamente clasificada como secreta, confidencial o reservada. La misma ley establece como un medio de difusión permanente el portal de transparencia, con el cual deben contar todas las instancias del Estado, obligándoseles a la presentación actualizada de información sobre: los datos generales de la entidad pública, las disposiciones y comunicados emitidos, su organización y organigrama, el texto único de procedimientos administrativos, el marco legal al que están sujetas; información presupuestal que incluya datos sobre los presupuestos ejecutados, proyectos de inversión, el cuadro de remuneraciones, los beneficios de los altos funcionarios y el personal en general; las adquisiciones de bienes y servicios que realicen incluyendo el detalle de los montos comprometidos, los proveedores, la cantidad y calidad de bienes y servicios adquiridos; las actividades oficiales que desarrollarán o desarrollaron; siendo esta lista no limitativa. Más aún, el 4 de octubre de 2013, la Presidencia del Consejo de Ministros publicó la Resolución Ministerial N° 252 - 2013 que amplía, detalla y establece los plazos para la actualización del portal de transparencia, incluyendo la declaración jurada de ingresos, bienes y rentas de los funcionarios obligados a presentar (34).

Que en cumplimiento con la normatividad vigente la Municipalidad Provincial de Paita ha diseñado y gestionado el Portal de Transparencia y acceso a la información.

Gráfico Nº 13: Pantalla Principal del Portal Web - MuniPaita

Fuente: Subgerencia de Sistemas e Informática (32).

i. Otros sistemas informáticos:

- Sistema de Logística
- Sistema de Biblioteca
- Sistema de Mercado
- Sistema de Almacén
- Sistema de Hospital
- Sistema OMAPED
- Sistema de Licencia de Funcionamiento.
- Sistema de Legajos
- Sistema de Inventario de Software.

Infraestructura tecnológica

La Infraestructura tecnológica con que cuenta la entidad es la siguiente:

Tabla Nº 4: Hardware – Equipos Informáticos del Palacio Municipal.

AMBIENTE	AREA MUNICIPAL	PC´S	IMPRESORA LASER	IMPRESO. MATRICIAL	TIQUETERA	PLOTER	LAPTOP	SWITCH
PRIMER PISO	CATASTRO	8	2			1	1	
	PERSONAL	9	2	1				
	SERVICIOS A LA COMUNIDAD	5	4				1	1
	SERVICIO DESARROLLO ECONOMICO	3	1					
	MESA DE PARTES	2	1					
	CAJA	1	1		1			
	ATENCION AL USUARIO	1	1					
	VIGILANCIA	1						
SEGUNDO PISO	ADMINISTRACION	3	2					
	TESORERIA	3	3					
	INFORMATICA	4	1					
TERCER PISO	LOGISTICA	5	2	2				
	CONTABILIDAD	8	1					
	EDICION DE VIDEO	3	1					1
CUARTO PISO	ASESORIA LEGAL	4	1					
	PROCURADURIA	4	1					
	PLANIFICACION Y PRESUPUESTO	3	2					
	ALCALDIA	5	1				1	
	SECRETARIA DE GERENCIA MUNICIPAL	2	1				1	
	SECRETARIA GENERAL	4	2					
	OCI	3	2					
	PRESUPUESTO	4	1					
	DESARROLLO URBANO	6	3					
	PROCESOS	3	2					
	LICENCIAS	4	1					
	INTITUTO VIAL	4	1					
	CATASTRO	1						
QUINTO PISO	OBRAS PUBLICAS	7	3				1	
	OPI	7						
	ESTUDIOS Y PROYECTOS	11	6			1		
		128	49	3	1	2	5	2

Fuente: Subgerencia de Sistemas e Informática (32).

Tabla Nº 5: Hardware – Equipos Informáticos de la GAT.

AMBIENTE	AREA MUNICIPAL	PC´S	IMPRESORA LASER	IMPR ESO. MATR	TIQUETERA	PLOTER	LAPTOP	SWITCH
ZONA ALTA ADM. TRIBUTARIA	ADMINISTRACION TRIBUTARIA	2	2				1	1
	RECAUDACION	9	4					
	FISCALIZACION	4	1					1
	COACTIVO	5	3					1
	CAJA	1	1		1			
	ATENCION AL USUARIO	1	1					
	NOTIFICACIONES	2	1					
		24	13	0	1	0	1	3

Fuente: Subgerencia de Sistemas e Informática (32).

De acuerdo a la información recopilada la Red Lan de la Municipalidad Provincial de Paita es soportada por sistemas operativos Windows Server 2012 y Windows Server 2008 según la tabla siguiente:

Tabla Nº 6: Sistemas Operativos de la Municipalidad de Paita.

SISTEMA OPERATIVO	SERVICIO
MICROSOFT WINDOWS SERVER 2012 ESTÁNDAR (APPSERVER)	SIAF SQL ACTIVE DIRECTORY (B.D.) B.D. ALMACEN B.D. HOSPITAL B.D. OMAPED SQL SERVER
MICROSOFT WINDOWS SERVER 2008R2 ENTERPRISE (MUNIPAITA00)	XAMPP B.D. MERCADO B.D. REGISTRO CIVIL B.D. TRIBUTACION MUNICIPAL (ADM. TRIB.) B.D. LIC. FUNCIONAMIENTO B.D. TRAMITE DOCUMENTARIO B.D. PLANILLAS
MICROSOFT WINDOWS SERVER 2003 ENTERPRISE EDITION (CATAS)	SISTEMA DE LEGAJOS SISTEMA ANTIGUO DE PLANILLAS (RESPALDO) SISTEMA DE CATASTRO INVENTARIO DE SOFTWARE
MICROSOFT WINDOWS SERVER 2008R2 ENTERPRISE (WIN-EEEC34T67JL)	CONSOLA ANTIVIRUS ESET ENDPOINT PROTECTION ADVANCE
MIKROTIK ROUTER OS (MIKRO-TIK)	ROUTER OS (WINBOX 5.2) PROXY

Fuente: Subgerencia de Sistemas e Informática (32).

Tabla Nº 7: Equipos de Comunicación y Transmisión de datos

SWITCH Y EQUIPOS LAN	EQUIPOS WAN, TELEFONIA Y VIDEOCAMARA
- 05 SWITCH DE 24 PUERTOS	- ANTENAS PARA RADIO ENLACES Y TORRES METALICAS
- 05 SWITCH DE 08 PUERTOS	- MIKROTIKROUTER BOARD RR1100
- 03 SWITCH DE 48 PUERTOS	- 01 CENTRAL TELEFONICA PANASONIC T616
- 01 SWITCH DE 04 PUERTOS	- 04 UNIDADES DE CONTROL DE CAMARAS NIGH OWL

Fuente: Subgerencia de Sistemas e Informática (32).

Tabla Nº 8: Servidores

SERVIDORES	DESCRIPCION Y FUNCIONES	SISTEMA OPERATIVO
APPSERVER	CONTROLADOR DE DOMINIO Y BASE DE DATOS	MICROSOFT WINDOWS SERVER 2012 ESTÁNDAR
MUNIPAITA00	SERVIDOR DE BASE DE DATOS	MICROSOFT WINDOWS SERVER 2008R2 ENTERPRISE
CATAS	SERVIDOR DE CATASTRO	MICROSOFT WINDOWS SERVER 2003 ENTERPRISE EDITION
WIN-EEEC34T67JL	CONSOLA ANTIVIRUS	MICROSOFT WINDOWS SERVER 2008R2 ENTERPRISE
MIKRO-TIK	SERVIDOR DE RUTEO	MIKROTIK ROUTER OS

Fuente: Subgerencia de Sistemas e Informática (32).

Tabla Nº 9: Estaciones de Trabajo

PROCESADOR	Nº EQUIPOS
CORE I7	**34**
CORE I5	**51**
CORE I3	**5**
CORE 2 DUO	**17**
DUAL CORE	**2**
PENTIUM (R)	**5**
CELERON	**4**
	118

Fuente: Subgerencia de Sistemas e Informática (32).

Tabla Nº 10: Sistemas Operativos

SISTEMA OPERATIVO	Nº EQUIPOS
WINDOWS 7 PROFESSIONAL	**110**
WINDOWS 7 ULTIMATE	**3**
WINDOWS 8 PROFESSIONAL	**1**
WINDOWS 8 SINGLE LANGUAGE	**1**
WINDOWS 8.1 PROFESSIONAL	**1**
WINDOWS 8.1 SINGLE LANGUAGE	**1**
WINDOWS XP PROFESSIONAL	**1**
	118

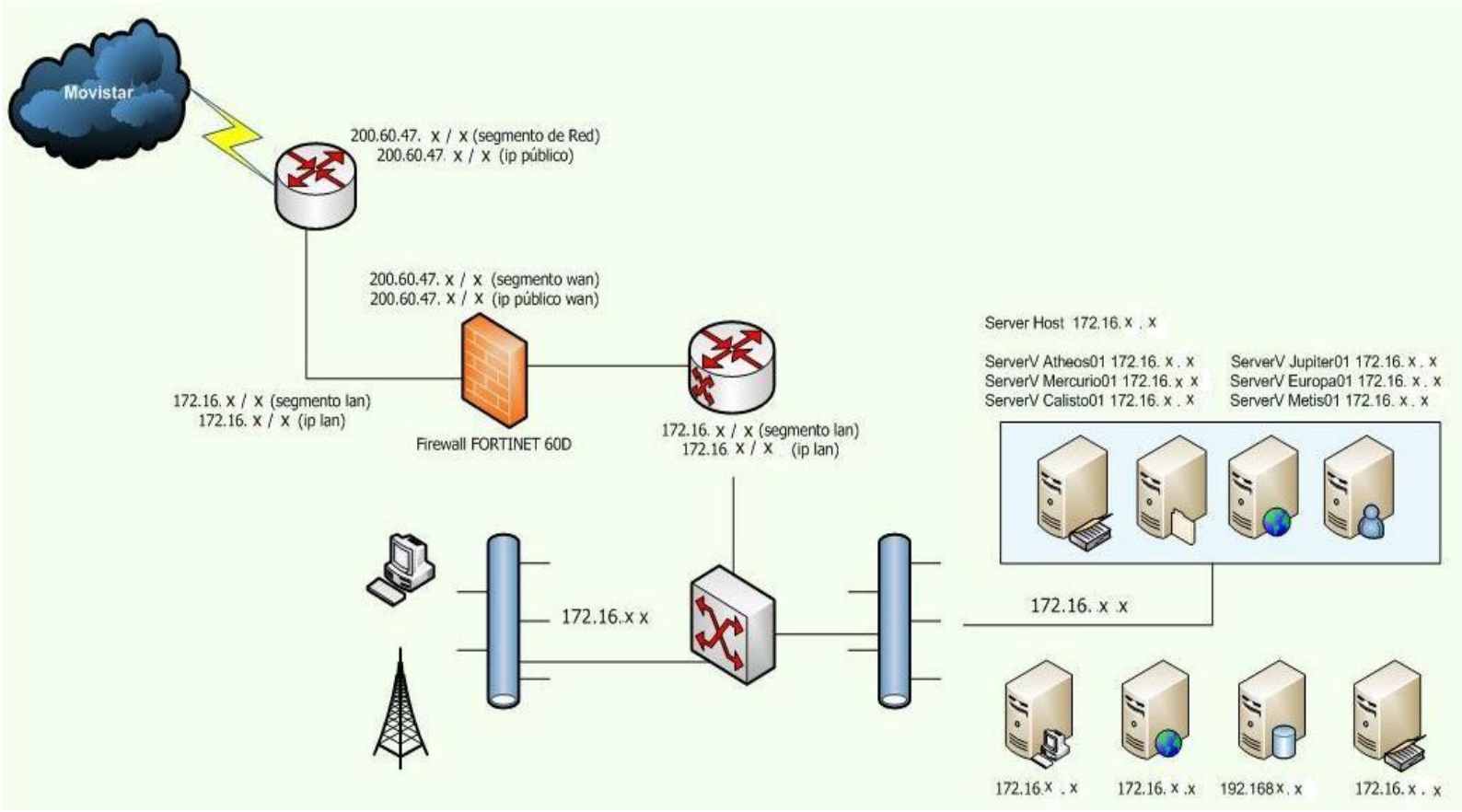
Fuente: Subgerencia de Sistemas e Informática (32).

Tabla Nº 11: Software – Inventario software - Licencias

	NOMBRE DEL SOFTWARE	CANTIDAD DE LICENCIAS	CANTIDAD NO LICENCIADAS
SOFTWARE	MICROSOFT WINDOWS PROFESSIONAL 8	10	
ANTIVIRUS	ESET ENDPOINT PROTECTION ADVANCE PC	224	
	ESET ENDPOINT PROTECTION ADVANCE SERVIDORES	4	
SOFTWARE OFIMATICA	MICROSOFT OFFICE 2013 ESTÁNDAR	101	129
GESTOR DE BASE DE DATOS	MICROSOFT SQL SERVER 2012	1	1
	VISUAL FOXPRO 8	1	
	SQL SERVER 2008 MANAGER		2
	MY SQL	1 LIBRE	
	MICROSOFT SQL CALL	22	
OTROS	7-ZIP	SOFTWARE LIBRE	
	FOXIT READER		
	MATAVIRUS		
	DRAFT SIGHT 2015*64		
	RENAME 2015		
SISTEMAS MUNICIPALES PROPIOS	SISTEMA SIAF	NO NECESITA LICENCIA	
	SISTEMA SGTM		
	SISTEMA DE TRAMITE DOCUMENTARIO		
	SISTEMA DE LOGISTICA		
	SISTEMA DE BIBLIOTECA		
	SISTEMA DE REGISTRO CIVIL		
	SISTEMA DE MERCADO		
	SISTEMA DEMUNA		

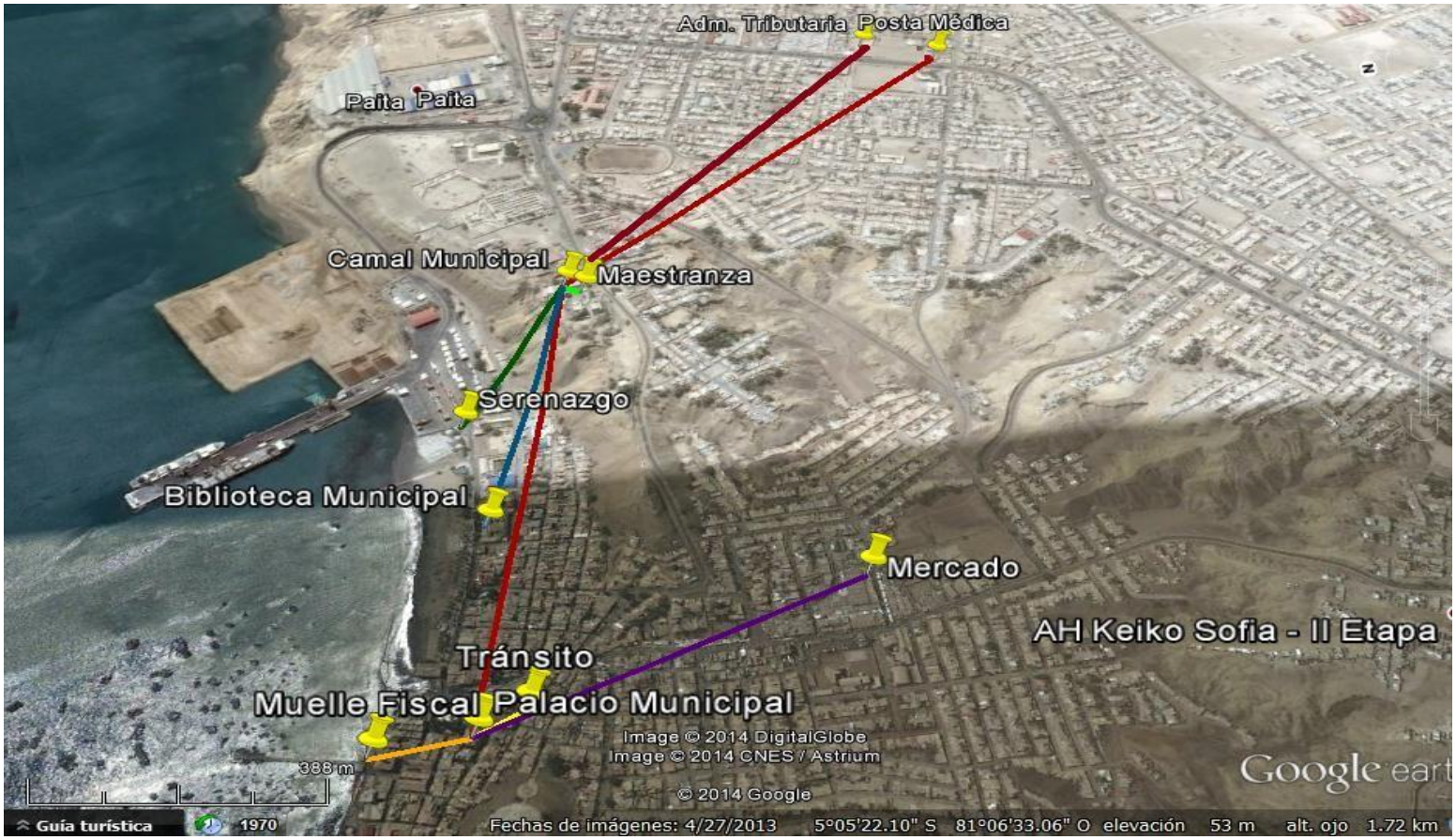
Fuente: Subgerencia de Sistemas e Informática (32).

Gráfico Nº 14: Mapa de la Red Institucional - 2016



Fuente: Subgerencia de Sistemas e Informática (32).

Gráfico Nº 15: Área de conectividad de la red de datos



Fuente: Subgerencia de Sistemas e Informática (32).

2.2.4. Las Tecnologías de información y comunicaciones (TIC)

Definición de Tecnologías de la Información

Se denominan Tecnologías de la Información y Comunicación (TIC), al conjunto de instrumentos tecnológicos que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones contenidas en señales de naturaleza acústica (Sonidos), óptica (Imágenes) o electromagnética (datos alfa numéricos) (35).

Gráfico Nº 16: El Proceso de la Información

Fuente: Universidad Politécnica de Madrid (36).

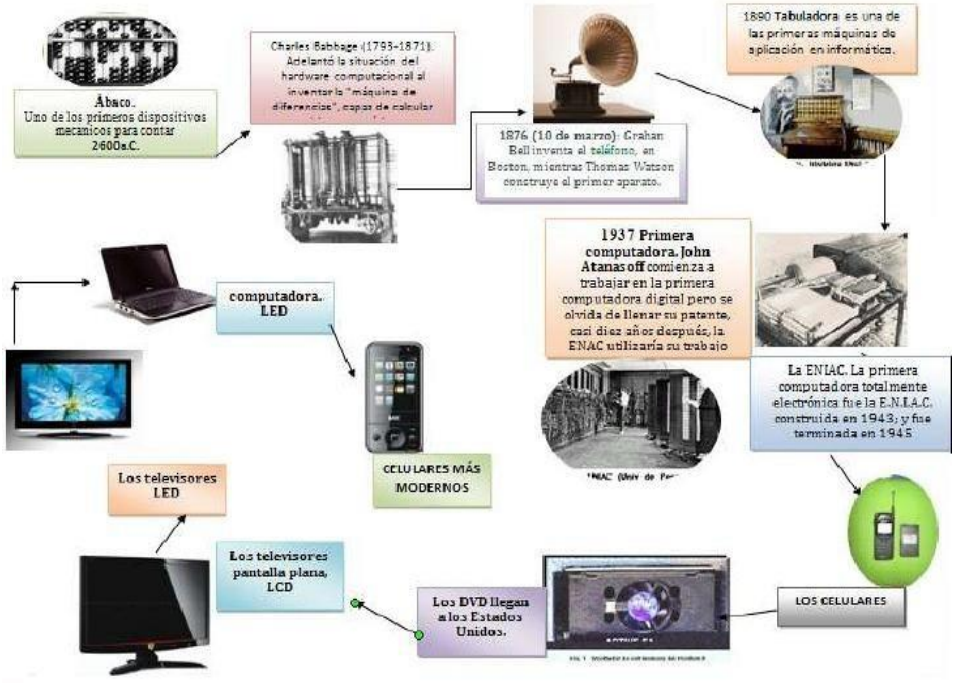
Evolución de las TIC

La revolución electrónica iniciada en la década de los 70’ constituye el punto de partida para el desarrollo creciente de la Era Digital. Los avances científicos en el campo de la electrónica tuvieron dos consecuencias inmediatas: la caída vertiginosa de los precios de las materias primas y la preponderancia de las Tecnologías de la Información (Information Technologies) que combinaban esencialmente la electrónica y el software. Pero, las investigaciones desarrolladas a principios de los años 80 han

permitido la convergencia de la electrónica, la informática y las telecomunicaciones posibilitando la interconexión entre redes. De esta forma, las TIC se han convertido en un sector estratégico para la "Nueva Economía". Desde entonces, los criterios de éxito para una organización o empresa dependen cada vez en gran medida de su capacidad para adaptarse a las innovaciones tecnológicas y de su habilidad para saber explotarlas en su propio beneficio. La Informática es la ciencia del tratamiento automático de la información a través de un computador (llamado también ordenador o computadora). Entre las tareas más populares que ha facilitado esta tecnología se encuentran: elaborar documentos, enviar y recibir correo electrónico, dibujar, crear efectos visuales y sonoros, maquetar folletos y libros, manejar la información contable en una empresa, reproducir música, controlar procesos industriales y jugar. Se podría establecer un punto de semejanza entre la revolución de las Tecnologías de la Información y la Revolución Industrial, cuya principal diferencia reside en la materia prima de su maquinaria, es decir, pasamos de una eclosión social basada en los usos de la energía a una sociedad cuyo bien primordial ha pasado a ser el conocimiento y la información. Pueden ser incluidas en esta gran área de las ciencias, la microelectrónica, la computación (hardware y software), las telecomunicaciones y (según opinión de algunos analistas) la ingeniería genética. Esta última, por decodificar, manipular y reprogramar la información genética de la materia viviente. Desde un punto de vista histórico, la revolución de las Tecnologías de la Información marca un momento crucial y decisivo en la sociedad mundial, pues ha penetrado en todas las áreas de vida humana, no como agente externo, sino como (muchas veces) motor que genera un flujo activo en las interrelaciones sociales. Durante la última década del siglo pasado, mucho se habló sobre una nueva era de oscurantismo informativo, ocasionado por esta suerte de carrera contra reloj por la adquisición y generación de información y conocimientos. Sin embargo, las nuevas tecnologías de la información, representan una oportunidad singular en el proceso de democratización del conocimiento, pues los usuarios pueden tomar el

control de la tecnología, que usan y generan, y producir y distribuir bienes y servicios. Podría pensarse que las TIC han abierto un territorio en el cual la mente humana es la fuerza productiva directa de mayor importancia en la actualidad. Por lo tanto, el ser humano es capaz de convertir su pensamiento en bienes y servicios y distribuirlos no ya en una frontera local, sino globalmente. Las TIC han modificado sustancial e irrevocablemente, la forma en que vivimos, dormimos, soñamos y morimos. En este caso, podríamos hacernos eco de las palabras de "Jean Paul Sartre" cuando dice que no se trata de preguntarnos si la historia tiene un sentido, sino de que ya que estamos metidos hasta el cuello debemos darle el sentido que nos parezca mejor y prestar toda nuestra colaboración para las acciones que lo requieran. Esto se aplica perfectamente a la participación ciudadana activa en el desarrollo de las Tecnologías de la Información en el país, lo que por ende incidirá en el crecimiento económico, político, social y cultural de la nación (37).

Gráfico Nº 17: Origen y Evolución de la TIC.



Fuente: es.slideshare.net (38)

Principales TIC existentes

Las principales TIC que usan las empresas son las siguientes:

- Línea Fija de Teléfono / fax: La línea fija de teléfono y fax es hoy día la tecnología de comunicación más efectiva en términos de costos para las pequeñas empresas de los países en desarrollo.

- Teléfono celular: Los teléfonos celulares son especialmente adecuados para usuarios del sector de los negocios. Estos dispositivos permiten a los empresarios contestar las llamadas de sus clientes de manera inmediata.

- Correo Electrónico: nos permite poder enviar una gran variedad de información y también documentos y fotografías, etc.

- Internet y la Red Global (WWW): Internet es una red global de computadoras que pueden comunicarse entre sí. El uso de Internet por parte de las pequeñas empresas en los países en desarrollo está difundiéndose con gran celeridad, pero sigue siendo aún muy limitado.

- La Web (la Red Global): Un sitio Web contiene páginas con datos (palabras, imágenes, sonidos, video) que están unidas entre sí electrónicamente. Cualquier persona que tenga acceso a Internet puede acceder a un sitio Web. Por lo tanto, la Red Global conecta a las pequeñas empresas de los países en desarrollo con un mercado potencial que cubre el mundo entero.

- Comercio electrónico: El comercio electrónico se utiliza para realizar transacciones comerciales electrónicamente, como comprar por Internet un artículo. Algunas pequeñas empresas están inmersas en el mundo del comercio electrónico (39).

Ventajas de las TIC

Los beneficios que aportan las Tic son las siguientes:

- Fácil acceso a una inmensa fuente información.
- Proceso rápido y fiable de todo tipo de datos.
- Canales de comunicación (on/off).
- Capacidad de almacenamiento.
- Automatización de trabajos.
- Interactividad.
- Digitalización de toda la información.

Áreas de Aplicación de las TIC

Se aplican en las siguientes áreas:

- Administrativa: Contable, financiera, Procedimientos, ERP.
- Procesos Productivos: Cad, cam, entrega de productos.
- Relaciones Externas: Proveedores, mercadeo y CRM.
- Control y Evaluación Gerencial: Sistemas de información, gestión de calidad, formación del equipo humano.

El Estado Peruano considerando importante cumplir un rol activo promoviendo el desarrollo de las condiciones adecuadas para alcanzar la denominada Sociedad de la Información mediante R.M. Nº 181-2003-PCM del 4 de junio de 2003 se crea la Comisión Multisectorial de Desarrollo de la Sociedad de la Información (CODESI) con el objeto de elaborar el Plan Nacional para el Desarrollo de la Sociedad de la Información en el Perú. En el año 2005 mediante la R.M. N°148-2005-PCM se dio por concluido el encargo conferido a la CODESI y se dispuso la publicación del Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana en el portal de la Presidencia del Consejo de Ministros. El Plan de desarrollo de la Sociedad de la Información en el Perú "La Agenda Digital Peruana" señala que "El Estado Peruano afronta el gran reto de impulsar el desarrollo del Gobierno Electrónico en una situación en la que la mayoría de la población pertenece a bajos niveles socioeconómicos y cuenta con escaso rango de bancarización, reducidos niveles de alfabetización digital (especialmente en las zonas rurales y alejadas), escaso presupuesto para invertir en TIC en las entidades públicas y una casi nula integración de sus sistemas informáticos, impidiendo esto último la operación electrónica interinstitucional en el Estado. Es necesario, además, la adecuación normativa y de procedimientos para que la administración pública acepte e incentive los procedimientos electrónicos en su operación diaria" (CODESI 2005:42). El Plan señala que los primordiales factores de éxito necesarios para alcanzar el desarrollo sostenible del Gobierno Electrónico. En el Plan se advierte que en el Perú "la aplicación de las TIC en la administración pública ha sido intensiva en algunas de sus entidades, dando como resultado islas de modernidad, cuyo desarrollo tecnológico establece una gran brecha con el nivel promedio de desarrollo de otras entidades públicas" (CODESI 2005: 43). El Plan de Desarrollo de la Sociedad de la Información en el Perú plantea los objetivos fundamentales, las estrategias y las acciones necesarias para el desarrollo del Gobierno

Electrónico en el Perú, así como de las unidades informáticas en la administración pública, y son las bases para su desarrollo, el cual potenciará la competitividad de las empresas y la mejora en la calidad de vida de la población peruana, en especial la de menores recursos. (CODESI 2005: 44). Sin embargo la estrategia no ha considerado temas como la inclusión e integración social, además de otros aspectos tan crucialesa la realidad peruana como la descentralización que significa la transferencia de recursos y competencias de gestión tanto a los gobiernos regionales como a los gobiernos locales (40).

2.2.5. Norma Técnica Peruana NTP

Las Normas Técnicas Peruanas

Son documentos de aplicación voluntaria, aprobadas por la Comisión de Reglamentos Técnicos y Comerciales – CNB del INDECOPI y elaboradas por los Comités Técnicos de Normalización quienes están conformados por representantes de los sectores involucrados en una actividad definida, que bajo la supervisión del INDECOPI elaboran proyectos de NTP relacionados con su campo de actividad, y participan: sector productor/exportador, técnico y consumo (41).

Información

Es un activo que brinda valor al negocio; por ello, se necesita tener una adecuada protección frente a la constante exposición a distintas amenazas y vulnerabilidades. Esta puede adoptar distintas formas, de ahí surge la importancia de conocerlas para poder protegerla adecuadamente, estas formas son: impresa o escrita en papel, almacenada electrónicamente, transmitida vía correo o e-mail, mostrada en videos, hablada en conversaciones (42).

Seguridad de Información

Es la protección de la confidencialidad, integridad y disponibilidad de la información; es decir, asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran (42).

Oficial de Seguridad de Información

El oficial de seguridad de la información, conocido como CISO por sus siglas en inglés (Chief Information Security Officer), es la persona encargada de planificar, presupuestar y verificar el rendimiento de los componentes de la seguridad de la información. Así como de realizar una correcta gestión de riesgo para la toma de decisiones. Las responsabilidades de cada oficial varían dependiendo de la organización en la que se encuentren, debido a la cultura organizacional que puede existir (43).

Política de Seguridad de Información

Las políticas de seguridad de información son aquellas normas que se establecen para guiar a los miembros de la organización a resguardar correctamente la seguridad de la información. Peltier et. Al. (43), en su libro "Information Security Fundamentals", considera a las políticas de seguridad de información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos menciona que estas cumplen con 2 roles importantes, un rol interno y otro externo.

- Rol Interno: Ya que se menciona a cada uno de los miembros de la organización que se espera que realicen y como se evaluará el

trabajo realizado.

- Rol Externo: Ya que sirve para mostrarle al mundo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y qué estamos trabajando para realizarlo.

Sistema de Gestión

Un sistema de gestión es una estructura probada para la gestión y mejora continua de políticas, procedimientos y procesos de una organización. La implementación de un sistema de gestión ayuda a mejorar la efectividad operativa, optimizar costos, lograr mejoras continuas, aumentar la satisfacción de las partes interesadas al negocio y renovar constantemente las estrategias de la organización (44).

Sistema de Gestión de Seguridad de Información

Conocido como SGSI o ISMS por sus siglas en inglés (Information System Management System) es un sistema de gestión para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, de esta manera un SGSI lo que busca es poder mantener la confidencialidad, integridad y disponibilidad de la información mientras minimiza los riesgos de seguridad de la información (45).

El círculo de DEMING se constituye como una de las principales herramientas para lograr la mejora continua en las organizaciones o empresas que desean aplicar la excelencia en sistemas de gestión. El ciclo Deming o también denominado como ciclo PHVA que quiere decir según sus iniciales (planear, hacer, verificar y actuar) o en ingles PDCA plan, do, check, act (46).

Gráfico Nº 18: Ciclo DEMING

Fuente: ONGEI (46).

- Plan (Establecer el SGSI): Implica, establecer la política del SGSI, sus objetivos, procesos y procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, con resultados acordes a las políticas y objetivos de toda la organización. El SGSI tiene que ir alineado con el plan estratégico de la compañía.

- Do (Implementar y operar el SGSI): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos que se vayan a definir en la planificación del SGSI.

- Check (Monitorizar y revisar el SGSI): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

- Act (Mantener y mejorar el SGSI): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y/o externas, revisiones del SGSI o cualquier otra información relevante para permitir la continua mejora del sistema (46).

Riesgo

Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad. HALVORSON (47), en el año 2008 explica tres naturalezas del riesgo, estos son los riesgos estratégicos, tácticos y operacionales.

- Los riesgos estratégicos son los que pueden estar ligados a la seguridad de la información; sin embargo, se encuentran más orientados a los riesgos de las ganancias y reputación de la organización, ya que se derivan de decisiones estratégicas que han sido tomadas o serán tomadas en la organización.

- Los riesgos tácticos son los asociados a los sistemas que vigilan la identificación, control y monitoreo de los riesgos que afectan a la información, son aquellos que afectan indirectamente a la información.

- Los riesgos operacionales son los relacionados a aquellos activos que pueden afectar los objetivos de una empresa (tales como presupuestos, cronogramas y tecnologías).

Para poder identificar el potencial daño o pérdida debido a un riesgo los dueños de los activos pueden responder estas cuatro preguntas:

- ¿Qué puede suceder? (¿Cuál es la amenaza?)

- ¿Qué tan malo puede ser? (¿Cuál es el impacto?)

- ¿Qué tan seguido puede suceder? (¿Cuál es la frecuencia?)

- ¿Qué tan ciertas son las respuestas de las tres primeras preguntas? (¿Cuál es el grado de confianza?) (48).

Administrar Riesgos

Es el uso de la información para estimar el impacto de los riesgos e identificar sus causas, de esta manera se pueden tomar medidas anticipadas ante un incidente (42).

Control

Los controles son medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales. "Una de las clasificaciones más generalizadas es:

- Preventivos: Reducen las vulnerabilidades.

- Detectivos: Descubren amenazas o escenarios previos a ellas permitiendo activar otros controles.

- Correctivos: Contrarrestan el impacto de la ocurrencia de una amenaza.

- Disuasivos: Reducen la probabilidad de ocurrencia de las amenazas".

En la NTP ISO/IEC 17799 (42), también se utiliza el control como un sinónimo de contramedida.

2.2.6. ISO/IEC

ISO (La Organización Internacional para la Normalización) e IEC (La Comisión Electrónica Internacional) forman el sistema especializado para la normalización mundial. Los órganos nacionales que son miembros de ISO o de IEC participan en el desarrollo de las Normas Internacionales a través de comités técnicos establecidos por la respectiva organización para ocuparse de campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en enlace con ISO y con IEC, también participan en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1 (45).

2.2.7. ISO/IEC 27000

Es una norma internacional que busca dar información general sobre los sistemas de gestión de seguridad de información, así como definir algunos términos que son usados por todos los estándares de la familia 27000. A diferencia de las otras normas de esta familia, esta es de libre distribución y se caracteriza por brindar un listado de las normas mencionadas junto con una pequeña descripción:

- ISO/IEC 27001: El estándar principal de la familia, brinda los requerimientos para el desarrollo y operación de SGSI incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de información. Se puede confirmar la eficacia de la implementación del SGSI mediante una auditoria o certificación (16).

- ISO/IEC 27002: Este estándar brinda la guía de implementación de la lista de las mejores prácticas y los más aceptados objetivos de control presentados como anexo en la ISO/IEC 27001, con el objetivo de facilitar la elección de controles para asegurar la seguridad de los activos de información.

- ISO/IEC 27003: Este estándar brinda información y una guía práctica para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI según lo establecido por la ISO/IEC 27001.

- ISO/IEC 27004: Este estándar provee guías prácticas para el uso de métricas que evalúen la efectividad, objetivos de control y controles usados en un SGSI.

- ISO/IEC 27005: Este estándar provee una guía para la gestión de los riesgos de seguridad de información según los requerimientos establecidos por la ISO/IEC 27001.

- ISO/IEC 27006: Este estándar se complementa con el ISO/IEC 17021 y brinda los requerimientos necesarios para la acreditación de la certificación de una organización que certifique los SGSI según la ISO/IEC 27001.

- ISO/IEC 27007: Provee una guía para conducir una auditoria de un SGSI así como las competencias necesarias de los auditores de sistemas de gestión de seguridad complementando la ISO/IEC 19011.

- ISO/IEC TR 27008: Es un reporte técnico que brinda una guía para la revisión de la implementación de los controles del SGSI (16).

- ISO/IEC 27010: Provee una guía para gestionar la seguridad de la información en caso la organización intercambie o comparta información importante, ya sea que pertenezca al sector público o

privado, que lo haga nacional o internacionalmente, o en el mismo sector u otros sectores del mercado en el que opera.

- ISO/IEC 27011: Provee una guía para apoyar la implementación de un SGSI en una empresa de telecomunicaciones.

- ISO/IEC 27013: Brinda una guía para la implementación integrada del ISO/IEC 27001 y el ISO/IEC 20000 (gestión de servicios de TI), ya sea implementándolos al mismo tiempo o uno después de otro.

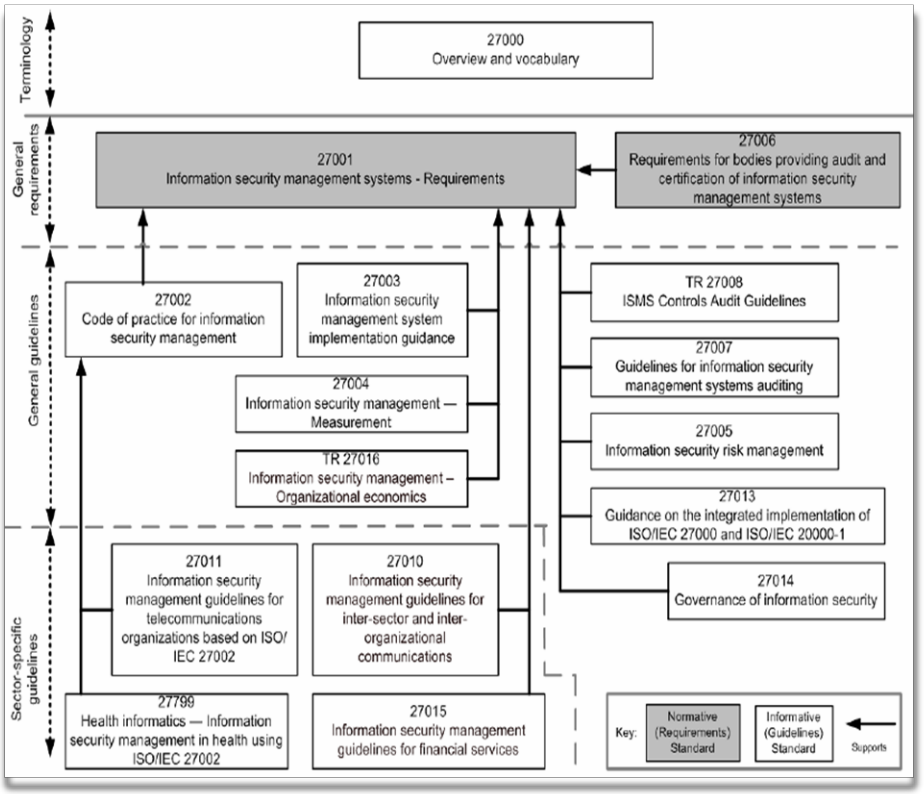
- ISO/IEC 27014: Brinda una guía para conocer los principios y procesos del gobierno de la seguridad de la información, que busca que las organizaciones puedan evaluar, dirigir y monitorear la gestión de la seguridad de la información.

- ISO/IEC TR 27015: Sirve como complemento a las normas de la familia ISO/IEC 27000 para la implementación, mantenimiento y mejora del SGSI en empresas que provean servicios financieros.

- ISO/IEC TR 27016: Es un reporte técnico que brinda una metodología que permite a las organizaciones saber cómo valorar adecuadamente los activos de información identificados, los riesgos potenciales a los activos, apreciar el valor de los controles que protegen a estos activos y determinar el nivel óptimo de recursos que deben ser usados para asegurarlos.

- ISO/IEC 27799:2008: Brinda una guía para apoyar la implementación de un Sistema de Gestión de Seguridad de la Información en las empresas de salud con la adaptación del ISO/IEC 27002 según los requerimientos de este sector (16).

Gráfico Nº 19: Relación de los estándares de la familia del SGSI



Fuente: ISO/IEC 27000 (45).

2.2.8. Norma Técnica de Gestión de Seguridad de la Información 27001 y su uso obligatorio

En el Perú, por R.M. Nº 004-2016-PCM, publicada el 14 de Enero del 2016 se aprobó el uso obligatorio de la NTP ISO/IEC 27001:2014. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2º edición en todas las entidades integrantes del Sistema Nacional de Informática (11).

Esta Norma Técnica Peruana reemplaza a la NTP-ISO/EIC 27001:2008 (revisada el 2013) y es una adopción de la norma ISO/EIC 27001:2013 y de la ISO/EIC 27001:2013/COR 1. La Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada en concordancia con las Guías Peruanas GP 001:1995 y GP 002:1995 (49).

a. Objeto y Campo de Aplicación

La Norma Técnica Peruana 27001:2014 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, dentro del contexto de la organización. Incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información.

b. Implementación

Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos años para la implementación y/o adecuación la norma. Sin embargo dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la seguridad de la información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico (ONGEI) de la Presidencia del Consejo de Ministros (49).

c. Certificación:

Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana NTP ISO/IEC 27001:2014, lo podrán realizar de forma opcional y con recursos propios de cada entidad.

d. Comité de Gestión de Seguridad de la Información:

Cada entidad designará un Comité de Gestión de Seguridad de la Información, el cual estará conformado por:

- El Titular de la entidad.

- El responsable de administración o quien haga sus veces.

- El responsable de planificación o quien haga sus veces.

- El responsable del área de informática o quien haga sus veces.

- El responsable del área legal o quien haga sus veces y

- El oficial de seguridad de la información.

Las funciones del Comité de Gestión de Seguridad de la Información, serán establecidas por cada entidad.

e. Responsabilidad de la implementación:

La responsabilidad de la implementación de la norma será del titular de cada entidad.

f. Contenido:

La Norma Técnica tiene el siguiente contenido:

Parte I: Norma NTP ISO/IEC 27001:2014.

1. Objeto de aplicación.

La Norma Técnica Peruana 27001:2014 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, dentro del contexto de la organización. Incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información (49).

2. Referencias Normativas.

   Las referencias normativas están señalada en la norma y son indispensables para su aplicación.

3. Términos y Definiciones.

   Se aplican los términos y definiciones proporcionados en ISO/IEC 27000.

4. Contexto de la Organización.

   - La organización debe determinar los aspectos externos e internos que son relevantes y que afectan su capacidad de lograr los resultados deseados.

   - La organización debe comprender las necesidades de las partes interesadas.

   - Finalmente debe determinar el alcance del sistema de gestión de seguridad de la información.

5. Liderazgo.

   - La alta dirección debe demostrar liderazgo y compromiso respecto al sistema de gestión de seguridad de la información.

   - La alta dirección debe establecer una política de seguridad de la información que fije objetivos y que esté disponible comunicada e informada.

- Es la organización de los roles, responsabilidades y autoridades (49).

6. Planificación.

   - La organización debe planificar acciones para abordar riesgos y oportunidades.

7. Soporte.

   - La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

8. Operación.

   - La organización debe controlar los procesos necesarios para cumplir con los requisitos de seguridad.

   - Se debe realizar una evaluación de riesgos de seguridad de la información.

   - Realizar el plan de manejo de riesgos de seguridad de la información.

9. Evaluación de Desempeño.

   - Realizar el monitoreo, la medición, análisis y evaluación del desempeño de la seguridad de la información y la efectividad del sistema de gestión de seguridad de la información (49).

10. Mejoras.

- La organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información.

Parte II: Informe Técnico:

1. Antecedentes.

Es una breve reseña histórica de la norma técnica peruana.

2. Base Legal.

- RM N° 129-2012-PCM Implementación Obligatoria de la NTP ISO IEC/27001:2008.

- LEY N° 29664 Ley que Crea el Sistema Nacional de Gestión de Desastres (SINAGERD).

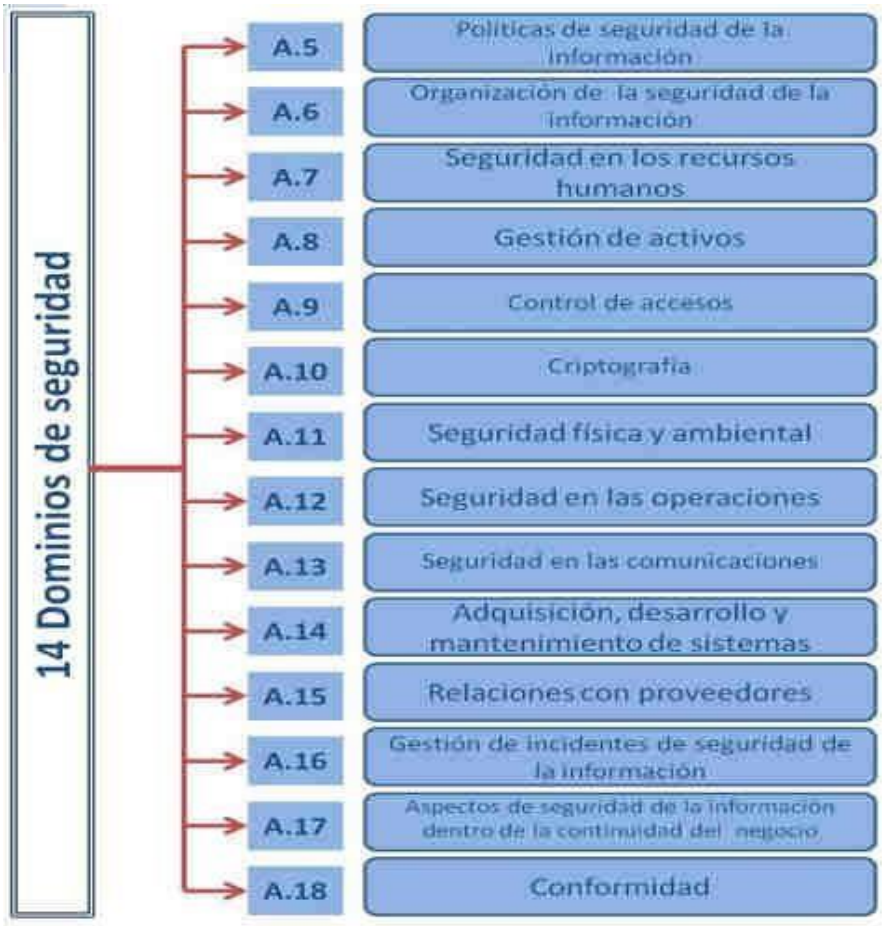
- Ley 29733, Ley de Protección de Datos Personales y su reglamento, aprobado por Decreto Supremo N° 003-2013-JUS.

- Decreto Supremo Nº 013-2003-PCM, Dictan medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público.

- Resolución Ministerial Nº 179-2004-PCM, que aprueba el uso obligatorio de la "Norma Técnica Peruana NTP-ISO/IEC 12207:2004, Tecnología de la Información, Procesos del ciclo de vida del software 1ª Edición" y modificatoria.

- R.M. Nº 004-2016-PCM, publicada el 14 de Enero del 2016 se aprueba el uso obligatorio de la NTP ISO/IEC 27001:2014. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2º edición en todas las entidades integrantes del Sistema Nacional de Informática (49).

Gráfico Nº 20: Estructura de la Seguridad NTP ISO/IEC 27001:2008



Fuente: Seguridad de Información – FONCODES (50).

Ventajas de los SGSI

La implantación de un SGSI es importante porque permite contar con un Plan de Continuidad del Negocio cuyo objetivo de control es neutralizar las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los sistemas de información y asegurar su reanudación oportuna (50).

Es mejor tener un plan para evitar la confusión durante el evento

- "Proactivo" Vs "Reactivo"
- Tomar las acciones correctivas cuando sea necesario
- Se deben establecer controles que mitiguen el riesgo
- Continuidad del servicio
- Respuesta ordenada ante un desastre

Gráfico Nº 21: Plan de Continuidad del Negocio

Fuente: Seguridad de Información – FONCODES (50).

Planes de Respuesta a Emergencias PCN

Es un conjunto de actividades y procedimientos aprobados con el objetivo estructurar y organizar los recursos humanos y los medios de seguridad disponibles de la organización, con el fin de preparar a todo el personal que labora en él, a reaccionar en forma rápida, eficaz, oportuna y coordinadamente en los primeros momentos que se presente una emergencia, hasta que lleguen los servicios de ayuda exterior(50).

Planes de Gestión de Crisis (CMP)

Es un conjunto de actividades y procedimientos aprobados, que define de manera precisa, las acciones a seguir para la optimización de las actividades desde el instante del incidente hasta la adopción, o no, del BCP (Business Continuity Plan) / DRP. (Disaster Recovery Plan)

Gráfico Nº 22: Razones para tener un Plan de Continuidad del Negocio

Fuente: Seguridad de Información – FONCODES (50).

Casos de éxito

En Ecuador, una investigación realizada en el año 2014 la cual se tituló "Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa" de la Universidad Católica de Santiago de Guayaquil", se pretende dar una adecuada solución de seguridad, haciendo énfasis en el análisis de la norma ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission) 27001 y su puesta en práctica en una empresa o institución. El estudio se encuentra dividido en tres capítulos. En el primero se efectúa un estudio de la seguridad informática. Durante el segundo capítulo se lleva a cabo una caracterización general de las normas ISO/IEC 27000, profundizando en la ISO/IEC 27001 que abarca lo concerniente a las técnicas de seguridad, los Sistemas de Gestión de Seguridad de la Información y los requerimientos a tener en cuenta. Por último, durante el tercer capítulo se implementa el Plan de Seguridad Informática de la empresa, con los análisis de riesgos, basado en el estándar mencionado. Este estudio se desarrolla teniendo en cuenta la necesidad de que la seguridad en la empresa cumpla cabalmente con los parámetros internacionales establecidos, contribuyendo así al mejoramiento de la misma y al propósito de obtener su certificación. llegando a las siguientes conclusiones: La puesta en funcionamiento de un SGSI basado en la norma ISO/IEC 27001 garantiza la ejecución de un conjunto de procesos que gestionen la accesibilidad de la información en la empresa. La implantación del estándar ISO/IEC 27001, a partir de cuatro fases fundamentales (Panificar, Hacer Verificar y Actuar), según el Ciclo de Deming, permite desarrollar una metodología de trabajo clara y estructurada. La revisión periódica de los controles que se han seleccionado e implementado reduce los riesgos de pérdida, robo o corrupción de la información en la empresa. En la empresa se pueden implementar los controles propuestos para incrementar la seguridad del sistema, incluyendo el de gestión de continuidad de funciones. Debido a

que el estándar ISO/IEC 27001 se relaciona con otros como el ISO/IEC 9001, y se adapta a las condiciones existentes en Ecuador, se pueden realizar varias certificaciones simultáneamente en esta empresa siempre que cumpla con lo dispuesto en cada una de las normas. El hecho de que pudieran ocurrir varias contingencias en la empresa evidencia que se deben prevenir las mismas y conocer las acciones a realizar en caso de que alguna de ellas suceda. Se muestra que el empleo del Plan de Tratamiento de Riesgos propuesto en este trabajo posibilita la aplicación de procedimientos y políticas de seguridad acordes con la norma ISO/IEC 27001. La implementación de la norma ISO/IEC 27001 en la empresa no solamente permite realizar la reducción de riesgos, sino que posibilita llevar a cabo la prevención de los mismos (51).

En Lima, una investigación de grado para optar el Título Profesional de Ingeniero de Computación y Sistemas realizada en el año 2012, la cual se nombró "Diseño e Implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos" de la Universidad de San Martin de Porres, concluye que en la actualidad, muchas empresas que están o desean incursionar en el ámbito financiero tienen problemas para resguardar la seguridad de su información; en consecuencia esta corre riesgos al igual que sus activos. El propósito de su investigación se centró en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), bajo una metodología de análisis y evaluación de riesgos, para luego implantar los controles necesarios que ayudaran a proteger sus activos tomando como referencia las Normas ISO 27001: 2005 e ISO 17799:2005. Esta implementación permitió un gran aumento en la seguridad de los activos de información de la empresa Card Perú SA., que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, el entorno y las tecnologías (52).

2.3. Sistema de hipótesis

2.3.1. Hipótesis principal

La propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016, minimizará la pérdida de información.

2.3.1. Hipótesis especificas

1. La evaluación de la situación actual de los procesos de seguridad en la Municipalidad Provincial de Paita, en el año 2016; permitirá identificar las falencias de seguridad de la información.

2. La inseguridad de la información existente en la Municipalidad Provincial de Paita, en el año 2016; justificará la factibilidad técnica, la inversión económica y operativa para el desarrollo de la propuesta, basadas en buenas prácticas, para la gestión de seguridad de la información.

3. La necesidad de una eficiente propuesta de políticas basadas, en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita, en el año 2016; respalda el desarrollo e implementación de la propuesta.

III. METODOLOGÍA

3.1. Diseño de la investigación

El tipo y diseño de la investigación es No Experimental, Descriptiva, de Corte Transversal y por las características de la variable es cuantitativa, puesto que solo se definieron y analizaron las variables, sin algún tipo de manipulación. Por otra parte dicha evaluación se realizó en un determinado periodo (año 2016), tomando en cuenta las condiciones e indicadores precedentes durante el mismo.

Se define como No Experimental o también conocido como post facto; por cuanto su estudio se basa en la observación de los hechos en pleno acontecimiento sin alterar en lo más mínimo ni el entorno ni el fenómeno estudiado (53).

Así mismo, se indica como Descriptiva; porque describe como es y cómo se manifiesta el problema**.** Su finalidad es describir y/o estimar parámetros. Se describen frecuencias y/o promedios; y se estiman parámetros con intervalos de confianza. El propósito del investigador es describir situaciones y eventos. Esto es decir como es y se manifiesta determinado fenómeno. Los estudios descriptivos buscan desarrollar una imagen o fiel representación (descripción) del fenómeno estudiado a partir de sus características. Describir en este caso es sinónimo de medir. Miden variables o conceptos con el fin de especificar las propiedades importantes de comunidades, personas, grupos o fenómeno bajo análisis. El énfasis está en el estudio independiente de cada característica, es posible que de alguna manera se integren las mediciones de dos o más características con el fin de determinar cómo es o cómo se manifiesta el fenómeno. Pero en ningún momento se pretende establecer la forma de relación entre estas características. En algunos casos los resultados pueden ser usados para predecir (54).

Por otro lado, el nivel es De Corte Transversal; pues el estudio se circunscribe a un momento puntual, un segmento de tiempo durante un tiempo a fin de medir o caracterizar la situación en ese tiempo específico (53).

Finalmente, por sus características es Cuantitativa; cuando la preponderancia del estudio de los datos se basa en la cuantificación y cálculo de los mismos, permite examinar los datos de manera científica, o de manera más específicamente en forma numérica, generalmente con ayuda de herramientas del campo de la estadística (53).

El diseño se grafica de la siguiente manera:

Donde:

M: Muestra

O: Observación

3.2. Población y Muestra

Población (P)

Tamayo y Tamayo (55), definen a la población como la totalidad del fenómeno que se estudia, donde las variables de población poseen una característica común, la cual se estudia y da origen a los datos generados de información. Una población está determinada por sus características definitorias. Por lo tanto, el conjunto de elementos que posea esta característica se denomina población o universo. Población es la totalidad del fenómeno a estudiar, donde las unidades de población poseen una característica común, la que se estudia y da origen a los datos de la investigación.

Para la presente investigación la población estuvo delimitada por un total de 152 trabajadores municipales que utilizan las tecnologías y los sistemas de información de la Municipalidad Provincial de Paita.

Tabla Nº 12: Población

Personal	Cantidad
Gerentes	10
Sub-gerentes	28
Empleados Nombrados bajo el Dec. Leg.276	53
Bajo el Régimen C.A.S.	40
Bajo el Régimen S.N.P.	21
Total Población	152

Fuente: Elaboración propia.

Muestra

En relación a la muestra, podemos anotar que el Diccionario de la Lengua Española RAE (56), define la muestra, en su segunda acepción, como "parte o porción extraída de un conjunto por métodos que permiten considerarla como representativa de él". Mientras que para Hernández et. Al. (57), "La muestra es en esencia de un subgrupo de la población. Digamos que es un subconjunto de elementos que pertenecen a ese conjunto definidos en sus características al que llamamos población".

Las unidades de análisis la constituyen los trabajadores municipales que utilizan las tecnologías y los sistemas de información de la Municipalidad Provincial de Paita y está conformada de la siguiente manera:

- La muestra seleccionada para la dimensión: Evaluación del Estado actual de la seguridad de la información será de 152 trabajadores municipales que desempeñan su labor directamente con computadoras y TIC.

- La muestra seleccionada para la dimensión: Factibilidad técnica, Económica y operativa de la propuesta será de 08 trabajadores municipales los cuales forman parte del Comité de Gestión de Seguridad de la Información establecido en el Artículo Quinto de la Resolución Ministerial Nº 004-2016-PCM.

- La muestra seleccionada para la dimensión: Propuesta de Políticas del Plan de Gestión de Seguridad de la Información será de 02 trabajadores municipales, siendo aplicado al Sub Gerente de Sistemas e Informática y al Sub Gerente de Recursos Humanos, con la finalidad de evaluar la información gerencial que manejan.

3.3. Técnicas e instrumentos.

3.3.1. Técnica

La técnica que se utilizó es la encuesta.

Encuesta:

Se denomina encuesta al conjunto de preguntas especialmente diseñadas y pensadas para ser dirigidas a una muestra de población, que se considera por determinadas circunstancias funcionales al trabajo, representativa de esa población, con el objetivo de conocer la opinión de la gente sobre determinadas cuestiones corrientes y porque no también para medir la temperatura de la gente acerca de algún hecho específico que se sucede en una comunidad determinada y que despierta especial atención entre la opinión pública y que capaz requiere de la realización de una encuesta para conocer más a fondo cuál es la sensación de la gente (58).

3.3.2. Instrumentos

El instrumento que se utilizó es el cuestionario.

Cuestionario:

El cuestionario es un procedimiento considerado clásico en las ciencias sociales para la obtención y registro de datos. Su versatilidad permite utilizarlo como instrumento de investigación y como instrumento de evaluación de personas, procesos y programas de formación. Es una técnica de evaluación que puede abarcar aspectos cuantitativos y cualitativos. Su característica singular radica en que para registrar la información solicitada a los mismos sujetos, ésta tiene lugar de una forma menos profunda e impersonal, que el "cara a cara" de la entrevista. Al mismo tiempo, permite consultar a una población amplia de una manera rápida y económica (59).

3.4. Procedimiento de recolección de datos.

Se seleccionó a las personas adecuadas y para poder aplicar los cuestionarios se realizó visitas a las diversas instalaciones de la Municipalidad Provincial de Paita, durante el desarrollo de los cuestionarios se pudo resolver cualquier duda en relación a las interrogantes planteadas. La recolección de datos se realizó mediante la aplicación de 03 cuestionarios cada uno contiene 10 preguntas cerradas para medir conocimientos, actitudes y opiniones.

El cuestionario "Diagnóstico del Estado Actual de la Seguridad de la Información en la Municipalidad Provincial de Paita" encontrado en el ANEXO Nº 3: CUESTIONARIO Cuestionario Nº 1, se aplicó a la toda la muestra constituida por 152 trabajadores municipales que desempeñan su labor directamente con computadoras.

El cuestionario "Factibilidad Técnica, Económica y Operativa de la Propuesta en la Municipalidad Provincial de Paita" encontrado en el ANEXO Nº 3: CUESTIONARIO Cuestionario Nº 2, se aplicó a 08 trabajadores municipales los cuales formaran parte del Comité de Gestión de Seguridad de la Información establecido en el Artículo 5º de la Resolución Ministerial Nº 004-2016-PCM conformado por el Gerente Municipal, el Gerente de Administración, el Gerente de Planeamiento y Presupuesto, el Sub Gerente de Sistemas e Informática, el Gerente de Asesoría Jurídica y el Sub Gerente de Recursos Humanos y dos Asistentes de la Sub Gerencia de Sistemas e Informática.

El cuestionario "Necesidad de la Propuesta de Políticas Basadas en Buenas Prácticas para la Gestión de Seguridad de la Información en la Municipalidad Provincial de Paita" encontrado en el ANEXO Nº 3: CUESTIONARIO Cuestionario Nº 3, se aplicó al Sub Gerente de Sistemas e Informática y al Sub Gerente de Recursos Humanos, con la finalidad de evaluar la información gerencial que manejan, en el sentido de corroborar el estado de la seguridad informática y los controles de pertinentes de la seguridad de la información.

3.5. Definición operacional de las variables en estudio

Variable	Definición Conceptual	Dimensiones	Indicadores	Definición Operacional
Propuesta de Políticas basadas en Buenas Prácticas para la Gestión de Seguridad de la Información	Las políticas de seguridad de información son aquellas normas que se establecen para guiar a los miembros de la organización a resguardar correctamente la seguridad de la información. Peltier et. Al. (43), en su libro "Information Security Fundamentals", considera a las políticas de seguridad de información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías.	• Evaluación del estado actual de la seguridad de la información.	- Conocimiento de Plan de Seguridad de Información. - Calidad de Seguridad de la información en la plataforma tecnológica. - Cambio positivo con la aplicación de un plan de seguridad de información	Si No
		• Factibilidad técnica, económica y operativa de la propuesta.	- Capacidad para liderar un proyecto. - Asistencia Técnica para el desarrollo del plan de seguridad de la información. - Aprobación de la elaboración del diseño de la propuesta del Plan de Seguridad de la Información - Costo de la implementación de políticas de seguridad de la información.	Si No
		• Propuesta de políticas del plan de gestión de seguridad de la información.	- Confidencialidad de la información. - Grado de responsabilidad en el empleo de la información - Protección de los recursos informáticos	Si No

Fuente: investigación realizada por López, Arelys (12).

3.6. Plan de análisis

Los datos obtenidos fueron codificados y luego ingresados en una hoja de cálculo del programa Microsoft Excel 2013. Además se procedió a la tabulación de los mismos. Se realizó el análisis de datos que sirvió para establecer las frecuencias y realizar el análisis de distribución de dichas frecuencias.

Los resultados se expresan en términos absolutos y en porcentajes, además para el análisis e interpretación de los datos, se utilizaron las técnicas propias de la estadística descriptiva, tomando como punto de referencia las frecuencias y porcentajes de las respuestas más significativas con relación a la percepción y vivencia de los encuestados.

IV. RESULTADOS

4.1. Resultados

A. Dimensión: EVALUACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN

Tabla Nº 13: Conocimiento de un plan de seguridad de información

Distribución de frecuencias y respuestas relacionadas con el conocimiento de lo que significa un Plan de Seguridad de Información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	63	41.45
No	89	58.55
Total	152	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Tiene usted conocimiento sobre lo que significa un plan de seguridad de información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 13 se observa que el 58.55% de los empleados municipales encuestados expresaron que NO tienen conocimiento sobre lo que significa un plan de seguridad de información, mientras que el 41.45% SI tiene conocimiento de su significado.

Tabla Nº 14: Aprobación del diseño de un plan de seguridad de información

Distribución de frecuencias y respuestas relacionadas con la aprobación de un Plan de Seguridad de la Información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	132	86.84
No	20	13.16
Total	152	100.00

Fuente: Aplicación del instrumento para medir la aprobación de los empleados municipales encuestados respecto a la pregunta: ¿Cree usted que el diseño de un plan de Seguridad de la Información permitirá mejorar la calidad tecnológica?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 14 se observa que el 86.84% de los empleados municipales encuestados expresaron que SI cree que el diseño de un plan de Seguridad de la Información permitirá mejorar y ampliar la calidad tecnológica, actualizando la plataforma existente, mientras que el 13.16% NO cree que el diseño mejore la calidad tecnológica.

Tabla Nº 15: Aceptación de la aplicación del plan de seguridad de la información

Distribución de frecuencias y respuestas relacionadas con la aceptación de la aplicación del Plan de Seguridad de la Información en la plataforma tecnológica; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	132	86.84
No	20	13.16
Total	152	100.00

Fuente: Aplicación del instrumento para medir la aceptación de los empleados municipales encuestados respecto a la pregunta: ¿Cree usted que se logrará un cambio positivo con la aplicación del plan de seguridad de información en la plataforma tecnológica?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 15 se observa que el 86.84% de los empleados municipales encuestados expresaron que SI creen que la aplicación del plan de seguridad de la información en la plataforma tecnológica logrará cambios positivos a nivel tecnológico, mientras que el 13.16% NO cree que se logrará un cambio positivo con la aplicación del plan de seguridad de información.

Tabla Nº 16: Aceptación de implementación del plan de seguridad de información

Distribución de frecuencias y respuestas relacionadas con la aceptación de la implementación del Plan de Seguridad de la Información en la plataforma tecnológica; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	130	85.53
No	22	14.47
Total	152	100.00

Fuente: Aplicación del instrumento para medir la aceptación de los empleados municipales encuestados respecto a la pregunta: ¿Aprobaría usted la implementación del plan de Seguridad de la Información para la plataforma tecnológica?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 16 se observa que el 85.53% de los empleados municipales encuestados expresaron que SI aprobarían la implementación del plan de seguridad de la información en la plataforma tecnológica para mejorar la calidad de la información que se maneja, mientras que el 14.47% NO aprobarían la implementación del plan de seguridad de la información.

Tabla Nº 17: Aprobación de programas de sensibilización

Distribución de frecuencias y respuestas relacionadas con la aprobación de programas dirigidos a sensibilizar sobre la Seguridad de la Información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	105	69.08
No	47	30.92
Total	152	100.00

Fuente: Aplicación del instrumento para medir la aceptación de los empleados municipales encuestados respecto a la pregunta: ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la Seguridad de la Información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 17 se observa que el 69.08% de los empleados municipales encuestados expresaron que SI están de acuerdo en que en la Municipalidad de Paita exista un programa para la sensibilización del personal, lo cual es un factor preponderante para el éxito de la implementación de un Plan de Seguridad de Información, mientras que el 30.92% NO aprobarían programas dirigidos a todos los empleados para sensibilizar sobre la Seguridad de la Información.

Tabla Nº 18: Colaboración con la implementación del plan de seguridad

Distribución de frecuencias y respuestas relacionadas con la Capacidad de colaboración para que el plan de seguridad pueda ser llevado a cabo en las instalaciones ediles; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	125	82.24
No	27	17.76
Total	152	100.00

Fuente: Aplicación del instrumento para medir la aceptación de los empleados municipales encuestados respecto a la pregunta: ¿Estaría usted dispuesto a colaborar para que este plan de seguridad pueda ser llevado a cabo en las instalaciones ediles?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 18 se observa que el 82.24% de los empleados municipales encuestados expresaron que SI están dispuestos a colaborar con la implementación del Plan de Seguridad de la Información en la Municipalidad de Paita, para obtener mejoras en la plataforma tecnológica, mientras que el 17.76% NO estarían dispuestos a colaborar con la implementación del Plan de Seguridad de la Información.

Tabla Nº 19: Conocimiento de un plan de recuperación ante desastres

Distribución de frecuencias y respuestas relacionadas con el Conocimiento de un plan de recuperación ante desastres; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	38	25.00
No	114	75.00
Total	152	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Sabe usted si existe un plan de recuperación ante desastres?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 19 se observa que el 75.00% de los empleados municipales encuestados expresaron que NO existe una estrategia de recuperación de datos ante desastres, lo que significa que se desconoce si se cuenta con un plan de recuperación para aplicaciones críticas y así proporcionar la continuidad de negocio, mientras que el 25.00% indican que SI existe una estrategia de recuperación de datos ante desastres.

Tabla Nº 20: Conocimiento de evaluaciones realizadas de riesgos

Distribución de frecuencias y respuestas relacionadas con el Conocimiento de evaluaciones realizadas de riesgos relacionados con la información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	16	10.53
No	136	89.47
Total	152	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Sabe usted si se ha realizado evaluación de riesgos relacionados con la información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 20 se observa que el 89.47% de los empleados municipales encuestados expresaron que la Municipalidad de Paita NO cuenta con el análisis de riesgos relativo a los sistemas de información lo cual constituye una pieza importante para la selección de controles a aplicar e incluso la base para elaborar el Plan de Seguridad de la Información, mientras que el 10.53% indican que SI se ha realizado evaluación de riesgos relacionados con la información.

Tabla Nº 21: Conocimiento de evaluaciones de vulnerabilidades de la red

Distribución de frecuencias y respuestas relacionadas con el Conocimiento sobre evaluaciones realizadas de vulnerabilidades de la red; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	11	7.24
No	141	92.76
Total	152	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Sabe usted si se ha realizado una evaluación de vulnerabilidades de la red?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 21 se observa que el 92.76% de los empleados municipales encuestados expresaron que la Municipalidad de Paita NO cuenta con el análisis de vulnerabilidad, lo cual es una debilidad en la seguridad de la información, pues permite que una amenaza pueda afectar a un activo, mientras que el 7.24% indican que SI se ha realizado evaluación de vulnerabilidades de la red.

Tabla Nº 22: Conocimiento sobre software antivirus actualizado

Distribución de frecuencias y respuestas relacionadas con el Conocimiento sobre software antivirus actualizado; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	75	49.34
No	77	50.66
Total	152	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Sabe usted si se cuenta con software antivirus actualizado?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 22 se observa que el 50.66% de los empleados municipales encuestados expresaron que la Municipalidad de Paita NO posee antivirus actualizado, lo cual es un elemento muy importante para evitar daños a la información y los procesos, mientras que el 49.34% indica que SI posee antivirus actualizado.

B. Dimensión: FACTIBILIDAD TECNICA, ECONÓMICA Y OPERATIVA DE LA PROPUESTA

Tabla Nº 23: Conocimiento e Importancia de la Norma ISO/IEC 27001:2014

Distribución de frecuencias y respuestas relacionadas con el Conocimiento e Importancia de la Norma ISO/IEC 27001:2014 como modelo para la implantación de un Sistema de Gestión de Seguridad de la Información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	8	100.00
No	0	0.00
Total	8	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Cree usted que la norma ISO/IEC 27001:2014 es, en sí misma, un modelo extenso y detallado, en el cual se especifican las etapas que se deben cumplir para la implantación de un Sistema de Gestión de Seguridad de la Información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 23 se observa que el 100.00% de los empleados encuestados expresaron que SI tiene conocimiento e importancia de la Norma ISO/IEC 27001:2014 como modelo para la implantación de un Sistema de Gestión de Seguridad de la Información, mientras que ninguno opinó lo contrario.

Tabla Nº 24: Capacidad de liderar el Proyecto

Distribución de frecuencias y respuestas relacionadas con la Capacidad de liderar el proyecto; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	1	12.50
No	7	87.50
Total	8	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Cree usted que se cuenta con personal capacitado para liderar el proyecto?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 24 se observa que el 87.50% de los empleados municipales encuestados expresaron que la Municipalidad NO cuenta con personal capacitado para liderar el proyecto, mientras que el 12.50% indica que SI existe personal capacitado para liderar el proyecto.

Tabla Nº 25: Capacitación o asistencia técnica brindada por la ONGEI

Distribución de frecuencias y respuestas relacionadas con la Capacitación o asistencia técnica brindada por la ONGEI; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	0	0.00
No	8	100.00
Total	8	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿La ONGEI ha brindado asistencia Técnica para el desarrollo del plan de seguridad de la información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 25 se observa que el 100.00% de los empleados municipales encuestados expresaron que la ONGEI NO ha brindado asistencia Técnica para el desarrollo del plan de seguridad de la información, mientras que ninguno opinó lo contrario.

Tabla Nº 26: Desarrollo de la propuesta en equipamiento informático suficiente

Distribución de frecuencias y respuestas relacionadas con la capacidad del desarrollo de la propuesta en relación al equipamiento informático suficiente; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	0	0.0
No	8	100.00
Total	8	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Cree usted que se cuenta con el equipo informático suficiente (computadoras y periféricos) para el desarrollo de la propuesta?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 26 se observa que el 100.00% de los empleados municipales encuestados expresaron que la Municipalidad NO cuenta con el equipo informático suficiente (computadoras y periféricos) para el desarrollo de esta propuesta, mientras que ninguno opinó lo contrario.

Tabla Nº 27: Aprobación del diseño del plan de seguridad de la información

Distribución de frecuencias y respuestas relacionadas con la aprobación de la elaboración del Diseño de la propuesta del Plan de Seguridad de la Información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	8	100.00
No	0	0.00
Total	8	100.00

Fuente: Aplicación del instrumento para medir la aceptación de los empleados municipales encuestados respecto a la pregunta: ¿La alta dirección apoya y aprueba la elaboración del Diseño de la propuesta del Plan de Seguridad de la Información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 27 se observa que el 100.00% de los empleados municipales encuestados expresaron que la alta dirección SI apoya y aprueba la elaboración del Diseño de la propuesta del Plan de Seguridad de la Información, lo cual es un factor preponderante para el éxito de la Propuesta, mientras que ninguno opinó lo contrario.

Tabla Nº 28: Disponibilidad para formarse en el desarrollo de cada fase del sistema de gestión de seguridad de la información

Distribución de frecuencias y respuestas relacionadas con la Disponibilidad para recibir capacitación en el desarrollo del diseño, implantación, operación y monitoreo del Sistema de Gestión de Seguridad de la Información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016; 2016.

Alternativa	n	%
Si	3	37.50
No	5	62.50
Total	8	100.00

Fuente: Aplicación del instrumento para medir la disponibilidad de los empleados municipales encuestados respecto a la pregunta: ¿Se cuenta con personal que está en la disposición y en la capacidad de formarse en el diseño, implantación, operación y monitoreo del Sistema de Gestión de Seguridad de la Información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 28 se observa que el 62.50% de los empleados encuestados expresaron que la Municipalidad NO cuenta con personal que está en la disposición y en la capacidad de formarse en el diseño, implantación, operación y monitoreo del Sistema de Gestión de la Seguridad de la Información, mientras que el 37.50% opinan que SI cuenta con personal que está en la disposición y en la capacidad de formarse en el diseño, implantación, operación y monitoreo del Sistema de Gestión de la Seguridad de la Información.

Tabla Nº 29: Disponibilidad de asumir costos de implementación de la propuesta

Distribución de frecuencias y respuestas relacionadas con la Disponibilidad para mejorar la seguridad y asumir costos de la implementación de estas políticas; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	8	100.00
No	0	0.00
Total	8	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Existe muy buena disposición para mejorar la seguridad de la información y se puede asumir el costo de la implementación de la propuesta?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 29 se observa que el 100.00% de los empleados municipales encuestados expresaron que SI Existe muy buena disposición por parte de la Municipalidad para mejorar la Seguridad y puede asumir el costo de la implementación de estas políticas, mientras que ninguno opinó lo contrario.

.

Tabla Nº 30: Conocimiento y experiencia en aspectos de seguridad tecnológica

Distribución de frecuencias y respuestas relacionadas con el Conocimiento y experiencia en aspectos de Seguridad Tecnológica; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	6	75.00
No	2	25.00
Total	8	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿El personal de la Dirección de Informática, tiene experiencia en el área de computación y están familiarizados con los aspectos de la seguridad tecnológica?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 30 se observa que el 75.00% de los empleados municipales encuestados expresaron que el personal de la Dirección de Informática SI tiene experiencia en el área de computación y están familiarizados con los aspectos de la seguridad tecnológica, mientras que el 25.00% indican que NO tienen experiencia en el área de computación ni están familiarizados con los aspectos de la seguridad tecnológica.

Tabla Nº 31: Conocimiento sobre incidentes de seguridad

Distribución de frecuencias y respuestas relacionadas con el Conocimiento sobre incidentes de seguridad; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	8	100.00
No	0	0.00
Total	8	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿El personal de la Dirección de Informática, está consciente de los incidentes de seguridad que han ocurrido y han solicitado mejorar la seguridad física y el control de acceso a las instalaciones?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 31 se observa que el 100.00% de los empleados municipales encuestados expresaron que el personal de la Dirección de Informática SI están conscientes de los incidentes de seguridad que han ocurrido y han solicitado mejorar la seguridad física y el control de acceso a las instalaciones, mientras que ninguno opinó lo contrario.

Tabla Nº 32: Colaboración en el desarrollo del plan de seguridad de información

Distribución de frecuencias y respuestas relacionadas con la Disponibilidad de colaboración en el desarrollo del plan de seguridad; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	8	100.00
No	0	0.00
Total	8	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿El personal de la Dirección de Informática está dispuesto a colaborar en el desarrollo del plan de seguridad?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 32 se observa que el 100.00% de los empleados municipales encuestados expresaron que el personal de la Dirección de Informática SI está dispuesto a colaborar en el desarrollo del plan de seguridad, mientras que ninguno opinó lo contrario.

C. Dimensión: NECESIDAD Y DISEÑO DE LA PROPUESTA DE POLITICAS DEL PLAN DE GESTION DE SEGURIDAD DE LA INFORMACION

Tabla Nº 33: Importancia de políticas de seguridad para la plataforma tecnológica

Distribución de frecuencias y respuestas relacionadas con la Importancia de la Existencia de Políticas de seguridad en la plataforma tecnológica; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	2	100.00
No	0	0.00
Total	2	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Considera usted que deben existir políticas de seguridad para la plataforma tecnológica?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 33 se observa que el 100.00% de los dos empleados municipales encuestados expresaron que SI consideran importante que deben existir políticas de seguridad para la plataforma tecnológica, mientras que ninguno opinó lo contrario.

Tabla Nº 34: Existencia de un documentos de políticas de seguridad

Distribución de frecuencias y respuestas relacionadas con el conocimiento de la existencia de un documento que defina las políticas de seguridad de la información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	0	0.00
No	2	100.00
Total	2	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Existe un documento que defina las políticas de seguridad de información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 34 se observa que el 100.00% de los dos empleados municipales encuestados expresaron que la Municipalidad NO cuenta con un documento que defina las políticas de seguridad de información, mientras que ninguno opinó lo contrario.

Tabla Nº 35: Conocimiento de algún estándar de seguridad de información

Distribución de frecuencias y respuestas relacionadas con el conocimiento de algún estándar de seguridad de información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	0	0.00
No	2	100.00
Total	2	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Conoce usted alguno de los estándares de seguridad de información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 35 se observa que el 100.00% de los empleados municipales encuestados expresaron que NO conocen alguno de los estándares de seguridad de información, mientras que ninguno opinó lo contrario.

.

Tabla Nº 36: Responsabilidad del personal en el manejo de la información

Distribución de frecuencias y respuestas relacionadas con el conocimiento de la responsabilidad directa del personal en el manejo de la información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	1	50.00
No	1	50.00
Total	0	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿El manejo de la Información de la Organización está en manos del personal que tiene responsabilidad directa sobre ella?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 36 se observa que existe un intermedio 50.00% para la respuesta afirmativa y 50.00% para la respuesta negativa, puesto que un empleado municipal encuestado expresó que el manejo de la Información de la Organización SI está en manos del personal que tiene responsabilidad directa sobre ella en el caso del personal estable, mientras que el otro expresó que el manejo de la Información NO está en manos del personal que tiene responsabilidad directa sobre ella, puesto que a veces es manipulada por pasantes o personal contratado temporalmente sin ningún control ni pacto de confidencialidad.

Tabla Nº 37: Conocimiento de programas de sensibilización

Distribución de frecuencias y respuestas relacionadas con el conocimiento de programas dirigidos de sensibilización sobre la Seguridad de la Información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	0	0.00
No	2	100.00
Total	2	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Indique si existen programas dirigidos a sensibilizar sobre la Seguridad de la Información para todos los empleados?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 37 se observa que el 100.00% de los empleados municipales encuestados expresaron que NO existen programas dirigidos a sensibilizar sobre la Seguridad de la Información para todos los empleados, mientras que ninguno opinó lo contrario.

Tabla Nº 38: Conocimiento de la existencia de acuerdos de confidencialidad

Distribución de frecuencias y respuestas relacionadas con el Conocimiento de la existencia de un documento de acuerdo de confidencialidad de la información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	0	0.00
No	2	100.00
Total	2	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Existe un documento donde los empleados, contratista y proveedores acuerden la confidencialidad de la información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 38 se observa que el 100.00% de los empleados municipales encuestados expresaron que la Municipalidad NO cuenta con un documento donde los empleados, contratista y proveedores acuerden la confidencialidad de la información, mientras que ninguno opinó lo contrario.

Tabla Nº 39: Importancia de realización de pruebas de penetración perimetral

Distribución de frecuencias y respuestas relacionadas con la importancia de realización de pruebas de penetración perimetral; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	0	0.00
No	2	100.00
Total	2	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Indique si se han realizado pruebas de penetración perimetral?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 39 se observa que el 100.00% de los empleados municipales encuestados expresaron que NO se han realizado pruebas de penetración perimetral lo cual es muy importante para evaluar la seguridad de los sistemas accesibles desde la red externa, mientras que ninguno opinó lo contrario.

.

Tabla Nº 40: Existencia de un documento de responsabilidades de los empleados

Distribución de frecuencias y respuestas relacionadas con el Conocimiento de la existencia de un documento que defina las responsabilidades para la contratación, terminación o cambio de cargo o funciones de los empleados; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	0	0.00
No	2	100.00
Total	2	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Existe un documento donde estén definidas las responsabilidades para la contratación, terminación o cambio de cargo o funciones de los empleados, con la finalidad de proteger los recursos informáticos?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 40 se observa que el 100.00% de los empleados municipales encuestados expresaron que NO existe un documento donde estén definidas las responsabilidades para la contratación, terminación o cambio de cargo o funciones de los empleados el cual es muy importante a la hora de evaluar responsabilidades, mientras que ninguno opinó lo contrario.

Tabla Nº 41: Conocimiento de planes de contingencia en pérdida de información

Distribución de frecuencias y respuestas relacionadas con el Conocimiento de planes de contingencia en caso de pérdida de información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	1	50.00
No	1	50.00
Total	2	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿Se cuenta con planes de contingencia en caso de pérdida de información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 41 se observa que existe un intermedio 50.00% para la respuesta afirmativa y 50.00% para la respuesta negativa, puesto que un empleado municipal encuestado expresó SI se cuenta con planes de contingencia en caso de pérdida de información, mientras que el otro expresó que NO se cuenta con planes de contingencia, lo cual es muy importante ya que define la continuidad del servicio que presta la entidad.

Tabla Nº 42: Conocimiento de revisiones periódicas de riesgos internos

Distribución de frecuencias y respuestas relacionadas con el conocimiento de revisiones periódicas de riesgos internos, políticas, procedimientos y controles; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	0	0.00
No	2	100.00
Total	2	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a la pregunta: ¿el área de informática realiza la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles relacionadas a la seguridad de la información?, en la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 42 se observa que el 100.00% de los empleados municipales encuestados expresaron el área de informática NO realiza la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles relacionadas a la seguridad de la información, mientras que ninguno opinó lo contrario.

a) DIMENSIÓN 01: EVALUACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN

Tabla Nº 43: Dimensión Evaluación del estado actual de la seguridad de la información

Distribución de frecuencias y respuestas relacionadas con la dimensión 01: Evaluación del estado actual de la seguridad de la información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	110	72.37
No	42	27.63
Total	152	100.00

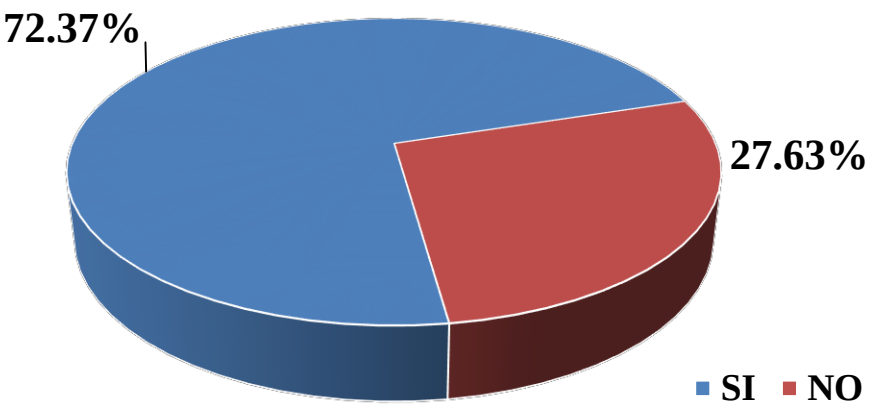
Fuente: Aplicación del instrumento para medir el estado actual de la seguridad de la información, basado en 10 preguntas aplicadas a los empleados municipales de la Municipalidad Provincial de Paita; 2016.

Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 43 se puede observar que el 72.37% de los empleados municipales encuestados opinan que SI se encuentran expuestos a riesgos y amenazas debiendo disponer de un plan de gestión de seguridad de la información, mientras el 27.63% indica que NO es necesario disponer de un plan de gestión de seguridad de la información.

Gráfico Nº 23: Resultados de la dimensión 01

Distribución porcentual de frecuencias y respuestas relacionadas con la dimensión: Evaluación del estado actual de la seguridad de la información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.



Fuente: Tabla Nº 43

b) DIMENSIÓN 02: FACTIBILIDAD TÉCNICA, ECONÓMICA Y OPERATIVA DE LA PROPUESTA

Tabla Nº 44: Dimensión de la Factibilidad Técnica, Económica y Operativa de la Propuesta

Distribución de frecuencias y respuestas relacionadas con la dimensión 02: Factibilidad Técnica, Económica y Operativa; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	8	100.00
No	0	0.00
Total	8	100.00

Fuente: Aplicación del instrumento para medir la Factibilidad Técnica, Económica y Operativa de la Propuesta, basado en 10 preguntas aplicadas a los empleados municipales de la Municipalidad Provincial de Paita; 2016.

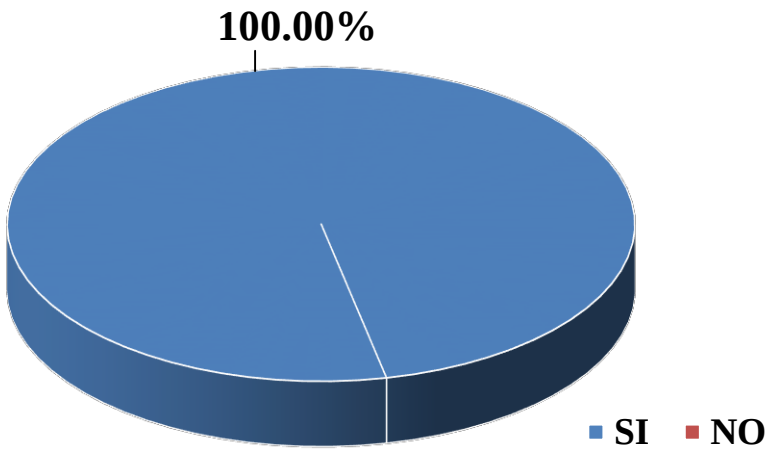
Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 44 se puede observar que el 100.00% de los empleados municipales encuestados opinan que SI existe factibilidad técnica, económica y operativa de la propuesta puesto que la norma es de carácter obligatoria en todas las entidades del estado la cual justifica la vialidad técnica. La factibilidad económica de esta propuesta también está garantizada ya que la municipalidad tiene conocimiento de los beneficios para salvaguardar la seguridad de la información por lo tanto aprueba la elaboración del diseño del plan de seguridad de la información. La factibilidad operativa está garantizada porque existe buena disposición por parte de la Municipalidad para mejorar la seguridad a fin de minimizar riesgos de pérdida de

información, así mismo existe buena disposición por parte del personal de la Subgerencia de Sistemas e Informática para recibir capacitación en aspectos de seguridad de la información.

Gráfico Nº 24: Resultados de la dimensión 02

Distribución porcentual de frecuencias y respuestas relacionadas con la dimensión: Factibilidad Técnica, Económica y Operativa; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.



Fuente: Tabla Nº 44

c) DIMENSIÓN 03: NECESIDAD Y DISEÑO DE LA PROPUESTA DE POLÍTICAS DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Tabla Nº 45: Dimensión de la Necesidad y diseño de la propuesta de políticas del plan de gestión de seguridad de la información

Distribución de frecuencias y respuestas relacionadas con la dimensión 03: Necesidad y diseño de la propuesta de políticas del plan de gestión de seguridad de la información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

Alternativa	n	%
Si	0	0.00
No	2	100.00
Total	2	100.00

Fuente: Aplicación del instrumento para evaluar la información gerencial respecto a la necesidad y diseño de la propuesta de políticas del plan de gestión de seguridad de la información, basado en 10 preguntas aplicadas a dos empleados municipales de la Municipalidad Provincial de Paita; 2016.

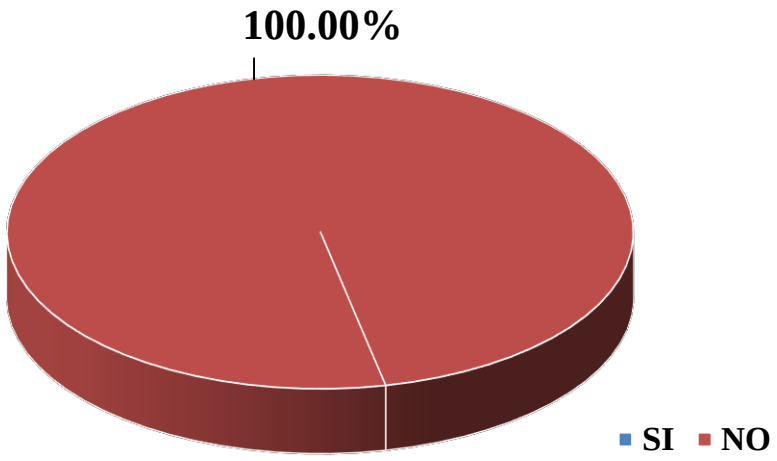
Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 45 se puede observar que el 100.00% de los empleados municipales encuestados opinaron que NO existen controles pertinentes en cuanto a la seguridad de la información, por lo tanto queda demostrado que es necesario la elaboración de una propuesta de plan de gestión de seguridad de la información, ya que ella permitirá brindar un esquema de seguridad más sólido y eficiente en el manejo de los sistemas de información, lo cual indica

que es necesaria la elaboración del diseño del plan de seguridad de la información.

Gráfico Nº 25: Resultados de la dimensión 03

Distribución porcentual de frecuencias y respuestas relacionadas con la dimensión: Necesidad y diseño de la propuesta de políticas del plan de gestión de seguridad de la información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.



Fuente: Tabla Nº 45

Tabla Nº 46: Resumen general por dimensiones

Distribución de frecuencias y respuestas relacionadas con las tres dimensiones definidas para las fases de estudio de evaluación de la seguridad de la información de los empleados municipales; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.

DIMENSIONES	SI		NO		TOTAL	
	n	%	n	%	n	%
Evaluación del estado actual de la seguridad de la información	110	72.37	42	27.63	152	100.00
Factibilidad técnica, Económica y operativa de la propuesta	8	100.00	0	0.00	8	100.00
Necesidad y diseño de la Propuesta de Políticas del Plan de Gestión de Seguridad de la Información	0	0.00	2	100.00	2	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los empleados municipales encuestados respecto a las fases de estudio de evaluación de la seguridad de la información de las tres dimensiones definidas para la investigación; en la Municipalidad Provincial de Paita; 2016.

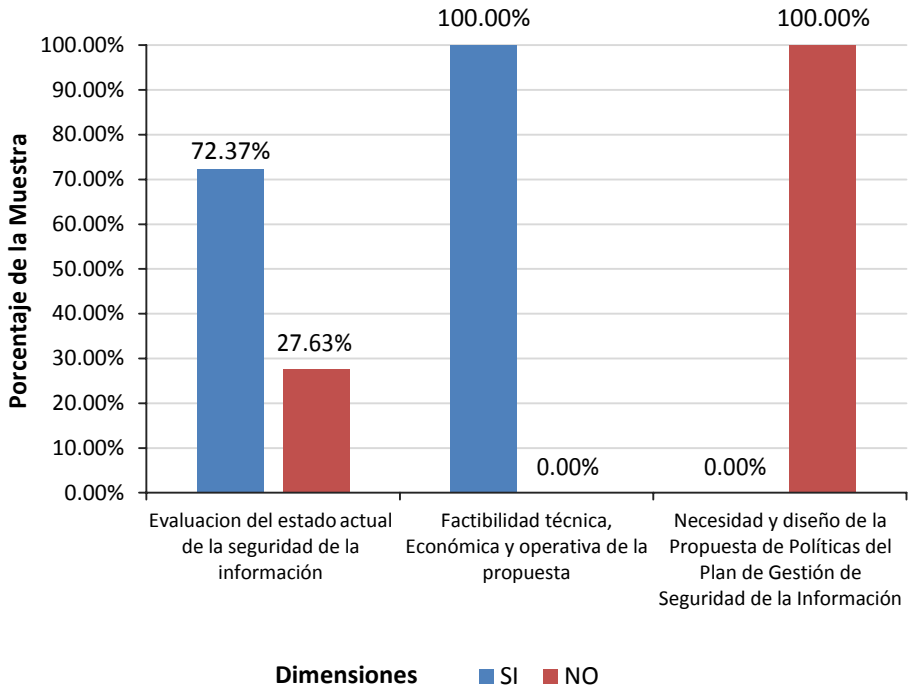
Aplicado por: De La Cruz, R.; 2016.

En la Tabla Nº 46 se puede observar que en las tres dimensiones el mayor porcentaje de los empleados municipales encuestados opinan que SI se encuentran expuestos a riesgos y amenazas debiendo disponer de un plan de gestión de seguridad de la información que permita minimizar el riesgo de pérdida de información, también se comprobó que existe factibilidad técnica,

económica y operativa para realizar el diseño e implantar la propuesta, así mismo los directivos que manejan información gerencial de recursos humanos e informática encuestados opinaron que NO existen controles pertinentes en cuanto a la seguridad de la información, por lo tanto queda demostrado que es necesario la elaboración de una propuesta de plan de gestión de seguridad de la información.

Gráfico Nº 26: Resumen general de las dimensiones

Distribución porcentual de las frecuencias y respuestas relacionadas con las tres dimensiones definidas respecto a las fases de estudio de evaluación de la seguridad de la información; para la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016.



Fuente: Tabla Nº 46

4.2. Análisis de resultados

El objetivo general de la presente investigación ha sido: Realizar el diseño de la Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016 de tal forma que minimice el riesgo de pérdida de información; en ese sentido y para poder cumplir con este objetivo fue necesario realizar una evaluación de la situación actual a fin de que este diseño identifique claramente los requisitos que permita resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma a través de una propuesta de mejora seria y técnica.

Para realizar esta sección de análisis de resultados se diseñó un cuestionario agrupado en 03 dimensiones y luego de los resultados obtenidos e interpretados en la sección anterior, se realiza el siguiente análisis:

1. En lo que respecta a la dimensión: Evaluación del estado actual de la seguridad de la información, la Tabla Nº 43 nos muestra los resultados donde se puede observar que el 72.37% de los empleados municipales encuestados expresaron que SI se encuentran expuestos a riesgos y amenazas en seguridad de información, este resultado es similar al resultado que ha obtenido López (12), en su investigación Anexo "D". Resúmenes de casos que en resumen obtuvo como resultado para una dimensión similar a la presente, un resultado de 72.50%. Esta coincidencia en los resultados se justifica porque en ambas instituciones públicas se evidencia que la mayoría de los empleados municipales desconocen el tema de seguridad de la información siendo necesario que exista un programa de sensibilización, no disponen de un plan de gestión de seguridad de la información, además no cuentan con el análisis de riesgos relativos a los sistemas de información lo cual constituye una pieza importante para la sección de controles a aplicar e incluso la base para elaborar el Plan de Seguridad de la Información, no cuentan con el análisis de vulnerabilidad, lo que refleja, evidentemente, el estado crítico actual de la

seguridad de la información en donde no han realizado una serie de medidas que permita disminuir el impacto de amenazas y riesgos de pérdida de información en la entidad.

2. En lo que respecta a la dimensión: Factibilidad técnica, económica y operativa de la propuesta, la Tabla Nº 44 nos muestra los resultados donde se puede observar que el 100.00% de los empleados municipales encuestados expresaron que SI existe factibilidad técnica, económica y operativa de la propuesta, este resultado es similar al resultado que ha obtenido López (12), en su investigación donde obtuvo como resultado para una dimensión similar a la presente, un resultado de 100.00% de aprobación. Esta coincidencia en los resultados se justifica porque en ambas instituciones públicas se evidencia que la norma aprobada es de carácter obligatoria en todas las entidades del estado la cual justifica la vialidad técnica. La factibilidad económica de esta propuesta también está garantizada ya que la Municipalidad tiene conocimiento de los beneficios para salvaguardar la seguridad de la información por lo tanto aprueba la elaboración del diseño del plan de seguridad de la información. La factibilidad operativa está garantizada porque existe buena disposición por parte de la Municipalidad para mejorar la seguridad a fin de minimizar riesgos de pérdida de información, así mismo existe buena disposición por parte del personal de la Subgerencia de Sistemas e Informática para recibir capacitación en aspectos de seguridad de la información.

3. En lo que respecta a la dimensión: Necesidad y diseño de la propuesta de políticas del plan de gestión de seguridad de la información, la Tabla Nº 45 nos muestra los resultados donde se puede observar que el 100.00% de los empleados municipales encuestados expresaron que NO existen controles pertinentes en cuanto a la seguridad de la información, este resultado es similar al resultado que ha obtenido López (12), en su investigación donde obtuvo como resultado para una dimensión similar a la presente, un resultado de 100.00%. Esta coincidencia en los resultados se justifica porque en ambas instituciones públicas se evidencia que deben existir políticas de seguridad en

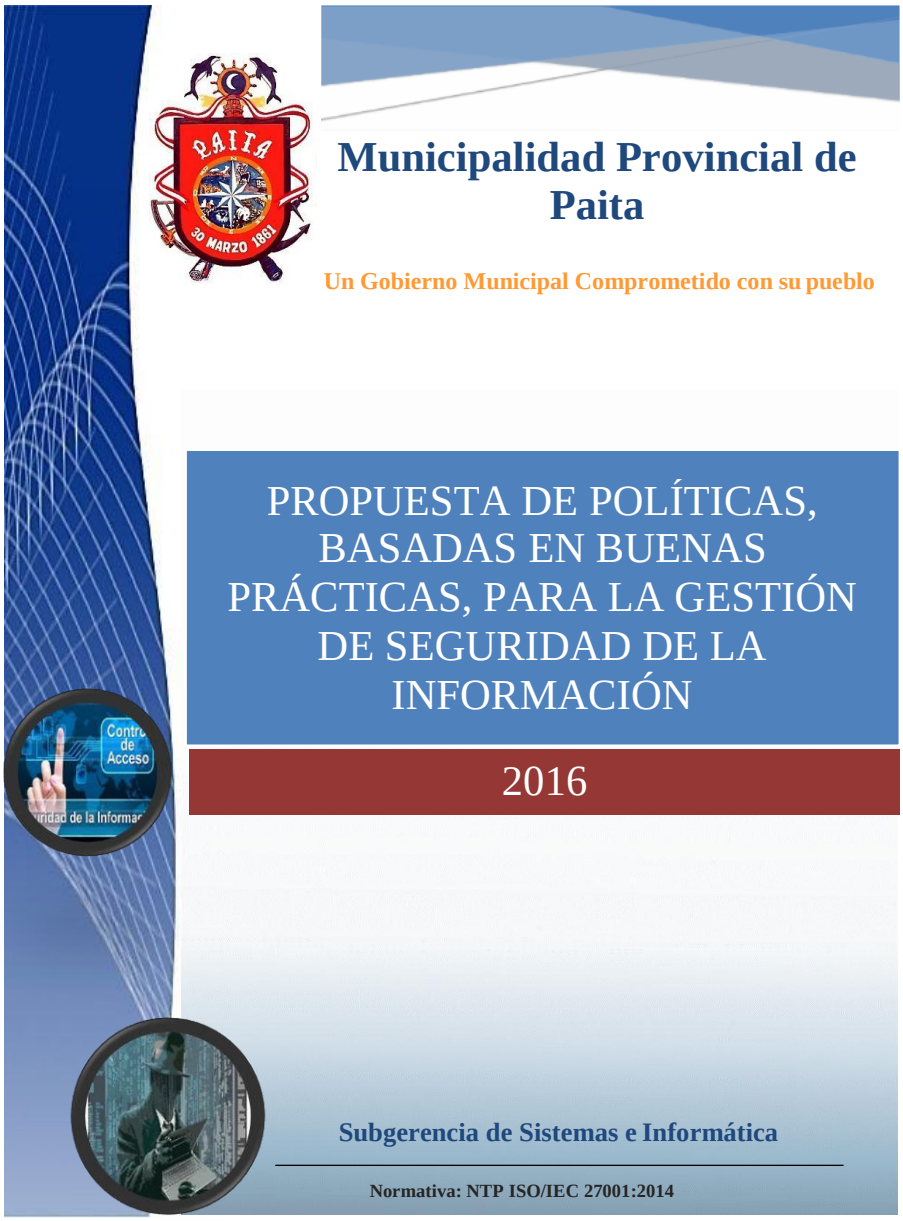
la plataforma tecnológica de la municipalidad las cuales deben estar documentadas y deben ser de conocimiento de todos los empleados, no se ha establecido un documento donde estén definidas las responsabilidades para la contratación, terminación o rotación de personal ni existe un acuerdo formal en donde los empleados, contratistas y proveedores acuerden confidencialidad de la información, lo cual es muy importante a la hora de evaluar responsabilidades, no se ha realizado pruebas de penetración perimetral que evalúe la seguridad de los sistemas accesibles desde internet, lo que refleja, evidentemente, la necesidad de contar con un diseño de gestión de seguridad de la información, ya que ella permitirá brindar un esquema de seguridad más sólido y eficiente en el manejo de los sistemas de información.

4.3. Diseño de Propuesta de Seguridad de la Información

Para el diseño de la propuesta se ha tomado como referencia el Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional de la República de Argentina (60).

4.3.1. Propuesta de mejora

Gráfico Nº 27: Modelo de Carátula



Fuente: Elaboración propia.

Tabla Nº 47: Encabezado para todas las páginas

	MUNICIPALIDAD PROVINCIAL DE PAITA **Gerencia Municipal – Subgerencia de Sistemas e Informática**	**Código: SGSI-001**
	Sistema de Gestión de Seguridad de la Información	**Fecha: xx /xx /xx** **Versión: 0.1**
	PROPUESTA DE POLÍTICAS, BASADAS EN BUENAS PRÁCTICAS, PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN **Directiva N° xxxxx -2016-SSI/MPP**	**Página x de xx**

Fuente: Modelo de Plantilla aprobado por la ONGEI (61).

Tabla Nº 48: Cuadro de Control Documental

Código	**:**	SGSI-001
Versión	**:**	0.1
Fecha aprobación	**:**	xx/xx/xxxx
Documento aprobación	**:**	
Fecha Inicio vigencia	**:**	
Resumen	**:**	Propuesta de Políticas, Basadas en Buenas Prácticas, para la Gestión de Seguridad de la Información.
Área ejecutora	**:**	Comité de Seguridad de la Información
Áreas involucradas	**:**	Todas las áreas
Páginas	**:**	xxxx

Fuente: Modelo de Plantilla aprobado por la ONGEI (61).

Tabla Nº 49: Cuadro de Control de Versiones

Código	**:**	SGSI-001
Versión	**:**	0.1
Fecha de la versión	**:**	xx/xx/xxxx
Creado por	**:**	SUBGERENCIA DE SISTEMAS E INFORMÁTICA
Aprobado por	**:**	GERENCIA MUNICIPAL
Nombre del archivo	**:**	SGSI-001 – Plan del Proyecto.docx
Nivel de confidencialidad	**:**	Baja

Fuente: Modelo de Plantilla aprobado por la ONGEI (61).

Tabla Nº 50: Cuadro de Historial de Revisiones

Fecha	Versión	Modificado/Creado por	Descripción de la modificación

Fuente: Modelo de Plantilla aprobado por la ONGEI (61).

Tabla Nº 51: Cuadro de Aprobación

Fecha	Nombre	Cargo	Sello y Firma

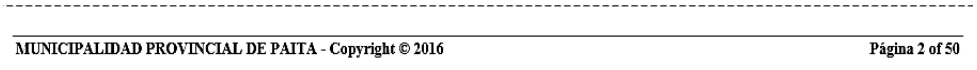
Fuente: Modelo de Plantilla aprobado por la ONGEI (61).

Tabla Nº 52: Cuadro de Mejora Continua

Fecha	Revisor/Auditor	Resumen Observaciones

Fuente: Modelo de Plantilla aprobado por la ONGEI (61).

Gráfico Nº 28: Pie de Página para todo el documento



Fuente: Modelo de Plantilla aprobado por la ONGEI (61).

ÍNDICE DE CONTENIDO

a. Objetivo… 149
b. Finalidad..... 149
c. Base Legal 149
d. Alcance..... 150
e. Vigencia y Actualización 150
f. Normas Generales 151
g. Política General de Seguridad de la Información..... 152
h. Lineamientos Específicos..... 152
1. Política de Seguridad de la Información.....152
1.1. Generalidades… 152
1.2. Alcance..... 152
1.3. Responsabilidad de su cumplimiento 153
1.4. Aspectos Generales 156
1.5. Sanciones Previstas por incumplimiento… 158
2. Organización de la seguridad de la información… 159
2.1. Generalidades… 159
2.2. Alcance..... 160
2.3. Responsabilidad… 160
2.4. Conformación de la Infraestructura de la Información.....163
2.4.1. Comité de Seguridad de la Información….....163
2.4.2. Responsabilidades en Materia de Seguridad de la Información 166
2.5. Asesoramiento Especializado en Materia de Seguridad de la Información… 171
2.6. Autorización para Instalaciones de Procesamiento de Información..... 171
2.7. Seguridad Frente al Acceso de Terceros… 172
2.8. Cooperación entre Organismos….....172
3. Seguridad de los recursos humanos.....172
3.1. Generalidades… 172

3.2. Alcance..... 173
3.3. Responsabilidad 173
3.4. Seguridad en la Definición de Puestos de Trabajo, Cargos o Servicios y la Asignación de Recursos 175
3.4.1.Incorporación de la Seguridad en los Puestos de Trabajo 175
3.4.2. Control y Política del Personal.....175
3.4.3. Compromiso de Confidencialidad 175
3.4.4. Términos y Condiciones de Empleo….....176
3.5. Capacitación del Usuario… 176
3.5.1. Formación y Capacitación en Materia de Seguridad..176
3.6. Respuesta a Incidentes y Anomalías en Materia de Seguridad 178
3.6.1. Comunicación de Incidentes Relativos a Seguridad...178
3.6.2. Comunicación de Debilidades Materia de Seguridad.179
3.6.3. Comunicación de Anomalías del Software.....179
3.6.4. Aprendiendo de los Incidentes..... 179
3.6.5. Procesos Disciplinarios 180
4. Gestión de los activos..... 180
4.1. Generalidades… 180
4.2. Alcance..... 181
4.3. Responsabilidad 182
4.4. Clasificación y control de Activos.....182
4.4.1. Inventario de activos.....182
4.4.2. Clasificación de la información….....183
4.4.3. Rotulado de la Información.....184
5. Criptografía 185
5.1. Generalidades..... 185
5.2. Alcance..... 185
5.3. Responsabilidad 185
5.4. Controles Criptográficos 186
5.4.1. Utilización de Controles Criptográficos….....186

5.4.2. Cifrado 187
5.4.3. Firma Digital 187
5.4.4. Servicios de No Repudio.....188
5.4.5. Administración de Claves 188
5.4.6. Normas, Procedimientos y Métodos.....189
6. Control de accesos.....191
6.1. Generalidades 191
6.2 Alcance..... 192
6.3 Responsabilidad 192
6.4 Control de Accesos.....195
6.4.1. Requerimientos para el Control de Acceso 195
6.4.2. Administración de Accesos de Usuarios….....197
6.4.3. Responsabilidades del Usuario.....202
6.4.4. Control de Acceso a la Red.....204
6.4.5. Control de Acceso al Sistema Operativo….....211
6.4.6. Control de Acceso a las Aplicaciones….....218
6.4.7. Computación Móvil y Teletrabajo….....220
7. Seguridad física y ambiental.....223
7.1. Generalidades… 223
7.2. Alcance..... 225
7.3. Responsabilidad 225
7.4. Política de Seguridad Física y Ambiental.....226
7.4.1. Perímetro de Seguridad Física.....226
7.4.2. Controles de Acceso Físico 228
7.4.3. Protección de Oficinas, Recintos e Instalaciones…..229
7.4.4. Desarrollo de Tareas en Áreas Protegidas.....231
7.4.5. Aislamiento de las Áreas de Almacenamiento….....232
7.4.6. Ubicación y Protección del Equipamiento y Copias de Seguridad 232
7.4.7. Suministros de Energía.....234
7.4.8. Seguridad del Cableado… 235
7.4.9. Mantenimiento de Equipos… 236

7.4.10. Seguridad de los Equipos fuera de las Instalaciones.237
7.4.11. Desafectación o Reutilización de los Equipos…….237
7.4.12. Políticas de Escritorios y Pantallas Limpias….....237
7.4.13. Retiro de los Bienes.....239
8. Seguridad de las operaciones.....239
8.1. Generalidades…..... 239
8.2. Alcance..... 239
8.3. Responsabilidad… 240
8.4. Procedimientos y Responsabilidades Operativas….....240
8.4.1. Documentación de los Procedimientos Operativos...240
8.4.2. Control de Cambios en las Operaciones….....241
8.4.3. Procedimientos de Manejo de Incidentes….....242
8.4.4. Separación de Funciones…..... 244
8.4.5. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas..... 245
8.4.6. Gestión de Instalaciones Externas….....246
9. Seguridad de las comunicaciones.....246
9.1. Generalidades…..... 246
9.2. Alcance..... 247
9.3. Responsabilidad… 247
9.4. Política de Comunicaciones….....249
9.4.1. Planificación y Aprobación de Sistemas… 249
9.4.2. Protección contra Software Malicioso… 251
9.4.3. Mantenimiento… 252
9.4.4. Administración de la Red…..... 254
9.4.5. Administración y Seguridad de los Medios de Almacenamiento..... 255
9.4.6. Intercambios de Información y Software..... 257
10. Adquisición, desarrollo y mantenimiento de sistemas de información 265
10.1. Generalidades..... 265
10.2. Alcance..... 266

10.3. Responsabilidad 266
10.4. Política de Adquisición, Desarrollo y Mantenimiento de Software 268
10.4.1. Requerimientos de Seguridad de los Sistemas..... 268
10.4.2. Seguridad en los Sistemas de Aplicación.....269
10.4.3. Seguridad de los Archivos del Sistema..... 272
10.4.4. Seguridad de los Procesos de Desarrollo y Soporte..276
11. Relaciones con los Proveedores.....282
11.1. Generalidades… 282
11.2. Alcance..... 283
11.3. Responsabilidad… 283
11.4. Seguridad Frente al Acceso de Terceros… 284
11.4.1. Identificación de Riesgos del Acceso de Terceras Partes..... 284
11.4.2. Requerimientos de Seguridad en Contratos o Convenios 285
11.4.3. Requerimientos de Seguridad en Contratos de Tercerización 287
11.4.4. Desarrollo Externo de Software 288
11.4.5. Términos y Condiciones de contrato.....289
12. Gestión de incidentes de seguridad de la información..... 289
12.1. Generalidades… 289
12.2. Alcance..... 290
12.3. Responsabilidad… 290
12.4. Monitoreo del Acceso y Uso de los Sistemas.....291
12.4.1. Registro de Eventos 291
12.4.2. Monitoreo del Uso de los Sistemas.....291
12.4.3. Sincronización de Relojes… 294
13. Gestión de la continuidad del negocio….....295
13.1. Generalidades… 295
13.2 Alcance..... 295
13.3. Política de Gestión de Continuidad..... 295

13.3.1. Administración de la Continuidad del Organismo..295
13.3.2. Continuidad de las Actividades y Análisis de los Impactos 296
13.3.3. Elaboración e Implementación del Plan de Seguridad y Continuidad de Tecnología de la Información….298
13.3.4. Marco para la Planificación de la Continuidad de las Actividades de la entidad.....299
13.3.5. Ensayo, Mantenimiento y Reevaluación del Plan de Seguridad y Continuidad de Tecnología de la Información 301
14. Cumplimiento..... 303
14.1. Generalidades..... 303
14.2. Alcance..... 304
14.3. Responsabilidad… 304
14.4. Cumplimiento de Requisitos Legales.....305
14.4.1. Identificación de la Legislación Aplicable 305
14.4.2. Derechos de Propiedad Intelectual.....305
14.4.3. Derecho de Propiedad Intelectual del Software.....306
14.4.4. Protección de los Registros de la Municipalidad Provincial de Paita..... 307
14.4.5. Protección de Datos y Privacidad de la Información Personal 312
14.4.6. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información..... 314
14.4.7. Regulación de Control para Uso de Criptografía…..315
14.4.8. Recolección de Evidencia.....315
i. Responsabilidades..... 316
j. Disposiciones Complementarias… 316
k. Definiciones… 317
l. Anexos… 318
m. Conformidad 318

a. Objetivo

Dar a la Municipalidad Provincial de Paita un marco de gestión para establecer objetivos, sentido de dirección general y principios para la acción relacionada a la seguridad de la información, dentro del contexto de la modernización de la gestión municipal y la normatividad vigente.

b. Finalidad

Establecer la línea base para el desarrollo e implementación de procedimientos y actividades de gestión que permitan salvaguardar la seguridad de la información y minimizar los efectos que provoquen amenazas o eventos adversos a la continuidad del funcionamiento de la Municipalidad Provincial de Paita.

c. Base Legal

- Constitución Política del Perú.

- Ley N° 27972 "Ley Orgánica de Municipalidades".

- Ley N° 27444 "Ley del Procedimiento Administrativo General".

- Resolución Jefatural N° 340-94-INEI, que aprueba la Directiva N° 015-94-INEI/SJI.

- Resolución de Contraloría General Nº 320-2006-CG "Normas de Control Interno".

- Resolución Ministerial Nº 246-2007-PCM que aprueba el Uso Obligatorio de la "Norma Técnica Peruana NTP-ISO/IEC 17799:2007".

- Resolución de Contraloría General Nº 458-2008-CG “Guía para la Implementación del Sistema de Control Interno de las entidades del Estado”.

- Resolución Ministerial Nº 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”.

d. Alcance

Esta Política aplica a los activos de información de propiedad de la Municipalidad Provincial de Paita, debiendo ser de conocimiento y cumplimiento obligatorio para todos los empleados (alcalde, gerentes, funcionarios y colaboradores), proveedores, contratistas, consultores y personal temporal de la Municipalidad Provincial de Paita, que tengan acceso a recursos de información de propiedad de la institución.

e. Vigencia y Actualización

La presente política será aprobada por Decreto de Alcaldía, y deberá ser revisada y actualizada, en caso corresponda, periódicamente por las instancias que correspondan, a fin de adecuarla a las nuevas exigencias normativas y cambios importantes en la estructura de la organización o en la base legal y normativa sobre la seguridad de la información, requiriendo en cada actualización el mismo nivel de aprobación.

Esta directiva entrará en vigencia a partir del día hábil siguiente al de su aprobación mediante Decreto de Alcaldía.

f. Normas Generales

1. La información y los recursos de procesamiento de información son de vital importancia como activos en la Municipalidad Provincial de Paita, y se deben tomar las medidas para protegerlos, bajo los principios de ética y la moral.

2. En el desarrollo de las actividades se deben tomar las medidas pertinentes que garanticen la confidencialidad, integridad y disponibilidad de los activos de información, viabilizando la competitividad, integridad y transparencia de la institución.

3. Los incidentes relacionados con la seguridad de la información deben ser reportados para su respectiva investigación, respuesta oportuna y recuperación efectiva.

4. Se debe velar por el cumplimiento de los requerimientos dispuestos en las disposiciones legales y contractuales aplicables a la Seguridad de la Información, que comprenden a la institución.

5. Periódicamente se deben identificar, evaluar, tratar y monitorear los riesgos de seguridad de la información relevantes a la institución.

6. El personal debe asumir una responsabilidad individual respecto a los criterios de confidencialidad, integridad y disponibilidad de los sistemas y tecnologías así como del uso de información privilegiada. Lo que refleja su compromiso hacia los clientes externos e internos de la Municipalidad Provincial de Paita.

g. Política General de Seguridad de la Información

La Municipalidad Provincial de Paita, entiende que se encuentra expuesta a riesgos de seguridad de la información, por ello ha decidido gestionar los mismos, considerando estándares internacionales y la normativa peruana vigente sobre la materia, considerando como estrategia orientar su cultura organizacional a la cultura de mejora continua.

h. Lineamientos Específicos.

1. Política de Seguridad de la Información

1.1. Generalidades

Esta política define los principales lineamientos para gestionar de forma adecuada la seguridad de la información, debiendo ser revisada y actualizada de forma anual o cuando surjan nuevas exigencias regulatorias en materia de seguridad de la información o cuando surjan cambios significativos en el ambiente interno u organizacional de la Municipalidad Provincial de Paita.

1.2. Alcance

Esta política se aplica a toda la Municipalidad Provincial de Paita, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

1.3. Responsabilidad de su cumplimiento

Todos los funcionarios, empleados y obreros, titulares de unidades orgánicas, autoridades políticas o personal técnico y sea cual fuere su nivel jerárquico son responsables de la implementación de esta política de seguridad de la información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha política, siendo los siguientes:

- El Despacho de Alcaldía de la Municipalidad Provincial de Paita, tendrá la función de aprobar la política de seguridad y sus futuras modificaciones.

- El Comité de Gestión de Seguridad de la Información de la Municipalidad Provincial de Paita, procederá a Planificar y coordinar el funcionamiento del sistema de seguridad de la información, además podrá proponer otras acciones o proyectos que sean necesarias para alcanzar los fines y objetivos del sistema de seguridad de la información de la Municipalidad Provincial de Paita.

- El Secretario Técnico del Comité de Gestión de Seguridad de la Información, será el responsable de convocar periódicamente las reuniones tanto ordinarias como extraordinarias, elaborar las actas, informar a los integrantes del comité y presentar los informes a quien lo solicite.

- El Oficial de Seguridad de la Información, será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente política, además será el responsable de practicar auditorías periódicas

sobre los sistemas y actividades vinculadas con la tecnología de información.

- El Especialista de Seguridad de la Información, será el responsable de la coordinación de Seguridad de la Información que apoya el desarrollo de actividades de planeación, operación, mantenimiento y evaluación del modelo de seguridad de la información, así como de los sistemas y servicios informáticos y de telecomunicaciones, diseño y desarrollo de proyectos en los temas relacionados con tecnología y seguridad de la información.

- El Responsable del Área Informática, cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología (clasificar la información de acuerdo con el grado de confiabilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia).

- El Responsable del Área de Administración, cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

- El Responsable del Área de Planeamiento y Presupuesto, cumplirá la función de proporcionar apoyo técnico en materia de planificación estratégica, presupuesto e inversiones, así mismo gestionará la aprobación planes de continuidad de operaciones para que puedan ser atendidos los requerimientos de seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas según el análisis de riesgo determinado para tal fin.

- El Responsable del Área Legal, verificará el cumplimiento de la presente política en la gestión de todos los contratos, acuerdos u otra documentación de la Municipalidad de Paita con sus empleados y con terceros. Asimismo, asesorará en materia legal a la Municipalidad Provincial de Paita, en lo que se refiere a la seguridad de la información.

- El Responsable del Área de Recursos Humanos, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Así mismo, tendrá a su cargo la notificación de la presente política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad, entre otros.

- Los usuarios de la información y de los sistemas son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información vigente.

1.4. Aspectos Generales

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la seguridad de la información, que incluyen los siguientes tópicos:

- **Organización de la Seguridad**

  Orientado a administrar la seguridad de la información dentro de la entidad y establecer un marco gerencial para controlar su implementación.

- **Seguridad de Recursos Humanos**

  Orientado a reducir los riesgos de error humano, comisión de ilícitos contra la entidad o uso inadecuado de instalaciones.

- **Gestión de Activos**

  Destinado a mantener una adecuada protección de los activos de la Municipalidad Provincial de Paita.

- **Control de Accesos**

  Orientado a controlar el acceso lógico a la información.

- **Criptografía**

  Dirigido a establecer procedimientos que exponga como se ha de llevar a cabo la generación de las claves y certificados, como se tiene que almacenar, actualizar, distribuir y por consiguiente revocar.

- **Seguridad Física y Ambiental**

  Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la entidad.

- **Seguridad de las Operaciones y Comunicaciones**

  Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

- **Adquisición, Desarrollo y Mantenimiento de Sistemas**

  Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su Adquisición, desarrollo y/o implementación y durante su mantenimiento.

- **Relaciones con Proveedores**

  Destinado a garantizar y asegurar protección a los activos de la organización que son accesibles por los proveedores. Así mismo; establecer una relación sólida con los proveedores a fin de adoptar un enfoque flexible de colaboración Cliente-Proveedor.

- **Gestión de Incidentes de Seguridad de la Información**

  Orientado a asegurar que los eventos y debilidades en seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva a tiempo.

- **Aspectos de la Seguridad de la Información dentro de la Continuidad del Negocio**

  Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

- **Cumplimiento**

  Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad en esta Política, la Municipalidad Provincial de Paita identificará los recursos necesarios e indicará formalmente las partidas presupuestarias correspondientes. No necesariamente implicará la asignación de partidas presupuestarias adicionales. El Comité de Gestión de la Seguridad de la Información revisará anualmente la presente Política, a efectos de mantenerla actualizada. Así mismo efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

1.5. Sanciones Previstas por incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

2. Organización de la seguridad de la información

2.1. Generalidades

Se debe conformar un equipo de trabajo de nivel gerencial denominado Comité de Seguridad de la Información (CSI) para iniciar, implementar y controlar la implementación de un Sistema de Gestión de Seguridad de la Información, así como la distribución de funciones y responsabilidades en forma adecuada.

Se debe designar a un funcionario con el perfil técnico adecuado para garantizar el cumplimiento de la Política de Seguridad de la Información el cual será denominado Oficial de Seguridad de la Información y reportara directamente al Comité de Gestión de Seguridad de la Información.

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la Municipalidad Provincial de Paita.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en seguridad de la información. Por otro lado debe tenerse en cuenta que ciertas actividades pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos

casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

2.2. Alcance

Esta política se aplica a todos los recursos de la Municipalidad Provincial de Paita y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

2.3. Responsabilidad

- El Despacho de Alcaldía de la Municipalidad Provincial de Paita, tendrá la función de aprobar la política de seguridad y sus futuras modificaciones en coordinación con la asesoría del Comité de Gestión de Seguridad de la Información, mediante Decreto de Alcaldía.

- El Comité de Gestión de Seguridad de la Información de la Municipalidad Provincial de Paita, tendrá a cargo el mantenimiento y la presentación de la presente política para su aprobación ante la máxima autoridad de la entidad, el seguimiento de acuerdo a las incidencias propias de cada área de las actividades relativas a la seguridad de la información y la proposición de asignación de funciones.

- El Secretario Técnico del Comité de Gestión de Seguridad de la Información, será el profesional responsable de convocar periódicamente las reuniones tanto ordinarias como

extraordinarias, elaborar las actas, informar a los integrantes del comité y presentar los informes a quien lo solicite.

- El Oficial de Seguridad de la Información, será el responsable de coordinar las acciones del Comité de Seguridad de la Información, de impulsar la implementación y el cumplimiento de la presente Política. Además será el responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta política y por las normas, procedimientos y prácticas que de ella surjan.

- El Especialista de Seguridad de la Información, será el funcionario responsable de la coordinación de Seguridad de la Información que apoya el desarrollo de actividades de planeación, operación, mantenimiento y evaluación del modelo de seguridad de la información, así como de los sistemas y servicios informáticos y de telecomunicaciones, diseño y desarrollo de proyectos en los temas relacionados con tecnología y seguridad de la información.

- El Responsable del Área Informática, cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología. Así mismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la entidad y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

- El Responsable del Área de Administración, cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

- El Responsable del Área de Planeamiento y Presupuesto, cumplirá la función de proporcionar apoyo técnico en materia de planificación estratégica, presupuesto e inversiones, así mismo gestionará la aprobación planes de continuidad de operaciones para que puedan ser atendidos los requerimientos de seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas según el análisis de riesgo determinado para tal fin.

- El Responsable del Área Legal, asesorará en materia legal a la Municipalidad Provincial de Paita referente a la seguridad de la información, verificará el cumplimiento de la presente política en la gestión de todos los contratos, acuerdos u otra documentación de la Municipalidad de Paita con sus empleados y con terceros. Asimismo, notificará a los proveedores sobre las modificaciones que se efectúen a la política de seguridad de la información.

- El Responsable del Área de Recursos Humanos, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente política a todo

el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad, entre otros.

- Los usuarios de la información y de los sistemas son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información vigente.

2.4. Conformación de la Infraestructura de la Información

2.4.1. Comité de Seguridad de la Información

La Municipalidad Provincial de Paita, de acuerdo a sus funciones crea el Comité de Seguridad de la Información, como instancia responsable de coordinar las acciones e iniciativas para la gestión del sistema de seguridad de la información. El mismo que contará con una Secretaría Técnica, quien cumplirá la función de llevar la custodia de archivos y actas y suministrar información a los miembros del Comité sobre los asuntos de su competencia relacionados con la implementación de la presente Política, el cual estará integrado por:

El Alcalde o su representante	Presidente
Profesional del área de sistemas	Secretario Técnico
Oficial de la seguridad de la información	Coordinador Gral.
Especialista de seguridad de la información	Apoyo
Gerente de Administración y Finanzas	Miembro
Gerente de Planeamiento y Presupuesto	Miembro
Gerente de Asesoría Jurídica	Miembro
Subgerente de Sistemas e Informática	Miembro
Subgerente de Recursos Humanos	Miembro

Funcionalidad del Comité de Seguridad de la Información

- La designación de los Integrantes del Comité de Gestión de Seguridad de la información de la Municipalidad Provincial de Paita tendrán un periodo de un año para ejercer sus funciones, pudiendo ser rectificados en el cargo previa resolución de alcaldía.

- Cada miembro titular del Comité de Gestión de Seguridad de la información de la Municipalidad Provincial de Paita, designara un representante de su área que actuará como miembro suplente solamente en ausencia temporal del miembro titular y debidamente acreditado, quien tendrá que asistir a las sesiones del Comité, con las mismas facultades, obligaciones y responsabilidades del Titular.

- Dicha designación será comunicada por los miembros titulares al Presidente del Comité en la primera sesión del Comité de Gestión de Seguridad de la información de la Municipalidad Provincial de Paita, quedando registrado en acta de sesión.

- El Comité se reunirá con carácter ordinario una vez cada bimestre y con carácter extraordinario, cuando lo decida su presidente o cuando surjan nuevas necesidades o incidentes de seguridad de la información.

- El Secretario del Comité realizará las actas de cada una de las reuniones, convocará la firma del acta y realizará el respectivo archivo del documento.

- A las sesiones del Comité podrán asistir en calidad de invitados las personas, que en cada caso, se estime pertinente.

- El quórum mínimo del Comité es de 06 miembros.

- Las decisiones no unánimes, se someterán a votación y se declara ganador la opción que obtenga al menos la mitad más uno del quórum mínimo del Comité.

Funciones adicionales

- Planificar y coordinar el funcionamiento del sistema de seguridad de la información.

- Definir la estructura organizativa y la estrategia de seguridad de la información, coordinada por la Subgerencia de Sistemas e informática.

- Revisar y proponer políticas normas y estándares para la regularización del sistema de seguridad de la información.

- Proponer la creación e implementación de la unidad orgánica responsable de la implementación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

- Coordinar los proyectos de mejora o cambio respecto a la seguridad de la información en aplicaciones o sistemas de la Municipalidad Provincial de Paita.

- Verificar y supervisar el cumplimiento de la de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.

- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

- Promover la difusión y apoyo a la seguridad de la información.

- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información frente a interrupciones imprevistas.

- Mantener relación técnico-normativo con la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI de la Presidencia del Concejo de Ministros, ente rector del Sistema Nacional de Informática.

- Proponer las funciones del Oficial de Seguridad de la Información.

- Otras que sean necesarias para alcanzar los fines y objetivos del sistema de seguridad de la información de la Municipalidad Provincial de Paita.

2.4.2. Responsabilidades en Materia de Seguridad de la Información

1. Oficial de Seguridad de la Información

Mediante Resolución de Alcaldía se asignarán las funciones al empleado designado Oficial de Seguridad de

la Información quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la Municipalidad Provincial de Paita, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente política.

Funciones adicionales:

- Velar por la seguridad de los sistemas de información de la Municipalidad Provincial de Paita.

- Supervisar todos los aspectos inherentes al cumplimiento de las acciones definidas en el presente plan de seguridad y continuidad de las tecnologías de la información.

- Practicar auditorias periódicas sobre los sistemas y actividades vinculadas con la tecnología de información.

- Informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por el plan de seguridad de activos y continuidad de las tecnologías de la información, y por las normas, procedimientos y prácticas que surjan.

2. Propietarios de la Información

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de responsabilidades, los responsables propuestos son los siguientes, el Comité de Seguridad puede acordar otros diferentes:

Conformación según Información:	Propietario
Información administrativa, contable, recursos humanos, logística, tesorería, control patrimonial y sistemas.	Gerencia de Administración y Finanzas
Información Presupuestal, de programación e inversiones, institucional y estadística	Gerencia de Planeamiento y Presupuesto
Información de contribuyentes, predios y estados de cuenta, de recaudación, de fiscalización y de ejecutoria coactiva.	Gerencia de Administración Tributaria

Los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservando la responsabilidad del cumplimiento de las mismas, dicha delegación será documentada y proporcionada al Oficial de Seguridad de la Información.

Funciones adicionales:

- Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma.

- Documentar y mantener actualizada la clasificación efectuada.

- Definir los usuarios que tendrán permisos de acceso a la información, de acuerdo a sus funciones y competencias.

3. **Del Responsable de la Subgerencia de Sistemas e Informática**

El responsable de la seguridad de la información es el Subgerente de Sistemas e Informática de la Municipalidad Provincial de Paita.

Funciones adicionales:

- Cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología (clasificar la información de acuerdo con el grado de confiabilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia).

- Efectuar tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

4. **Del Responsable de la Subgerencia de Recursos Humanos**

El responsable de la seguridad de la información es el Subgerente de Recursos Humanos de la Municipalidad Provincial de Paita.

Funciones adicionales:

- Notificar a todo el personal que ingresa, de sus obligaciones respecto al cumplimiento de las políticas de seguridad de la información y de todas las normas, procedimientos y prácticas que de ella surjan.

- Notificar a todo el personal del plan de seguridad de activos y continuidad de las tecnologías de la información, y de los cambios que se produzcan.

- Implementar la suscripción de los Compromisos de Confidencialidad y ejecutar las tareas de capacitación continua en materia de seguridad de la información

5. Del Responsable de la Gerencia de Asesoría Jurídica

El responsable de la seguridad de la información es el Gerente de Asesoría Jurídica de la Municipalidad Provincial de Paita.

Funciones adicionales:

- Asesorará en materia legal en lo que se refiere a la seguridad de la información

- Verificar el cumplimiento de la política de seguridad de activos y continuidad de las tecnologías de la información en todos los contratos, acuerdos u otra documentación de la Municipalidad Provincial de Paita con sus empleados y con terceros.

6. **De los Usuarios de la información y de los sistemas informáticos**

Son responsables de la seguridad de la información todos los empleados de la Municipalidad Provincial de Paita.

Funciones adicionales:

- Conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de activos y continuidad de las tecnologías de la información.

2.5. Asesoramiento Especializado en Materia de Seguridad de la Información

El Especialista de Seguridad de la Información será el encargado de coordinar, aplicar sus conocimientos y las experiencias disponibles, a fin de brindar ayuda en la toma de decisiones en materia de seguridad.

2.6. Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los Propietarios de la Información involucrados, en coordinación conjuntamente con el Oficial de Seguridad de la Información, considerando su propósito y uso, a fin de garantizar que se cumplan todas las políticas y requerimientos de seguridad pertinentes.

Se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades.

En consecuencia, su uso será evaluado en cada caso por el Oficial de Seguridad de la Información y deberá ser autorizado por el responsable de la Subgerencia de Sistemas e Informática y por el responsable del área al que se destinen los recursos.

2.7. Seguridad Frente al Acceso de Terceros

Destinado a garantizar y asegurar protección a los activos de la organización que son accesibles por los proveedores. Así mismo; establecer una relación sólida con los proveedores a fin de adoptar un enfoque flexible de colaboración Cliente-Proveedor.

2.8. Cooperación entre Organismos

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrá contacto con la Oficina Nacional de Gobierno Electrónico – ONGEI organismo especializados en temas relativos a la seguridad informática.

3. Seguridad de los recursos humanos

3.1. Generalidades

Se debe verificar la idoneidad, el perfil técnico, profesional, psicológico y antecedentes penales de las personas que se requiere contratar en la entidad, e incluir la firma de acuerdo de cumplimiento se seguridad de la información a los

colaboradores de la Municipalidad Provincial de Paita y terceros que puedan tener acceso a la información sensible.

Realizar programas de concientización y entrenamiento para asegurar que los colaboradores de la Municipalidad Provincial de Paita asuman sus responsabilidades relacionadas con la Seguridad de la Información, estableciéndose procesos disciplinarios para casos de incumplimiento.

Los terceros que incumplan las políticas de seguridad se sujetaran a lo establecido en el contrato.

Al término de la vinculación laboral o contractual, se debe asegurar la devolución de activos de información asignados y el retiro de los accesos a sistemas informáticos de la Municipalidad Provincial de Paita que se hayan otorgado.

3.2. Alcance

Esta Política se aplica a todo el personal de la entidad, cualquiera sea su situación contractual, y al personal externo que efectúe tareas dentro del ámbito de la entidad.

3.3. Responsabilidad

- El responsable de la Subgerencia de Recursos Humanos incluirá obligaciones relativas a la seguridad de la información en las convocatoria para la contratación de los puestos de trabajos, cargos o servicios, realizará la función de informar y notificar a todo el personal que ingresa sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas,

procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente política, de los cambios que se produzcan en ella, la implementación de la suscripción de los Compromisos de Confidencialidad y coordinará las tareas de capacitación de usuarios respecto de la presente Política, entre otros.

- El Oficial de Seguridad de la Información tendrá a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación al Comité de Gestión de Seguridad de la Información y a los propietarios de la información.

- El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Oficial de Seguridad de la Información maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

- El Responsable de la Oficina de Asuntos Jurídicos participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en la entidad, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

- Todo el personal de la entidad es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

3.4. Seguridad en la Definición de Puestos de Trabajo, Cargos o Servicios y la Asignación de Recursos

3.4.1. Incorporación de la Seguridad en los Puestos de Trabajo

Las funciones y responsabilidades serán incorporadas en la descripción de los puestos de trabajo. Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

3.4.2. Control y Política del Personal

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto, alcanzan a la entidad.

3.4.3. Compromiso de Confidencialidad

Como parte de sus términos y condiciones iniciales de empleo u contratación, los empleados, cualquiera sea su situación contractual, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la entidad. La copia firmada del Compromiso deberá ser retenida en forma segura por la Subgerencia de Recursos Humanos. Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades

que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado. Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre: Suscripción inicial del Compromiso por parte de la totalidad del personal. Revisión del contenido del Compromiso anualmente. Método de re suscripción en caso de modificación del texto del Compromiso.

3.4.4. Términos y Condiciones de Empleo

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información. Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la entidad y del horario normal de trabajo. Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

3.5. Capacitación del Usuario

3.5.1. Formación y Capacitación en Materia de Seguridad de la Información

Todos los empleados de la Municipalidad Provincial de Paita y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la entidad, recibirán una

adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la entidad. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El responsable de la Subgerencia de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política. Debiéndose revisar el material correspondiente a la capacitación cada seis meses, a fin de evaluar la pertinencia de su actualización.

Las siguientes áreas serán encargadas de producir el material de capacitación:

Área	Campo
Recursos Humanos	Cultura Organizacional y Seguridad de las Tecnologías de la Información
Asesoría Legal	Implicaciones legales en Seguridad de la Información y Derechos de Propiedad Intelectual
Informática	Procesos Técnicos y Prácticas Comunes de Seguridad de la Información

El personal que ingrese a la entidad recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se habilitarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

3.6 Respuesta a Incidentes y Anomalías en Materia de Seguridad

3.6.1. Comunicación de Incidentes Relativos a Seguridad

Los incidentes relativos a la seguridad serán comunicados a través de canales gerenciales apropiados tan pronto como sea posible. Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Oficial de Seguridad de la Información sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Así mismo, mantendrá al Comité de Seguridad de la Información al tanto de la ocurrencia de incidentes de seguridad.

Todos los empleados y contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

3.6.2. Comunicación de Debilidades Materia de Seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Oficial de Seguridad de la Información, se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

3.6.3. Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar: Registrar los síntomas del problema y los mensajes que aparecen en pantalla. Establecer las medidas de aplicación inmediata ante la presencia de una anomalía. Alertar inmediatamente al Oficial de Seguridad de la Información. o del Activo de que se trate.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado, adecuadamente habilitado.

3.6.4. Aprendiendo de los Incidentes

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será

evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

3.6.5. Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas, escalonarías y convencionales que rigen al personal de la Administración Pública, para los empleados que violen la Política, Normas y Procedimientos de Seguridad de la entidad.

4. Gestión de los activos

4.1. Generalidades

- Municipalidad Provincial de Paita, a través de oficina de control patrimonial o quien haga sus veces debe elaborar y mantener un inventario de los activos y activos de información para el proceso de evaluación de riesgos de seguridad de la información, asignando responsables de velar por la protección de dichos activos.

- Se debe identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos relacionados con su procesamiento.

- Los activos que posee como parte importante de la administración de riesgos son: Inventario de Software. Inventario de Hardware. Inventario de Data. Inventario de Documentación General. Inventario de Servicios Informáticos y de Comunicaciones.

- Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

- Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios.

- La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada en dichos sistemas o en medios portátiles, transmitida a través de redes, servicios públicos en líneas, aplicaciones móviles o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

- La información puede pasar a ser obsoleta y por lo tanto, es necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

4.2. Alcance

Esta política se aplica a toda la información administrada en la Municipalidad Provincial de Paita, cualquiera sea el soporte en que se encuentre.

4.3. Responsabilidad

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Oficial de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente política.

4.4. Clasificación y control de Activos

4.4.1. Inventario de activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información, tomando como referencia el inventario realizado por la Subgerencia de Control Patrimonial.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad anual.

4.4.2. Clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad. A continuación se establece el criterio de clasificación de la información en función a las mencionadas características:

Característica	Clase	Criterio
Confidencialidad	0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la entidad o no. PUBLICO
	1	Información que puede ser conocida y utilizada por todos los empleados de la entidad y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la entidad, el Sector Público o terceros. RESERVADA – USO INTERNO
	2	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la entidad, al Sector Público o a terceros. RESERVADA – CONFIDENCIAL
	3	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la entidad, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público o a terceros. RESERVADA SECRETA
Integridad	0	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de la entidad.
	1	Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la entidad, el Sector Público o terceros.
	2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la entidad, el Sector Público o terceros.
	3	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la entidad, al Sector Público o a terceros.
Disponibilidad	0	Información cuya inaccesibilidad no afecta la operatoria de la entidad.
	1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para la entidad, el Sector Público o terceros.
	2	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la entidad, al Sector Público o a terceros.
	3	Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas a la entidad, al Sector Público o a terceros.

Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.). Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

Categoría	Criterio
Criticidad Baja	ninguno de los valores asignados superan el 1
Criticidad Media	alguno de los valores asignados es 2
Criticidad Alta	alguno de los valores asignados es 3

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos: Asignarle una fecha de efectividad. Comunicárselo al depositario del recurso. Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados tales como sistemas, equipamiento, servicios, etc. y los perfiles funcionales que deberán tener acceso a la misma. En adelante se mencionará como “información clasificada” o “datos clasificados” a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

4.4.3. Rotulado de la Información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de

información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información: Copia; Almacenamiento; Transmisión por correo o mensajería, fax, correo electrónico; Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

5. Criptografía

5.1. Generalidades

- Se deben establecer procedimientos formales para el uso, protección, y tiempo de vida de las claves criptográficas que se utilizan para proteger los activos de información, que así lo amerite la Municipalidad Provincial de Paita.

5.2. Alcance

Esta política se aplica a toda la información administrada en la Municipalidad Provincial de Paita, cualquiera sea el soporte en que se encuentre.

5.3. Responsabilidad

El Oficial de Seguridad de la Información, junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos.

El Oficial de Seguridad de la Información definirá junto con el Responsable de la Subgerencia de Sistemas e Informática, los métodos de encripción a ser utilizados.

5.4. Controles Criptográficos

5.4.1. Utilización de Controles Criptográficos.

Se debe establecer la Política y las funciones para la implementación de los controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

a. Se utilizarán controles criptográficos en los siguientes casos:

    1. Para la protección de claves de acceso a sistemas, datos y servicios.

    2. Para la transmisión de información clasificada, fuera del ámbito de la entidad.

    3. Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Oficial de Seguridad Informática.

b. Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

Se debe verificar algoritmos y longitudes de clave que a la fecha se consideran seguros. Se recomienda esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes.

5.4.2. Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad Informática, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al implementar la Política de la entidad en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica, para efectos se debe verificar la Regulación de Controles para el uso y métodos de Criptografía.

5.4.3. Firma Digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente. Se implementan mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Se tomarán recaudos para proteger la confidencialidad de las claves privadas.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

Los algoritmos de firma digital a utilizar y la longitud de clave a emplear, deben ser descritos en el cuadro de cifrado asimétrico de la Política de Utilización de Controles Criptográficos.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular. Al utilizar firmas y certificados digitales, se considerará la legislación vigente que describa las condiciones bajo las cuales una firma digital es legalmente válida.

En algunos casos podría ser necesario establecer acuerdos especiales para respaldar el uso de las firmas digitales. A tal fin se deberá obtener asesoramiento legal con respecto al marco normativo aplicable y la modalidad del acuerdo a implementar.

5.4.4. Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

5.4.5. Administración de Claves

Se implementará un sistema de administración de claves criptográficas para respaldar la utilización por parte de la entidad de los dos tipos de técnicas criptográficas, a saber:

- Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.

- Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada. Se aplicarán con éste propósito los algoritmos criptográficos de acuerdo a los Controles Criptográficos que se aprueben.

Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

5.4.6. Normas, Procedimientos y Métodos

Se redactarán las normas y procedimientos necesarios para:

a. Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.

b. Generar y obtener certificados de clave pública de manera segura.

c. Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.

d. Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.

e. Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.

f. Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, cuando las claves están comprometidas o cuando un usuario se desvincula de la entidad (en cuyo caso las claves también deben archivarse).

g. Recuperar claves pérdidas o alteradas como parte de la administración de la continuidad de las actividades de la entidad, por ejemplo para la recuperación de la información cifrada.

h. Archivar claves, por ejemplo, para la información archivada o resguardada. O Destruir claves.

J. Registrar y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso de 12 meses.

Además de la administración segura de las claves secretas y privadas, deberá tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Este certificado se generará de forma que vincule de manera única la información relativa al propietario del par de claves pública/privada con la clave pública.

En consecuencia es importante que el proceso de administración de los certificados de clave pública sea absolutamente confiable. Este proceso es llevado a cabo por una entidad denominada Autoridad de Certificación (AC).

6. Control de accesos

6.1. Generalidades

- Establecer procedimientos formales para el registro y eliminación de usuarios, de modo de garantizar que se otorguen y quiten accesos a los sistemas y servicios de información, en consistencia con los niveles de autorización de los usuarios, además de la revisión respectiva de los mismos.

- Establecer mecanismos parar prevenir el acceso no autorizado a los sistemas de información, servicios de la red interna.

- El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de

derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

- Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

- La cooperación de los usuarios es esencial para la eficacia de la seguridad.

6.2 Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información de la entidad, cualquiera sea la función que desempeñe.

Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

6.3 Responsabilidad

- El Oficial de Seguridad de la Información estará a cargo de: 1) Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de

computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido. 2) Definir pautas de utilización de Internet para todos los usuarios. 3) Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente. 4) Controlar la asignación de privilegios a usuarios. Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios. 5) Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc. 6) Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo. 7) Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría. 8) Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma. En sus funciones de auditoria tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

- Los Propietarios de la Información estarán encargados de: 1) Evaluar los riesgos a los cuales se expone la información con el objeto de Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso. 2) Definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos. 3) Aprobar y solicitar la asignación de privilegios a usuarios. Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información. 4) Definir un cronograma de depuración de registros de auditoría en línea en función a normas vigentes y a sus propias necesidades.

- Los Responsable de las Unidades Orgánicas, junto con el Oficial de Seguridad de la Información, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

- El Responsable de la Subgerencia de Sistemas e Informática cumplirá las siguientes funciones: 1) Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes. 2) Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios. 3) Evaluar el costo y el impacto de la implementación de "enrutadores" o "gateways" adecuados para subdividir la red y recomendar el esquema apropiado. 4) Implementar el control de puertos, de conexión a la red y de ruteo de red. Implementar el registro

de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos. 5) Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento. 6) Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios: biometría, verificación de firma, uso de autenticadores de hardware. 7) Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria. 8) Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios. 9) Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente. 10) Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

- El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

6.4 Control de Accesos

6.4.1. Requerimientos para el Control de Acceso

a. Política de Control de Accesos

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos: 1) Identificar los requerimientos de seguridad de cada una de las aplicaciones. 2) Identificar

toda la información relacionada con las aplicaciones. 3) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes. 4) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios. 5) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo. Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

b. Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán: 1) Indicar expresamente si las reglas son obligatorias u optativas. 2) Establecer reglas sobre la premisa "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente". 3) Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario. 4) Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador. 5) Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

6.4.2. Administración de Accesos de Usuarios

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

a. Registro de Usuarios

El Oficial de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender: 1) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. 2) El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas. 3) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información. 4) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la entidad, por ejemplo que no compromete la separación de tareas. 5) Entregar a los usuarios un detalle escrito de sus derechos de acceso. 6) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso. 7) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización. 8) Mantener un registro formal de todas las personas registradas para utilizar el

servicio. 9) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la entidad o sufrieron la pérdida/robo de sus credenciales de acceso. 10) Efectuar revisiones periódicas con el objeto de cancelar identificadores y cuentas de usuarios redundantes, inhabilitar cuentas inactivas por más de 60 días, eliminar cuentas inactivas por más de 120 días, en el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas. 11) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios. 12) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

b. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos: 1) Identificar los privilegios asociados a cada producto del sistema: sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos. 2) Asignar los privilegios a individuos sobre la

base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional. 3) Mantener un proceso de autorización y un registro de todos los privilegios asignados. 4) Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización. 5) Establecer un período de vigencia para el mantenimiento de los privilegios en base a la utilización que se le dará a los mismos luego del cual los mismos serán revocados. 6) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Oficial de Seguridad de la Información.

c. Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos: 1) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad. 2) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario. 3) Generar contraseñas

provisorias seguras para otorgar a los usuarios. 4) Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección texto claro en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban. 5) Almacenar las contraseñas sólo en sistemas informáticos protegidos. 6) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica tales como verificación de huellas dactilares, verificación de firma, uso de autenticadores de hardware como las tarjetas de circuito integrado, etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Oficial de Seguridad de la Información conjuntamente con el Responsable de la Subgerencia de Sistemas e Informática y el Propietario de la Información lo determine necesario o lo justifique.

Se debe configurar los sistemas de tal manera que: 1) Las contraseñas tengan no menos de 8 caracteres. 2) Suspendan o bloqueen permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta deberá pedir la rehabilitación ante quien corresponda. 3) Solicitar el cambio de la contraseña cada 45 días. 4) Impedir que las últimas 12 contraseñas sean reutilizadas. 5) Determinar el tiempo de vida mínima de días para las contraseñas.

d. Administración de Contraseñas Críticas

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de

software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

El Oficial de Seguridad de la Información definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente: 1) Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido. 2) Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas. 3) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente. 4) La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma. 5) Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado. 6) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Oficial de Seguridad de la Información.

e. Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares de 4 meses, a fin de revisar

los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles: 1) Revisar los derechos de acceso de los usuarios a intervalos 4 meses. 2) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 2 meses. 3) Revisar las asignaciones de privilegios a intervalos de 4 meses, a fin de garantizar que no se obtengan privilegios no autorizados.

6.4.3. Responsabilidades del Usuario

a. Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas: 1) Mantener las contraseñas en secreto. 2) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas. 3) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas. 4) Cambiar las contraseñas provisorias en el primer inicio de sesión. 5) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro. 6) Notificar de acuerdo a lo establecido en "Comunicación de

Incidentes Relativos a la Seguridad", cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad. 7) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el responsable del Activo de Información de que se trate, que: sean fáciles de recordar, no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, tales como nombres, números de teléfono, fecha de nacimiento, etc., no tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

b. Equipos Desatendidos en Áreas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, como estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Oficial de Seguridad de la Información debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca

de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas: 1) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, como un protector de pantalla protegido por contraseña. 2) Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, como contraseña de acceso cuando no se utilizan.

6.4.4. Control de Acceso a la Red

a. Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a toda la entidad, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Responsable de la Subgerencia de Sistemas e Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Orgánica que lo solicite para el personal a su cargo.

Este control es particularmente importante para las

conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la entidad.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán: 1) Identificar las redes y servicios de red a los cuales se permite el acceso. 2) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso. 3) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta Política será coherente con la Política de Control de Accesos de la entidad

b. Camino Forzado

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de la entidad, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado. Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

En caso de implementar controles a los sistemas existentes se debe tener en cuenta: 1) Asignar números telefónicos o líneas, en forma dedicada. 2) Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos. 3) Limitar las opciones de menú y submenú de cada uno de los usuarios. 4) Evitar la navegación ilimitada por la red. 5) Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red. 6) Controlar activamente las comunicaciones con origen y destino autorizado a través de un gateway utilizando firewalls. 7) Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera de la entidad.

Los requerimientos relativos a caminos forzados se basarán en la Política de Control de Accesos de la entidad.

El Oficial de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

c. Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la entidad. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Oficial de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate,

realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando: 1) Un método de autenticación físico por ejemplo tokens de hardware, para lo que debe implementarse un procedimiento que incluya la asignación de la herramienta de autenticación, el Registro de los poseedores de autenticadores, el Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó, el Método de revocación de acceso del autenticador, en caso de compromiso de seguridad. 2) Un protocolo de autenticación por ejemplo desafío/ respuesta, para lo que debe implementarse un procedimiento que incluya: Establecimiento de las reglas con el usuario. Establecimiento de un ciclo de vida de las reglas para su renovación. 3) También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Los procedimientos y controles de re-llamada, o dial-back, pueden brindar protección contra conexiones no autorizadas a las instalaciones de procesamiento de información de la entidad. Al aplicar este tipo de control, la entidad no debe utilizar servicios de red que incluyan desvío de llamadas. Si por alguna causa es preciso mantener el desvío de llamadas, no será posible aplicar el control de re-llamada. Asimismo, es importante que el proceso de re-llamada garantice que se produzca a su término, una desconexión real del lado de la entidad.

d. Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la entidad. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad de la entidad. En el punto anterior se mencionan algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

e. Protección de los Puertos (Ports) de Diagnóstico Remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto "Autenticación de Usuarios para Conexiones Externas". También para este caso deberá tenerse en cuenta el punto "Camino Forzado".

f. Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que

sean convenientes. Estos perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos.

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos y los requerimientos de acceso el Responsable de la Subgerencia de Sistemas e Informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados Control de Conexión a la Red y Control de Ruteo de Red para subdividir la red. Luego decidirá, junto con el Oficial de Seguridad de la Información, el esquema más apropiado a implementar.

g. Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Oficial de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de la Unidad Orgánica a cargo del personal que lo solicite. Asimismo, se definirán las pautas de

utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Dicho control será comunicado a los usuarios de acuerdo a lo establecido en el punto “Compromiso de Confidencialidad”. Para ello, el Oficial de Seguridad de la Información junto con el Responsable de la Subgerencia de Sistemas e Informática analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de “firewalls”, “proxies”, etc.

h. Control de Conexión a la Red

Sobre la base de lo definido en el punto "Requerimientos”, se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los “gateways” que separen los diferentes dominios de la red (Subdivisión de Redes).

Los entornos a las que deben implementarse restricciones son: Correo electrónico. Transferencia de archivos. Acceso interactivo. Acceso a la red fuera del horario laboral.

i. Control de Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites de la entidad, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de

direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

j. Seguridad de los Servicios de Red

El Oficial de Seguridad de la Información junto con el Responsable de la Subgerencia de Sistemas e Informática, definirán las pautas para garantizar la seguridad de los servicios de red de la entidad, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas: Mantener instalados y habilitados sólo aquellos servicios que sean utilizados. Controlar el acceso lógico a los servicios, tanto a su uso como a su administración. Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar. Instalar periódicamente las actualizaciones de seguridad. Dicha configuración será revisada periódicamente por el Oficial de Seguridad de la Información.

6.4.5. Control de Acceso al Sistema Operativo

a. Identificación Automática de Terminales

El Oficial de Seguridad de la Información junto con el Responsable de la Subgerencia de Sistemas e Informática, realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique: El método de identificación automática de terminales utilizado. El detalle de transacciones permitidas por terminal.

b. Procedimientos de Conexión de Terminales

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación deberá: 1) Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión. 2) Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora. 3) Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión. 4) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta. 5) Limitar el número de intentos de conexión no exitosos permitidos y registrar los intentos no exitosos. Impedir

otros intentos de identificación, una vez superado el límite permitido. Desconectar conexiones de comunicaciones de datos. 6) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión. 7) Desplegar la siguiente información, al completarse una conexión exitosa: Fecha y hora de la conexión exitosa anterior. Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

c. Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para la entidad, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo autenticadores de hardware), deberá implementarse un procedimiento que incluya: 1) Asignar la herramienta de autenticación. 2) Registrar los

poseedores de autenticadores. 3) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó. 4) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

d. Sistema de Administración de Contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe: 1) Imponer el uso de contraseñas individuales para determinar responsabilidades. 2) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso. 3) Imponer una selección de contraseñas de calidad según lo señalado en el punto "Uso de Contraseñas". 4) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto "Uso de Contraseñas". 5) Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas. 6) Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas. 7) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas. 8) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación. 9) Almacenar las

contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional. 10) Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware por ejemplo claves de impresoras, hubs, routers, etc. 11) Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

e. Uso de Utilitarios de Sistema

La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles: 1) Utilizar procedimientos de autenticación para utilitarios del sistema. 2) Separar entre utilitarios del sistema y software de aplicaciones. 3) Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados. 4) Evitar que personas ajenas a la entidad tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas. 5) Establecer autorizaciones para uso ad hoc de utilitarios de sistema. 6) Limitar la disponibilidad de utilitarios de sistema, por ejemplo durante el transcurso de un cambio autorizado. 7) Registrar todo uso de utilitarios del sistema. 8) Definir y documentar los niveles de autorización para utilitarios del sistema. 9) Remover todo el software basado en utilitarios y software de sistema innecesarios.

f. Alarmas Silenciosas para la Protección de los Usuarios

Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Oficial de Seguridad de la Información junto con el Responsable de la Subgerencia de Sistemas e Informática. En este caso, se definirán y asignarán funciones y procedimientos para responder a la utilización de una alarma silenciosa.

g. Desconexión de Terminales por Tiempo Muerto

El Responsable de Seguridad de la Información, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad de la entidad, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para las PC's, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un empleado debe abandonar su puesto

de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

h. Limitación del Horario de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo áreas públicas o externas que estén fuera del alcance de la gestión de seguridad de la entidad.

Entre los controles que se deben aplicar, se enuncian: 1) Utilizar lapsos predeterminados, por ejemplo para transmisiones de archivos en lote, o sesiones interactivas periódicas de corta duración. 2) Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria. 3) Documentar debidamente los agentes que no tienen restricciones horarias y las razones de su autorización. También cuando el Propietario de la Información autorice excepciones para una extensión horaria ocasional.

6.4.6. Control de Acceso a las Aplicaciones

a. Restricción del Acceso a la Información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política de la entidad para el acceso a la información.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos: 1) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el Propietario de la Información. 2) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario. 3) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución. 4) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas. 5) Revisar periódicamente

dichas salidas a fin de garantizar la remoción de la información redundante. 6) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

b. Aislamiento de los Sistemas Sensibles

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones: 1) Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación. 2) Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos. 3) Coordinar con el Responsable del Área informática, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación. 4) Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones. 5) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación.

6.4.7. Computación Móvil y Teletrabajo

a) Computación Móvil

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información de la entidad. Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o PDA Asistente Personal Digital, Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.. Esta lista no es taxativa, ya que deberán incluirse todos los dispositivos que pudieran contener información confidencial.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos: 1) La protección física necesaria. 2) El acceso seguro a los dispositivos 3) La utilización de los dispositivos en lugares públicos. 4) El acceso a los sistemas de información y servicios de la entidad a través de dichos dispositivos. 5) Las técnicas criptográficas a utilizar para la transmisión de información clasificada. 6) Los mecanismos de resguardo de la información contenida en los dispositivos. 7) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de

pérdida, robo o hurto. En consecuencia deberá entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones: 1) Permanecer siempre cerca del dispositivo. 2) No dejar desatendidos los equipos. 3) No llamar la atención acerca de portar un equipo valioso. 4) No poner identificaciones de la entidad en el dispositivo, salvo los estrictamente necesarios. 5) No poner datos de contacto técnico en el dispositivo. 6) Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de la entidad, los que incluirán: 1) Revocación de las credenciales afectadas. 2) Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

b) Trabajo Remoto o Teletrabajo

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo a la Municipalidad.

El trabajo remoto sólo será autorizado por el responsable de la Unidad Orgánica, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Oficial de Seguridad de la Información, cuando se verifique que son adoptadas

todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios de la entidad, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos: 1) La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local. 2) El ambiente de trabajo remoto propuesto. 3) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la entidad, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno. 4) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos. 5) Evitar la instalación/desinstalación de software no autorizada por la entidad.

Los controles y disposiciones comprenden: 1) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto. 2) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red de la entidad y los sistemas internos y servicio a los cuales el

trabajador remoto está autorizado a acceder. 3) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto. 4) Incluir seguridad física. 5) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información. 6) Proveer el hardware y el soporte y mantenimiento del software. 7) Definir los procedimientos de backup y de continuidad de las operaciones. 8) Efectuar auditoría y monitoreo de la seguridad. 9) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas. 10) Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

7. Seguridad física y ambiental

7.1. Generalidades

- Establecer procedimientos de mantenimiento de los equipos de procesamiento de información con el fin de asegurar su continua disponibilidad e integridad.

- Se pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

- Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

- El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la entidad, de accesos físicos no autorizados.

- El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones de la entidad como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

- El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas de la entidad. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente a la entidad pero situado físicamente fuera de la misma ("housing") así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información a la entidad ("hosting").

- La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes

medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

- Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

7.2. Alcance

Esta política se aplica a todos los recursos físicos relativos a los sistemas de información de la Municipalidad Provincial de Paita: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

7.3. Responsabilidad

El Oficial de Seguridad de la Información definirá junto con el Responsable de la Subgerencia de Sistemas e Informática y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente punto.

El Responsable de la Subgerencia de Sistemas e Informática asistirá al Oficial de Seguridad de la Información en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de

acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la entidad.

Los Responsables de Unidades Orgánicas definirán los niveles de acceso físico del personal de la entidad a las a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su cargo a los empleados de la entidad cuando lo crean conveniente.

El Oficial de Seguridad de la Información, quien contará con el apoyo del Especialista de Seguridad de la Información revisarán los registros de acceso a las áreas protegidas.

Todo el personal de la entidad es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario.

7.4. Política de Seguridad Física y Ambiental

7.4.1. Perímetro de Seguridad Física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las instalaciones de procesamiento de información.

La entidad utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable de la Subgerencia de Sistemas e Informática con el asesoramiento del Oficial de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda: 1) Definir y documentar claramente el perímetro de seguridad. 2) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc. 3) Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementará algún medio alternativo de control de acceso físico al área o edificio. El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa. 4) Extender las barreras físicas necesarias desde el piso hasta el techo, a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación. 5) Identificar claramente todas las puertas de salida de emergencia de un perímetro de seguridad.

El Oficial de Seguridad de la Información llevará un registro actualizado de los sitios protegidos, indicando: 1) Identificación del Edificio y Área. 2) Principales elementos a proteger. 3) Medidas de protección física.

7.4.2. Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Oficial de Seguridad de la Información junto con el Responsable de la Subgerencia de Sistemas e Informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características: a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia. b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos: Listado de Personas habilitadas ubicado sobre la puerta de acceso, tarjeta magnética que registre el número de identificación personal. c) Se mantendrá un registro protegido (video) para permitir auditar todos los accesos. d) Implementar el uso de la identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible. e) Revisar y actualizar

cada tres meses los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Orgánica de la que dependa. f) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará el Oficial de Seguridad de la Información conjuntamente con el Especialista de Seguridad de la Información.

7.4.3. Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas o estándares en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas de la entidad:

Ítem	Área Protegida	Ubicación
1.	Data Center	Oficina del Data Center – Oficina Principal Palacio Municipal.
2.	Oficina Alternativa	Todas las Oficinas que se encuentren fuera del Palacio Municipal.

Se establecen las siguientes medidas de protección para áreas protegidas: a) Ubicar las instalaciones críticas en lugares a

los cuales no pueda acceder personal no autorizado. b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores. c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información. d) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales. e) Implementar los siguientes mecanismos de control para la detección de intrusos: lista de personal autorizado sobre la puerta de acceso, identificación personal fotocheck, acceso vía tarjeta magnética con palabra clave y registro de video u otro que sea aprobado. Los mismos serán instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles. f) Separar las instalaciones de procesamiento de información administradas por la entidad de aquellas administradas por terceros. g) Restringir el acceso público a las guías, directorios y listados que identifican las ubicaciones de las instalaciones de procesamiento de información sensible. h) Almacenar los materiales peligrosos o combustibles en lugares seguros a una distancia prudencial de las áreas protegidas de la entidad. Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos. i) Almacenar los equipos redundantes y la información de resguardo back-up en un sitio seguro y distante del lugar de procesamiento, para evitar daños

ocasionados ante eventuales contingencias en el sitio principal. El resguardo del Data Center será ubicado en la Caja Fuerte del Palacio Municipal y/o en la Oficina que se designe fuera del Palacio Municipal.

7.4.4. Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí: a) Dar a conocer al personal la existencia del área protegida, o de las actividades que se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones. b) Evitar la ejecución de trabajos por parte de terceros sin supervisión. c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas. d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas. e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad. f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicha área o el Responsable de la Subgerencia de Sistemas

e Informática y el Oficial de Seguridad de la Información. g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

7.4.5. Aislamiento de las Áreas de Almacenamiento

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos: a) Limitar el acceso a las áreas de almacenamiento, desde el exterior de la sede de la entidad, sólo al personal previamente identificado y autorizado. b) Diseñar el área de almacenamiento de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio. c) Proteger todas las puertas exteriores del almacén cuando se abre la puerta interna. d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área del almacén hasta el lugar de uso. e) Registrar el material entrante al ingresar al sitio pertinente.

7.4.6. Ubicación y Protección del Equipamiento y Copias de Seguridad

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos: a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado. b)

Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso. c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida. d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:

Ítem	Amenaza Potencial	Control
1.	Robo o hurto	Seguridad permanente en el edificio municipal y oficinas fuera del palacio.
2.	Incendio	Ubicación de extintores dentro y fuera del Data Center y almacén de copias de seguridad.
3.	Inundaciones o filtraciones de agua.	Ubicación alejada de tomas de agua
4.	Polvo	Oficinas con puertas y ventanas cerradas.
5.	Vibraciones	Oficinas independientes
6.	Interferencia en el suministro eléctrico	Conexión directa a la toma eléctrica y sistema UPS
7.	Radiación electromagnética	Almacén de copias de seguridad alejado de fuentes de radiación electromagnética
8.	Sismos	Copia de seguridad redundante en edificio u oficina distinto al del Data Center

e) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. f) Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede de la entidad.

7.4.7. Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control: a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía. b) Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la entidad. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Oficial de Seguridad de la Información conjuntamente con los Propietarios de la Información o personal a su cargo. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida. c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el Oficial de Seguridad de la Información conjuntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de

combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

7.4.8. Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones: a) Cumplir con los requisitos técnicos vigentes. b) Utilizar cableado empotrado en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a la protección alternativa mediante canaletas según normas técnicas del cableado estructurado. c) Proteger el cableado de red contra intercepción no autorizada o daño mediante controles pertinentes y evitando trayectos que atraviesen áreas públicas. d) Separar los cables

de energía de los cables de comunicaciones para evitar interferencias. e) Proteger el tendido del cableado troncal backbone mediante la utilización de ductos blindados.

Para los sistemas sensibles o críticos, se implementarán los siguientes controles adicionales: a) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección. b) Utilizar rutas o medios de transmisión alternativos.

7.4.9. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar: a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsable de la Subgerencia de Sistemas e Informática quien mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo. b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento. c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado. d) Registrar el retiro de equipamiento de la sede de la entidad para su mantenimiento. e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

7.4.10. Seguridad de los Equipos Fuera de las Instalaciones.

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la entidad, será autorizado por el responsable de la Subgerencia de Control Patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la entidad para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma. Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito de la entidad, cuando sea conveniente.

7.4.11. Desafectación o Reutilización de los Equipos.

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

7.4.12. Políticas de Escritorios y Pantallas Limpias.

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de

reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos: a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo. b) Guardar bajo llave la información sensible o crítica de la entidad preferentemente en una caja fuerte o gabinete a prueba de incendios cuando no está en uso, especialmente cuando no hay personal en la oficina. c) Desconectar de la red, sistema, servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso como: utilización de protectores de pantalla con contraseña. Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción. d) Proteger los puntos de recepción y envío de correo electrónico y las máquinas de fax no atendidas. e) Bloquear las fotocopiadoras o protegerlas de alguna manera del uso no autorizado fuera del horario normal de trabajo. f) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

7.4.13. Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede de la Municipalidad Provincial de Paita o de las Oficinas alternas al Palacio Municipal sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la entidad, las que serán llevadas a cabo por la Subgerencia de Control Patrimonial que será reportado al Oficial de Seguridad de la Información. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

8. Seguridad de las operaciones

8.1. Generalidades

- En resguardo de la operación correcta y segura de las instalaciones de tecnologías de la información, se deben mantener documentados y actualizados los procedimientos operativos informáticos, controlar y documentar los cambios previamente autorizados sobre la plataforma tecnológica, y efectuar una separación de tareas y áreas de responsabilidad.

8.2. Alcance

Esta política se aplica a toda la información administrada en la Municipalidad Provincial de Paita, cualquiera sea el soporte en que se encuentre.

8.3. Responsabilidad

El Oficial de Seguridad de la Información junto con el Responsable de la Subgerencia de Sistemas e Informática y el Responsable del Área Legal de la entidad evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el Oficial de Seguridad de la Información y el Responsable de la Subgerencia de Sistemas e Informática, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

El Oficial de Seguridad de la Información, revisará las actividades que no hayan sido posibles agregar. Asimismo, revisará los registros de actividades del personal operativo.

8.4. Procedimientos y Responsabilidades Operativas

8.4.1. Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Oficial de Seguridad de la Información. Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo: a) Procesamiento y manejo de la información. b)

Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas. c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas. d) Restricciones en el uso de utilitarios del sistema. e) Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas. f) Instrucciones especiales para el manejo de "salidas", como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas. g) Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades: a) Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones. b) Instalación y mantenimiento de las plataformas de procesamiento. c) Monitoreo del procesamiento y las comunicaciones. d) Inicio y finalización de la ejecución de los sistemas. e) Programación y ejecución de procesos. f) Gestión de servicios. g) Resguardo de información. h) Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones. i) Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones. j) Uso del correo electrónico.

8.4.2. Control de Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio

deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Oficial de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable de la Subgerencia de Sistemas e Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos: a) Identificación y registro de cambios significativos. b) Evaluación del posible impacto de dichos cambios c) Aprobación formal de los cambios propuestos. d) Planificación del proceso de cambio. e) Prueba del nuevo escenario. f) Comunicación de detalles de cambios a todas las personas pertinentes. g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

8.4.3. Procedimientos de Manejo de Incidentes

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes: a) Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo: fallas operativas, códigos maliciosos, Intrusiones, fraude informático, error humano, catástrofes naturales. b) Comunicar los incidentes a través de canales

gerenciales apropiados tan pronto como sea posible. c) Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales diseñados para recuperar sistemas y servicios tan pronto como sea posible: definición de las primeras medidas a implementar, análisis e identificación de la causa del incidente, planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario, comunicación con las personas afectadas o involucradas con la recuperación, del incidente, notificación de la acción a la autoridad y/u organismo pertinente. d) Registrar pistas de auditoría y evidencia similar para: análisis de problemas internos, uso como evidencia en relación con una probable violación contractual o infracción normativa o en marco de un proceso judicial, negociación de compensaciones por parte de los proveedores de software y de servicios. e) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando: acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado, documentación de todas las acciones de emergencia emprendidas en forma detallada, comunicación de las acciones de emergencia al titular de la unidad orgánica y revisión de su cumplimiento, constatación de la integridad de los controles y sistemas de la entidad en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del Responsable del Área Legal de la entidad en el tratamiento de incidentes de seguridad ocurridos.

8.4.4. Separación de Funciones

Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

Si este método de control no se pudiera cumplir en algún caso, se implementarán controles como: a) Monitoreo de las actividades. b) Registros de auditoría y control periódico de los mismos. c) Supervisión por parte del Oficial de Seguridad de la Información, siendo independiente al área que genera las actividades auditadas.

Asimismo, se documentará la justificación formal por la cual no fue posible efectuar la segregación de funciones.

Se asegurará la independencia de las funciones de auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos: a) Separar actividades que requieren convivencia para defraudar, por ejemplo efectuar una orden de compra y verificar que la mercadería fue recibida. b) Diseñar controles, si existe peligro de convivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

8.4.5. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Para ello, se tendrán en cuenta los siguientes controles: a) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios. b) Separar las actividades de desarrollo y prueba, en entornos diferentes. c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo. d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión. e) Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes. f) El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

Para el caso que no puedan mantener separados los distintos ambientes en forma física, deberán implementarse los controles adecuados.

8.4.6. Gestión de Instalaciones Externas

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio y se incluirán en el contrato, contemplando las siguientes cuestiones específicas: a) Identificar las aplicaciones sensibles o críticas que convenga retener en la entidad. b) Obtener la aprobación de los propietarios de aplicaciones específicas. c) Identificar las implicancias para la continuidad de los planes de las actividades de la entidad. d) Especificar las normas de seguridad y el proceso de medición del cumplimiento. e) Asignar funciones específicas y procedimientos para monitorear todas las actividades de seguridad. f) Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Dichas consideraciones deberán ser acordadas entre el Oficial de Seguridad de la Información, el Responsable de la Subgerencia de Sistemas e Informática y el Responsable del Área Legal de la Municipalidad de Paita.

9. Seguridad de las comunicaciones

9.1. Generalidades

- Establecer procedimientos formales para el registro y eliminación de usuarios, de modo de garantizar que se otorguen y quiten accesos a los sistemas y servicios de información, en consistencia con los niveles de autorización de los usuarios, además de la revisión respectiva de los mismos.

- Se debe aplicar medidas efectivas de protección para el software utilizado en los sistemas de cómputo, la información que estos procesan, y la información transmitida por sistemas de comunicación de datos en la red interna de la Institución, incluyendo la mensajería electrónica y los intercambios de información con cualquier entidad externa.

- Se debe monitorear el uso de la red y sistemas de información a fin de detectar las actividades no autorizadas.

- Los sistemas de información están comunicados entre sí, tanto dentro de la entidad como con terceros fuera de él. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan. Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

9.2. Alcance

Todas las instalaciones de procesamiento y transmisión de información de la entidad.

9.3. Responsabilidad

El Oficial de la Seguridad de la Información tendrá a su cargo, entre otras responsabilidades de: a) definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información. b) Controlar los mecanismos de

distribución y difusión de información dentro de la entidad. c) Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. d) Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para las aplicaciones de Gobierno Electrónico. e) Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento. f) Definir y documentar una norma clara con respecto al uso del correo electrónico. g) Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes de la entidad. h) Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios. i) Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Responsable de la Subgerencia de Sistemas e Informática tendrá a su cargo, entre otras responsabilidades lo siguiente: a) Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones. b) Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades. c) Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario. d) Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración. e) Desarrollar y verificar el cumplimiento de procedimientos para

comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas. f) Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados). g) Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, memorias USB e informes impresos y para la eliminación segura de los mismos. h) Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.

El Oficial de la Seguridad de la Información junto con el Responsable de la Subgerencia de Sistemas e Informática y el Responsable del Área Legal de la entidad evaluarán los contratos y acuerdos con terceros.

Cada Propietario de la Información, junto con el Oficial de la Seguridad de la Información y el Responsable de la Subgerencia de Sistemas e Informática, determinará los requerimientos para resguardar la información.

9.4. Política de Comunicaciones

9.4.1. Planificación y Aprobación de Sistemas

a. Planificación de la Capacidad

El Responsable de la Subgerencia de Sistemas e Informática o su asistente, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado. Para ello

tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información de la entidad para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

b. Aprobación del Sistema

El Responsable de la Subgerencia de Sistemas e Informática y el Oficial de la Seguridad de la Información sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos: 1) Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras. 2) Garantizar la recuperación ante errores. 3) Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas. 4) Garantizar la implementación de un conjunto acordado de controles de seguridad. 5) Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento. 6) Considerar el efecto que tiene el nuevo sistema en la seguridad global de la entidad. 7) Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

9.4.2. Protección contra Software Malicioso

a. Controles Contra Software Malicioso

El Oficial de la Seguridad de la Información definirá controles de detección y prevención para la protección contra software malicioso. El Responsable de la Subgerencia de Sistemas e Informática, o su asistente, implementarán dichos controles.

El Oficial de la Seguridad de la Información desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones: 1) Prohibir el uso de software no autorizado por la entidad. 2) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar. 3) Instalar y actualizar periódicamente software de detección y reparación de virus, examinando computadoras y medios informáticos, como medida precautoria y rutinaria. 4) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles 5) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la entidad, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas. 6) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen

incierto, o en archivos recibidos a través de redes no confiables. 7) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos. 8) Concientizar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

9.4.3. Mantenimiento

a. Resguardo de la Información

El Responsable de la Subgerencia de Sistemas e Informática en coordinación con el Oficial de la Seguridad de la Información y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Responsable de la Subgerencia de Sistemas e Informática dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de la entidad. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la entidad.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos: 1) Definir un esquema de rótulo de las copias de

resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente. 2) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados. 3) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para la entidad. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad y requisitos legales a los que se encuentre sujeta. 4) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo. 5) Probar periódicamente los medios de resguardo. 6) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

b. Registro de Actividades del Personal Operativo

El Responsable de la Subgerencia de Sistemas e Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda: 1) Tiempos de inicio y cierre del sistema. 2) Errores del sistema y medidas correctivas tomadas. 3) Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas 4) Ejecución de operaciones críticas 5) Cambios a información crítica

El Oficial de la Seguridad de la información contrastará los registros de actividades del personal operativo con relación a los procedimientos operativos.

9.4.4. Administración de la Red

a. Controles de Redes

El Oficial de la Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la entidad, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones: 1) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias. 2) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas. 3) Garantizar mediante

actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El Responsable de la Subgerencia de Sistemas e Informática implementará dichos controles.

9.4.5. Administración y Seguridad de los Medios de Almacenamiento

a. Administración de Medios Informáticos Removibles

El Responsable de la Subgerencia de Sistemas e Informática, con la asistencia del Oficial de la Seguridad de la Información, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, Memorias USB e informes impresos.

Se deberán considerar las siguientes acciones para la implementación de los procedimientos: 1) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la entidad. 2) Requerir autorización para retirar cualquier medio de la entidad y realizar un control de todos los retiros a fin de mantener un registro de auditoría. 3) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Se documentarán todos los procedimientos y niveles de autorización.

b. Eliminación de Medios de Información

El Responsable de la Subgerencia de Sistemas e Informática, junto con el Oficial de la Seguridad de la Información definirá procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura: Documentos en papel. Voces u otras grabaciones. Papel carbón. Informes de salida. Cintas de impresora de un solo uso. Cintas magnéticas. Discos o Memorias removibles. Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor). Listados de programas. Datos de prueba. Documentación del sistema.

c. Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información. En los procedimientos se contemplarán las siguientes acciones: 1) Incluir en la protección a documentos, sistemas informáticos, redes, puntos de red, computación móvil, comunicaciones móviles, correo electrónico, correo de voz, comunicaciones de voz en general, multimedia, servicios de internet, telefonía y mensajería, uso de máquinas de fax y cualquier otro potencialmente sensible. 2) Restringir el acceso solo al personal debidamente autorizado. 3) Mantener un registro formal de los receptores autorizados de datos. 4) Garantizar que los datos de entrada son

completos, que el procesamiento se lleva a cabo correctamente y que se valida las salidas. 5) Proteger los datos en espera. 6) Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

d. Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes criterios para su protección: 1) Almacenar la documentación del sistema en forma segura. 2) Restringir el acceso a la documentación del sistema al personal estrictamente necesario el cual será autorizado por el Propietario de la Información.

9.4.6. Intercambios de Información y Software

a. Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre entidades para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la entidad involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos: 1) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones. 2) Procedimientos de notificación de emisión, transmisión, envío y recepción. 3) Normas técnicas para el empaquetado y la transmisión. 4) Pautas para la identificación del prestador del servicio de correo. 5) Responsabilidades y obligaciones en caso de pérdida de

datos. 6) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida. 7) Términos y condiciones de la licencia bajo la cual se suministra el software. 8) Información sobre la propiedad de la información suministrada y las condiciones de su uso. 8) Normas técnicas para la grabación y lectura de la información y del software. 9) Controles especiales que puedan requerirse para proteger datos sensibles, (claves criptográficas, etc.).

b. Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar: 1) La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir. 2) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores. 3) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen: Uso de recipientes cerrados. Entrega en mano. Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso). En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

c. Seguridad del Gobierno Electrónico

El Oficial de la Seguridad de la Información verificará que los procedimientos de aprobación de Software incluyan los siguientes aspectos para las aplicaciones de Gobierno Electrónico: 1) Autenticación: Nivel de confianza recíproca suficiente sobre la identidad del usuario y la entidad. 2) Autorización: Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc. Forma de comunicarlo al otro participante de la transacción electrónica. 3) Procesos de oferta y contratación pública: Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos. 4) Trámites en línea: Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción. 5) Verificación: Grado de verificación apropiado para constatar la información suministrada por los usuarios. 6) Cierre de la transacción: Forma de interacción más adecuada para evitar fraudes. 7) Protección a la duplicación: Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. 8) No repudio: Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió. 9) Responsabilidad: Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

Se darán a conocer a los usuarios, los términos y condiciones aplicables.

Todas las medidas vinculadas al plan de gobierno electrónico de la entidad deberán dictarse conforme lo dispuesto por la ONGEI.

d. Seguridad del Correo Electrónico

El Oficial de la Seguridad de la Información verificará que los procedimientos de uso del correo electrónico incluyan los siguientes aspectos: 1) se debe cumplir con la "Ley que Regula el Uso del Correo Electrónico Comercial no Solicitado (SPAM)". 2) Siendo el correo electrónico institucional una herramienta importante de comunicación e intercambio de información entre personas y entidades, resulta necesario promover su correcta aplicación como recurso de comunicación inter institucional, regulando su uso racional para optimizar su aprovechamiento, obedeciendo procedimientos para el uso del servicio de correo electrónico en la entidad. Por lo que los usuarios del correo electrónico de la entidad cumplirán con las "Normas para el Uso del Servicio de Correo Electrónico en la Entidades de la Administración Pública".

e. Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando: 1) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio. 2) La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos. 3) Las posibles vulnerabilidades a errores, por ejemplo,

consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio. 4) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada. 5) El impacto de un cambio en el medio de comunicación en los procesos de la entidad. 6) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación. 7) Las implicancias de la publicación externa de listados de personal, accesibles al público. 8) El acceso de usuarios remotos a las cuentas de correo electrónico. 9) El uso inadecuado por parte del personal.

f. Política de Correo Electrónico

El Oficial de la Seguridad de la Información junto con el Responsable de la Subgerencia de Sistemas e Informática definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos: 1) Protección contra ataques al correo electrónico, por ejemplo virus, intercepción, etc. 2) Protección de archivos adjuntos de correo electrónico. 3) Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos. 4) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio. 5) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados. 6) Aspectos operativos para garantizar el correcto funcionamiento del servicio: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del

buzón del usuario, etc. 7) Definición de los alcances del uso del correo electrónico por parte del personal de la entidad. 8) Potestad de la entidad para auditar los mensajes recibidos o emitidos por los servidores de la entidad, lo cual se incluirá en el "Compromiso de Confidencialidad"

Entender al correo electrónico como una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, la entidad debe informar claramente a sus empleados: a) cuál es el uso que la entidad espera que los empleados hagan del correo electrónico provisto por la entidad; y b) bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

g. Seguridad de los Sistemas Electrónicos de Oficina

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales, equipos de fax, etc.

Al interconectar dichos medios, se considerarán las

implicancias en lo que respecta a la seguridad y a las actividades propias de la entidad, incluyendo: 1) Vulnerabilidades de la información en los sistemas de oficina, por ejemplo la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo. 2) Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo el uso de boletines electrónicos institucionales. 3) Exclusión de categorías de información sensible de la entidad, si el sistema no brinda un adecuado nivel de protección. 4) Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo aquellas que trabaja en proyectos sensibles. 5) La aptitud del sistema para dar soporte a las aplicaciones de la entidad, como la comunicación de órdenes o autorizaciones. 6) Categorías de personal y contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.7) Retención y resguardo de la información almacenada en el sistema. 8) Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

h. Sistemas de Acceso Público

Se tomarán medidas para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación de la entidad que emite la publicación. Es posible que la información de un sistema de acceso público.

Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación. Todos los sistemas de acceso público deberán prever que: 1) La información se obtenga, procese y proporcione de acuerdo a la normativa vigente. 2) La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna. 3) La información sensible sea protegida durante el proceso de recolección y su almacenamiento. 4) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo. 5) Se registre al responsable de la publicación de información en sistemas de acceso público. 7) La información se publique teniendo en cuenta las normas establecidas al respecto. 8) Se garantice la validez y vigencia de la información publicada.

i. Otras Formas de Intercambio de Información

Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo, contemplando las siguientes acciones: 1) Concientizar al personal sobre la toma de debidas precauciones, por ejemplo no revelar información sensible como para evitar ser escuchado o interceptado, al hacer una llamada telefónica, por: Personas cercanas, en especial al utilizar teléfonos móviles. Terceros que tengan acceso a la comunicación mediante la Intervención de la línea telefónica, y otras formas de escucha subrepticias, a través del acceso físico al aparato o a la línea telefónica, o

mediante equipos de barrido de frecuencias al utilizar teléfonos móviles. Terceros en el lado receptor. 2) Recordar al personal que no sostengan conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas. 3) No dejar mensajes en contestadores automáticos puesto que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como resultado de un error de discado. 4) Recordar al personal los problemas ocasionados por el uso de máquinas de fax, en particular: el acceso no autorizado a sistemas incorporados de almacenamiento de mensajes con el objeto de recuperarlos. La programación deliberada o accidental de equipos para enviar mensajes a determinados números.

10. Adquisición, desarrollo y mantenimiento de sistemas de información

10.1. Generalidades

- Para los cambios en los sistemas existente o para su adquisición se debe determinar los requisitos de seguridad, ya sean desarrollados internamente o tercerizados; estos requisitos de seguridad deben contemplar las verificaciones del procesamiento correcto de las aplicaciones y la protección del código y datos en producción.

- Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se

deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

- Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

- Todo sistema de información nuevo o actualizado debe cumplir con el proceso de ciclo de vida del sistema establecido para el desarrollo alineado a la NTP ISO/IEC 15288:2014, esto debe ser verificado y sustentado antes de su puesta en producción.

10.2. Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por la entidad en donde residan los desarrollos mencionados.

10.3. Responsabilidad

El Oficial de Seguridad de la Información junto con el Propietario de la Información tendrán las siguientes

responsabilidades: a) Definir los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos. 2) Definir en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos.

Oficial de Seguridad de la Información junto con el Responsable de la Subgerencia de Sistemas e Informática, definirán los métodos de encriptación a ser utilizados.

Asimismo, el Oficial de Seguridad de la Información cumplirá las siguientes funciones: a) Definir los procedimientos de administración de claves. b) Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas. c) Garantizar el cumplimiento de los requerimientos de seguridad para el software. d) Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El Responsable de la Subgerencia de Sistemas e Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de implementador y administrador de programas fuentes al personal de su área que considere adecuado. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas. Así mismo, propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

El Responsable del Área de Administración incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. El Responsable del Área Legal participará en dicha tarea.

10.4. Política de Adquisición, Desarrollo y Mantenimiento de Software

10.4.1. Requerimientos de Seguridad de los Sistemas

a. Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información propios o de terceros y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones: 1) Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas

usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar. 2) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas. 3) Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

10.4.2. Seguridad en los Sistemas de Aplicación

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando: a) La validación de datos de entrada. b) El procesamiento interno. c) La autenticación de mensajes interfaces entre sistemas. d) La validación de datos de salida.

a. Validación de Datos de Entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles: 1) Control de secuencia. 2) Control de monto límite por operación y tipo de usuario. 3) Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados. 4) Control de paridad. 5) Control contra valores cargados en las tablas de datos. 6) Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones: 1) Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, etc. 2) Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo. 3) Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

b. Controles de Procesamiento Interno

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores. Para ello se implementarán: 1) Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos. 2) Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la

ejecución de programas fuera de secuencia o cuando falle el procesamiento previo. 3) Procedimientos que establezcan la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones. 4) Procedimientos que realicen la validación de los datos generados por el sistema. 5) Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras. 6) Procedimientos que controlen la integridad de registros y archivos. 7) Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado. 8) Procedimientos que aseguren la correcta ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

c. Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles criptográficos.

d. Validación de Datos de Salidas

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo: 1) Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles. 2) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos. 3) Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la

información. 4) Procedimientos para responder a las pruebas de validación de salidas. 5) Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

10.4.3. Seguridad de los Archivos del Sistema

Los desarrollos y actividades de soporte a los sistemas se llevaran a cabo de manera segura, controlando el acceso a los archivos del mismo.

a. Control del Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

Toda aplicación, desarrollada por el Organismo o por un tercero tendrá un único Responsable designado formalmente por el Responsable de la Subgerencia de Sistemas e Informática.

Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrán acceder a los ambientes de producción.

El Responsable de la Subgerencia de Sistemas e Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de implementador al personal de su área que considere adecuado, quien tendrá como funciones principales: 1) Coordinar la implementación de

modificaciones o nuevos programas en el ambiente de Producción. 2) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes. 3) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final. 4) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son: 1) Guardar sólo los ejecutables en el ambiente de producción. 2) Llevar un registro de auditoría de las actualizaciones realizadas. 3) Retener las versiones previas del sistema, como medida de contingencia. 4) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc. 5) Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia. 6) Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

b. Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente: 1) Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar

idénticos procedimientos de control de acceso que en la base de producción. 2) Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización. 3) Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

c. Control de Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos serán realizadas a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos. Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Oficial de Seguridad de la Información definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente: 1) Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato. 2) El Propietario de la Información afectada y el Oficial de Seguridad de la Información aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita. 3) Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que

ésta dure. 4) Se designará un encargado de implementar los cambios, el cual no será personal de Desarrollo del Sistema. En el caso de que esta función no pueda ser segregada, se aplicarán controles 5) Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Oficial de Seguridad de la Información.

d. Control de Acceso a las Bibliotecas de Programas Fuentes

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles: 1) El Responsable de la Subgerencia de Sistemas e Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de administrador de programas fuentes al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y deberá: a) Proveer al encargado del desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente/ejecutable. b) Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha/hora de compilación y estado en modificación, en producción. c) Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada. d) Administrar las distintas versiones de una aplicación. e) Asegurar que un mismo programa fuente no sea

modificado simultáneamente por más de un desarrollador. 2) Denegar al administrador de programas fuentes permisos de modificación sobre los programas fuentes bajo su custodia. 3) Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen. 4) Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción compilación, a fin de garantizar tal correspondencia. 5) Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática. 6) Evitar que la función de administrador de programas fuentes sea ejercida por personal que pertenezca al sector de Desarrollo y/o Mantenimiento. 7) Prohibir la guarda de programas fuentes históricos que no sean los correspondientes a los programas operativos en el ambiente de producción. 8) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes. 9) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos en los procedimientos que surgen de la presente política.

10.4.4. Seguridad de los Procesos de Desarrollo y Soporte

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto se controlarán los entornos y el soporte dado a los mismos.

a. Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones. Para ello se establecerá un procedimiento que incluya las siguientes consideraciones: 1) Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso. 2) Mantener un registro de los niveles de autorización acordados. 3) Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma. 4) Identificar todos los elementos que requieren modificaciones software, bases de datos, hardware. 5) Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios. 6) Obtener aprobación formal por parte del Responsable de la Subgerencia de Sistemas e Informática para las tareas detalladas, antes que comiencen las tareas. 7) Solicitar la revisión del Oficial de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software. 8) Efectuar las actividades relativas al cambio en el ambiente de desarrollo. 9) Obtener la aprobación por parte del usuario autorizado y del área de pruebas o quien haga sus veces mediante pruebas en el ambiente correspondiente. 10) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación

operativa. 11) Mantener un control de versiones para todas las actualizaciones de software. 12) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados. 13) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria. 14) Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en "Control del Software Operativo".

b. Revisión Técnica de los Cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya: 1) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio. 2) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación. 3) Asegurar la actualización del Plan de Continuidad de las Actividades de la entidad.

c. Restricción del Cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y

previa autorización del Responsable de la Subgerencia de Sistemas e Informática, se deberá: 1) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas. 2) Determinar la conveniencia de que la modificación sea efectuada por la entidad, por el proveedor o por un tercero. 3) Evaluar el impacto que se produce si la entidad se hace cargo del mantenimiento. 4) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

d. Canales Ocultos y Código Malicioso

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario. En este sentido, se redactarán normas y procedimientos que incluyan: 1) Adquirir programas a proveedores acreditados o productos ya evaluados. 2) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas. 3) Controlar el acceso y las modificaciones al código instalado. 4) Utilizar herramientas para la protección contra la infección del software con código malicioso.

e. Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen puntos específicos tales

como: acuerdos de licencias, propiedad de código y derechos conferidos, Verificación del cumplimiento de las condiciones de seguridad contempladas en requerimientos de seguridad en contratos de tercerización, acuerdos de custodia de las fuentes del software y cualquier otra información requerida en caso de quiebra de la tercera parte.

Toda aplicación generada en el sector de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalen programas fraudulentos. Es conveniente implementar algún software para la administración de versiones y para la transmisión de programas entre los ambientes definidos, con un registro asociado para su control.

A manera de sugerencia se debe adoptar el siguiente modelo formado por tres ambientes que debe ser adaptado a sus características propias, teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

1. Ambiente de Desarrollo Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El analista o programador desarrollador tiene total dominio sobre el ambiente. Puede recibir algún fuente para modificar, quedando registrado en el sistema de control de versiones que administra el "Administrador de programas fuentes".

El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera que el programa está terminado,

lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

2. Ambiente de Pruebas El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto, junto con el usuario de ser posible.

El Testeador realiza las pruebas con los datos de la base de pruebas. Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctos de acuerdo a las especificaciones y considera que la documentación presentada es completa, entonces remite el programa fuente al implementador de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

3. Ambiente de Producción Es donde se ejecutan los sistemas y se encuentran los datos productivos. Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el "Administrador de programas fuentes" y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

El "Implementador" compila el programa fuente dentro del ambiente de producción en el momento de realizar el pasaje para asegurar de esta forma que hay una correspondencia biunívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de programas fuentes.

Deberían aplicarse procedimientos de la misma naturaleza y alcance para las modificaciones de cualquier otro elemento que forme parte del sistema, por ejemplo: modelo de datos de la base de datos o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos, Productos middleware) deberían cumplir idénticos pasos, sólo que las implementaciones las realizarán los propios administradores.

Cabe aclarar que tanto el personal de desarrollo, como el proveedor de los aplicativos, no deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

11. Relaciones con los proveedores

11.1. Generalidades

- Se debe establecer un protocolo de selección, registro, seguimiento a los proveedores externos de la Municipalidad Provincial de Paita, con la finalidad de mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización.

- Los contratistas, proveedores y terceros que tengan acceso a los activos de información están obligados a cumplir las políticas de seguridad de la información.

11.2. Alcance

Esta política se aplica a toda la Municipalidad Provincial de Paita, a sus recursos, activos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

11.3. Responsabilidad

El Oficial de Seguridad de la Información junto con el Propietario de la Información tendrá la responsabilidad de definir los controles a ser implementados en los sistemas desarrollados internamente o Exteriormente por terceros, en función de una evaluación previa de riesgos.

El Responsable de la Subgerencia de Sistemas e Informática, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas. Además podrá otorgar permisos al sistema o base de datos al proveedor monitoreando sus acciones.

El Responsable del Área de Administración incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. El Responsable del Área Legal participará en dicha tarea.

Los contratistas, proveedores y terceros que tengan que realizar labores dentro o fuera de la Municipalidad Provincial de Paita ya sea por medios lógicos o físicos que involucren el manejo de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad de la información.

11.4. Seguridad Frente al Acceso de Terceros

Destinado a garantizar y asegurar protección a los activos de la Municipalidad de Paita que son accesibles por los proveedores. Así mismo; establecer una relación sólida a fin de adoptar un enfoque flexible de colaboración Cliente-Proveedor.

11.4.1. Identificación de Riesgos del Acceso de Terceras Partes

Cuando exista la necesidad de otorgar acceso a terceros respecto a la información de la Municipalidad Provincial de Paita, el Oficial de Seguridad de la Información y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos: a) El tipo de acceso requerido físico/lógico y a qué recurso. b) Los motivos para los cuales se solicita el acceso. c) El valor de la información. d) Los controles empleados por la tercera parte. e) La incidencia de este acceso en la seguridad de la información

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Municipalidad Provincial de Paita, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras

áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

11.4.2. Requerimientos de Seguridad en Contratos o Convenios

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

a. Cumplimiento de la Política de seguridad de la información de la entidad. 1) Protección de los activos de la entidad, incluyendo: Procedimientos para proteger los bienes de la entidad, abarcando los activos físicos, la información y el software; Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos; Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo. 2) Restricciones a la copia y divulgación de información.

b. Descripción de los servicios disponibles.

c. Permiso para la transferencia de personal cuando sea necesario.

d. Nivel de servicio esperado y niveles de servicio aceptables.

e. Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.

f. Existencia de Derechos de Propiedad Intelectual. Y Definiciones relacionadas con la protección de datos.

g. Acuerdos de control de accesos que contemplen: 1) Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios. 2) Proceso de autorización de accesos y privilegios de usuarios. 3) Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

h. Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

i. Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.

j. Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

k. Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

l. Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

m. Proceso claro y detallado de administración de cambios.

n. Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

o. Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

p. Controles que garanticen la protección contra software malicioso.

q. Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

r. Relación entre proveedores y subcontratistas.

11.4.3. Requerimientos de Seguridad en Contratos de Tercerización

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadora de la Municipalidad Provincial de Paita, contemplarán además de los puntos especificados en "Requerimientos de Seguridad en Contratos o Acuerdos con Terceros", los siguientes aspectos:

a. Forma en que se cumplirán los requisitos legales aplicables.

b. Medios para garantizar que todas las partes involucradas

en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.

c. Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible

d. Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.

e. Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.

f. Niveles de seguridad física que se asignarán al equipamiento tercerizado.

g. Derecho a la auditoría por parte de la Municipalidad Provincial de Paita sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad hoc.

Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

11.4.4. Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos: 1) Acuerdos de licencias, propiedad de código y derechos conferidos - Derechos de Propiedad Intelectual. 2) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

3) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc. 4) Verificación del cumplimiento de las condiciones de seguridad contempladas en requerimientos de Seguridad en Contratos de Tercerización. 5) Acuerdos de custodia de las fuentes del software y cualquier otra información requerida en caso de quiebra de la tercera parte.

11.4.5. Términos y Condiciones de contrato

Los términos y condiciones de contrato establecerán la responsabilidad del proveedor en materia de seguridad de la información.

Los derechos y obligaciones del contrato relativos a la seguridad de la información, en relación con las leyes de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones del contrato.

12. Gestión de incidentes de seguridad de la información

12.1. Generalidades

- Se deben establecer procedimientos operativos para gestionar apropiadamente las vulnerabilidades y eventos detectados.

- Todo incidente se seguridad de la información debe ser reportado al Oficial de Seguridad de la Información para su

registro y adecuado tratamiento.

12.2. Alcance

Esta Política se aplica a todos los procesos críticos identificados de la entidad.

12.3. Responsabilidad

- El Oficial de Seguridad de la Información junto con el Propietario de la Información tendrán que definir un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

- El Responsable de la Subgerencia de Sistemas e Informática y el Oficial de Seguridad de la información deberán realizar la evaluación de riesgos debiendo disponer de herramientas de auditoria o utilitarios adecuados para llevar a cabo el control de los registros.

- El Oficial de Seguridad de la Información tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

- Los Propietarios de la Información registrarán aquellos eventos que consideren críticos bajo su responsabilidad.

12.4. Monitoreo del Acceso y Uso de los Sistemas

12.4.1. Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir: a) Identificación del usuario. b) Fecha y hora de inicio y terminación. c) Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma. d) Registros de intentos exitosos y fallidos de acceso al sistema. e) Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.

Los Propietarios de la Información junto con el Oficial de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

12.4.2. Monitoreo del Uso de los Sistemas

a. Procedimientos y Área de Riesgo

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo.

El alcance de estos procedimientos deberá corresponder a la evaluación de riesgos que realice el Responsable de la Subgerencia de Sistemas e Informática y el Oficial de Seguridad de la Información.

Las actividades que pueden ser objeto de control y monitoreo son las siguientes:

1. Acceso no autorizado, incluyendo detalles como: a) Identificación del usuario. b) Fecha y hora de eventos clave. c) Tipos de eventos. d) Archivos a los que se accede. e) Utilitarios y programas utilizados.

2. Todas las operaciones con privilegio, como: a) Utilización de cuenta de supervisor. b) Inicio y cierre del sistema. c) Conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos. d) Cambio de fecha/hora. e) Cambios en la configuración de la seguridad. f) Alta de servicios.

3. Intentos de acceso no autorizado, como: a) Intentos fallidos. b) Violaciones de la Política de Accesos y notificaciones para "gateways" de red y "firewalls". c) Alertas de sistemas de detección de intrusiones.

4. Alertas o fallas de sistema como: a) Alertas o mensajes de consola. b) Excepciones del sistema de registro. c) Alarmas del sistema de administración de redes. d)

Accesos remotos a los sistemas.

b. Procedimientos y Área de Riesgo

Los factores de riesgo que se deben considerar son los siguientes: 1) La criticidad de los procesos de aplicaciones. 2) El valor, la sensibilidad o criticidad de la información involucrada. 3) La experiencia acumulada en materia de infiltración y uso inadecuado del sistema. 4) El alcance de la interconexión del sistema en particular las redes públicas.

Los Propietarios de la información registraran aquellos eventos que consideren críticos para la operatividad sus actividades bajo su responsabilidad.

c. Registro y Revisión de Eventos

El Oficial de Seguridad de la Información en conjunto con el especialista de la Seguridad de la Información, implementarán un procedimiento de registro y revisión de los archivos de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados, La periodicidad de dichas revisiones será definida por los Propietarios de la Información y el Oficial de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.

Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuales de los registros más significativos se copiarán automáticamente en registros auxiliares.

Por otra parte, el Responsable de la Subgerencia de Sistemas e Informática, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control de los registros.

En la asignación de funciones en materia de seguridad de la información, se deberá separar las funciones entre quienes realizan la revisión y aquellos cuyas actividades están siendo monitoreadas.

Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de garantizar que no ocurra son: 1) La desactivación de la herramienta de registro. 2) La alteración de mensajes registrados. 3) La edición o supresión de archivos de registro. 4) La saturación de un medio de soporte de archivos de registro. 5) La falla en los registros de los eventos. 6) La sobre escritura de los registros.

El Oficial de Seguridad de la Información podrá efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

12.4.3. Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes. Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

13. Gestión de la continuidad del negocio.

13.1. Generalidades

- Se debe considerar aspectos necesarios para el tratamiento de los riesgos de continuidad del Negocio que debe involucrar todos los niveles de la Municipalidad Provincial de Paita.

- Se debe contar con planes de continuidad operativa y contingencia que cubran los recursos informáticos e infraestructura tecnológicas.

- Dicho plan debe mantenerse actualizado y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades de la entidad y asegurar la reanudación oportuna de las operaciones indispensables.

13.2 Alcance

Esta Política se aplica a todos los procesos críticos identificados de la entidad.

13.3. Política de Gestión de Continuidad

13.3.1. Administración de la Continuidad del Organismo

El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la Municipalidad Provincial de Paita.

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la entidad frente a interrupciones imprevistas, lo cual incluye las siguientes funciones: a) Identificar y priorizar los procesos críticos de las actividades de la entidad. b) Asegurar que todos los integrantes de la entidad comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de la entidad. c) Elaborar y documentar una estrategia de continuidad de las actividades de la entidad consecuente con los objetivos y prioridades acordados. d) Proponer medidas de reducción de los riesgos en las actividades de la entidad de conformidad con la estrategia de continuidad acordada. e) Establecer un cronograma de pruebas periódicas, proponiendo una asignación de funciones para su cumplimiento. f) Coordinar actualizaciones periódicas del plan y procesos implementados. g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la entidad. h) Proponer las modificaciones al Plan de Seguridad y Continuidad de Tecnología de la Información.

13.3.2. Continuidad de las Actividades y Análisis de los Impactos

Con el fin de establecer el Plan de Seguridad y Continuidad de las Actividades de la entidad se deben contemplar los siguientes puntos: a) Identificar los riesgos que puedan ocasionar interrupciones en los procesos de

las actividades, como fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc. b) Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación. c) Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de la Información, Usuarios de la Información de que se trate, el Oficial de la Seguridad de la Información y el Responsable de la Subgerencia de Sistemas e Informática, considerando todos los procesos de las actividades de la entidad y no limitándose a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación de esta actividad, se desarrollará el Plan de Seguridad y Continuidad de Tecnología de la Información para determinar el enfoque global con el que se abordará la continuidad de las actividades de la Municipalidad. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la máxima autoridad de la

Municipalidad de Paita para su aprobación.

13.3.3. Elaboración e Implementación del Plan de Seguridad y Continuidad de Tecnología de la Información

Los propietarios de la Información y Usuarios de la información, con la asistencia del Oficial de la Seguridad de la Información y el Subgerente de Sistemas e Informática, elaborarán el Plan de Seguridad y Continuidad de Tecnología de la Información necesario para garantizar la continuidad de las actividades de la Municipalidad Provincial de Paita.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos: a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia. b) Analizar los posibles escenarios de contingencia y definir las medidas de reducción a implementar en cada caso. c) Implementar procedimientos de emergencia o medidas de contingencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes. d) Documentar los procedimientos y procesos acordados. e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis. f) Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas: 1. Objetivo del plan. 2. Mecanismos de coordinación y comunicación entre equipos personal

involucrado. 3. Procedimientos de divulgación. 4. Requisitos de la seguridad. 5. Procesos específicos para el personal involucrado. 6. Responsabilidades Individuales. g) Probar y actualizar los planes.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades de la entidad requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

13.3.4. Marco para la Planificación de la Continuidad de las Actividades de la entidad

Se mantendrá un solo marco para el Plan de Seguridad y Continuidad de las actividades de la Municipalidad de Paita, a fin de garantizar que sea uniforme e identificar prioridades de prueba y mantenimiento.

El Plan de Seguridad y Continuidad de Tecnología de la Información especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, tales como los planes de evacuación o los recursos de emergencia existentes.

Estas modificaciones deberán ser propuestas por el Comité de Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad de las actividades de la Municipalidad de Paita, tendrá en cuenta los siguientes puntos: a) Prever las condiciones de implementación del plan que describa el proceso a seguir cómo evaluar la situación, qué personas estarán involucradas, etc. antes de poner en marcha los mismos. b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones de Tecnología de la Información de la entidad y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales. c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de la entidad o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos. d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la entidad. e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo. f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo

eficaces. g) Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones del plan de continuidad, debe ser considerado entre las responsabilidades del Oficial de seguridad de la información. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

13.3.5. Ensayo, Mantenimiento y Reevaluación del Plan de Seguridad y Continuidad de Tecnología de la Información.

Debido a que el Plan de Seguridad y Continuidad de Tecnología de la Información de la Municipalidad Provincial de Paita puede fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción: a) El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas del Plan de Seguridad y Continuidad de Tecnología de la Información. b) El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado comité.

Se deberán utilizar diversas técnicas para garantizar que el Plan de Seguridad y Continuidad de Tecnología de la Información funcionará ante un hecho real, y éstas incluirán por lo menos: a) Efectuar pruebas de discusión de diversos escenarios discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones. b) Realizar simulaciones especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis. c) Efectuar pruebas de recuperación técnica garantizando que los sistemas de información puedan ser restablecidos con eficacia. d) Realizar ensayos completos probando que la entidad, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas de la entidad se tomarán en cuenta, además, los siguientes mecanismos: a) Efectuar pruebas de recuperación en un sitio alternativo ejecutando los procesos de las actividades de la entidad en paralelo, con operaciones de recuperación fuera del sitio principal. b) Realizar pruebas de instalaciones y servicios de proveedores garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos.

El Plan de Seguridad y Continuidad de Tecnología de la Información de la entidad será revisado y actualizado periódicamente cada seis meses, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios de la entidad para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

Cada uno de los Responsables de Procesos es el responsable de las revisiones periódicas del Plan de Seguridad y Continuidad de Tecnología de la Información en los aspectos de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades de la entidad aún no reflejadas en dicho plan.

Deberá prestarse atención, especialmente, a los cambios de: personal; direcciones o números telefónicos; estrategia de la entidad; ubicación, instalaciones y recursos; legislación; contratistas, proveedores y contribuyentes críticos; procesos, o procesos nuevos / eliminados; tecnologías; requisitos operacionales; requisitos de seguridad; hardware, software y otros equipos tipos, especificaciones, y cantidad; requerimientos de los sitios alternativos y registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el Comité de Seguridad de la Información para su aprobación por el superior jerárquico que corresponda. Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el personal involucrado tenga conocimiento de los cambios incorporados.

14. Cumplimiento

14.1. Generalidades

- Se deben establecer mecanismos para garantizar el cumplimiento de las normas en materia de seguridad de la información.

- El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

- Los requisitos normativos y contractuales pertinentes a cada sistema de información estarán debidamente definidos y documentados.

- El Área Legal, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

14.2. Alcance

Esta política se aplica a todo el personal de la Municipalidad Provincial de Paita, cualquiera sea su situación contractual. Asimismo se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas de la entidad y a las auditorías efectuadas sobre los mismos.

14.3. Responsabilidad

El Oficial de la Seguridad de la Información cumplirá las siguientes funciones: a) Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros. b) Realizar revisiones periódicas de todas las áreas de la Municipalidad a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. c) Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos. d) Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

El Responsable del Área Legal, con la asistencia del Oficial de la Seguridad de la Información, cumplirá las siguientes funciones: a) Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. b) Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Los Responsables de las unidades orgánicas velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente política, dentro de su área de responsabilidad.

Todos los empleados de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente política y la normativa vigente.

14.4. Cumplimiento de Requisitos Legales

14.4.1. Identificación de la Legislación Aplicable

Todos los requisitos normativos y contractuales pertinentes para cada sistema de información serán definidos y documentados claramente. Todos los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos, serán igualmente definidos y documentados.

14.4.2. Derechos de Propiedad Intelectual

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual, mediante la implementación de procedimientos adecuados. Los empleados únicamente podrán utilizar

material autorizado por la Municipalidad Provincial de Paita.

La entidad solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Se deberán tener presente la ley de Propiedad Intelectual: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

14.4.3. Derecho de Propiedad Intelectual del Software

El software es considerado una obra intelectual que goza de la protección de la Ley de Propiedad Intelectual. La ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción.

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El Oficial de la Seguridad de la Información, con la asistencia del Área Legal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles: a) Normas

y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software. b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja. c) Mantener un adecuado registro de activos. d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc. e) Implementar controles para evitar el exceso del número máximo permitido de usuarios. f) Verificar que sólo se instalen productos con licencia y software autorizado. g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias. h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros. i) Utilizar herramientas de auditoría adecuadas. j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

14.4.4. Protección de los Registros de la Municipalidad Provincial de Paita

Los registros críticos de la Municipalidad Provincial de Paita se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la entidad.

Los registros se clasificarán en diferentes tipos, tales como registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos

detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, microformas, medios magnéticos u ópticos.

Las claves criptográficas asociadas con archivos cifrados se mantendrán en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario.

Se considerara la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante.

Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos tanto legibilidad de formato como medios durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia.

El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal o normativa. Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para la entidad.

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas: a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información. b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos. c) Mantener un inventario de programas fuentes de información clave. d) Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

En particular, se deberán tener presente las siguientes normas:

- Ley Marco del Empleo Público Ley 28175 Artículo 16 Inc. f) Obliga a todo empleado a actuar con transparencia en el ejercicio de su función y guardar secreto y/o reserva de la información pública calificada como tal por las normas sobre la materia y sobre aquellas que afecten derechos fundamentales.

- Ética en el Ejercicio de la Función Pública: Obliga a todas las personas que se desempeñen en la función pública a abstenerse de utilizar información adquirida en el cumplimiento de sus funciones para realizar actividades no relacionadas con sus tareas oficiales o de permitir su uso en beneficio de intereses privados.

- Código de Ética de la Función Pública: Establece que el funcionario público debe abstenerse de difundir toda información que hubiera sido calificada como reservada o secreta conforme a las disposiciones vigentes, ni la debe

utilizar, en beneficio propio o de terceros o para fines ajenos al servicio, información de la que tenga conocimiento con motivo o en ocasión del ejercicio de sus funciones y que no esté destinada al público en general.

- Decreto Legislativo Nº 635 Código Penal : Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial.

- Ley N° 30096, publicada el 22 octubre 2013 Ley de Delitos Informáticos: previene y sanciona las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidos mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia, esta ley se encuentra tipificado los delitos de Atentado a la integridad de datos informáticos, Tráfico ilegal de datos, Interceptación de datos informáticos, entre otras.

- Delito de Violación a la Intimidad.- Art. 154 del Código Penal.

- Delito de Hurto agravado por Transferencia Electrónica de Fondos, telemática en general y empleo de claves secretas.- Arts. 185 y 186 del Código Penal.

- Delito de Falsificación de Documentos Informáticos. - Artículo 19 del Decreto Legislativo 681 modificado por la

Ley 26612 - Norma que regula el valor probatorio del documento informático.

- Delitos contra la fe pública, que son aplicables a la falsificación y adulteración de microformas digitales tenemos los siguientes: 1) Falsificación de documentos. Art. 427. 2) Falsedad ideológica. Artículo 428. 3) Omisión de declaración que debe constar en el documento. Artículo 429. 4) Delito de Fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos Artículo 198º inciso 8. 5) Delito contra los derechos de autor de software. Decreto Legislativo Nº 822, modificó el Código Penal: Arts. 217, 218, 219 y 220.

- Ley de Propiedad Intelectual Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo las compilaciones de datos o de otros materiales.

- Ley 29733 Ley de Protección de Datos Personales. El tratamiento de datos personales deberá realizarse con pleno respeto de los derechos fundamentales de sus titulares, garantizándose principalmente el derecho fundamental a la protección de los datos personales previsto en la Constitución Política del Perú, en un marco de los demás derechos fundamentales que en ella se reconocen. Refiere que sólo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. En este último caso, precisa la ley, el consentimiento debe ser previo, informado, expreso e inequívoco, y en el caso de datos sensibles, el consentimiento para efectos de su tratamiento debe efectuarse por escrito.

14.4.5. Protección de Datos y Privacidad de la Información Personal

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

La Municipalidad Provincial de Paita redactará un "Compromiso de Confidencialidad", el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por la entidad.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. A través del "Compromiso de Confidencialidad" se deberá advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

En particular, se deberán tener presente las siguientes normas:

- Ley 29733 Ley de Protección de Datos Personales. El tratamiento de datos personales deberá realizarse con pleno respeto de los derechos fundamentales de sus titulares, garantizándose principalmente el derecho fundamental a la protección de los datos personales

previsto en la Constitución Política del Perú, en un marco de los demás derechos fundamentales que en ella se reconocen. Refiere que sólo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. En este último caso, precisa la ley, el consentimiento debe ser previo, informado, expreso e inequívoco, y en el caso de datos sensibles, el consentimiento para efectos de su tratamiento debe efectuarse por escrito.

- Confidencialidad. Impide la divulgación a terceros, o su utilización sin previo consentimiento y de manera contraria a los usos comerciales honestos, de información secreta y con valor comercial que haya sido objeto de medidas razonables para mantenerla secreta.

- Código Penal: Revelación de la intimidad el Art.156 sanciona a aquel que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa.

- Código Penal: Uso indebido de archivos computarizados el Art.157 sanciona al funcionario público que indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas.

- Ley Marco del Empleo Público Ley 28175 Artículo 16 Inc f) Obliga a todo empleado a actuar con transparencia en el ejercicio de su función y guardar secreto y/o reserva de la información pública calificada como tal por las normas sobre la materia y sobre aquellas que afecten derechos fundamentales.

Asimismo, deberá considerarse lo establecido en el Decreto, que regula el acceso a la información pública por parte de los ciudadanos.

14.4.6. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información de la entidad se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

En particular, se debe respetar lo dispuesto por las siguientes normas:

- Ley Marco del Empleo Público: Salvaguardar los intereses del Estado y emplear austeramente los recursos públicos, destinándolos sólo para la prestación del servicio público.

- Código de Ética de la Función Pública: Obliga a las personas que se desempeñen en la función pública a guardar reserva respecto de hechos o informaciones de los que tenga conocimiento.

14.4.7. Regulación de Control para Uso de Criptografía

Al utilizar firmas digitales o electrónicas, se deberá considerar lo dispuesto por la Ley y su decreto reglamentario, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

Se debe obtener asesoramiento antes de transferir a otro país información cifrada o controles criptográficos. Para ello se puede consultar a la Dirección de Política y Estrategia de Seguridad y Defensa Nacional de la Dirección General de Política y Estrategia del Ministerio de Defensa, a fin de saber si el material exportable requiere algún tratamiento especial.

14.4.8. Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, la entidad garantizará que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones: a) Almacenar los

documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados. b) Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal por lo tanto se deben tomar todos los recaudos establecidos para la obtención y preservación de la evidencia.

i. Responsabilidades

Tabla Nº 53: Cuadro de Responsabilidades Propuesto

Elaboración	Conformidad	Aprobación	Aplicación	Verifica Cumplimiento	Distribución
Subgerente de Sistemas e Informática	Gerente Municipal	Alcaldía	Todo el Personal	Oficina de Control Institucional	Secretaria General

Fuente: Modelo de Plantilla aprobado por la ONGEI (61).

j. Disposiciones Complementarias

- El incumplimiento a la presente directiva dará lugar a las correspondientes sanciones administrativas, independientemente de las sanciones civiles y/o penales a las que dé lugar.

k. Definiciones

1. **Información.-** Se refiere a toda comunicación o representación de conocimiento en cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

2. **Activo.-** En el contexto de seguridad de la información se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Se pueden clasificar en: Activos de información (datos, manuales de usuario, entre otros), Documentos en papel (contratos), Activos de Software (aplicación, software de sistemas, entre otros), Activos físicos (computadoras, servidores, medios magnéticos, enrutadores, entre otros), Personal (estudiantes, clientes, empleados, entre otros). Imagen de la compañía y reputación – Servicios (comunicaciones, entre otros).

3. **Seguridad de la Información.-** Característica de la información que ese logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla con los criterios de confidencialidad, integridad y disponibilidad, definidos de la siguiente manera:

   - **Confidencialidad**: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.

   - **Integridad**: La información debe ser completa, exacta y válida.

   - **Disponibilidad**: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

4. **Incidente.-** Un incidente de seguridad de información es definido por uno o una serie de eventos inesperados y no deseados que tienen una alta probabilidad de comprometer las operaciones de la organización y de amenazar la seguridad de la información.

5. **Riesgo.-** La condición en que existe la posibilidad que un evento ocurra e impacte negativamente sobre los objetivos de la Municipalidad Provincial de Paita.

l. Anexos

- Sin Anexos.

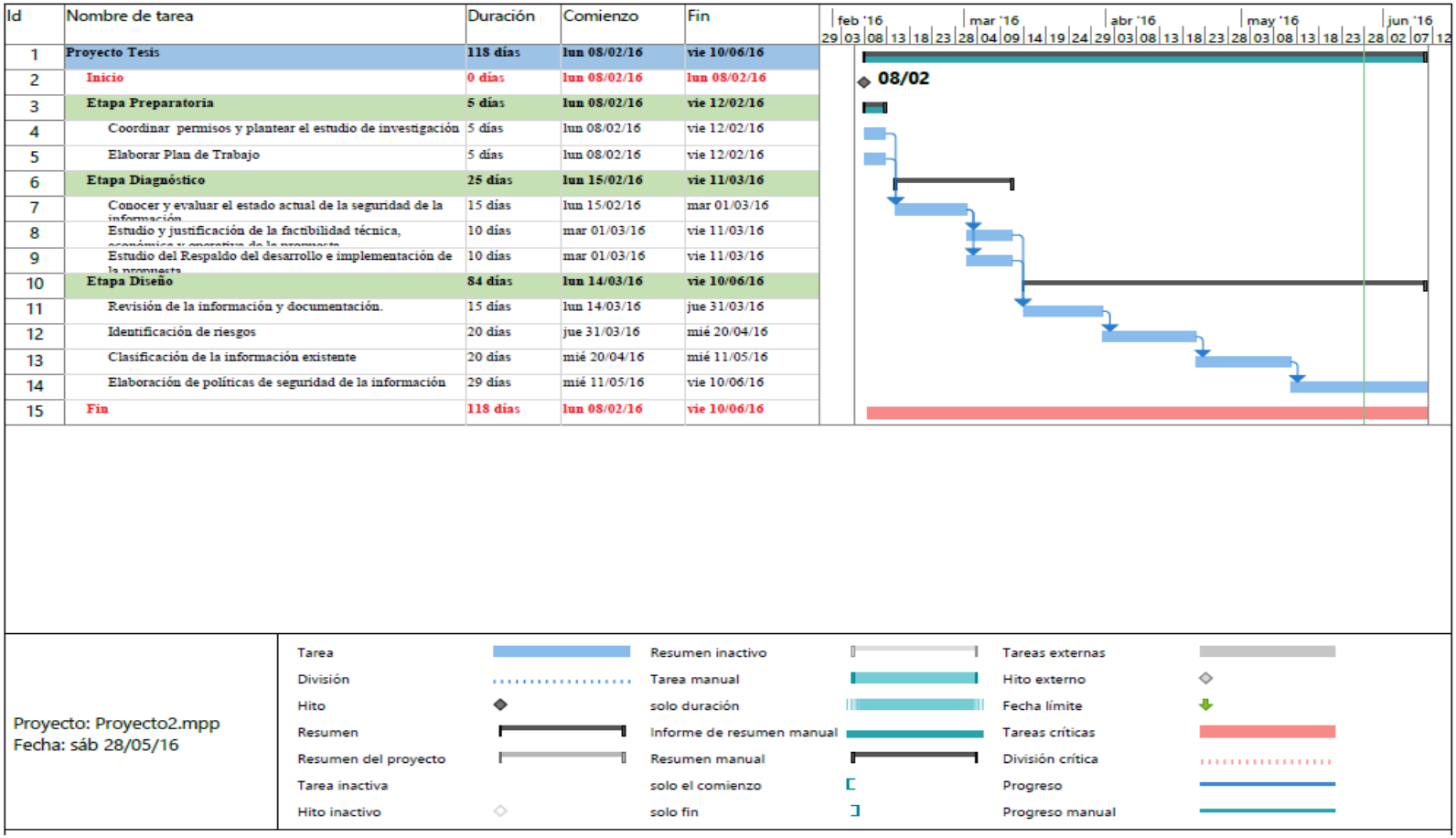
m. Conformidad

Tabla Nº 54: Cuadro de conformidad y aprobación del proyecto

Unidad Orgánica	Nombre	Sello y Firma
Gerencia Municipal		
Subgerencia de Sistemas e Informática		

Fuente: Modelo de Plantilla aprobado por la ONGEI (61).

4.3.2. Diagrama de Gantt para el diseño de la propuesta



Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Proyecto Tesis**	**118 días**	**lun 08/02/16**	**vie 10/06/16**
2	**Inicio**	**0 días**	**lun 08/02/16**	**lun 08/02/16**
3	**Etapa Preparatoria**	**5 días**	**lun 08/02/16**	**vie 12/02/16**
4	Coordinar permisos y plantear el estudio de investigación	5 días	lun 08/02/16	vie 12/02/16
5	Elaborar Plan de Trabajo	5 días	lun 08/02/16	vie 12/02/16
6	**Etapa Diagnóstico**	**25 días**	**lun 15/02/16**	**vie 11/03/16**
7	Conocer y evaluar el estado actual de la seguridad de la información	15 días	lun 15/02/16	mar 01/03/16
8	Estudio y justificación de la factibilidad técnica, económica y operativa de la propuesta	10 días	mar 01/03/16	vie 11/03/16
9	Estudio del Respaldo del desarrollo e implementación de la propuesta	10 días	mar 01/03/16	vie 11/03/16
10	**Etapa Diseño**	**84 días**	**lun 14/03/16**	**vie 10/06/16**
11	Revisión de la información y documentación.	15 días	lun 14/03/16	jue 31/03/16
12	Identificación de riesgos	20 días	jue 31/03/16	mié 20/04/16
13	Clasificación de la información existente	20 días	mié 20/04/16	mié 11/05/16
14	Elaboración de políticas de seguridad de la información	29 días	mié 11/05/16	vie 10/06/16
15	**Fin**	**118 días**	**lun 08/02/16**	**vie 10/06/16**

Imagen elaborada con Software licenciado "Proyect 2013"

4.3.3. Presupuesto del diseño de la propuesta

Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información

Principales Rubros	Acciones necesarias para lograr cada resultado	U.M.	Cantidad	Costo Unitario S/.	Costo Total a Precios de Mercado S/.
Expediente Técnico		Estudio	1	3,000.00	3,000.00
Costo Directo					17,000.00
Resultado 1: Clasificación de la Información existente	- Revisión de la información y documentación. - Identificación de riesgos. - Clasificación de la información existente. - Elaboración de políticas de seguridad de la información	Global	1	13,000.00	13,000.00
Supervisión		Global	1	1,500.00	1,500.00
Gastos Generales		Global	1	2,500.00	2,500.00
Total S/.					20,000.00

Fuente: elaboración propia tomando como referencia el (Código SNIP: 268985)

V. CONCLUSIONES

Según los resultados obtenidos en esta investigación, se concluye que: la Municipalidad Provincial de Paita carece de políticas y controles eficientes en cuanto a la protección de los activos de la información (los servidores públicos y/o contratistas, la creación de información, los procesos, las tecnologías de información incluido el hardware y el software y las instalaciones), por esta razón si resulta beneficioso el diseño e implementación de la propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016, el mismo que permitirá minimizar la pérdida de información, con lo que queda demostrado que la hipótesis general es aceptada.

También se concluyó que:

1. En la Tabla Nº 43 se puede observar que el 72.37% de los empleados municipales encuestados opinan que SI se encuentran expuestos a riesgos y amenazas debiendo disponer urgente de un plan de gestión de seguridad de la información, este resultado coincide con el indicado en la hipótesis especifica que indicaba que la evaluación de la situación actual de los procesos de seguridad en la Municipalidad Provincial de Paita, en el año 2016; permitirá identificar las falencias de seguridad de la información por lo que se concluye que la hipótesis planteada queda aceptada.

2. En la Tabla Nº 44 se puede observar que el 100.00% de los empleados municipales encuestados opinan que SI existe factibilidad técnica, económica y operativa de la propuesta puesto que la norma es de carácter obligatoria en todas las entidades del estado la cual justifica la vialidad técnica. La factibilidad económica de esta propuesta también está garantizada ya que la municipalidad tiene conocimiento de los beneficios para salvaguardar la seguridad de la información por lo tanto aprueba la elaboración del diseño del plan de seguridad de la información. La factibilidad operativa está garantizada porque existe

buena disposición por parte de la Municipalidad para mejorar la seguridad a fin de minimizar riesgos de pérdida de información, así mismo existe buena disposición por parte del personal de la Sub Gerencia de Sistemas e Informática para recibir capacitación en aspectos de seguridad informática, este resultado coincide con el indicado en la hipótesis especifica que indicaba que la inseguridad de la información existente en la Municipalidad Provincial de Paita, en el año 2016; justificará la factibilidad técnica, la inversión económica y operativa para el desarrollo de la propuesta, basadas en buenas prácticas, para la gestión de seguridad de la información por lo que se concluye que la hipótesis planteada queda aceptada.

3. En la Tabla Nº 45 se puede observar que el 100.00% de los empleados municipales encuestados opinaron que NO existen controles pertinentes en cuanto a la seguridad de la información, por lo tanto queda demostrado que es necesario la elaboración de una propuesta de plan de gestión de seguridad de la información, ya que ella permitirá brindar un esquema de seguridad más sólido y eficiente en el manejo de los sistemas de información, este resultado coincide con el indicado en la hipótesis especifica que indicaba que la necesidad de una eficiente propuesta de políticas basadas, en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita, en el año 2016; respalda el desarrollo e implementación de la propuesta por lo que se concluye que la hipótesis planteada queda aceptada.

VI. RECOMENDACIONES

1. Se sugiere que la Municipalidad Provincial de Paita nombre al equipo de trabajo denominado Comité de Seguridad de la Información (CSI) para que pueda iniciar sus funciones y distribuir responsabilidades en forma adecuada, las mismas que tienen por finalidad aprobar, implementar, divulgar y controlar la implementación de la propuesta de políticas basadas, en buenas prácticas, para la gestión de seguridad de la información.

2. Se propone que la Municipalidad Provincial de Paita estructure adecuadamente la Subgerencia de Sistemas e Informática a la categoría organizacional de Gerencia de Tecnologías y Sistemas de Información cuyas funciones deberían estar desagregadas a cada oficina o Subgerencia especializada las cuales se encargarían de desarrollar cada una sus funciones específicas para que pueda lograr una mejor coherencia funcional por constituirse en una pieza clave para el desarrollo organizacional en todas las áreas administrativas y más aún, en la implementación de la propuesta de seguridad de la información.

3. Se aconseja que la Municipalidad Provincial de Paita asigne un presupuesto orientado a la implementación de la plataforma tecnológica y de los controles del sistema de gestión de la seguridad de la información, capacitaciones y charlas de concientización, servicios de consultoría y revisiones anuales, para que se pueda asegurar la continuidad de la política de seguridad de la información hay que tener en cuenta que los directivos debe conocer que lo que se invierte en el mismo no es un gasto, más bien es una inversión.

4. Se plantea que la Municipalidad Provincial de Paita establezca un plan de capacitaciones en temas relacionados con la seguridad de la información para que los funcionarios adquieran competencias y destrezas en el uso adecuado de la misma, de igual forma incluir en el proceso de inducción, la socialización de las políticas de seguridad de la información.

5. Se sugiere que una vez culminada la socialización de las normas el funcionario o aspirante al puesto de trabajo firme el documento de divulgación donde debe expresarse que conoce las reglas de confidencialidad y buenas prácticas en el manejo integral de la información, para que sus acciones contribuyan al logro de objetivos por área y al cumplimiento de metas organizacionales.

REFERENCIAS BIBLIOGRÁFICAS

1. Medrano S. Apeisc.org - Seguridad de la Información. [Online].; 2016 [cited 2016 Abril 24. Available from: http://www.apeisc.org/seguridad-de-la-informacion/seguridad-de-la-informacion/.
2. Roldan J. blog.mp3.es. [Online].; 2016 [cited 2016 Abril 22. Available from: http://blog.mp3.es/alerta-digital-la-seguridad-informatica-en-2013-infografia/.
3. Gestión Técnologica y de la Información - Adm. Central del Municipio de Santiago de Cali. Politica de Seguidad de la Información. In ; 2014; Santiago de Cali. p. 5.
4. América Sistemas. América Sistemas Noticiero Digital Nº 790. [Online]. Lima; 2015 [cited 2016 Marzo 18. Available from: http://www.americasistemas.com.pe/especialistas-debaten-sobre-gestion-de-las-vulnerabilidades-en-entornos-corporativos/.
5. Ministerio de Economía y Finanzas. Politica de Seguridad de la Información del Ministerio de Economía y Finanzas. Resolucion Ministerial. Lima: MEF; 2014.
6. Olaya García, Victor; Imagen Institucional MPP. Importancia de la Autonomía Municipal. Boletín "El Ciudadano" Nº 7. 2007 Noviembre.
7. Cruz B. Paita Virtual. [Online].; 2014 [cited 2016 Abril 20. Available from: http://paitavirtual.com/prensa/?p=157.
8. Municipalidad Provincial de Paita. Reglamento de Organización de Funciones - ROF. Manual de referencia. PAITA:; 2011.
9. Oficina Nacional de Gobierno Electrónico e Informática - ONGEI. Estrategia Nacional de Gobierno Electrónico 2013 - 2017. 2012.
10. Presidencia del Consejo de Ministros. Ley Nº 27658 "Ley Marco de Modernización de la Gestión del Estado. Normas Legales - Diario Oficial El Peruano. 2002 Enero: p. 6.
11. Presidencia del Consejo de Ministros. Resolución Ministerial Nº 004-2016-PCM - Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. 2a. Edición". Normas Legales - El Peruano. 2016 Enero: p. 2.

12. López A. Diseño de un Plan de Gestión de Seguridad de la Información. Caso: Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara. Tesis Post-grado. Barquisimeto: Univeridad Centroccidental "Lisandro Alvarado" - Venezuela, Ciencias y Tecnologías; 2011.
13. Barragán I, Góngora I, Martínez E. Implementación de Politicas de Seguridad Informática para la M.I. Municipalidad de Guayaquil aplicando la Norma ISO/IEC 27002. Tesis de Grado. Guayaquil: Escuela de Diseño y Comunicación Visual, Analisis de Sistemas; 2011.
14. Sanchez Arias K. Diseño de Políticas de Seguridad de Información para la Alcaldía Municipal de Rio de Oro, Cesar. Tesis de Grado. Ocaña: Universidad Francisco de Paula Santander Ocaña, Facultad de Ingenierias; 2014.
15. De La Cruz CW, Vasquez JC. Elaboración y Aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad tecnológica de la USAT. Tesis de Grado. Trujillo: Universidad Católica Santo Toribio, Ingeniería de Sistemas y Computación; 2008.
16. Aguirre Mollehuanca DA. Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A. Tesis de Grado. Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería; 2014.
17. Talavera Alvarez VR. Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de acuerdo a la ISO/IEC 27001:2013. Tesis de Grado. Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería; 2015.
18. Congreso Constituyente Democrático. Constitución Política del Perú. In Oficialía Mayor del Congreso; 1993; Lima. p. 60.
19. Quiñones Li A, Lozano I, Cucho M, Tello Rozas P, Acuña R. Perú: Metodología para el diseño de una planificación estrategica interrelacionada con la Administración Presupuestaria en las entidades del sector público caso: "RENIEC". Tesina Master a Distancia. España - Perú: Universidad Nacional de Educación a Distancia, Gerencia Pública para Directivos Iberoamericanos; 2010.
20. García Riega AJ. Organización Municipal. Lima: Contraloría General de la República, Escuela Nacional de Control; 2010.

21. Acosta D. Las Municipalidades y Los Gobiernos Regionales Acosta D, editor. Lima: Instituto de Investigación y Capacitación Municipal - INICAM; 1988.
22. Congreso de la República. Ley de Bases de la Descentralización, Ley 27783. Diario de los Debates - Segunda Legislatura Ordinaria. 2002 Junio.
23. Toledo P. La Autonomía Municipal: ¿Una utopía? Temas de Gestión Pública y Actualidad. 2008 Mayo.
24. Instituto nacional de Estadística e Informática. Directorio Nacional de Municipalidades Provinciales, Distritales y de Centros Poblados 2015 Lima: Talleres de la Oficina de Impresiones del Instituto nacional de Estadística e Informática; 2015.
25. Municipalidad Provincial de Paita. munipaita.gob.pe. [Online]. Paita; 2015 [cited 2016 Marzo 3. Available from: http://munipaita.gob.pe/portal/.
26. Subgerencia de Desarrollo Institucional. Organigrama de la Subgerencia de Sistemas e Informática de la Municipalidad de Paita. 2011.
27. Subgerencia de Sistemas e Informática de la Municipalidad de Paita. Analisis Estrategico de la Subgerencia de Sistemas e Informática. 2015.
28. Quiñones Y. Blog Las TIC en el mundo empresarial. [Online].; 2015 [cited 2016 Abril 20. Available from: http://mundoempresarialtic.blogspot.pe/2015/03/importancia-de-las-ticen-las-empresas.html.
29. Ministerio de Economía y Finanzas. Portal del Ministerio de Economía y Finanzas. [Online].; 2016 [cited 2016 Mayo 04. Available from: http://www.mef.gob.pe/index.php?option=com_content&view=article&id=2028&%20Itemid=101421.
30. Ministerio de Economía y Finanzas. Concepto de SIAF. 2010.
31. Ministerio de Economía y Finanzas. Exposicion del Sistema Integrado de Gestión Administrativa SIGA. 2010.
32. Subgerencia de Sistemas e Informática de la Municipalidad de Paita. Inventario de Infraestructura Técnologica y Sistemas Informáticos. 2016.
33. Ruiz Inga F. Manual de Usuario SGTM. 2012.

34. Paucarmayta V. MIM al Día 04. MIM Perú Promoviendo el Buen Gobierno Municipal. 2014 Enero; 04.
35. Mercado Lorberg I. Diferencias conceptuales entre TICs Vs. NTICs. In. p. 2.
36. Castejón L, Feijoo C, Ortega V, Peréz J. Introducción a la Ingeniería. Madrid: Unversidad Politécnica de Madrid, Departamento de Señales, Sistemas y Radiocomunicaciones ; 2005.
37. Milena Bonilla F. sites.google.com. [Online].; 2012 [cited 2016 Mayo 07. Available from: https://sites.google.com/site/ticsyopal5/assignments/homeworkforweekofoctober18th.
38. Cerón DX. es.slideshare.net/. [Online].; 2011 [cited 2016 Abril 21. Available from: http://es.slideshare.net/dianaxice/desarrollo-de-las-tics-9344935.
39. Duncombe R, Heeks R. Información Tecnología y la Pequeña Empresa. Una Guia para agencias de cooperación con las empresas en los países en desarrollo. In IDPM, University of Manchester; 2003; Reino Unido. p. 36.
40. Villafuerte Quiroga D. Estudio de diagnóstico de información y comunicación en la Provincia de San Pablo. Estudio de Diagnóstico. Lima: Soluciones Practicas ITDG; 2009.
41. yovera Aliaga A. Importancia de las Normas Técnicas Peruanas. 2010.
42. Comisión de Reglamentos Técnicos y Comerciales - INDECOPI. Norma Técnica Peruana NTP-ISO/IEC 17799:2007 "EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da. Edición. In ; 2007; Lima. p. 173.
43. Peltier T, Peltier J, Blackley J. Information Security Fundamentals USA: Auerbach Publications; 2004.
44. BSI. BSIGroup.Com. [Online].; 2013 [cited 2016 Abril 10. Available from: http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/De-un-vistazo/Que-son-los-sistemas-de-gestion/.
45. ISO 27001. Portal de ISO 27001 en español. [Online]. [cited 2016 Marzo 27. Available from: http:/www.iso27000.es/iso27000.html.

46. Frayssinet Delgado, Maurice; Oficina Nacional de gobierno Electrónico e Informática. Taller de Implementación de la Norma ISO 27001. 2014 Mayo 27.
47. Halvorson N. "Information Risk Management: A Process Approach to Risk Diagnosis and treatment". Information Security Management handbook. 6th ed. USA: Auerbach Publications; 2008.
48. Ozier W. "Risk Analysis and Assessment" Information Security Management Handbook. 5th ed. USA.: Auerbach; 2004.
49. Núñez Ponce J. julionunezderechoinformatico.blogspot.pe. [Online]. Lima; 2016 [cited 2016 Marzo 1. Available from: http://julionunezderechoinformatico.blogspot.pe/2016/01/norma-tecnica-de-gestion-de-seguridad.html.
50. Reátegui Morales, Juan Carlos; FONCODES. Taller Seguridad Información ISO 27001:2014. 2015.
51. Sandoval Vargas CA. Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa. Tesis de Grado. Guayaquil: Universidad Católica de Santiago de Guayaquil, Sistema de Posgrado ; 2014.
52. Barrantes Porras CE, Hugo Herrera JR. Diseño e Implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos. Tesis de Grado. Lima: Universidad San Matin de Porres, Escuela Profesional de Ingeniería de Computación y Sistemas; 2012.
53. Alvarez JC. Tipos y Niveles de Investigación.
54. Grajales T. Tipos de Investigación. 2000.
55. Tamayo y Tamayo M. El proceso de la Investigación Científica Editores GN, editor. México: Limusa S.A; 2002.
56. RAE. Diccionario de la Lengua Española. Diccionario de la Lengua Española. [Online].; 2012 [cited 2016 Mayo 09. Available from: http://lema.rae.es/drae/srv/search?key=muestra.
57. Hernández Sampieri R, Fernández Collado C, Baptista Lucio P. Metodología de la Investigación. 3rd ed. Mexico: McGraw-Hill Interamericana; 2003.

58. Definición ABC. Definición de Encuesta. [Online].; 2016 [cited 2016 abril 23. Available from: http://www.definicionabc.com/comunicacion/encuesta.php.

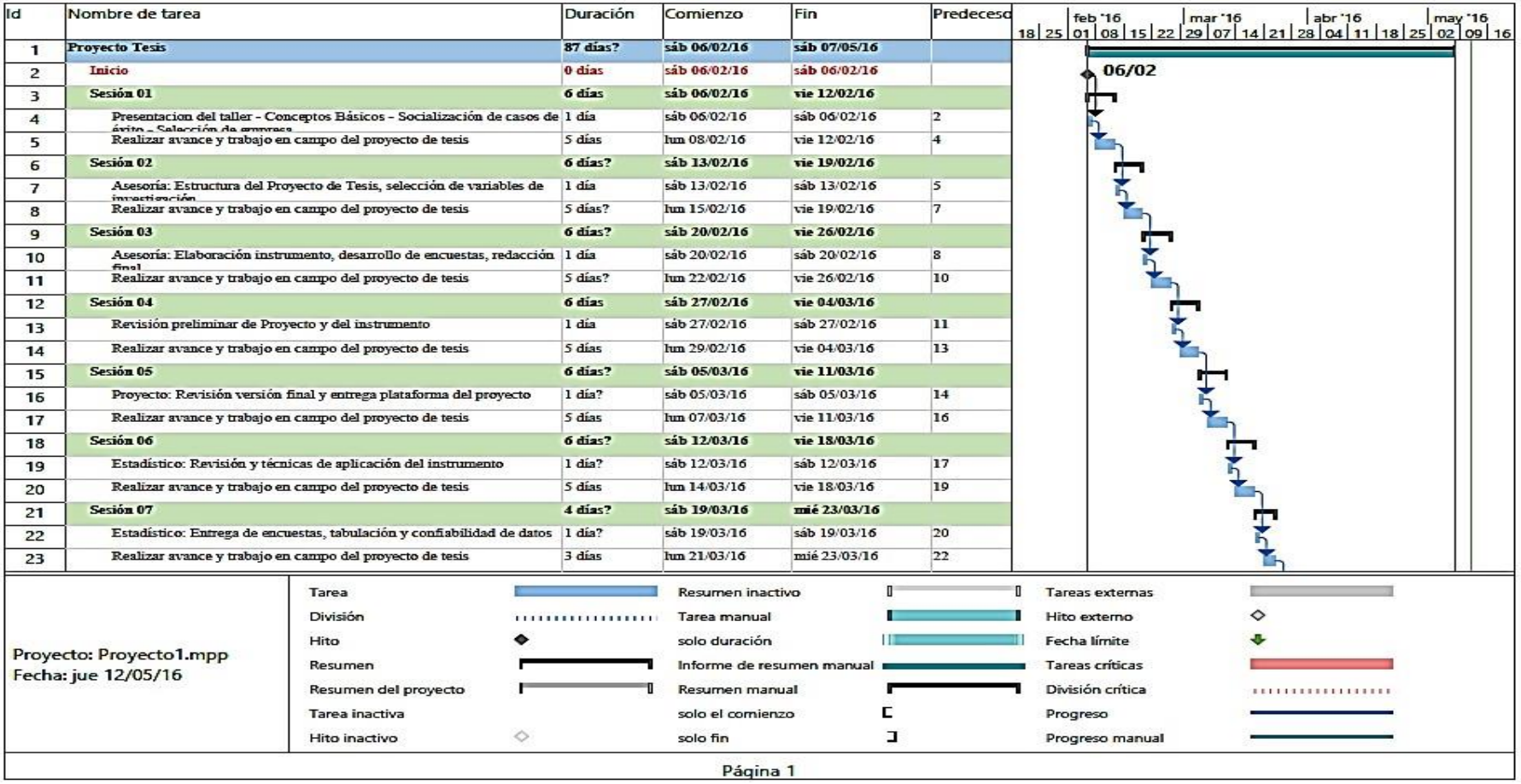
59. García Muñoz T. El Cuestionario como instrumento de investigación / evaluación. 2003.

60. Oficina Nacional de Tecnologías de Información (ONTI) de la Subsecretaría de Gestión Pública de la Jefatura de Gabinetes de Ministros de la República de Argentina. Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. 2005.

61. Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros del Perú. Plantilla Modelo - Sistema de Gestión de Seguridad de la Información. 2014. puede acceder a través del enlace http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552.

ANEXOS

ANEXO Nº 1: CRONOGRAMA DE ACTIVIDADES

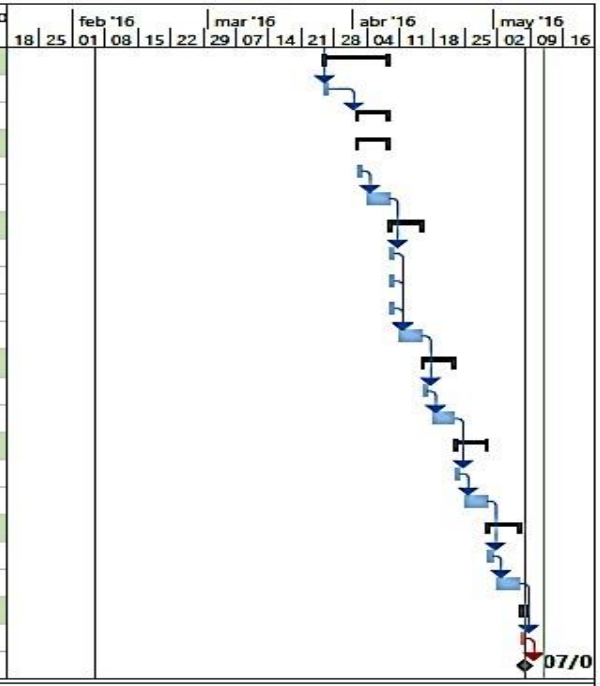


Id	Nombre de tarea	Duración	Comienzo	Fin	Predeceso
1	**Proyecto Tesis**	**87 días?**	**sáb 06/02/16**	**sáb 07/05/16**	
2	**Inicio**	**0 días**	**sáb 06/02/16**	**sáb 06/02/16**	
3	**Sesión 01**	**6 días**	**sáb 06/02/16**	**vie 12/02/16**	
4	Presentacion del taller - Conceptos Básicos - Socialización de casos de éxito - Selección de empresa	1 día	sáb 06/02/16	sáb 06/02/16	2
5	Realizar avance y trabajo en campo del proyecto de tesis	5 días	lun 08/02/16	vie 12/02/16	4
6	**Sesión 02**	**6 días?**	**sáb 13/02/16**	**vie 19/02/16**	
7	Asesoría: Estructura del Proyecto de Tesis, selección de variables de investigación	1 día	sáb 13/02/16	sáb 13/02/16	5
8	Realizar avance y trabajo en campo del proyecto de tesis	5 días?	lun 15/02/16	vie 19/02/16	7
9	**Sesión 03**	**6 días?**	**sáb 20/02/16**	**vie 26/02/16**	
10	Asesoría: Elaboración instrumento, desarrollo de encuestas, redacción final	1 día	sáb 20/02/16	sáb 20/02/16	8
11	Realizar avance y trabajo en campo del proyecto de tesis	5 días?	lun 22/02/16	vie 26/02/16	10
12	**Sesión 04**	**6 días**	**sáb 27/02/16**	**vie 04/03/16**	
13	Revisión preliminar de Proyecto y del instrumento	1 día	sáb 27/02/16	sáb 27/02/16	11
14	Realizar avance y trabajo en campo del proyecto de tesis	5 días	lun 29/02/16	vie 04/03/16	13
15	**Sesión 05**	**6 días?**	**sáb 05/03/16**	**vie 11/03/16**	
16	Proyecto: Revisión versión final y entrega plataforma del proyecto	1 día?	sáb 05/03/16	sáb 05/03/16	14
17	Realizar avance y trabajo en campo del proyecto de tesis	5 días	lun 07/03/16	vie 11/03/16	16
18	**Sesión 06**	**6 días?**	**sáb 12/03/16**	**vie 18/03/16**	
19	Estadístico: Revisión y técnicas de aplicación del instrumento	1 día?	sáb 12/03/16	sáb 12/03/16	17
20	Realizar avance y trabajo en campo del proyecto de tesis	5 días	lun 14/03/16	vie 18/03/16	19
21	**Sesión 07**	**4 días?**	**sáb 19/03/16**	**mié 23/03/16**	
22	Estadístico: Entrega de encuestas, tabulación y confiabilidad de datos	1 día?	sáb 19/03/16	sáb 19/03/16	20
23	Realizar avance y trabajo en campo del proyecto de tesis	3 días	lun 21/03/16	mié 23/03/16	22

Imagen elaborada con Software licenciado “Proyect 2013”

ANEXO Nº 1: CRONOGRAMA DE ACTIVIDADES

Id	Nombre de tarea	Duración	Comienzo	Fin	Predeceso
24	**Sesión 08**	**12.79 días**	**sáb 26/03/16**	**vie 08/04/16**	
25	Asesoría: Analisis de Resultados, conclusiones, recomendaciones de la tesis	1 día	sáb 26/03/16	sáb 26/03/16	23
26	**Realizar avance del proyecto de tesis**	**6 días**	**sáb 02/04/16**	**vie 08/04/16**	25
27	**Sesión 09**	**6 días**	**sáb 02/04/16**	**vie 08/04/16**	
28	Trabajo de campo desarrollo de tesis	1 día	sáb 02/04/16	sáb 02/04/16	
29	Realizar avance y trabajo en campo del proyecto de tesis	5 días	lun 04/04/16	vie 08/04/16	28
30	**Sesión 10**	**6 días**	**sáb 09/04/16**	**vie 15/04/16**	
31	Tesis: Revisión y entrega en plataforma	1 día	sáb 09/04/16	sáb 09/04/16	29
32	Artículo Científico: Asesoría para redacción y entrega en plataforma	1 día	sáb 09/04/16	sáb 09/04/16	
33	Diapositivas: Asesoría desarrollo y defensa	1 día	sáb 09/04/16	sáb 09/04/16	
34	Preparación para sustentación de tesis	5 días	lun 11/04/16	vie 15/04/16	33,31,32
35	**Sesión 11**	**6 días**	**sáb 16/04/16**	**vie 22/04/16**	
36	Diapositivas: Entrega, dinámica de sustentación	1 día	sáb 16/04/16	sáb 16/04/16	34
37	Preparación para sustentación de tesis	5 días	lun 18/04/16	vie 22/04/16	36
38	**Sesión 12**	**6 días**	**sáb 23/04/16**	**vie 29/04/16**	
39	Diapositivas: Entrega, dinámica de sustentación	1 día	sáb 23/04/16	sáb 23/04/16	37
40	Preparación para sustentación de tesis	5 días	lun 25/04/16	vie 29/04/16	39
41	**Sesión 13**	**6 días**	**sáb 30/04/16**	**vie 06/05/16**	
42	Pre-Banca	1 día	sáb 30/04/16	sáb 30/04/16	40
43	Preparación para sustentación de tesis	5 días	lun 02/05/16	vie 06/05/16	42
44	**Sesión 14**	**1 día**	**sáb 07/05/16**	**sáb 07/05/16**	
45	Sustentación de Tesis	1 día	sáb 07/05/16	sáb 07/05/16	43
46	**Fin**	**0 días**	**sáb 07/05/16**	**sáb 07/05/16**	45



Proyecto: Proyecto1.mpp
Fecha: jue 12/05/16

Tarea	Resumen inactivo	Tareas externas
División	Tarea manual	Hito externo
Hito	solo duración	Fecha límite
Resumen	Informe de resumen manual	Tareas críticas
Resumen del proyecto	Resumen manual	División crítica
Tarea inactiva	solo el comienzo	Progreso
Hito inactivo	solo fin	Progreso manual

Página 2

Imagen elaborada con Software licenciado “Proyect 2013”

ANEXO Nº 2: PRESUPUESTO

DESCRIPCIÓN	CANTIDAD	COSTO UNITARIO	TOTAL PARCIAL S/.	TOTAL S/.
1. BIENES DE CONSUMO				
1.1. Papel bond A-4 80	01 millar	35.00	35.00	
1.2. Tóner para impresora	01 unidad	45.00	45.00	
1.3. Cartucho de Tinta HP negra	01 unidad	35.00	35.00	
1.4. Cartucho de Tinta HP color	01 unidad	55.00	55.00	
1.5. CD - ROM	05 unidades	0.70	3.50	
1.6. Lapiceros	03 unidades	2.00	6.00	
1.7. Corrector	01 unidad	2.50	2.50	
1.8. Resaltador	01 unidad	2.00	2.00	
1.9. Folder Manila A4	02 unidades	0.50	1.00	
1.10. Clips	01 unidad	0.50	0.50	
1.11. Grapas	01 unidad	2.00	2.00	
1.12. Perforador	01 unidad	12.00	12.00	
1.13. Grapador	01 unidad	15.00	15.00	
1.14. Memoria USB	01 unidad	35.00	35.00	
			249.50	249.50
2. SERVICIOS				
2.1. Fotocopias	100 hojas	0.10	10.00	
2.2. Anillados / Empastado	03 unidades	15.00	45.00	
2.3. Servicios de Internet	04 meses	30.00	120.00	
2.4. Energía Eléctrica	04 meses	30.00	120.00	
2.5. Pasajes locales	04 meses	50.00	200.00	
			495.00	495.00
TOTAL				744.50

Fuente: Elaboración Propia

ANEXO Nº 3: CUESTIONARIO

Cuestionario Nº 1

DIAGNÓSTICO DEL ESTADO ACTUAL DE LA DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE PAITA

Instrucciones: Lea detalladamente y marque con una "X" la opción según corresponda

Preguntas	SI	NO
1. ¿Tiene usted conocimiento sobre lo que significa un plan de seguridad de información?		
2. ¿Cree usted que el diseño de un plan de Seguridad de la Información permitirá mejorar la calidad tecnológica?		
3. ¿Cree usted que se logrará un cambio positivo con la aplicación del plan de seguridad de información en la plataforma tecnológica?		
4. ¿Aprobaría usted la implementación del plan de Seguridad de la Información para la plataforma tecnológica?		
5. ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la Seguridad de la Información?		
6. ¿Estaría usted dispuesto a colaborar para que este plan de seguridad pueda ser llevado a cabo en las instalaciones ediles?		
7. ¿Sabe usted si existe un plan de recuperación ante desastres?		
8. ¿Sabe usted si se ha realizado evaluación de riesgos relacionados con la información?		
9. ¿Sabe usted si se ha realizado una evaluación de vulnerabilidades de la red?		
10. ¿Sabe usted si se cuenta con software antivirus actualizado?		

Cuestionario Nº 2

FACTIBILIDAD TÉCNICA, ECONÓMICA Y OPERATIVA DE LA PROPUESTA EN LA MUNICIPALIDAD PROVINCIAL DE PAITA

Instrucciones: Lea detalladamente y marque con una "X" la opción según corresponda

Preguntas	SI	NO
1. ¿Cree usted que la norma ISO/IEC 27001:2014 es, en sí misma, un modelo extenso y detallado, en el cual se especifican las etapas que se deben cumplir para la implantación de un Sistema de Gestión de Seguridad de la Información?		
2. ¿Cree usted que se cuenta con personal capacitado para liderar el proyecto?		
3. ¿La ONGEI ha brindado asistencia Técnica para el desarrollo del plan de seguridad de la información?		
4. ¿Cree usted que se cuenta con el equipo informático suficiente (computadoras y periféricos) para el desarrollo de la propuesta?		
5. ¿La alta dirección apoya y aprueba la elaboración del Diseño de la propuesta del Plan de Seguridad de la Información?		
6. ¿Se cuenta con personal que está en la disposición y en la capacidad de formarse en el diseño, implantación, operación y monitoreo del Sistema de Gestión de Seguridad de la Información?		
7. ¿Existe muy buena disposición para mejorar la seguridad de la información y se puede asumir el costo de la implementación de la propuesta?		
8. ¿El personal de la Dirección de Informática, tiene experiencia en el área de computación y están familiarizados con los aspectos de la seguridad tecnológica?		
9. ¿El personal de la Dirección de Informática, está consciente de los incidentes de seguridad que han ocurrido y han solicitado mejorar la seguridad física y el control de acceso a las instalaciones?		
10. ¿El personal de la Dirección de Informática está dispuesto a colaborar en el desarrollo del plan de seguridad?		

Cuestionario Nº 3

NECESIDAD DE LA PROPUESTA DE POLÍTICAS BASADAS EN BUENAS PRÁCTICAS PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE PAITA

Instrucciones: Lea detalladamente y marque con una "X" la opción según corresponda

Preguntas	SI	NO
1. ¿Considera usted que deben existir políticas de seguridad para la plataforma tecnológica?		
2. ¿Existe un documento que defina las políticas de seguridad de información?		
3. ¿Conoce usted alguno de los estándares de seguridad de información?		
4. ¿El manejo de la Información de la Organización está en manos del personal que tiene responsabilidad directa sobre ella?		
5. ¿Indique si existen programas dirigidos a sensibilizar sobre la Seguridad de la Información para todos los empleados?		
6. ¿Existe un documento donde los empleados, contratista y proveedores acuerden la confidencialidad de la información?		
7. ¿Indique si se han realizado pruebas de penetración perimetral?		
8. ¿Existe un documento donde estén definidas las responsabilidades para la contratación, terminación o cambio de cargo o funciones para los empleados, con la finalidad de proteger los recursos informáticos?		
9. ¿se cuenta con planes de contingencia en caso de pérdida de información?		
10. ¿El área de Informática realiza la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles relacionados a la seguridad de la información?		

ANEXO Nº 4: COSTO DEL PROYECTO EN EL MERCADO: SISTEMA NACIONAL DE INVERSIÓN PÚBLICA (CODIGO SNIP: 268985)

FORMATO SNIP 04 : PERFIL SIMPLIFICADO - PIP MENOR

(Directiva Nº 001-2011-EF/68.01 aprobada por Resolución Directoral Nº 003-2011-EF/68.01)
Los acápites señalados con (*) no serán considerados en el caso de los PIP MENORES que consignen un monto de inversión menor o igual a S/. 300,000.
(La información registrada en este perfil tiene carácter de Declaración Jurada)

I. ASPECTOS GENERALES

1. **CÓDIGO DEL PROYECTO:** **2186546** (CÓDIGO SNIP: 268985)
2. **NOMBRE DEL PIP MENOR:** INSTALACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION EN LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO, PROVINCIA DE TRUJILLO - LA LIBERTAD
3. **RESPONSABILIDAD FUNCIONAL (Según Anexo SNIP-04)**

FUNCION:	PLANEAMIENTO, GESTIÓN Y RESERVA DE CONTINGENCIA
DIVISIÓN FUNCIONAL:	INFORMACIÓN PÚBLICA
GRUPO FUNCIONAL:	INFORMACIÓN PÚBLICA
RESPONSABILIDAD FUNCIONAL:	OPI PCM,OPI AMBIENTE
OPI RESPONSABLE DE LA EVALUACION:	OPI MUNICIPALIDAD PROVINCIAL DE TRUJILLO

RUBROS / FUENTES DE FINANCIAMIENTO

Rubro	Fase de Inversión		Monto de Operación y Mantenimiento
	Monto	%	
Total	0	0.0%	0

CATEGORÍA PRESUPUESTAL

EL PIP NO TIENE ASIGNADA UNA CATEGORÍA PRESUPUESTAL.

4. **UNIDAD FORMULADORA**

SECTOR:	GOBIERNOS LOCALES
PLIEGO:	MUNICIPALIDAD PROVINCIAL DE TRUJILLO
NOMBRE:	PROYECTO ESPECIAL PLAN DE DESARROLLO TERRITORIAL DE TRUJILLO-PLANDET
Persona Responsable de Formular el PIP Menor:	ING. JUAN CARLOS LLAVE RODRIGUEZ
Persona Responsable de la Unidad Formuladora:	MARITZA ELSA HURTADO CASTRO

5. **UNIDAD EJECUTORA RECOMENDADA**

DEPARTAMENTO	LA LIBERTAD
PROVINCIA	TRUJILLO
NOMBRE:	MUNICIPALIDAD PROVINCIAL DE TRUJILLO
Persona Responsable de la Unidad Ejecutora:	ING. CARLOS CHUNGA MONTERO
Órgano Técnico Responsable	GERENTE DE SISTEMAS - MPT

Lista de unidades ejecutoras

Nº	Detalle

6. **UBICACION GEOGRAFICA**

Nº	Departamento	Provincia	Distrito	Localidad
1	LA LIBERTAD	TRUJILLO	TRUJILLO	

II. IDENTIFICACION

7. DESCRIPCIÓN DE LA SITUACION ACTUAL

LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO ES UNA INSTITUCIÓN PÚBLICA QUE PARA CUMPLIR ADECUADAMENTE CON SUS ACTIVIDADES Y EJECUTAR EFICIENTEMENTE SUS PROCESOS, REQUIERE CONTAR CON UNA INFRAESTRUCTURA TECNOLÓGICA DE REDES Y COMUNICACIONES QUE SOPORTE LOS DIVERSOS SERVICIOS Y SISTEMAS INFORMÁTICOS IMPLEMENTADOS; Y BRINDE CONTINUIDAD, SEGURIDAD Y FLEXIBILIDAD EN LA ADMINISTRACIÓN Y MANEJO DE LA INFORMACIÓN, POR LO QUE SE ESTÁ IMPLEMENTANDO UN CENTRO DE DATOS, DONDE SE ALOJARÁN LOS SERVIDORES, EQUIPOS DE COMUNICACIÓN, TELEFONÍA; CONTANDO DE ESTA FORMA CON UN AMBIENTE SEGURO EL CUAL CUMPLE CON ESTÁNDARES NACIONALES E INTERNACIONALES. COMPLETANDO LA SOLUCIÓN ANTES EXPUESTA, SE REQUIERE LA IMPLEMENTACIÓN DE NORMAS TÉCNICAS DE SEGURIDAD DE LA INFORMACIÓN QUE PERMITA LA GESTIÓN ÓPTIMA DE LA SEGURIDAD DE LA INFORMACIÓN. ACTUALMENTE EXISTE LA NORMA TECNICA PERUANA QUE HA SIDO ELABORADA POR EL COMITE TECNICO PERMANENTE DE CODIFICACION E INTERCAMBIO ELECTRONICO DE DATOS (EDI), MEDIANTE EL SISTEMA 1 O ADOPCION, ESTA NORMA HA SIDO PREPARADA CON EL FIN DE OFRECER UN MODELO PARA ESTABLECER, IMPLEMENTAR, OPERAR, MONITOREAR, MANTENER Y MEJORAR UN EFECTIVOSISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (ISMS). LA ADOPCION DE UN ISMS DEBE FORMAR PARTE DE UNA DESICION ESTRATEGICA PARA LAS ORGANIZACIONES QUE IMPLEMENTES ESTE SISTEMA DE SEGURIDAD.

Nº	Principales Indicadores de la Situación Actual (máximo 3)	Valor Actual
1	SGSI IMPLEMENTADA DE ACUERDO A NORMA EN LA GERENCIA DE TRANSPORTE, TRÁNSITO Y SEGURIDAD VIAL (EN %)	0
2	SGSI IMPLEMENTADA DE ACUERDO A NORMA EN SISTEMA INTEGRADO DE GESTIÓN ADMINISTRATIVA (EN %)	0
3	SGSI IMPLEMENTADA DE ACUERDO A NORMA EN TECNOLOGÍA DE LA INFORMACIÓN (EN %)	0

8. PROBLEMA CENTRAL Y SUS CAUSAS

INADECUADO SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO

Nº	Descripción de las principales causas (máximo 8)	Causas Indirectas
Causa 1:	INADECUADA GESTION DE RIESGOS DE LA INFORMACIÓN	DEFICIENTE CLASIFICACIÓN DE LA INFORMACIÓN
Causa 2:	INADECUADA GESTION DE RIESGOS DE LA INFORMACIÓN	INEXISTENCIA DE UN PLAN DE PREVENCION DE RIESGOS EN LA INFORMACIÓN
Causa 3:	INADECUADA GESTION DE RIESGOS DE LA INFORMACIÓN	DEFICIENTES MECANISMO Y PROCEDIMIENTOS DE TRATAMIENTO DE RIESGOS
Causa 4:	INADECUADA GESTION DE RIESGOS DE LA INFORMACIÓN	INEXISTENCIA DE PROGRAMAS DE CONCIENTACIÓN EN SEGURIDAD DE LA INFORMACIÓN

9. OBJETIVO Y MEDIOS FUNDAMENTALES

9.1 Objetivo

ADECUADO SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE TRUJILLO

9.2 Medios fundamentales

Nº	Descripción medios fundamentales
1	EFIECIENTE CLASIFICACIÓN DE LA INFORMACIÓN
2	EXISTENCIA DE UN PLAN DE PREVENCION DE RIESGOS EN LA INFORMACIÓN
3	EFICIENTES MECANISMO Y PROCEDIMIENTOS DE TRATAMIENTO DE RIESGOS
4	EXISTENCIA DE PROGRAMAS DE CONCIENTACIÓN EN SEGURIDAD DE LA INFORMACIÓN

10. DESCRIPCION DE LAS ALTERNATIVAS DE SOLUCION AL PROBLEMA

Descripción de cada Alternativa Analizada	Componentes (Resultados necesarios para lograr el Objetivo	Acciones necesarias para lograr cada resultado	Número de Beneficiarios Directos
	Resultado 1: CLASIFICACIÓN	REVISIÓN DE LA INFORMACIÓN Y DOCUMENTACIÓN, ELABORACIÓN DE	

Alternativa 1: REVISIÓN DE LA INFORMACIÓN Y DOCUMENTACIÓN, ELABORACIÓN DE POLÍTICAS DE SEGURIDAD, IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS, TRATAMIENTO Y SELECCIÓN DE CONTROLES, ELABORACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS; DETERMINACIÓN DE MECANISMOS DE MEDICIÓN DE LA EFECTIVIDAD, IMPLEMENTACIÓN Y/O ACTUALIZACIÓN DE LA DOCUMENTACIÓN, IMPLEMENTACIÓN DE PROCEDIMIENTOS Y CONTROLES PARA LA GESTIÓN DE INCIDENTES, Y ACCIONES CORRECTIVAS Y PREVENTIVAS E IMPLEMENTACIÓN DEL PROGRAMA DE FORMACIÓN Y CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN Y CURSO DE CAPACITACIÓN DE IMPLEMENTACIÓN DE SISTEMAS DE SEGURIDAD.	DE LA INFORMACIÓN EXISTENTE EN LA MUNICIPALIDAD	POLÍTICAS DE SEGURIDAD, IDENTIFICACIÓN DE RIESGOS Y CLASIFICACIÓN DE LA INFORMACIÓN EXISTENTE.	2,282
	Resultado 2: PLAN DE PREVENCION DE RIESGOS EN LA INFORMACIÓN	EVALUACIÓN DE RIESGOS, TRATAMIENTO Y SELECCIÓN DE CONTROLES. ELABORACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS.	
	Resultado 3: MECANISMOS Y PROCEDIMIENTOS DE TRATAMIENTO DE RIESGOS	DETERMINACIÓN DE MECANISMOS DE MEDICIÓN DE LA EFECTIVIDAD, IMPLEMENTACIÓN Y/O ACTUALIZACIÓN DE LA DOCUMENTACIÓN, IMPLEMENTACIÓN DE PROCEDIMIENTOS Y CONTROLES PARA LA GESTIÓN DE INCIDENTES, Y ACCIONES CORRECTIVAS Y PREVENTIVAS, MEDIANTE INDICADORES DE GESTIÓN.	
	Resultado 4: PROGRAMAS DE CONCIENTACIÓN EN SEGURIDAD DE LA INFORMACIÓN	IMPLEMENTACIÓN DEL PROGRAMA DE FORMACIÓN Y CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN Y CURSO DE CAPACITACIÓN DE IMPLEMENTACIÓN DE SISTEMAS DE SEGURIDAD.	

III. FORMULACION Y EVALUACION

11. HORIZONTE DE EVALUACION

Número de años del horizonte de evaluación (entre 5 y 10 años):	10
Sustento técnico del horizonte de evaluación elegido:	

12. ANALISIS DE LA DEMANDA (*)

Enunciar los principales parámetros y supuestos considerados para la proyección de la demanda.

13. ANALISIS DE LA OFERTA (*)

Describir los factores de producción que determinan la oferta actual del servicio. Enunciar los principales parámetros y supuestos considerados para la proyección de la oferta.

14. BALANCE OFERTA DEMANDA (*)

15. COSTOS DEL PROYECTO

Modalidad de ejecución ADMINISTRACION INDIRECTA - POR CONTRATA

15.1.1 Costos de inversión de la alternativa seleccionada (a precios de mercado)

Principales Rubros	U.M.	Cantidad	Costo Unitario	Costo Total a Precios de Mercado
EXPEDIENTE TECNICO	ESTUDIO	1.0	5,000.0	5,000.0
COSTO DIRECTO				200,070.0
Resultado 1	GLOBAL	1.0	20,007.0	20,007.0
Resultado 2	PLAN	1.0	40,014.0	40,014.0
Resultado 3	INDICADORES	1.0	100,035.0	100,035.0
Resultado 4	PROGRAMA	1.0	40,014.0	40,014.0
SUPERVISION	GLOBAL	1.0	7,000.0	7,000.0
GASTOS GENERALES	GLOBAL	1.0	11,115.0	11,115.0
UTILIDADES	GLOBAL	1.0	11,115.0	11,115.0
Total				**234,300.0**

15.1.2 Costos de inversión de la alternativa seleccionada (a precios sociales) (*)

15.2 Costos de operación y mantenimiento sin proyecto

Items de Gasto	Año 1	Año 2	Año 3	Año 4	Año 5	Año 6	Año 7	Año 8	Año 9	Año 10
RRHH	0	0	0	0	0	0	0	0	0	0
Total a Precios de Mercado	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Total a Precios Sociales	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

15.3 Costos de operación y mantenimiento con proyecto para la alternativa seleccionada

Items de Gasto	Año 1	Año 2	Año 3	Año 4	Año 5	Año 6	Año 7	Año 8	Año 9	Año 10
RRHH	7,200	7,200	7,200	7,200	7,200	7,200	7,200	7,200	7,200	7,200
Total a Precios de Mercado	**7,200**	**7,200**	**7,200**	**7,200**	**7,200**	**7,200**	**7,200**	**7,200**	**7,200**	**7,200**
Total a Precios Sociales	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

15.4 Costo por Habitante Directamente Beneficiado	102.67

15.5 Comparación de costos entre alternativas (*)

16. BENEFICIOS (alternativa recomendada)

16.1 Beneficios Sociales (cuantitativo) (*)

Enunciar los principales parámetros y supuestos para la estimación de los beneficios sociales
NO SE HAN CONSIDERADO BENEFICIOS CUANTITATIVOS

16.2 Beneficios sociales (cualitativo)

CONFIANZA DE LOS CLIENTES Y PROVEEDORES. CUMPLIMIENTO REGULATORIO Y NORMATIVO. MEJOR ESTRUCTURA ORGANIZACIONAL PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. MEJORAR LA EFECTIVIDAD OPERATIVA. REDUCIR COSTOS. PROTEGER LA MARCA Y REPUTACIÓN. LOGRAR MEJORAS CONTINUAS. POTENCIAR LA INNOVACIÓN. ADECUADA GESTIÓN DE ACCESOS E IDENTIDADES. INCREMENTO DE LA CONCIENTIZACIÓN DEL PERSONAL CON RESPECTO A LOS TEMAS DE SEGURIDAD DE LA INFORMACIÓN. VENTAJA COMPETITIVA A TRAVÉS DE LA CERTIFICACIÓN DE LA NORMA.

17. EVALUACION SOCIAL (*)

18. CRONOGRAMA DE EJECUCION

18.1 Cronograma de Ejecución Física (% de avance)

Principales Rubros	Trimestre I	Trimestre II	Trimestre III	Trimestre IV
EXPEDIENTE TECNICO	100	0	0	0
COSTO DIRECTO				
Resultado 1	100	0	0	0
Resultado 2	50	50	0	0
Resultado 3	0	100	0	0
Resultado 4	0	0	100	0
SUPERVISION	40	40	20	0
GASTOS GENERALES	40	40	20	0
UTILIDADES	40	40	20	0

18.2 Cronograma de Ejecución Financiera (% de avance)

Principales Rubros	Trimestre I	Trimestre II	Trimestre III	Trimestre IV
EXPEDIENTE TECNICO	100	0	0	0
COSTO DIRECTO				
Resultado 1	100	0	0	0
Resultado 2	50	50	0	0
Resultado 3	0	100	0	0
Resultado 4	0	0	100	0
SUPERVISION	40	40	20	0
GASTOS GENERALES	40	40	20	0
UTILIDADES	40	40	20	0

19. SOSTENIBILIDAD

19.1 Responsable de la Operación y mantenimiento del PIP

MUNICIPALIDAD PROVINCIAL DE TRUJILLO

19.2 ¿Es la Unidad Ejecutora la responsable de la Operación y Mantenimiento del PIP con cargo a su Presupuesto Institucional? SI

19.3 ¿El área donde se ubica el proyecto ha sido afectada por algún desastre natural? NO

20. IMPACTO AMBIENTAL

Impactos Negativos	Tipo	Medidas de Mitigación	Costo
NO SE CONSIDERA POR EL TIPO DE PROYECTO	Durante la Construcción	NO SE CONSIDERA POR EL TIPO DE PROYECTO	0
NO SE CONSIDERA POR EL TIPO DE PROYECTO	Durante la Operación	NO SE CONSIDERA POR EL TIPO DE PROYECTO	0

21. TEMAS COMPLEMENTARIOS

22. EVALUACIONES REALIZADAS SOBRE EL PROYECTO DE INVERSIÓN PÚBLICA

Fecha	Estudio	Evaluación	Unidad Evaluadora	Observación
29/08/2013 11:18 a.m.	PERFIL	EN MODIFICACION	OPI MUNICIPALIDAD PROVINCIAL DE TRUJILLO	No se ha registrado observación
13/09/2013 12:33 p.m.	PERFIL	EN MODIFICACION	OPI MUNICIPALIDAD PROVINCIAL DE TRUJILLO	No se ha registrado observación
19/09/2013 08:02 a.m.	PERFIL	APROBADO	OPI MUNICIPALIDAD PROVINCIAL DE TRUJILLO	No se ha registrado observación

23. REGISTRO DE DOCUMENTOS FÍSICOS DE ENTRADA - SALIDA

Tipo	Documento	Fecha	Unidad
S	OFICIO NRO 557-2013-MPT/PLANDET	21/08/2013	PROYECTO ESPECIAL PLAN DE DESARROLLO TERRITORIAL DE TRUJILLO- PLANDET
E	OFICIO NRO 557-2013-MPT/PLANDET	22/08/2013	OPI MUNICIPALIDAD PROVINCIAL DE TRUJILLO
S	Oficio N 1029-2013-MPT/GPP	16/09/2013	OPI MUNICIPALIDAD PROVINCIAL DE TRUJILLO
S	Formato SNIP 06 Nº 18-2013/MPT/GPP/OPI/E	16/09/2013	OPI MUNICIPALIDAD PROVINCIAL DE TRUJILLO

24. DOCUMENTOS COMPLEMENTARIOS

Documento	Observación	Fecha	Tipo	Origen
OFICIO Nº 1031-2013-MPT/GPP	(COMUNICACIÓN DE VIABILIDAD) *	19/09/2013	Entrada	DGPM

25. FECHA DE REGISTRO EN EL BP: 21/08/2013

FECHA DE ULTIMA ACTUALIZACION: 16/09/2013

26. DATOS DE LA DECLARATORIA DE VIABILIDAD

N° DE INFORME TECNICO:	Formato SNIP 06 Nº 18-2013/MPT/GPP/OPI/E
ESPECIALISTA:	Arq. Constante Castillo Alva
RESPONSABLE:	Econ. Pedro Chalen Costa
FECHA:	16/09/2013

FIRMAS

ING. JUAN CARLOS LLAVE RODRIGUEZ	**MARITZA ELSA HURTADO CASTRO**
Responsable de la Formulación del Perfil	**Responsable de la Unidad Formuladora**