



UNL

Universidad
Nacional
de Loja



Carrera de Ingeniería en
Sistemas / Computación

Facultad de Energía, las Industrias y los Recursos Naturales no Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

“Diseño de un modelo de Gestión de Seguridad de la Información, bajo el estándar ISO/IEC 27001:2013 para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja”

***Tesis previa a la Obtención del
Título de Ingeniero en Sistemas***

Autora: Karla Andrea Correa Cumbicus

Director: Ing. Cristian Ramiro Narváez Guillen.

Loja-Ecuador
2020

CERTIFICACIÓN

Ing. Cristian Ramiro Narváez Guillen, Mg. Sc.

DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS DE LA UNIVERSIDAD NACIONAL DE LOJA, DIRECTOR DE TESIS

CERTIFICA:

Que la egresada Karla Andrea Correa Cumbicus, realizó el trabajo de titulación denominado “**Diseño de un modelo de Gestión de Seguridad de la Información, bajo el estándar ISO/IEC 27001:2013 para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.**” bajo mi dirección y asesoramiento, mismo que fue revisado, enmendado y corregido minuciosamente. En virtud que el Trabajo de Titulación reúne, a satisfacción las cualidades de fondo y forma exigidas para un trabajo de este nivel, autorizo su presentación, sustentación y defensa ante el tribunal respectivo.

Loja, 13 de marzo del 2020.

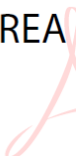


CRISTIAN
RAMIRO
NARVAEZ
GUILLEN

Ing. Cristian Ramiro Narváez Guillen
DOCENTE CARRERA DE INGENIERIA EN SISTEMAS
CI: 110410138-9
cristian.narvaez@unl.edu.ec
Código 30440
cc:/archivo personal

Autoría

Yo, **KARLA ANDREA CORREA CUMBICUS** declaro ser la autora del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de esta. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de la tesis en el Repositorio Institucional – Biblioteca Virtual.

Firma: KARLA ANDREA
CORREA
CUMBICUS  KARLA ANDREA
CORREA CUMBICUS
2020.07.27 17:08:12
-05'00'

Cédula: 1105707499

Fecha: 27 de julio del 2020

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo, **Karla Andrea Correa Cumbicus**, declaro ser la autora de la tesis titulada: “**DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, BAJO EL ESTÁNDAR ISO/IEC 27001:2013 PARA LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN DEL GOBIERNO PROVINCIAL DE LOJA**”, como requisito para optar al grado de: **INGENIERO EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional. Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la universidad. La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de tesis que realice un tercero. Para constancia de esta autorización, en la ciudad de Loja, a los veintisiete días del mes de julio del dos mil veinte.

Firma: KARLA ANDREA CORREA CUMBICUS
KARLA ANDREA CORREA CUMBICUS
2020.07.27 17:09:39
-05'00'

Autor: Karla Andrea Correa Cumbicus

Cédula: 1105707499

Dirección: Loja (Crisantemos entre Anturios 241-42 y Helechos)

Correo Electrónico: karlacorrea17@gmail.com

Teléfono:072104155 **Celular:** 0987449590

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Cristian Ramiro Narváez Guillen Mg. Sc.

Tribunal de Grado: Ing. Hernán Leonardo Torres Carrión Mg. Sc.

Ing. Mario Enrique Cueva Hurtado Mg. Sc.

Ing. Andrés Roberto Navas Castellanos Mg. Sc.

Dedicatoria

A mi Madre, Gloria; por formarme como persona con tu amor y apoyo incondicional, este triunfo es el primero de muchos que te dedicaré.

A mi hermana, Laura; por ser mi primer ejemplo de perseverancia y responsabilidad, desde pequeña te he admirado y lo seguiré haciendo por todo lo que haces y lo que eres, un ejemplo de bondad y amor.

A mi hermana, Cecibel; por estar conmigo y enseñarme con tu ejemplo a amar a tu profesión, y sobre todo por cada cuidado, consejo y deseo de superación.

A mi hermana, María; por muchas risas y consejos, y por enseñarme lo que no se aprende en la universidad, siempre serás un ejemplo de constancia y amor para mí.

A mi hermana, Mirka; por cada momento compartido, por cada risa, por ser mi confidente, por todo el amor y apoyo incondicional que me brindas siempre y sobre todo por confiar en mí ciegamente.

A mi hermano, Carlitos; por ser más que un hermano y ayudar a mi formación.

A mi hermana, Karla; por tu ayuda y palabras de aliento, son mi motivación para conseguir todo lo que me proponga.

A mis hermanos, Alan y Gaby; gracias por su confianza y compañía en momentos de alegría y de dificultad.

A mis sobrinos, Carlos Fernando, Bryan, Isaac, Antonio, David, Justin, Mateo y Nicole por ser quienes seguirán mis pasos, ustedes son mi inspiración para seguir mi camino con la responsabilidad de hacer lo correcto y para que vean en mí un ejemplo, y puedan llegar a ser mejores.

A mis amigas; Nancy, Jennifer y Natasha; por formar parte de mi familia, en estos diez años de amistad se han convertidos en más que amigas y son las hermanas que yo escogí, gracias por estar presentes en cada alegría y sobre todo momentos de dificultad.

Agradecimiento

A mis docentes, por contribuir en mi formación académica, han sido un pilar fundamental para culminar con éxitos mis estudios, gracias por su paciencia y consejos.

Al Ingeniero Cristian Ramiro Narváz Guillen, por su ayuda y excelente asesoría para mejorar cada detalle del proyecto de titulación, por dedicar su tiempo y conocimiento para culminar con éxito este proyecto de titulación.

Al Ingeniero Boris Marcel Díaz Pauta, por su clases y excelentes asesorías que sirvieron como aporte a este proyecto, en especial por compartir sus conocimientos y experiencias laborales, me llevo un grato recuerdo y me retiro con un infinito agradecimiento y admiración hacia su persona.

Al Ingeniero Luis Antonio Chambas Eras, por sus asesorías académicas durante todo el proceso de redacción de la memoria final.

A la Dirección de Tecnología de la Información del Gobierno Provincial de Loja, en especial a su director, el Ingeniero Pablo Vallejo por permitirme realizar el presente TT, en tan prestigiosa Institución.

A mi madre Gloria, aún no se han inventado las palabras que me gustaría expresar para agradecer todo lo que me has dado y hecho por mí, mi vida entera es poco para dedicarme agradecer por tu amor, dedicación y tiempo; por luchar para que pueda cumplir mis sueños, gracias a ti hoy cumplo este objetivo en mi vida.

A mis hermanos y hermanas, por ser quienes confían cada momento en mí, por cada consejo y deseo de prosperidad hoy puedo culminar una etapa más en mi vida

A mis compañeros, Christian, Nixon, Jasón, Luis, Fernando, Jerpson, Jessica, Pablo y Jaritza por su ayuda durante momentos de poco entendimiento, por cada momento compartido en las aulas y fuera de ellas y por ser más que compañeros de clase y conformar parte de mi vida.

Índice de Contenidos

CERTIFICACIÓN.....	II
AUTORÍA.....	III
DEDICATORIA.....	V
AGRADECIMIENTO.....	VI
ÍNDICE DE CONTENIDOS.....	VII
1. TÍTULO.....	1
2. RESUMEN.....	2
3. INTRODUCCIÓN.....	4
4. REVISIÓN DE LITERATURA.....	4
4.1. SEGURIDAD DE LA INFORMACIÓN.....	6
4.1.1. Seguridad Informática.....	6
4.1.2. Diferencia entre Seguridad Informática y de la Información.....	6
4.1.3. Objetivos de la Seguridad de la Información.....	7
4.2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI.....	8
4.2.1. Ciclo de Vida del SGSI.....	8
4.3. NORMA ISO/IEC 27001:2013.....	11
4.3.1. Secciones de la Norma ISO/IEC 27001:2013.....	11
4.4. GESTIÓN DE RIESGOS.....	13
4.4.1. Sistema de Gestión de Riesgo Operativo.....	14
5. MATERIALES Y MÉTODOS.....	15
5.1. CONTEXTO.....	15
5.2. PROCESO.....	15
5.3. RECURSOS.....	18
5.4. PARTICIPANTES.....	19
6. RESULTADOS.....	20
FASE 1: REALIZAR UN DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN DEL GOBIERNO PROVINCIAL DE LOJA POR MEDIO DE LOS PROCESOS DESCRITOS EN LA NORMA ISO/IEC 27001:2013.....	21
6.1.1. Recolectar Información sobre los Controles de Seguridad Aplicados Actualmente en la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.....	21
6.1.2. Recolectar Información de los activos tecnológicos existentes en la dirección de tecnología de la información del gobierno provincial de Loja.....	23
6.1.3. Recolectar Información sobre las actividades y roles del personal.....	28
6.1.4. Recolectar Información sobre los procesos organizacionales.....	30
6.1.5. Definir Alcance del Modelo.....	30
6.1.6. Realizar una evaluación de los Riesgos.....	30
6.1.7. Establecer criterios para la aceptación de riesgos.....	34

6.1.8. Identificar los riesgos, amenazas y vulnerabilidades que presentan los activos de información.....	37
6.1.9. Analizar la información y elaborar un informe de la situación actual en la dirección de tecnología de la información.	43
FASE 2: DEFINIR POLÍTICAS DE SEGURIDAD BAJO EL ESTÁNDAR ISO/IEC 27001:2013. ANEXO A (CONTROLES) NECESARIOS PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN DEL GOBIERNO PROVINCIAL.	44
6.2.1. Política de Seguridad de la Información	44
6.2.2. Declaración de Aplicabilidad.	44
6.2.3. Políticas de Organización de la Seguridad de la Información	44
6.2.4. Políticas de Seguridad de Recursos Humanos.	45
6.2.5. Políticas de Gestión de Recursos.	45
6.2.6. Políticas de Control de Acceso.....	45
6.2.7. Políticas de Criptografía.....	46
6.2.8. Políticas de Seguridad Física y ambiental.....	46
6.2.9. Políticas de Seguridad Operacional.....	46
6.2.10. Políticas de Seguridad de las Comunicaciones.....	46
6.2.11. Políticas de Adquisición, Desarrollo y Mantenimiento de Sistemas.....	47
6.2.12. Políticas de Relaciones con los Proveedores.....	47
6.2.13. Políticas de Gestión de Incidentes en Seguridad de la Información.....	47
6.2.14. Políticas de Aspectos de Seguridad de la Información de la Gestión de la continuidad del Negocio.....	48
6.2.15. Políticas de Cumplimiento.....	48
FASE 3: DEFINIR UN MODELO PARA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN DEL GOBIERNO PROVINCIAL DE LOJA BAJO LA NORMA ISO/IEC 27001:2013.	49
6.3.1. Definir las fases del modelo de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013.....	49
6.3.2. Elaborar la documentación necesaria para la ejecución del modelo gestión de la seguridad de la Información bajo la norma ISO/IEC 27001:2013.....	53
FASE 4: VALORAR EL MODELO MEDIANTE LA IMPLEMENTACIÓN DEL MISMO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN DEL GOBIERNO PROVINCIAL DE LOJA BAJO LA NORMA ISO/IEC 27001:2013.....	56
6.4.1. Definir el Plan de Pruebas.....	56
6.4.2. Definir el Escenario de Pruebas.....	56
6.4.3. Ejecutar el modelo de acuerdo con el plan de pruebas.....	57
7. DISCUSIÓN.....	64
7.1. Desarrollo de la Propuesta Alternativa	64
7.2. Valoración Técnica, Económica y Científica.....	66
8. CONCLUSIONES	69

9. RECOMENDACIONES.....	70
10 BIBLIOGRAFÍA.....	71
11. ANEXOS.....	76
ANEXO 1: ACUERDOS ACTUALES.....	76
ANEXO 2: CONTROLES DE LA ISO/IEC 27001:2013 DEL ANEXO A.....	83
ANEXO 3: DOCUMENTO SOBRE EL ALCANCE DEL MGSÍ.....	88
ANEXO 4: COMPARATIVA DE METODOLOGÍAS.....	93
ANEXO 5: MATRIZ DE RIESGOS.....	107
ANEXO 6: INFORME SITUACIÓN ACTUAL.....	111
ANEXO 7: DOCUMENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.....	116
ANEXO 8: DECLARACIÓN DE APLICABILIDAD.....	122
ANEXO 9: POLÍTICA SOBRE DISPOSITIVOS MÓVILES Y TELETRABAJO.....	158
ANEXO 10: TRAE TU PROPIO DISPOSITIVO BYOD.....	163
ANEXO 11: DECLARACIÓN DE ACEPTACIÓN DE DOCUMENTOS.....	169
ANEXO 12: DECLARACIÓN DE CONFIDENCIALIDAD.....	171
ANEXO 13: POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN.....	172
ANEXO 14: POLÍTICA DE USO ACEPTABLE.....	181
ANEXO 15: POLÍTICA DE CONTROL DE ACCESO.....	189
ANEXO 16: POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS.....	199
ANEXO 17: POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIO.....	204
ANEXO 18: POLÍTICA DE CREACIÓN DE COPIAS DE SEGURIDAD.....	208
ANEXO 19: POLÍTICA DE GESTIÓN DE CAMBIOS.....	212
ANEXO 20: PROCEDIMIENTOS OPERATIVOS PARA TI Y COMUNICACIÓN.....	216
ANEXO 21: POLÍTICA DE TRANSFERENCIA DE LA INFORMACIÓN.....	222
ANEXO 22: POLÍTICA DE DESARROLLO SEGURO.....	226
ANEXO 23: APÉNDICE ESPECIFICACIÓN DE REQUISITOS.....	231
ANEXO 24: POLÍTICA DE SEGURIDAD PARA PROVEEDORES.....	232
ANEXO 25: APÉNDICE CLÁUSULAS DE SEGURIDAD PARA PROVEEDORES.....	237
ANEXO 26: PROCEDIMIENTO PARA GESTIÓN DE INCIDENTES.....	239
ANEXO 27: APÉNDICE REGISTRO DE INCIDENTES.....	244
ANEXO 28: POLÍTICA DE CONTINUIDAD DEL NEGOCIO.....	245
ANEXO 29: DECLARACIÓN DE CUMPLIMIENTO.....	251
ANEXO 30: INFORME DE PRUEBAS.....	252
ANEXO 31: APÉNDICE – FORMULARIO DE PRUEBAS.....	260
ANEXO 32: CERTIFICADO DE LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN DEL GOBIERNO PROVINCIAL DE LOJA.....	261
ANEXO 33: CARTA DE COMPROMISO.....	262
ANEXO 34: PERMISO DE ADVISERA.....	271
ANEXO 35: COMPROBANTE DE COMPRA ISO27001.....	271
ANEXO 36: APÉNDICE PLAN DE CAPACITACIÓN Y CONCIENCIACIÓN.....	273
ANEXO 37: CERTIFICACIÓN TRADUCCIÓN SUMMARY.....	276

Índice de Figuras

FIGURA 1. DIFERENCIA ENTRE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN-----	7
FIGURA 2. CICLO DE VIDA SGSI-----	9
FIGURA 3. ORGÁNICO ESTRUCTURAL.-----	29
FIGURA 4. FUNCIONES DE LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN.-----	29
FIGURA 5. MAPA TÉRMICO-----	36
FIGURA 6. MAPA DE CALOR DE LA SITUACIÓN ACTUAL.-----	42
FIGURA 7. ANÁLISIS ESTADÍSTICO DE LA SITUACIÓN ACTUAL.-----	42
FIGURA 8. FASES DEL MODELO.-----	50
FIGURA 9. PLAN DE PRUEBAS-----	56
FIGURA 10. MAPA DE CALOR FINALIZADAS LAS PRUEBAS.-----	63
FIGURA 11. GRÁFICO ESTADÍSTICO DESPUÉS DE LAS PRUEBAS.-----	63

Índice de Tablas

TABLA I.....	9
TABLA II.....	11
TABLA III.....	23
TABLA IV.....	31
TABLA V.....	32
TABLA VI.....	34
TABLA VII.....	35
TABLA VIII.....	36
TABLA IX.....	37
TABLA X.....	38
TABLA XI.....	58
TABLA XII.....	60
TABLA XIII.....	66
TABLA XIV.....	67
TABLA XV.....	67
TABLA XVI.....	68
TABLA XVII.....	68
TABLA XVIII.....	83
TABLA XIX.....	93
TABLA XX.....	104
TABLA XXI.....	106

1. Título

“Diseño de un modelo de Gestión de Seguridad de la Información, bajo el estándar ISO/IEC 27001:2013 para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja”.

2. Resumen

Seguridad de la Información se ha convertido en un campo muy aplicado actualmente en el ámbito tecnológico y operativo, porque ayuda a mantener nuestra información lo menos expuesta a terceros no autorizados. Con este fin, el presente Trabajo de Titulación tiene como objetivo diseñar un modelo para la Gestión de Seguridad de la Información, bajo el estándar ISO/IEC 27001:2013 para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

Para cumplir con este propósito, se toma como referencia los principios y las directrices que plantea la norma ISO/IEC 27001 en la versión 2013; y así proponer un modelo acorde a la situación actual y análisis de riesgos de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

Como resultado final se presenta un Modelo con seis fases: en la fase uno se realiza un diagnóstico de la situación actual de la institución, en relación a los procesos, controles, activos, roles y actividades del personal; las necesidades y requisitos legales que debe cumplir; durante la fase dos se lleva a cabo el proceso de gestión de riesgos utilizando la metodología SARO, donde se categoriza los riesgos, luego se establece los criterios de aceptación para finalmente obtener una matriz de riesgos. Para la fase tres se define los controles adecuados para mitigar los riesgos y mantener las incidencias al mínimo, mediante la creación de diversos documentos de políticas de seguridad con controles en cada política. En la fase cuatro se implementa los controles y procedimientos propuestos en la fase tres. En la fase cinco se valida el modelo mediante la ejecución de un plan de pruebas y presentando como resultado un informe de pruebas. Finalmente, se establece una sexta fase donde se aplican medidas correctivas para el funcionamiento adecuado del modelo.

Al finalizar se concluyó que el modelo ayuda a la prevención y detección de riesgos y vulnerabilidades que afectan a la información en cualquier formato; teniendo como resultado final un modelo que permite adoptar de forma efectiva un enfoque basado en procesos para la gestión de sus actividades y recursos.

Summary

Information Security is a topic currently applied highly in technological and operational fields because it helps minimize information exposed to unauthorized third parties, preventing information loss that leads to productive and financial problems. With the goal of reducing a problem in society and contributing a solution that improves the protection of information in a government entity, this Degree Project aims to design a model for Information Security Management under the ISO / IEC 27001:2013 standard for the Information Technology Directorate of the Loja Provincial Government.

The technology used is ISO / IEC 27001:2013, following the processes outlined, an evaluation of the 114 controls proposed in the standard was made, determining if they are applicable to the institution based on the risk analysis and the SARO methodology and evaluating the current level of compliance applied by the Information Technology Directorate of the Loja Provincial Government.

As a final result, a Model with six phases is presented, the first phase reveals the situation of the institution, in relation to the processes, controls, assets, roles and activities of the staff, this phase serves as a guide to start proposing the project to the managers; in the second phase, the risk management process was carried out using the SARO methodology; in the third phase, appropriate controls to mitigate risks and keep incidents to a minimum are defined; in the fourth phase, the controls proposed in phase three are implemented; in the fifth phase the model was validated using a test plan; and, finally, in the sixth phase, corrective measures are applied for the model's functionality.

It was concluded that the model helps prevent and detect risks and vulnerabilities that affect information in any format; with reliable information as a final result, which is essential in the manager's process of decision-making.

3. Introducción

En la actualidad la información es el activo más valioso y protegido por las empresas, esta puede optar diversas formas: impresa, escrita en papel, correo electrónico, digital, videos e incluso cuando hablamos con otra persona [1], dicha información está expuesta a amenazas y vulnerabilidades en todo momento lo que generalmente representa pérdidas económica[2]; la Seguridad de la Información mediante la aplicación de la ISO/IEC 27001:2013 no proporciona un proceso de buenas prácticas y una lista de controles ayuda a mitigar dichos riesgos para evitar daños que puedan terminan costándole mucho dinero a la empresa o institución[3].

Ante estas circunstancias, las empresas se ven en la necesidad de establecer estrategias y controles adecuados que permitan trabajar en un ambiente confiable y seguro, primando la protección de la información crítica y sus activos tecnológicos para garantizar una gestión segura de los procesos del negocio[3].

Para dar solución a esta necesidad, el presente Trabajo de Titulación tiene como objetivo principal Diseñar un modelo de Gestión de Seguridad de la Información, bajo el estándar ISO/IEC 27001:2013 para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

Para cumplir con el objetivo general del Trabajo de Titulación se definió cuatro objetivos específicos, los cuales son: a) Realizar un diagnóstico de la situación actual de la seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja por medio de los procesos descritos en la norma ISO/IEC 27001:2013; b) Definir políticas de seguridad bajo el estándar ISO/IEC 27001:2013 Anexo A (controles) necesarios para gestionar la seguridad de la Información para la Dirección de Tecnología de la Información del Gobierno Provincial; c) Definir un modelo para gestión de seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja bajo la norma ISO/IEC 27001:2013; d) Valorar el modelo mediante la implementación del mismo para la gestión de seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

La estructura del documento de Trabajo de Titulación es la siguiente:

- **Análisis de Trabajos Similares:** se abordan conceptos relacionados con la Seguridad de la Información, los principios que la rigen, terminología, definiciones, entre otros conceptos que ayudaron a sustentar los conocimientos aplicados en la ejecución del trabajo de titulación.
- **Materiales y Métodos:** permite detallar el contexto, proceso, los recursos (científicos, técnicos y éticos) y participantes aplicados para conseguir los objetivos específicos.
- **Resultados:** sirve para presentar toda la información relevante obtenida en la ejecución del Trabajo de Titulación.
- **Discusión:** se especifica la aceptación de la hipótesis alternativa y se analiza los resultados obtenidos desde el punto de vista del investigador con trabajos relacionados al tema de Investigación.
- **Conclusiones:** permite enumerar los resultados más relevantes rescatados obtenido al finalizar el trabajo de titulación.
- **Recomendaciones:** plantea aspectos a considerar para el desarrollo de futuros trabajos relacionados con Seguridad de la Información.

4. Revisión de Literatura

En esta sección se abordan conceptos relacionados a la Seguridad de la Información, los principios que la rigen, terminología, definiciones, entre otros. Se realizó la revisión de documentos obtenidos de fuentes confiables. Todo ello con la finalidad de obtener una idea clara sobre la temática del proyecto y su alcance.

4.1. Seguridad de la Información

La Seguridad de la Información está enfocada en proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema de información, para ayudar a una organización a cumplir con la misión y objetivos de negocio; mediante la implementación de controles preventivos y reactivos donde la información es el activo primordial, estos controles deben tener como punto principal el establecimiento de políticas, normas internas y externas, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo los activos de información [4]–[6].

4.1.1. Seguridad Informática

La seguridad informática es parte de la seguridad de la información; esta se encarga de la seguridad en el medio informático, mediante un conjunto de reglas, procesos y normas diseñadas para salvaguardar la información y los datos almacenados en un sistema informático, los medios de protección ayudan a mitigar y minimizar los riesgos asociados a la infraestructura tecnológica abarcando hardware y software [7],[8].

4.1.2. Diferencia entre Seguridad Informática y de la Información

Es importante tener presente la diferencia entre seguridad informática y seguridad de la información. Pese a su estrecha relación, se debe tener claro que: la seguridad informática se encarga de la seguridad, protección y resguardo de todo aquello relacionado al medio informático, mientras que; la seguridad de la información no se limita a eliminar virus, evitar que hackers puedan acceder a la red o suprimir el spam en el correo electrónico, la seguridad de la información abarca procedimientos que deben seguir los empleados y la dirección para garantizar la protección y resguardo de la información, la misma que puede estar presente en diferentes medios o formas[9],[10].

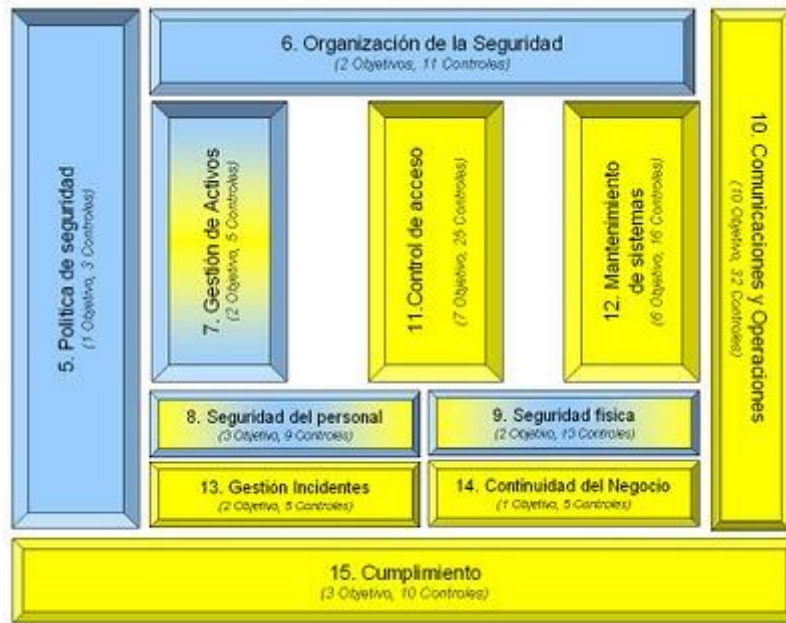


Figura 1. Diferencia entre Seguridad Informática y de la Información [11].

En la Figura 1 se presenta con mayor claridad la relación entre seguridad informática y de la información dentro de una organización. Las áreas sombreadas con color azul hacen referencia a la seguridad de la información y las áreas de color amarillo a la seguridad informática. Las áreas con dos colores, son las que hacen referencia a las dos, es decir que van de la mano [11].

4.1.3. Objetivos de la Seguridad de la Información

Los Objetivos principales de la seguridad de la información son los siguientes:

4.1.3.1. Disponibilidad

Asegura que los usuarios autorizados tengan acceso a la información y los activos asociados cuando sea requerido, es un requisito necesario para garantizar que el sistema trabaje puntualmente y que no se deniegue el servicio a ningún usuario autorizado. La Disponibilidad protege que la información sufra un borrado no autorizado de datos, de causar cualquier tipo de denegación de servicio y de los intentos de utilizar el sistema para propósitos no autorizados [12],[13].

4.1.3.2. Integridad

Salvaguarda la exactitud de la información en su procesamiento, es otras palabras que la información quede almacenada como quiere el usuario, sin ser alterada por terceros. De acuerdo con [12]–[14] la Integridad se presenta en dos fases.

- **Integridad de Datos:** los datos no son alterados por usuarios no autorizados, mientras se almacenan, procesas o trasmiten.
- **Integridad de Sistema:** el sistema no altera la información cuando realiza una función deseada

4.1.3.3. Confiabilidad

Asegura que la información sea accesible solo por aquellos que están autorizados, en otras palabras la confiabilidad es la base de la confianza que tiene como objetivo que las medidas de seguridad funcionen como se idearon; y cumpla con el principio de proteger el sistema y la información que procesa[12],[13].

4.2. Sistema de Gestión de Seguridad de la Información SGSI.

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de Seguridad de la Información, también conocido como ISMS por su equivalente en inglés (Information Security Management System) [15].

Es un enfoque sistemático que ayuda a pequeñas, medianas y grandes empresas a mantener seguros los activos de información. Incluye personas, procesos y sistemas de TI mediante la aplicación de un proceso de gestión de riesgos[16].

4.2.1. Ciclo de Vida del SGSI

El Dr. Williams Edwards Deming propuso el “Círculo de Deming” que es utilizado por la ISO/IEC 27001, este ciclo de vida está basado en la mejora continua, a través de la repetición de las fases de "Planificar-Hacer-Verificar-Actuar" conocido como (PHVA) o (PDCA) por sus siglas en inglés "Plan-Do-Check-Act). En la Figura 2 se presenta las fases del ciclo de vida del SGSI[14,][18].

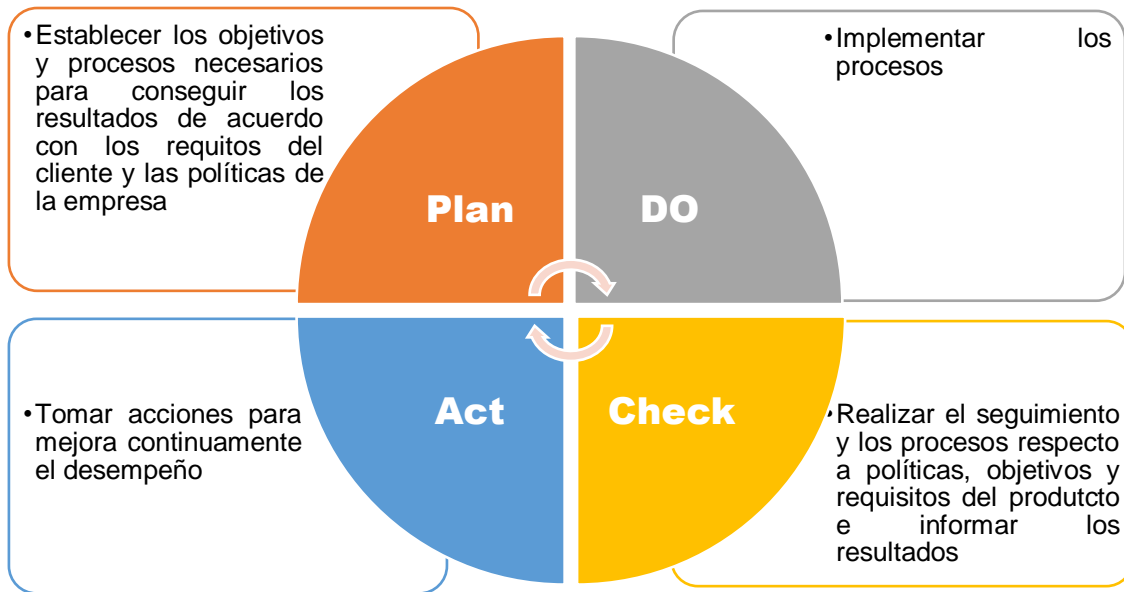


Figura 2. Ciclo de Vida SGSI[19].

La TABLA I ilustra las actividades del ciclo de vida "Planificar-Hacer-Verificar-Actuar" PHVA del Sistema de Gestión de Seguridad de la Información [20].

TABLA I.
FASES Y PROCESOS DEL SGSI [20].

Fase	Actividades
Planificar (Plan) Establecer el SGSI	<ul style="list-style-type: none"> • Establecer el contexto. • Alcance y Límites. • Definir Política del SGSI. • Definir enfoque de evaluación de riesgos. • Identificación de Riesgos. • Análisis y Evaluación de Riesgos. • Evaluar alternativas para el tratamiento de riesgos. • Aceptación de Riesgos. • Declaración de Aplicabilidad.
Hacer (DO) Implementar y Operar el SGSI	<ul style="list-style-type: none"> • Implementar plan de tratamiento de riesgos.

	<ul style="list-style-type: none"> • Implementar los controles seleccionados. Definir las métricas. • Implementar programas de formación y Sensibilización. • Gestionar la operación del SGSI. • Gestionar Recursos. • Implementar procedimientos y controles para la gestión de incidentes de seguridad.
<p>Verificar (Check) Hacer seguimiento y revisar el SGSI</p>	<ul style="list-style-type: none"> • Ejecutar procedimientos de seguimiento y revisión de controles. • Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. • Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. • Revisión de la evaluación de riesgos periódicamente. • Realizar auditorías internas. • Revisión de alcance y líneas de mejoras del SGSI por la Dirección. • Actualizar los planes de seguridad. • Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI.
<p>Actuar (Act) Mantener y mejorar el SGSI</p>	<ul style="list-style-type: none"> • Implementar las mejoras identificadas para el SGSI. • Implementar las acciones correctivas y preventivas pertinentes. • Comunicar acciones y mejoras a todas las partes involucradas. • Asegurarse que las mejoras logran los objetivos previstos.

4.3. Norma ISO/IEC 27001:2013.

“ISO (la Organización Internacional de Normalización) y IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización mundial”[21]. Estas organizaciones crearon la norma ISO/IEC 27001 que tiene la versión 2005 y 2013. Esta Norma Internacional está diseñada para ser aplicable a todos los usuarios, incluidas las pequeñas y medianas organizaciones; y ha sido preparada para proporcionar requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información[22].

4.3.1. Secciones de la Norma ISO/IEC 27001:2013.

En la TABLA II se presenta las 10 secciones que tiene la ISO/IEC 27001 más el anexo A; las secciones 0 a 3 son introductorias y no son obligatorias para la implementación, mientras que las secciones 4 a 10 son obligatorias. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad[23][24].

TABLA II
SECCIONES ISO/IEC 27001:2013[23].

Sección	Explicación
Sección 0 - Introducción	Explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.
Sección 1 - Alcance	Explica que esta norma es aplicable a cualquier tipo de organización y la obligatoriedad de cumplir con los requisitos específicos.
Sección 2 - Referencias normativas	Hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 - Términos y definiciones	Hace referencia a los términos y definiciones utilizados en la norma ISO/IEC 27000.
Sección 4 - Contexto de la organización	Esta sección es parte de la fase de Planificación del ciclo PHVA, identifica los problemas externos e internos de la organización, también define las partes interesadas, sus requisitos y el alcance del SGSI.
Sección 5 - Liderazgo	Esta sección es parte de la fase de Planificación del ciclo PHVA y define la relación y la responsabilidad de la alta dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.
Sección 6 - Planificación	Esta sección es parte de la fase de Planificación del ciclo PHVA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.
Sección 7 - Apoyo	Esta sección es parte de la fase de Planificación del ciclo PHVA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 - Funcionamiento	Esta sección es parte de la fase de Planificación del ciclo PHVA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.
Sección 9 - Evaluación del desempeño	Esta sección forma parte de la fase de Verificar del ciclo PHVA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.
Sección 10 - Mejora	Esta sección forma parte de la fase de Mejora del ciclo PHVA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.
Anexo A	Este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

Los 114 controles del Anexo A también se incluyen en el “reglamento de seguridad de la información, buen uso del internet, correo electrónico, control de los recursos informáticos y de telecomunicaciones de la contraloría general del estado” [25]

4.4. Gestión de Riesgos.

La gestión de riesgos se define como el proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de los desastres, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse[26].

4.4.1. Sistema de Gestión de Riesgo Operativo

Las Organizaciones deben conocer las diferentes etapas y elementos de la Administración de Riesgos Operativos (SARO), contribuyendo a reducción de la probabilidad de que ocurran aquellos eventos no previstos junto con los impactos que los mismos originarían[27].

4.4.2. Fases de Saro

Las fases para considerar en todo tipo de sistema de administración de riesgos operativos son:

- **Identificación:** Debe realizarse con anterioridad a la ejecución de cualquier proceso con el fin de identificar los riesgos operativos que han ocurrido, así como, aquellos riesgos operativos en potencia que van a suponer una serie de obstáculos de cara al logro de los objetivos definidos.
- **Medición o Evaluación:** Una vez que los riesgos operativos de los diferentes procesos han sido identificados, el siguiente paso es evaluar la posibilidad de materialización de estos (en función de la frecuencia con la que los mismos suceden) así como, definir el impacto que los mismos podrían generar en caso de ocurrencia. Como resultado de esta segunda etapa, establecemos el llamado riesgo inherente, que no es más que el nivel de riesgos que presenta una actividad concreta, sin aplicarle ningún tipo de control.
- **Control o Mitigación:** En esta tercera etapa, se busca definir las medidas de control que permitan reducir la probabilidad de ocurrencia y/o los impactos ocasionados por los riesgos inherentes detectados
- **Monitoreo:** se debe llevar a cabo el seguimiento adecuado a los riesgos con el fin de ir analizando su evolución[27].

5. Materiales y Métodos

De acuerdo con el Reglamento de Régimen Académico que rige a las Instituciones de Educación Superior de Ecuador, en el artículo 21, numeral 3, se estipula que un Trabajo de Titulación (TT) se basará en procesos de investigación e intervención [28]. Por otro lado, todo TT deberá consistir en una propuesta innovadora que contenga como mínimo una investigación exploratoria y diagnóstica, además, de acuerdo con el artículo 72 del mismo reglamento, la investigación a nivel de grado es de carácter exploratorio [29] y descriptivo [29]. La investigación exploratoria ayudó a definir el problema de investigación y a obtener información inicial sobre el tema a desarrollar, la investigación descriptiva ayudó a definir la situación actual de la dirección de tecnología de la información.

5.1. Contexto

El proyecto de Titulación se desarrolló en la Universidad Nacional de Loja, en la Facultad de Energía, Carrera de Ingeniería en Sistemas; la experimentación se llevó a cabo en la Dirección de Tecnología de la Información del Gobierno Provincial de Loja donde se desarrollaron los escenarios de pruebas y aprobación, que posteriormente permitirá extrapolar el modelo a otras instituciones con roles similares.

5.2. Proceso

Para alcanzar el objetivo general del presente proyecto de investigación se usó el siguiente proceso para cada uno de los objetivos específicos:

5.2.1. Diagnóstico de la situación actual de la seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja por medio de los procesos descritos en la norma ISO/IEC 27001:2013

- a. Se recolectó información de los controles de seguridad aplicados actualmente en la dirección de tecnología de la información del gobierno provincial de Loja (Ver sección 6. Resultados, subsección fase 1, apartado 6.1.1).
- b. Se recolectó Información de los activos tecnológicos existentes en la dirección de tecnología de la información del gobierno provincial de Loja (Ver sección 6. Resultados, subsección fase 1, apartado 6.1.2).

- c. Se recolectó información sobre las actividades y roles del personal (Ver sección 6. Resultados, subsección fase 1, apartado 6.1.3).
- d. Se recolectó información sobre los procesos que llevan a cabo (Ver sección 6. Resultados, subsección fase 1, apartado 6.1.4).
- e. Se definió el Alcance del MGSÍ (Ver sección 6. Resultados, subsección fase 1, apartado 6.1.5)
- f. Se realizó una evaluación de riesgos (Ver sección 6. Resultados, subsección fase 1, apartado 6.1.6)
- g. Se estableció criterios para aceptación de riesgos (Ver sección 6. Resultados, subsección fase 1, apartado 6.1.7).
- h. Se identificó los riesgos, amenazas y vulnerabilidades que presentan los activos de información del GPL (Ver sección 6. Resultados, subsección fase 1, apartado 6.1.8).
- i. Se elaboró un informe de la situación actual en la dirección de tecnología de la información del gobierno provincial de Loja (Ver sección 1. Resultados, subsección fase 2, apartado 6.1.9).

5.2.2. Definición de políticas de seguridad bajo el estándar ISO/IEC 27001:2013. Anexo A (controles) necesarios para gestionar la seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial.

- a. Se definió Políticas de Seguridad de la Información (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.1).
- b. Se definió la declaración de Aplicabilidad (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.2).
- c. Se definió Políticas de Organización de la Seguridad de la Información (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.3).
- d. Se definió Políticas de Seguridad de Recursos Humanos (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.4).
- e. Se definió Políticas de Gestión de Recursos (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.5).
- f. Se definió Políticas de Control de Acceso (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.6).
- g. Se definió Políticas de Criptografía (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.7).

- h. Se definió Políticas de Seguridad Física y ambiental (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.8).
- i. Se definió Políticas de Seguridad Operacional (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.9).
- j. Se definió Políticas de Seguridad de las Comunicaciones (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.10).
- k. Se definió Políticas de Adquisición, desarrollo y mantenimiento de Sistemas (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.11).
- l. Se definió Políticas de Relaciones con los proveedores (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.12).
- m. Se definió Políticas de Gestión de Incidentes en Seguridad de la Información (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.13).
- n. Se definió Políticas de Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.14).
- o. Se definió Políticas de Cumplimiento (Ver sección 6. Resultados, subsección fase 2, apartado 6.2.15).

5.2.3. Definición de un modelo para gestión de seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja bajo la norma ISO/IEC 27001:2013.

- a. Definición de las fases del modelo de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013 (Ver sección 6. Resultados, subsección fase 3, apartado 6.3.1).
- b. Elaboración la documentación necesaria para la elaboración del modelo gestión de la seguridad de la Información bajo la norma ISO/IEC 27001:2013 (Ver sección 6. Resultados, subsección fase 3, apartado 6.3.2).

5.2.4. Valoración del modelo mediante la implementación del mismo para la gestión de seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja

- a. Se definió un plan de pruebas. (Ver sección 6. Resultados, subsección fase 4, apartado 6.4.1).

- b. Se definió un escenario de pruebas (Ver sección 6. Resultados, subsección fase 4, apartado 6.4.2).
- c. Se ejecutó el modelo de acuerdo con el plan de pruebas (Ver sección 6. Resultados, subsección fase 4, apartado 6.4.4).

5.3. Recursos

Para dar respuesta a la pregunta de investigación y cumplir los objetivos planteados se usarán los siguientes recursos:

5.3.1. Científicos:

- Método científico: Este método se empleó en la recolección de información relacionada con el Trabajo de Titulación, a través de una investigación de documentos provenientes de fuentes confiables. Se reunió, seleccionó y analizó los datos necesarios para el desarrollo de las actividades y tareas del proyecto.
- Observación activa: mediante conversaciones espontáneas y observación directa se logró obtener información de las cuatro primeras actividades de la fase 1, sobre los controles, roles, activos y procesos de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja (Ver sección 6. Resultados, subsección fase 1, apartados 1.1 a 1.4).
- Encuesta: gracias a una encuesta realizada al Director de Tecnología de la Información, se estableció la situación actual de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja en cuanto a la implementación de los controles que manejan en relación a la seguridad de la información (Ver sección 6. Resultados, subsección fase 1, apartados 6.1.1 a 6.1.4).
- Método Analítico: fue uno de las más importantes, en primera instancia permitió identificar las necesidades de seguridad de la información en la Dirección de Tecnología de la Información del Gobierno Provincial de Loja. Necesidades que se ven reflejadas en el alcance y la aplicabilidad del modelo.

5.3.2. Técnicos:

- Metodología para Análisis de Riesgos: se seleccionó SARO como metodología para el Análisis de Riesgo, SARO es “el proceso de análisis de las exposiciones al riesgo

que enfrenta una empresa por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de información y por eventos externos”[30], esta técnica se la utilizó para realizar una correcta gestión de riesgos (Ver Sección 6. Resultados, Subsección Fase 1, Apartados 6.1.6 al 6.1.8).

- ISO/IEC-27001:2013: documentos que “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”[31], estos documentos sirven de guías durante todo el proceso de plantear el modelo, especialmente para la fase 2 y 3 del Proyecto de Titulación(Ver Sección 6. Resultados Subsección fase 2, apartados 6.2.1 al 6.2.15). Todas las plantillas utilizadas para implementación de la ISO/IEC 27001:2013 son propiedad de Adviesera.

5.3.3. Éticos:

- Acuerdo de Confidencialidad: mediante la carta de compromiso firmada entre la Facultad de Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja y la Dirección de Tecnología de la Información, se estableció un acuerdo de confidencialidad para evitar publicar información crítica que dañe la integridad de la Dirección de Tecnología de la Información (Ver sección 11. Anexos, Anexo 30).

5.4. Participantes

El proyecto de titulación fue ejecutado por Karla Andrea Correa Cumbicus, estudiante de la Carrera de Ingeniería en Sistemas, con la dirección técnica del Ingeniero Cristian Ramiro Narváez Guillen y Boris Marcel Díaz Pauta; y, asesoramiento académico del Ing. Luis Antonio Chamba Eras, Docentes de la Universidad Nacional de Loja. Además, con la colaboración del Ing. Pablo Raúl Vallejo, Ing. Rafael Almeida, Ing. Paulina Vidal, Ing. Fabian Calle, Cristian Lalangui, Ing. Jairo Silva, Personal de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

6. Resultados

Esta sección estuvo enfocada al cumplimiento de los objetivos, tanto el general como los específicos, este proceso fue dividido en cuatro fases, con sus respectivas tareas y actividades, las cuales se cumplió de forma ordenada y óptima.

En la fase 1, se realizó un reconocimiento de la situación actual del Gobierno Provincial de Loja, mediante el levantamiento de información (Controles, Procesos, Activos de Información, etc.); y, un análisis de riesgos de acuerdo con los procesos descritos en la norma ISO/IEC 27001:2013.

En la fase 2, se definió políticas descritas en el Anexo A de la norma ISO/IEC 27001:2013, para ayudar a gestionar la seguridad de la información en el Gobierno Provincial de Loja.

En la fase 3, se propone el modelo de gestión de seguridad de la Información, las fases a llevar a cabo y la documentación necesaria para ejecutar el modelo basado en la norma ISO/IEC 27001:2013.

En la fase 4, se ejecuta el modelo para poder validar su eficacia y eficiencia mediante un plan de pruebas y ejecutando la matriz de riesgos por segunda vez, para validar el modelo y comprobar como disminuye el mapa de calor.

Fase 1: Realizar un diagnóstico de la situación actual de la seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja por medio de los procesos descritos en la norma ISO/IEC 27001:2013.

En esta fase se realizó un diagnóstico de la situación actual de la dirección de tecnología de la información del Gobierno Provincial de Loja, teniendo como referencia los 114 controles que sugiere la ISO/IEC 27001:2013 en el ANEXO A.

6.1.1. Recolectar Información sobre los Controles de Seguridad Aplicados Actualmente en la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

En la Dirección de Tecnología de la Información del Gobierno Provincial de Loja se han definido diferentes acuerdos acordes con los objetivos y el contexto institucional, estos convenios son firmados por el Analista de Sistemas del departamento y el funcionario de la institución que utilizará el servicio.

Los acuerdos aplicados actualmente (Ver Anexo 1) son supervisadas y aprobadas por la dirección de tecnologías de la información, teniendo en cuenta la importancia de los servicios que brinda a los demás departamentos de la Institución.

Los acuerdos y procesos de la dirección de tecnología de la información del Gobierno Provincial de Loja están definidas en base al reglamento de seguridad de la información, buen uso del internet, correo electrónico, control de los recursos informáticos y de telecomunicaciones de la contraloría general del estado [25] con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información.

6.1.1.1. Recolectar Información en Base a la ISO/IEC 270001:2013 en el ANEXO A.

La ISO 270001:2013 en el ANEXO A contempla una lista de 114 controles que pueden ser aplicados para gestionar la seguridad de la información. Teniendo como antecedente esta lista controles (Ver Anexo 2), se hizo el levantamiento de información de los controles que aplica actualmente la dirección de tecnología de información.

De acuerdo con el Anexo 2, la dirección de tecnología de la información aplica 31 de los 114 controles de la ISO/IEC 27001:2013.

6.1.1.2. Información de Acuerdo con la Normativa de Contraloría General

Con base a la Normativa general del estado sobre la seguridad de la información, buen uso de internet, correo electrónico, control de los recursos informáticos y de telecomunicaciones[25], se realizó el levantamiento de información para establecer los acuerdos aplicados en la dirección de tecnología de la información del GPL.

Los acuerdos que tiene como referencia un documento formal son las siguientes:

Acuerdo de Confidencialidad

El usuario es el único responsable del acceso al sistema y los datos que maneja el mismo, y demás procedimientos de seguridad de acceso, de producirse un mal manejo de información el usuario perderá los privilegios otorgados hasta que se tome las medidas respectivas.

Acuerdo de Uso de Usuario y Contraseña

El usuario y contraseña que se proporciona son de naturaleza personal y confidencial, los mismos que pueden ser utilizadas únicamente por el funcionario que recibe el acceso, con el fin de garantizar la integridad de la información.

Acuerdo de Divulgación de Información

Toda la información con carácter confidencial que otorga a los usuarios y sea divulgada o dado un mal uso, el usuario será sancionado con la pérdida de privilegios o cese de funciones dependiendo de la falta cometida.

6.1.2 Recolectar Información de los activos tecnológicos existentes en la dirección de tecnología de la información del gobierno provincial de Loja.

Para recolectar información referente a la administración de los activos de información de la Dirección de Tecnología de la Información del GPL, se realizó mediante las actas entregadas a cada funcionario con los activos que tienen bajo custodia. A continuación, se muestra en la TABLA III todos los activos existen en el departamento, organizadas de acuerdo con su categoría.

TABLA III
INVENTARIO DE ACTIVOS

Código	Tipo	Cantidad	Característica	Descripción	Responsable
Lic001	Licencia	1			Ing. Pablo Vallejo
Lic002	Licencia	1			Ing. Paulina Vidal
Lic003	Licencia	1			Cristian Lalangui
Lic004	Licencia	1			Ing. Pablo Vallejo
Lic005	Licencia	1			Tatiana Belizaca

SO001	Sistema Operativo	2			Ing. Pablo Vallejo
SO002	Sistema Operativo	2			Ing. Paulina Vidal Ing. Rafael Almeida.
SO003	Sistema Operativo	3			Tatiana Belizaca Cristian Lalangui
SO004	Sistema Operativo	1			Ing. Rafael Almeida
SO004	Sistema Operativo	1			Ing. Fabian Calle
Sof002	software	1			Ing. Fabian Calle
Sof003	software	1			Ing. Fabian Calle
Sof004	software	1			Ing. Fabian Calle
Sof005	software	1			Ing. Fabian Calle
Sof006	software	1			Ing. Fabian Calle
Sof007	software	1			Ing. Fabian Calle

INFORMACIÓN CONFIDENCIAL

Sof008	software	1			Ing. Fabian Calle
Sof009	software	1			Ing. Fabian Calle
Sof010	software	1			Ing. Fabian Calle
AM001	Aplicación Móvil	1			Ing. Fabian Calle
AM001	Aplicación de Antivirus	1			Cristian Lalangui.
SW001	Sistema Web	1			Ing. Fabian Calle
SW001	Sistema Web	1			Ing. Fabian Calle
Ser001	Servicio	1			Ing. Rafael Almeida

INFORMACIÓN CONFIDENCIAL

Ser002	Servicio	1			Ing. Rafael Almeida
Ser003	Servicio	1			Ing. Rafael Almeida
Ser004	Servicio	1			Ing. Rafael Almeida
Ser005	Servicio	1			Ing. Rafael Almeida
Ser006	Servicio	1			Ing. Rafael Almeida
Ser007	Servicio	1			Ing. Rafael Almeida
Ser008	Servicio	1			Ing. Rafael Almeida
Ser009	Servicio	1			Ing. Rafael Almeida
Ser010	Servicio	1			Ing. Rafael Almeida
Tec001	Tecnología	12			Ing. Paulina Vidal
Tec002	Tecnología	2			Ing. Paulina Vidal
Tec003	Tecnología	1			Ing. Paulina Vidal

INFORMACIÓN CONFIDENCIAL

Tec004	Tecnología	1			Ing. Paulina Vidal
Tec005	Tecnología	1			Ing. Paulina Vidal
Tec006	Tecnología				Ing. Paulina Vidal
Tec007	Tecnología	3			Ing. Paulina Vidal
Tec008	Tecnología	14			Funcionarios de la Dirección de Tecnología de la
Tec009	Tecnología	10			Funcionarios de la Dirección de Tecnología de la
Tec0010	Tecnología	10			Funcionarios de la Dirección de Tecnología de la
Tec011	Tecnología	1			Ing. Pablo Vallejo
Tec012	Tecnología	2			Ing. Pablo Vallejo

INFORMACIÓN CONFIDENCIAL

Tec013	Tecnología	1			Ing. Pablo Vallejo
Tec014	Tecnología	2			Ing. Pablo Vallejo
Tec015	Tecnología	2			Ing. Pablo Vallejo
Tec016	Tecnología	2			Ing. Pablo Vallejo
Tec017	Tecnología	3			Christian Lalangui

INFORMACIÓN CONFIDENCIAL

6.1.3. Recolectar Información sobre las actividades y roles del personal.

En la Figura 3 se presenta el orgánico estructural de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.



Figura 3. Orgánico Estructural.

En la Figura 4 se presenta a cada departamento con las funciones acordes al servicio que brinda a las demás Direcciones del Gobierno Provincial; los funcionarios cumplen un cargo de acuerdo a las necesidades del departamento.

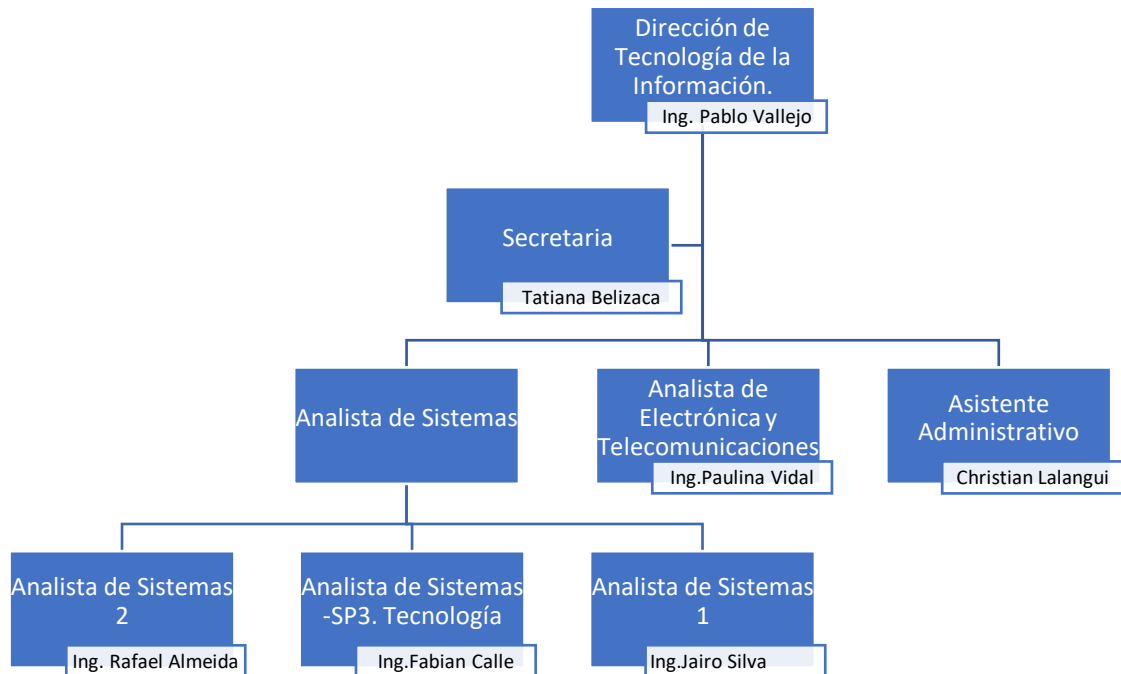


Figura 4. Funciones de la Dirección de Tecnología de la Información.

De acuerdo con la Figura 4, cada persona tiene la responsabilidad de preservar los activos entregados para mantener la integridad de la información, las funciones que cumple cada funcionario se encuentran descritas en la Resolución RP-RDE-035-2016 [32], sin embargo no cuentan con documentos formales para la delegación de funciones para cada miembro de la Dirección de Tecnología de la Información.

6.1.4. Recolectar Información sobre los procesos organizacionales.

Actualmente la Dirección de Tecnología de la Información realiza procesos propios de las entidades gubernamentales a nivel de apoyo, para la ejecución de planes, programas, proyectos y directrices para el buen desempeño de la gestión de la institución.

Cuando decimos que tiene procesos a nivel de apoyo, nos referíamos que tienen a su cargo actividades de soporte humano, materiales y servicios, logísticos requeridos por otros departamentos o por el mismo. Los procesos definidos actualmente se los realiza de forma empírica y no formal.

6.1.5. Definir Alcance del Modelo

En el alcance se definió los límites Modelo de Gestión de Seguridad de la Información en la Dirección de Tecnología de la Información del Gobierno Provincial de Loja, el alcance se aplica a toda la documentación del Modelo.

Tomando en cuenta los requisitos legales, normativos, contractuales y de otra índole, el alcance del Modelo de Gestión de Seguridad de la Información se definió de acuerdo con los siguientes aspectos: Procesos y Servicios, Unidades Organizativas, Ubicaciones, Redes e Infraestructura de TI y Exclusiones del Alcance (Ver Anexo 3).

6.1.6. Realizar una evaluación de los Riesgos.

Uno de los requisitos que exige la norma ISO/IEC 27001:2013 es realizar una evaluación de Riesgos, para iniciar este proceso, primero se realizó una comparativa entre diversas metodologías para análisis de riesgos (Ver Anexo 4); teniendo como referencia esta comparativa de las características más importantes, ventajas y desventajas, se seleccionó SARO como metodología para ser aplicada, considerando que es la metodología apropiada gracias a su sencillez, idioma y fases.

Una vez seleccionada la Metodología, se categorizó los riesgos que puedan presentarse en la Dirección de Tecnología de la Información, dividiendo los riesgos en categorías relevantes como esta en la TABLA IV, para una mayor comprensión de las amenazas y vulnerabilidades que puedan presentarse.

TABLA IV.
CATEGORÍA DE LOS RIESGOS.

Categoría	Descripción
Gestión	Riesgos relacionados a la aplicación incorrecta de gestión de TI.
Operación	Incumplimiento de Directrices, procedimientos, estándares en los procesos operativos.
Infraestructura	Riesgos relacionados con las fallas potenciales de la infraestructura tecnológica.
Seguridad	Eventos que atentan contra la confidencialidad, integridad y disponibilidad de la información.
Recurso Humano	Relacionados con el desempeño de los colaboradores.

Una vez categorizados los riesgos, se procedió a identificar cada uno de los riesgos que puedan presentarse, en la TABLA V se puede observar una lista de todos los riesgos identificados con la respectiva categoría a la que pertenecen.

TABLA V.
DESCRIPCIÓN DE RIESGOS.

ID	Descripción del Riesgo	Categoría
1		Gestión
2		Gestión
3		Gestión
4		Gestión
5		Gestión
6		Gestión
7		Gestión
8		Gestión
9		Gestión
10		Gestión
11		Gestión
12		Gestión
13		Gestión
14		Gestión
15		Gestión
16		Gestión
17		Operación
18		Operación
19		Operación

INFORMACIÓN CONFIDENCIAL

20		Operación
21		Operación
22		Operación
23		Operación
24		Operación
25		Operación
26		Operación
27		Operación
28		Infraestructura
29		Infraestructura
30		Infraestructura
31		Infraestructura
32		Infraestructura
33		Infraestructura
34		Seguridad
35		Seguridad
36		Seguridad
37		Seguridad
38		Seguridad
39		Seguridad
40		RRHH
41		RRHH

INFORMACIÓN CONFIDENCIAL

6.1.7. Establecer criterios para la aceptación de riesgos.

Para establecer los criterios para la aceptación de riesgos se los elaboró en base a la metodología seleccionada en el presente proyecto de titulación, es decir SARO [33].

6.1.7.1 Probabilidad

Para identificar la frecuencia de que ocurra cada riesgo se creó cinco valores de acuerdo a la metodología SARO [33], como se puede observar en la TABLA VI.

TABLA VI.
PROBABILIDAD DE LOS RIESGOS.

Nivel	Descripción
1. Muy Bajo	Muy bajo, puede ocurrir de 0 a 1 vez al año.
2. Bajo	Bajo, puede ocurrir cada semestre de 0 a 2 veces al año.
3. Medio	Medio, puede ocurrir cada trimestre de 0 a 5 veces al año.
4. Alto	Alto, puede ocurrir cada mes de 0 a 15 veces al año.
5. Muy Alto	Muy alto, puede ocurrir cada Quincena de 0 a 24 veces al año.

1.1. 7.2 Impacto

Para identificar el posible efecto que impida alcanzar los objetivos institucionales se creó cinco valores como podemos observar en la TABLA VII de acuerdo a la metodología aplicada, como lo es SARO [33].

TABLA VII.
IMPACTO DE LOS RIESGOS.

Nivel	Descripción
1. Insignificante	Daño insignificante, poca afectación a los objetivos institucionales, no afecta a las interrupciones de la institución, interrupción momentánea en la disponibilidad de la información, eventos que impiden al personal laborar con normalidad momentáneamente.
2. Menor	Daño menor, afecta levemente a los objetivos institucionales, interrupción momentánea de los servicios de TI, interrupción de 4 horas en la disponibilidad de la información, eventos que impiden al personal laborar por 4 horas.
3. Moderado	Daño moderado, afecta significativamente a los objetivos institucionales, interrupción significativa en los servicios TI, interrupción de 12 horas en la disponibilidad de la información, eventos que impiden al personal laborar por 12 horas.
4. Mayor	Daño mayor, el logro de los objetivos institucionales se ve afectado mayormente, interrupción de 24 horas en los servicios TI, Indisponibilidad de la Información e Impiden laborar al personal por 24 horas.
5. Catastrófico	Daño Catastrófico, Eventos que impedirán alcanzar los objetivos institucionales, no se termina el tiempo de recuperación de los servicios de TI y disponibilidad de la información, no se determina el tiempo de recuperación del personal.

1.1.7.3. Severidad

Para medir la severidad del riesgo se utilizó tres valores de acuerdo a como lo establece SARO [33], esos valores se visualizan en la TABLA VIII, donde se determinó un valor según el impacto y la probabilidad de que suceda un riesgo, es decir el nivel de exposición de los activos.

TABLA VIII.
SEVERIDAD DE RIESGO.

Valor	Nivel del Riesgo
6 a 9	Alto
3 y 4	Medio
1 y 2	Bajo

1.1.7.4. Mapa Térmico

En la Figura 5 se presenta el modelo el mapa térmico donde según la calificación del impacto y probabilidad el riesgo es calificado por un color de acuerdo con el número de severidad que tenga. El color rojo presenta severidad muy alta (crítico), el naranja alto (grave), el amarillo medio (tolerable) y el verde bajo (aceptable).

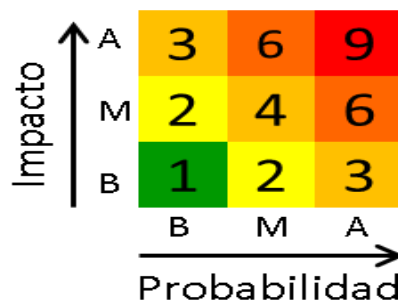


Figura 5. Mapa Térmico [33].

Teniendo como referencia al mapa término, los riesgos que tengan un valor de uno y dos, serán considerados como riesgo inherente o riesgos residuales.

6.1.8. Identificar los riesgos, amenazas y vulnerabilidades que presentan los activos de información

Teniendo en cuenta la evaluación de riesgos (Sección 6. Resultados, Apartado 6.1.6) y los criterios para aceptación de riesgos (Sección 6. Resultados, Apartado 6.6.1.7), se identificó las amenazas y vulnerabilidades que puedan presentarse en la Dirección de Tecnología de la Información; y, que puedan afectar a la confiabilidad, integridad y disponibilidad de la información, dichos riesgos y el proceso de evaluación se presentan en una matriz de evaluación de riesgos (Ver Anexo 5); los elementos que se utilizó en dicha matriz se presentan en la TABLA IX.

TABLA IX.
ELEMENTOS DE LA MATRIZ DE RIESGO.

N° de Riesgo	Número para identificar el riesgo.
Riesgo	Riesgo identificado en la sección 1.6 de Resultados.
Tipo de Riesgo	Categorización del Riesgo de acuerdo con la sección 1.6 de Resultados.
Fuente	Causa del Riesgo.
Consecuencia	Efecto en caso de que el riesgo ocurra.
Síntoma	Señal de alarma o advertencia que ayuda a identificar cuando un riesgo pueda suceder.
Impacto	Impacto en caso de que el riesgo se presente.
Probabilidad	Probabilidad de que el riesgo se presente.
Valor (1 al 9)	Valor de acuerdo con el mapa térmico de la sección 1.7.4 de Resultados.
Nivel (A/M/B)	Con base en valor de severidad de la sección 1.7.3 de Resultados.
Respuesta	Acción que se llevará a cabo para eliminar, mitigar o transferir el riesgo.
Responsable de la acción de Respuesta.	Nombre del responsable de ejecutar la acción de respuesta.

En la TABLA X se presentan los riesgos identificados con una criticidad alta y media, inicialmente se identificó 42 riesgos (Ver Anexo 5) pero se trabajará con los 34 riesgos que se considera que puedan causar una pérdida económica y afectar a la prestación de servicios de la Dirección de Tecnología de la Información.

TABLA X.
MATRIZ DE RIESGOS.

Matriz de Riesgos											
Proyecto:		Modelo de Seguridad de la Información									
ID:		F1.1									
Fecha de inicio:		22/01/2019									
Fecha de fin:		31/01/2019									
No. de Riesgo	Riesgo	Tipo de riesgo	Riesgo		Síntoma	Impacto (A/M/B)	Probabilidad (A/M/B)	Evaluación		Respuesta	Responsable de la acción de respuesta
			Fuente	Consecuencia				Valor (1 al 9)	Nivel (A/M/B)		
1	INFORMACIÓN CONFIDENCIAL					M	M	4	Medio	Realizar una correcta comunicación y participación del usuario final para el levantamiento de requerimientos.	Ing. Fabian Calle
2						M	M	4	Medio	Pruebas del producto final basadas en casos de usos. Aprobación del Análisis y Diseño antes de empezar a desarrollar.	Ing. Fabian Calle
3						A	M	6	Alto	Mayor Comunicación entre el proveedor y el comprador, establecer compromisos de entrega y garantías.	Ing. Pablo Vallejo
4						A	M	6	Alto	Adquisición de productos con arquitectura abierta.	Ing. Pablo Vallejo
5						A	M	6	Alto	Software para gestionar solicitudes de servicios y establecer niveles de soporte, con tiempo de espera e importancia de la incidencia.	Cristian Lalangui Ing. Fabian Calle

INFORMACIÓN
CONFIDENCIAL

6	A	M	6	Alto	Se analizan las cláusulas de las políticas y se giran las instrucciones de cada caso.	Ing. Pablo Vallejo
7	B	A	3	Medio	Información constante a los usuarios de las políticas para reportar incidentes, por correo electrónico o mediante capacitaciones.	Ing. Rafael Almeida
8	A	M	6	Alto	Controlar continuamente el avance del proyecto. Balancear las tareas de los colaboradores.	Ing. Pablo Vallejo
9	A	B	3	Medio	Verificar que se sigue la metodología correcta en los proyectos. Validar que se cumplen con los estándares establecidos.	Ing. Pablo Vallejo
10	A	M	6	Alto	Desarrollar un software exclusivamente para el control de licencias.	Ing. Pablo Vallejo
11	A	M	6	Alto	El usuario final no tiene privilegios para la instalación de software.	Cristian Lalangui
12	A	B	3	Medio	Realizar un esquema de seguridad para restringir accesos y establecer prioridades de los usuarios.	Ing. Paulina Vidal
13	A	B	3	Medio	Controlar el acceso al Data Center mediante cámaras de seguridad y biométrica. Sensores de Temperatura y Humedad	Ing. Paulina Vidal
14	A	B	3	Medio	Revisar documentación del proveedor. Aplicar primero en equipos de pruebas. Autorizar cada parche que será utilizado.	Cristian Lalangui Ing. Pablo Vallejo
15	A	B	3	Medio	Capacitación a los técnicos en productos nuevos. Se solicita al usuario una firma para aprobar la solución implementada.	Cristian Lalangui
16	M	M	4	Medio	Documentar cada problema con la solución implementada.	Cristian Lalangui
17	M	M	4	Bajo	Monitoreo constantes de los cambios tecnológicos implementados.	Ing. Rafael Almeida

INFORMACIÓN
CONFIDENCIAL

18	A	M	6	Alto	Definir procedimientos e instruido al personal. Bitácora de suspensión de servicios.	Ing Pablo Vallejo Ing. Rafael Almeida
19	A	M	6		Tener un servidor de respaldo con la misma información y programas que el principal.	Ing Pablo Vallejo Ing. Rafael Almeida
20	A	M	6	Alto	Comunicar mediante correo electrónico a los usuarios sobre el personal autorizado para instalar software.	Ing. Pablo Vallejo
21	A	M	6	Alto	Implementar sistema para que el usuario cambie la contraseña cada seis meses.	Ing. Rafael Almeida Ing. Fabian Calle
22	M	M	4	Medio	Implementar una red interna moderna y segura que tenga en cuenta estándares internacionales.	Ing. Paulina Vidal
23	M	M	4	Medio	Adquirir Generadores Electricos.	Ing. Pablo Vallejo
24	A	B	3	Medio	Plan de mantenimiento de los servidores, equipos de contingencia en caso de fallar el principal.	Ing Pablo Vallejo Ing. Paulina Vidal
25	A	B	3	Medio	Adecuar el ambiente del data center teniendo como referencia estándares internacioneles.	Ing. Paulina Vidal
26	A	B	3	Medio	Tener en cuenta en el POA el presupuesto para sistemas contra incendios.	Ing. Pablo Vallejo
27	A	M	6	Alto	Definición de politicas con responsabilidad a los usuarios.	Ing. Pablo Vallejo
28	A	M	6	Alto	Establecer perfiles limitados para modificación de equipos finales.	Cristian Lalangui
29	A	M	6	Alto	Definir roles y una descripción de cada uno.	Ing. Rafael Almeida

30	<p>INFORMACIÓN CONFIDENCIAL</p>	A	M	6	Alto	Control en el cumplimiento de las políticas de seguridad de la información.	Ing. Pablo Vallejo
31		A	M	6	Alto	Implementar mas controles de seguridad para ingresar, guella didital, contraseñas personalizadas.	Ing. Pablo Vallejo
32		A	M	6	Alto	Privilegios de Usuario Limitados, adquirir licencias.	Ing. Pablo Vallejo Cristian Lalangui.
33		M	A	6	Alto	Capacitaciones al personal con dificultades técnicas.	Cristian Lalangui.
34		A	B	3	Medio	Revisión del perfil de contratación.	Ing. Pablo Vallejo

De acuerdo al Matriz de Riesgo se logró determinar el Mapa de Calor (Ver Figura 6), se puede concluir que existen 34 riesgos con un nivel de criticidad alto y medio y 7 riesgos con un nivel bajo.

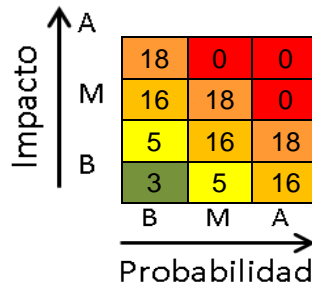


Figura 6. Mapa de Calor de la Situación Actual.

En la Figura 7 se presentan los resultados del Análisis de Riesgos de una forma gráfica para ayudar a entender mejor la situación actual y conocer cuántos riesgos pueden impactar a la disponibilidad de los servicios de TI y en función de su criticidad establecer los controles y las acciones correctivas y preventivas.

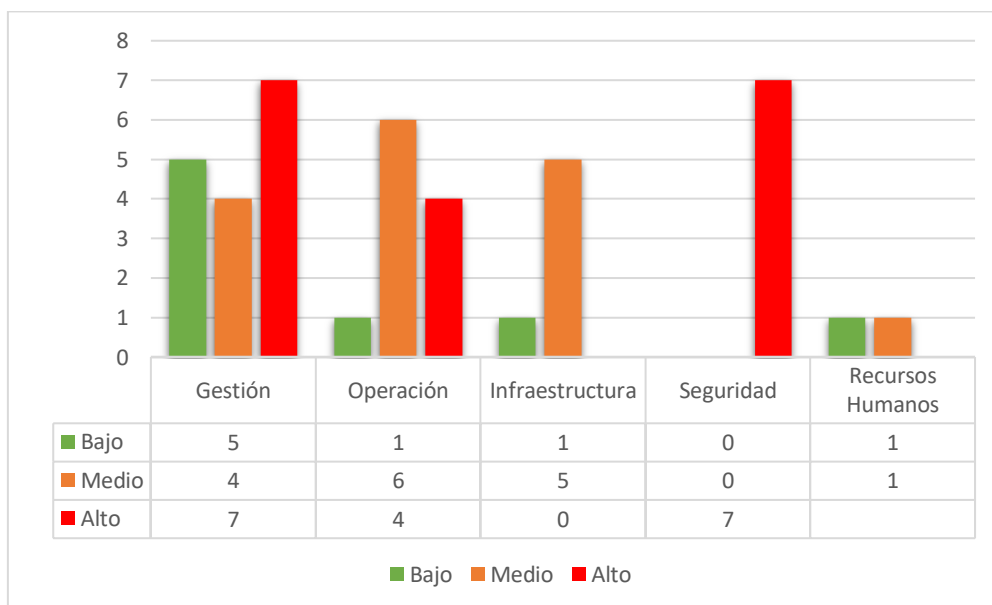


Figura 7. Análisis Estadístico de la Situación Actual.

6.1.9. Analizar la información y elaborar un informe de la situación actual en la dirección de tecnología de la información.

El documento de informe de la situación actual (Anexo 6) contiene un resumen de procesos, controles, roles y actividades, como se recolectó la información relacionada con los activos, un breve resumen de la metodología de evaluación de riesgo, y finalmente se enumeran todos los riesgos que tienen un valor elevado de acuerdo con el cálculo del mapa térmico.

Fase 2: Definir políticas de seguridad bajo el estándar ISO/IEC 27001:2013. Anexo A (controles) necesarios para gestionar la seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial.

En esta sección se elaboró todas las políticas y controles del Anexo A de la ISO/IEC 27001:2013 que son aplicables a la Dirección del Tecnología de la Información del Gobierno Provincial de Loja, aplicando un total de 106 controles de seguridad de la información para mitigar los riesgos con un impacto alto, este análisis se lo realizó en el documento de declaración de aplicabilidad, donde analizamos los 114 controles de la ISO/IEC y de acuerdo al análisis de riesgos se determina que controles debe aplicarse y como se deberá aplicar.

6.2.1. Política de Seguridad de la Información

El propósito de esta Política de alto nivel (Ver Anexo 7) fue definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información, es el primer control que se aplica en esta fase porque ayuda con el cumplimiento de los objetivos institucionales y estrategia de la organización, sirviendo como base para la creación de las políticas restantes.

6.2.2. Declaración de Aplicabilidad.

La declaración de aplicabilidad fue uno de los documentos más importantes dentro de esta fase, es el documento donde se especificó qué controles son adecuados para implementar en la Dirección de Tecnología de la Información, cuáles son los objetivos de esos controles, cómo se implementan y el estado de la implementación. También tiene como objetivo aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados. En este documento (Ver Anexo 8) se analiza uno a uno los 114 controles detallados en el Anexo A de la norma ISO/IEC 27001:2013.

6.2.3. Políticas de Organización de la Seguridad de la Información

Las políticas de organización de la seguridad de la Información pertenecen a la primera sección de la ISO/IEC 27001:2013 en el Anexo A, dentro de esta sección se encuentran la política sobre dispositivos móviles y teletrabajo (Ver anexo 9), donde se aplicaron

controles para evitar el acceso no autorizado a dispositivos dentro o fuera la de Dirección de Tecnología de la Información; y, la política de trae tu propio dispositivo (Ver Anexo 10) más conocida como Bring Your Own Device (BYOD) donde se aplicaron controles que ayudan a la Dirección de Tecnología de la Información a mantener el control sobre la información mientras se accede a dicha información a través de dispositivos que no pertenecen a la organización.

6.2.4. Políticas de Seguridad de Recursos Humanos.

En esta sección del Anexo A de la ISO/IEC 27001, se elaboró dos documentos que son primordiales para el modelo; uno es la declaración de aceptación de los documentos del modelo de gestión de seguridad de la información (Ver Anexo 11), donde el usuario acepta todos los documentos relacionados con las políticas y se compromete a respetarlas; el otro documento es la Declaración de confidencialidad (Ver Anexo 12), donde se compromete a dar un tratamiento confidencial y no revelar a terceros información relacionada con la Dirección de Tecnología de la Información durante y después de finalizar el contrato.

6.2.5. Políticas de Gestión de Recursos.

En esta sección se elaboró dos documentos, el documento de Políticas de Clasificación de la Información (Ver Anexo 13), donde el principal objetivo de esta política fue garantizar que la información sea protegida a un nivel adecuado, para eso se estableció criterios de clasificación y niveles de confidencialidad de la información (pública, uso interno, restringida, confidencial), y como debe ser etiquetada la información; y, el documento de Políticas de Uso Aceptable (Ver Anexo 14), este documento sirvió para definir reglas para el uso de sistemas o de otros activos de información, como por ejemplo las actividades prohibidas al momento de utilizar los activos, devolución de activos, procedimiento para copias de seguridad, responsabilidad sobre la clave, uso de la clave y correo, etc.

6.2.6. Políticas de Control de Acceso.

En la política de control de Acceso (Anexo 15) se estableció controles para asegurar el acceso de usuarios autorizados a todos los sistemas, redes y servicios; mediante perfiles y derechos de usuarios a cada uno de los sistemas de información y una adecuada gestión de privilegio a cada servicio y cada perfil de usuario.

6.2.7. Políticas de Criptografía.

En la política de criptografía (Ver Anexo 16) tiene como objetivo definir el uso de los controles y claves criptográficas para proteger la confidencialidad, integridad y disponibilidad de la información, principalmente se enfocó en los sistemas individuales o la información que manejan a través de controles criptográficos donde se especificó para cada sistema la herramienta criptográfica, el algoritmo de encriptación y la longitud de la clave.

6.2.8. Políticas de Seguridad Física y ambiental.

En esta sección se definió un documento sobre políticas de pantalla y escritorio limpio (Ver Anexo 17), donde se aplicó controles para evitar el acceso no autorizado a la información en los puestos de trabajo, como también en las instalaciones y a los equipos compartidos.

6.2.9. Políticas de Seguridad Operacional.

En esta sección se definió diferentes controles que fueron plasmados en tres documentos diferentes; el primer documento es la política de creación de copias (Ver Anexo 18), en esta política se especificó el procedimiento para crear copias de seguridad; el segundo documento son medidas de seguridad definidas en la política de gestión de cambio (Ver Anexo 19), su objetivo primordial fue definir cómo se controlan los cambios en los sistemas de información; y, finalmente el documento de procedimientos operativos para TI y comunicación (Ver Anexo 20), su principal objetivo es garantizar el funcionamiento correcto y seguro de la tecnología de la información y comunicación, mediante controles para la gestión de seguridad de la red, servicios de red, eliminación y destrucción de equipos y soporte.

6.2.10. Políticas de Seguridad de las Comunicaciones.

En esta Sección se elaboró el documento de políticas de transferencia de la información (Ver Anexo 21), con el objetivo de asegurar la seguridad de la información y el software cuando son intercambiados dentro o fuera de la organización, mediante controles donde se establece los canales de comunicación electrónica y controles para las relaciones con entidades externas.

6.2.11. Políticas de Adquisición, Desarrollo y Mantenimiento de Sistemas.

En esta sección se elaboró la política de desarrollo seguro (Ver Anexo 22) más un apéndice de especificación de requisitos (Ver Anexo 23), en esta política se definieron controles para asegurar el desarrollo seguro de software y sistemas, mediante medidas de seguridad relacionadas con el desarrollo y mantenimiento, como por ejemplo como se hará la evaluación de riesgos para el proceso de desarrollo seguro, los principios de la ingeniería segura, requerimientos de seguridad, verificación y pruebas de la implementación de requerimientos de seguridad, los repositorios de códigos fuentes del software, el proceso a seguir para control de versiones y cambios, y la manera correcta de proteger los datos de pruebas.

6.2.12. Políticas de Relaciones con los Proveedores.

En esta sección se definió la política de seguridad para proveedores (Ver Anexo 24), con el objetivo tener controles que ayuden a la dirección de tecnología de la información a identificar los riesgos relacionados con proveedores, seleccionar a los proveedores adecuados, definir las cláusulas de seguridad del contrato, la forma adecuada en la que debe realizarse la revisión y control de los servicios para verificar que se están cumpliendo, y los cambios o finalización de servicios del proveedor. Adicional se creó un apéndice (Ver Anexo 25) con las cláusulas que se incluirán en el momento de redactar un contrato con un proveedor.

6.2.13. Políticas de Gestión de Incidentes en Seguridad de la Información.

En esta sección se elaboró el documento de procedimiento para gestión de incidentes (Ver Anexo 26) con la finalidad de garantizar la detección temprana de eventos y debilidades de seguridad, como también la rápida reacción y respuesta ante incidentes de seguridad; para eso se crearon controles que facilitan la recepción y clasificación de incidentes, procesos para el tratamiento de debilidades o eventos, medidas de seguridad para realizar un adecuado tratamiento de incidentes menores y graves, normas para aprender a partir de los incidentes, medidas disciplinarias por cada violación de las reglas. Adicional se creó el apéndice registro de incidentes (Ver Anexo 27), que servirá de ayuda para llevar un control de los incidentes o eventos que se presenten en un futuro.

6.2.14. Políticas de Aspectos de Seguridad de la Información de la Gestión de la continuidad del Negocio.

El documento de política para continuidad de negocio (Ver Anexo 28) relacionada con la seguridad de la información tiene prioridad definir el objetivo, alcance y reglas básicas para la gestión de la continuidad del negocio, donde se detallaron los productos y servicios claves, para garantizar que se cumplan todas las condiciones para reanudar las actividades comerciales ante el caso de un desastre u otro incidente disruptivo y cómo recuperará sus actividades dentro de plazos establecidos. Esta política intenta mantener a un nivel aceptable el daño producido por un incidente disruptivo.

6.2.15. Políticas de Cumplimiento.

En la Declaración de Cumplimiento (Anexo 29) se estableció un compromiso entre el colaborador y la Dirección de Tecnología de la Información, para ayudar a la identificación de las leyes y regulaciones aplicables, además de aceptar no romper las políticas y normas de seguridad planteadas en la sección 6. Resultados, subsección fase 2, apartado 6.2.1 al 6.2.14.

FASE 3: Definir un modelo para gestión de seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja bajo la norma ISO/IEC 27001:2013.

En esta sección se presentan las fases del modelo, el proceso y la documentación referente a cada fase. El modelo se basa en un ciclo de vida continuo, por lo que una vez finalizadas las 6 fases se debe volver a iniciar el ciclo. Para la ejecución del modelo debe existir una secuencia de fases no se pueden realizar actividades en paralelo. Es decir, no se pueden ejecutar tareas de implementación mientras aún se están desarrollando actividades de planificación.

6.3.1. Definir las fases del modelo de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013.

En la Figura 8, se presenta las fases del modelo de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013, las fases son de mejora continua es decir que cuando se termine la fase seis, vuelve a empezar la fase uno. El modelado esta basado en el estándar BPMN versión 2.0.

6.3.1.1. Fase 1 Planificar Proyecto.

Para empezar con la ejecución del modelo, primero se requiere obtener el apoyo de los Directivos, para lograr esta actividad se realiza antes un subproceso donde se identifican las necesidades que se solventarán al implementar este modelo, se lo puede realizar mediante un levantamiento de información o actualizando la información ya disponible de controles, activos, procesos, roles y actividades del personal; una vez identificada la situación actual se procederá a investigar los requisitos legales, normativos, contractuales y de otra índole que regulan a los Gobiernos Autónomos descentralizados.

En esta fase se define el alcance del Modelo de Gestión de Seguridad de la Información, donde incluye los procesos y servicios, ubicaciones, redes e infraestructura de TI que serán consideradas en el alcance, y las exclusiones de este.

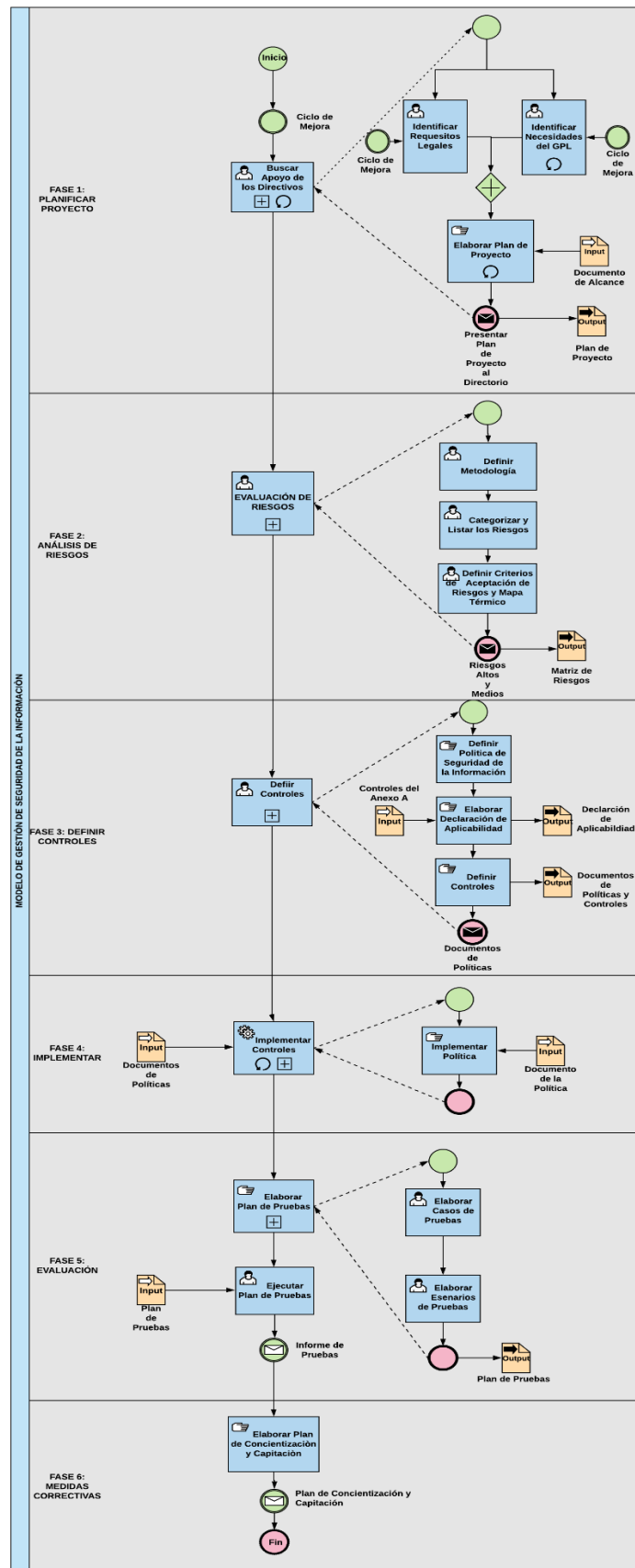


Figura 8. Fases del Modelo.

Para concluir, en esta fase se presentará un plan de proyecto con toda la información anterior a los directivos del Gobierno Provincial de Loja con el objetivo de conseguir el apoyo y los recursos necesarios para poner en ejecución el Modelo de Gestión de Seguridad de la Información. Si se consigue el apoyo se procederá a ejecutar la fase dos, caso contrario se volverá a iniciar el subproceso las veces que sea necesario.

6.3.1.2 Fase 2 Análisis de Riesgo.

En la fase 2, se define una metodología de evaluación del riesgo apropiada para el Modelo de Gestión de Seguridad de la Información y esta metodología debe ser compatible con la ISO/IEC 27001.

Además, se categoriza e identifica los riesgos que pueden presentarse, luego se establece los criterios de aceptación del riesgo; y finalmente se determina el mapa término para evaluar el impacto de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.

6.3.1.3. Fase 3 Definir Controles.

En la fase 3, se inicia con la elaboración de una política de seguridad de la información que incluya el marco general y los objetivos de seguridad de la información de la institución, requerimientos legales o contractuales relativos a la seguridad de la información y este documento debe ser aprobada por la dirección.

Además, se elabora el documento de declaración de aplicabilidad, este incluye los controles adecuados para implementar en la institución, cuáles son los objetivos de esos controles y cómo se implementan. También se aprobarán riesgos residuales y, la implementación de los controles mencionados. El documento de aplicabilidad incluye todos los controles detallados en el Anexo A de la norma ISO 27001; los controles serán creados acordes con la declaración de aplicabilidad, teniendo en cuenta que siempre debe estar dentro de las 13 secciones del Anexo A.

Dichas secciones se describen a continuación:

- **Organización de la seguridad de la información:** controles de cómo se asignan las responsabilidades, controles para los dispositivos móviles y el teletrabajo.
- **Seguridad de los Recursos Humanos:** controles antes, durante y después de contratar a colaboradores.
- **Gestión de recursos:** controles acerca de los privilegios de sistemas y servicios, también incluye controles para la clasificación de la información.
- **Control de Acceso:** controles de acceso, gestión de acceso de los usuarios, control de acceso para el sistema y las aplicaciones, y responsabilidades del usuario.
- **Criptografía:** controles relacionados con la gestión de encriptación y claves.
- **Seguridad física y ambiental:** controles para políticas de escritorio y pantalla despejadas.
- **Seguridad Operacional:** muchos de los controles relacionados con la gestión de la producción en TI.
- **Seguridad de las Comunicaciones:** controles relacionados con la seguridad de redes, servicios de redes, transferencia de información, mensajería, etc.
- **Adquisición, desarrollo y mantenimiento de Sistemas:** controles que definen los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte.
- **Relaciones con los proveedores:** controles acerca de qué incluir en los contratos, y cómo hacer el seguimiento a los proveedores.
- **Gestión de Incidentes en Seguridad de la Información:** controles para reportar los eventos y debilidades, definir responsabilidades, procedimientos de respuesta.
- **Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio:** controles para política de continuidad de negocios.
- **Cumplimiento:** controles que requieren la identificación de las leyes y regulaciones aplicables.

6.3.1.4. Fase 4 Implementar.

En la fase 4, se implementa todos los controles seleccionados en la declaración de aplicabilidad, teniendo como referencia los documentos de las 13 secciones del Anexo A, explicadas en la sección 6. Resultados, subsección fase 3, apartado 6.3.1.3

6.3.1.5. Fase 5 Evaluación

En esta fase el modelo plantea una evaluación, primero se elabora un plan de pruebas para evaluar cuantos controles se están aplicando y cuales están funcionando como deberían; además que se ejecuta nuevamente la Matriz de Gestión de Riesgos para verificar como bajo el mapa térmico después de la puesta en prueba del modelo.

6.3.1.6. Fase 6 Medidas Correctivas

En la fase 6 se elabora un documento de medidas correctivas, es decir una lista de actividades a realizar con responsabilidades, tareas y plazos bien definidos, además se elabora un plan de capacitación y concientización que debe ser socializado entre los colaboradores del departamento para que se sepan dónde se deben informar los problemas, quién debe revisarlos y los directivos tomen decisión sobre cómo resolverlos, quién es responsable de eliminarlos, etc.

6.3.2. Elaborar la documentación necesaria para la ejecución del modelo gestión de la seguridad de la Información bajo la norma ISO/IEC 27001:2013.

Para poner en ejecución el modelo para gestión de la seguridad se requiere documentos en cada una de las fases, el código de cada documento está dividido en dos partes, la primera especifica la fase en la que se utilizará; por ejemplo, FA01 para la fase uno, FA02 para la fase dos, etc., la segunda parte es el orden de los documentos, por ejemplo, DOC1 corresponde al documento uno, DOC2 corresponde al documento dos, y así sucesivamente. A continuación, los documentos a utilizar en cada fase:

6.3.2.1. Fase 1 Planificar Proyecto.

En esta fase es necesario realizar un documento externo con libre estructura para presentar el proyecto a los directivos, teniendo como antecedente el documento de alcance del proyecto (FA01-DOC1), levantamiento de la información de la situación

actual con relación a los activos, controles, procesos y roles del personal; y, la lista requisitos legales, normativos, contractuales y de otra índole.

6.3.2.2. Fase 2 Análisis de Riesgo.

Para llevar a cabo esta fase se necesita es necesario seguir el proceso explicado en la sección 6. Resultados, subsección fase 3, apartado 6.3.1.2, adicional a eso se recomienda utilizar la Matriz SARO (Sistema de Administración de Riesgo Operativo) con el código FA02-DOC1.

6.3.2.3. Fase 3 Definir Controles.

En esta fase es donde se elabora una mayor cantidad de documentos, para seguir un orden adecuado del modelo se recomienda utilizar los documentos con los códigos FA03-DOC1 al FA03-DOC17, adicional a esto se encuentran los apéndices, los cuales no tienen código porque son documentos opcionales.

6.3.2.4. Fase 4 Implementación.

En esta fase es recomendable implementar todos los controles mencionados en la fase tres, para ello se recomienda un documento con estructura libre donde se especifique el orden de implementación, la fecha y el responsable de ejecutar los controles.

6.3.2.5. Fase 5 Evaluación.

En esta fase se debe leer toda la documentación de Modelo de Gestión de Seguridad de la Información para familiarizarse con los controles (políticas, procedimientos y anexos), es recomendable crear una lista de verificación o utilizar el Apéndice Formulario de Pruebas (PLP01). Durante la ejecución de la evaluación se debe caminar por la dirección de tecnología de la información y hablar con los empleados, revisar las computadoras y otros equipos, observar la seguridad física, etc., cuando haya concluido el proceso de evaluación, se debe escribir un informe de pruebas.

6.3.2.6. Fase 6 Medidas Correctivas.

Se elabora un documento donde se define las reglas básicas para resolver acciones correctivas: cómo plantear una, dónde están documentadas, quién tiene que tomar qué decisiones, cómo controlar su ejecución, etc.; también debe constar cuáles serán las acciones correctivas, es decir los registros de no conformidades reales, decisiones y actividades realizadas para resolverlos, luego se debe socializar este documento con

los colaboradores para que sepan cuáles son las acciones a tomar y cuál debe ser el proceso a seguir por parte de ello. En el presente TT se planteó un Apéndice que servirá como Modelo para un Plan de Capacitación y Concienciación (Ver Anexo 36).

6.4.3. Ejecutar el modelo de acuerdo con el plan de pruebas.

Para validar el modelo se ejecutó el Plan de pruebas con cada caso, el resultado de esa ejecución se presenta en la TABLA X; en el informe de Plan de Pruebas (Ver Anexo 30) se puede comprobar como los riesgos con nivel de criticidad media y alta disminuyeron considerablemente

TABLA XI.
EJECUCIÓN PLAN DE PRUEBAS.

CASOS DE PRUEBAS Control de Versión: 1.0 Código de Documento: PLP01													
ETAPA DE DISEÑO								ETAPA DE EJECUCIÓN					
ID	PRUEBA REALIZADA	SISTEMA	OPCIÓN DE ACCESO	CASO DE PRUEBA	PASOS DEL CASO	PREREQUISITOS	DATOS DE ENTRADA	RESULTADO ESPERADO	FECHA EJECUCIÓN	CONTROL APLICADO	EJECUTADO POR	RESULTADOS OBTENIDOS	OBSERVACIONES
1	Negativa								27/02/2020	Política de Control de Acceso	Karla Correa	Prueba Exitosa	Ninguna
2	Positiva								27/02/2020	Política de Control de Acceso	Karla Correa	Prueba Exitosa	Ninguna
3	Positiva								27/02/2020	Política de Control de Acceso	Karla Correa	Prueba Exitosa	Ninguna
4	Positiva								27/02/2020	Política Trae tu propio dispositivo (BYOD)	Karla Correa	Prueba Exitosa	Ninguna
5	Positiva								27/02/2020	Declaración de Confidencialidad	Karla Correa	Prueba Exitosa	Ninguna
6	Positiva								27/02/2020	Política de Clasificación de la Información	Karla Correa	Prueba Exitosa	Ninguna
7	Positiva								27/02/2020	Política Uso Aceptable	Karla Correa	Prueba Exitosa	Ninguna
8	Positiva								27/02/2020	Política del Uso de Controles Criptográficos	Karla Correa	Prueba Exitosa	Ninguna
9	Positiva								27/02/2020	Política de Pantalla y Escritorio Limpio	Karla Correa	Prueba Exitosa	Ninguna
10	Positiva								27/02/2020	Procedimientos Operativos para TI y Comunicación	Karla Correa	Prueba Exitosa	Ninguna
11	Positiva								27/02/2020	Política de Transferencia de la Información	Karla Correa	Prueba Exitosa	Ninguna

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN
CONFIDENCIAL

12	Positiva					27/02/2020	Politica de Creación de Copias de Seguridad	Karla Correa	Prueba Exitosa	Ninguna
13	Positiva					27/02/2020	Politica de Desarrollo Seguro	Karla Correa	Prueba Exitosa	Ninguna
14	Negativa					27/02/2020	Politica de Control de Acceso	Karla Correa	Prueba Exitosa	Ninguna
15	Positiva					27/02/2020	Politica de Seguridad para Proveedores	Karla Correa	Prueba Exitosa	Ninguna
16	Positiva					27/02/2020	Declaración de aceptación de los documentos del modelo de gestión de seguridad de la información	Karla Correa	Prueba Exitosa	Ninguna
17	Positiva					27/02/2020	Politica de Control de Acceso	Karla Correa	Prueba Exitosa	Ninguna
18	Positiva					27/02/2020	Politica del Uso de Controles Criptograficos	Karla Correa	Prueba Exitosa	Ninguna
Resultado de Pruebas: Casos Planificados: 18 Casos Exitosos: 18 Casos Fallidos: 0 Casos no Ejecutados: 0										

En la TABLA XII se puede observar cómo disminuyeron los riesgos con criticidad alta y media, lo que nos ayuda a comprobar la efectividad del modelo.

TABLA XII
MATRIZ DE RIESGOS FINAL

Matriz de Riesgos											
Proyecto:		Modelo de Seguridad de la Información									
ID:		Fa.1									
Fecha de inicio:		17/02/2020									
Fecha de fin:		24/02/2020									
No. de Riesgo	Riesgo	Tipo de riesgo	Riesgo		Síntoma	Impacto (A/M/B)	Probabilidad (A/M/B)	Evaluación		Control Aplicado	Responsable de la acción de respuesta
			Fuente	Consecuencia				Valor (1 al 9)	Nivel (A/M/B)		
1	INFORMACIÓN CONFIDENCIAL					M	B	2	Bajo	Política de Seguridad con Proveedores Apéndice: Cláusulas de seguridad para proveedores y socios	Ing. Pablo Vallejo Ing. Fabian Calle
2						M	B	2	Bajo	Política de Desarrollo Seguro	Ing. Fabian Calle
3						B	B	1	Bajo	Política de Seguridad con Proveedores Apéndice: Cláusulas de seguridad para proveedores y socios	Ing. Pablo Vallejo Ing. Fabian Calle
4						B	B	1	Bajo	Política de Desarrollo Seguro	Ing. Pablo Vallejo
5						B	M	2	Bajo	Política de Desarrollo Seguro	Ing. Fabian Calle
6						A	B	3	Medio	Política de Seguridad con Proveedores Apéndice: Cláusulas de seguridad para proveedores y socios	Ing. Pablo Vallejo Ing. Fabian Calle
7						A	B	3	Medio	Política de Seguridad con Proveedores Apéndice: Cláusulas de seguridad para proveedores y socios	Ing. Pablo Vallejo
8						A	B	3	Medio	Política de Seguridad con Proveedores	Ing. Pablo Vallejo Ing. Fabian Calle
9						M	B	2	Bajo	Declaración de Aplicabilidad (Controles A.7.1.1 y A.7.1.2)	Ing. Pablo Vallejo
10						A	B	3	Medio	Declaración de aceptación de los documentos del modelo de gestión de seguridad de la información	Ing Pablo Vallejo

INFORMACIÓN
CONFIDENCIAL

11		B	B	1	Bajo	Procedimiento para Gestión de Incidentes Apéndice: Registro de Incidentes	Cristian Lalangui
12		B	M	2	Bajo	N/A	Ing. Rafael Almeida
13		A	B	3	Medio	Política de Desarrollo Seguro Apéndice: Especificaciones de requisitos de los sistemas de información	Ing. Fabian Calle
14		A	B	3	Medio	Política de Desarrollo Seguro Apéndice: Especificaciones de requisitos de los sistemas de información	Ing. Fabian Calle
15		A	B	3	Medio	Política de Desarrollo Seguro	Ing. Fabian Calle
16		A	B	3	Medio	Política de Seguridad con Proveedores Apéndice: Cláusulas de seguridad para proveedores y socios	Cristian Lalangui
17		A	B	3	Medio	Política de Control de Acceso Política de Uso de Controles Criptográficos	Ing. Paulina Vidal
18		A	B	3	Medio	Política de Pantalla y Escritorio Limpio	Ing. Paulina Vidal
19		B	B	1	Bajo	Política de Desarrollo Seguro	Ing. Fabian Calle
20		A	B	3	Medio	Política de Uso Aceptable Política de Control de Acceso	Ing. Rafael Almeida Ing. Pablo Vallejo
21		A	B	3	Medio	Procedimiento para Gestión de Incidentes Apéndice: Registro de Incidentes	Cristian Lalangui
22		M	B	2	Bajo	Apéndice: Registro de Incidentes	Cristian Lalangui
23		M	B	2	Bajo	Apéndice: Registro de Incidentes	Ing. Rafael Almeida
24		A	B	3	Medio	Procedimientos Operativos para TI y Comunicación	Ing. Pablo Vallejo Ing. Rafael Almeida
25		A	B	3	Medio	Política de Continuidad del Negocio	Ing. Pablo Vallejo Ing. Rafael Almeida
26		A	B	3	Medio	Política de Uso Aceptable Política de Control de Acceso	Ing. Pablo Vallejo
27		A	B	3	Medio	Declaración de confidencialidad Política de Uso Aceptable	Ing. Rafael Almeida Ing. Fabian Calle

INFORMACIÓN
CONFIDENCIAL

28	M	B	2	Bajo	<i>Política de Continuidad del Negocio</i>	Ing. Paulina Vidal
29	M	B	2	Bajo	<i>Política de Continuidad del Negocio</i>	Ing. Pablo Vallejo
30	B	B	1	Bajo	<i>Política de Pantalla y Escritorio Limpio</i>	Ing. Paulina Vidal
31	A	B	3	Medio	<i>Política de Continuidad del Negocio</i>	Ing. Pablo Vallejo Ing. Paulina Vidal
32	A	B	3	Medio	<i>Política de Continuidad del Negocio</i>	Ing. Paulina Vidal
33	A	B	3	Medio	<i>Política de Continuidad del Negocio</i>	Ing. Pablo Vallejo
34	A	B	3	Medio	<i>Declaración de confidencialidad Política de Uso Aceptable</i>	Ing. Pablo Vallejo
35	A	B	3	Medio	<i>Política de Uso de Controles Criptográficos</i>	Ing. Rafael Almeida
36	A	B	3	Medio	<i>Política de Control de Acceso</i>	Ing. Rafael Almeida
37	A	B	3	Medio	<i>Declaración de confidencialidad Declaración de Cumplimiento</i>	Ing. Pablo Vallejo
38	A	B	3	Medio	<i>Política de Pantalla y Escritorio Limpio</i>	Ing. Paulina Vidal
39	A	B	3	Medio	<i>Política de Control de Acceso</i>	Ing. Rafael Almeida Ing. Jairo Silva
40	M	B	2	Media	<i>Declaración de Aplicabilidad (Controles A.7.1.1 y A.7.1.2)</i>	Ing. Pablo Vallejo
41	B	B	1	Baja	N/A	Ing. Pablo Vallejo
42	A	B	3	Medio	<i>Declaración de Aplicabilidad (Controles A.7.1.1 y A.7.1.2)</i>	Ing. Pablo Vallejo

El mapa de calor (Figura 10) que se presenta, es el mapa obtenido una vez finalizadas las pruebas del modelo, se puede observar que los riesgos con nivel de criticidad alta, riesgos con criticidad media pasaron de 16 a 26, y con criticidad baja de 8 a 14. Es decir, ahora tenemos menor probabilidad que se presente un riesgo que pueda ocasionar daños económicos.

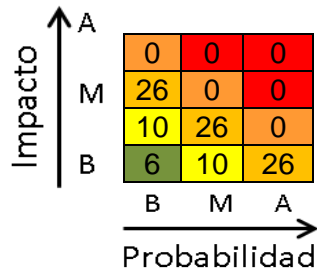


Figura 10. Mapa de Calor Finalizadas las Pruebas.

En la Figura 11 se presentan los resultados del Análisis de Riesgos una vez finalizadas las pruebas de una forma gráfica para validar como disminuyeron los riesgos



Figura 11. Gráfico Estadístico después de las Pruebas.

7. Discusión

El presente proyecto de titulación presenta a la Dirección de Tecnología de la Información del Gobierno Provincial de Loja, un modelo de gestión de seguridad de la información encaminado a establecer mecanismos de control adecuados para adoptar un nivel apropiado de seguridad a los activos de información pertenecientes a la institución, ayudando con ello a crear una cultura de seguridad de la información en el personal, dando los primeros pasos para la gestión de la información bajo estándares internacionales con la Norma ISO/IEC 27001.

7.1. Desarrollo de la Propuesta Alternativa

El presente Trabajo de Titulación “Diseño de un modelo de Gestión de Seguridad de la Información, bajo el estándar ISO/IEC 27001:2013 para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.”, se lo desarrolló en cuatro fases con el propósito de cumplir todos los objetivos planteados en el Anteproyecto. A continuación, se detallan las actividades realizadas para dar cumplimiento a cada uno de los objetivos.

Objetivo 1: Realizar un diagnóstico de la situación actual de la Seguridad de la Información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja por medio de los procesos descritos en la norma ISO/IEC 27001:2013

Los resultados de este objetivo permitieron identificar la situación actual de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja, para conocer sus amenazas y vulnerabilidades, y principalmente las medidas de seguridad aplicadas con el objetivo de mantener la información segura y confiable. Este objetivo es primordial para iniciar con el planteamiento del modelo, gracias a los resultados obtenidos en la Gestión de Riesgos (Ver Sección de 6 Resultados, Subsección 6.1, Apartados 6.1.6 a la 6.1.8)

Objetivo 2: Definir políticas de seguridad bajo el estándar ISO/IEC 27001:2013. Anexo A (controles) necesarios para gestionar la Seguridad de la Información para la Dirección de Tecnología de la Información del Gobierno Provincial

Los resultados de este objetivo se establecieron son controles de seguridad, empezando por la Política de Seguridad de la Información (Ver Anexo 7) para que sirva como referencia para otras políticas, seguidamente del documento de Declaración de Aplicabilidad (Ver Anexo 8), en este documento se establece que controles debemos aplicar y porque motivo debemos hacerlo, luego se planteó una serie de controles que los dividió en 14 secciones (Ver Sección 6 Resultados, Subsección 6.2 Apartado 6.2.2.3- Sección 2.15 de Resultados y Anexos 9 al 28) para ayudar mitigar los riesgos.

Estos resultados son primordiales para la ejecución del Modelo de Gestión de Seguridad de la Información, cada política establecida es una herramienta para combatir malos hábitos de seguridad, además de ser una guía de diversos controles que se pueden aplicarse a cualquier empresa que quiera cuidar su información privada.

Objetivo 3: Definir un modelo para gestión de Seguridad de la Información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja bajo la norma ISO/IEC 27001:2013

Con este objetivo se planteó las fases y el proceso que requiere el modelo de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013 para ejecutarlo (Ver Sección 6 Resultados, subsección 6.3.1, Apartado 6.3.1.1 al 6.3.1.6), y la documentación que requiere cada fase (Ver Sección 6 Resultados, subsección 6.3.2, Apartado 6.3.2.1 al 6.3.2.6).

Debemos tener en cuenta que el Modelo de Gestión de Seguridad de la Información bajo el estándar ISO/IEC 27001, es aplicable no solo al Departamento de Tecnología de la Información del Gobierno Provincial de Loja sino a cualquier empresa que desee hacer uso del mismo únicamente cambiarían los controles que se deben aplicar en la fase dos.

Objetivo 4: Valorar el modelo mediante la implementación del mismo para la Gestión de Seguridad de la Información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja bajo la norma ISO/IEC 27001:2013.

Los resultados de este objetivo avalan la funcionalidad del Modelo de Gestión de Seguridad de la Información, este modelo fue probado por equipo de la Dirección de Tecnología de la Información conjuntamente con la autora del presente Trabajo de Titulación, obteniendo como resultado un modelo funcional que ayuda a disminuir las amenazas y vulnerabilidades.

7.2. Valoración Técnica, Económica y Científica

La valoración del Trabajo de Titulación se expresa describiendo los beneficios presentados en cuatro aspectos:

7.2.1. Valoración Técnica

- A través del gestor bibliográfico Mendeley se automatizó la recolección de información confiable, este permite organizar las referencias de manera sencilla desde la Fuente.
- Mediante la Adquisición de la ISO/IEC 27001:2013.

7.2.2. Valoración Económica

Para llevar a cabo los objetivos que se plantearon en este proyecto fue necesaria la inversión en recursos como hardware y software, servicios, imprevistos y talento humano. Los cuales son detallados a continuación:

7.2.2.1. Talento Humano

El TT involucra al tesista y la asesoría de un docente de la Carrera cuyo costo es asumido por la Universidad Nacional de Loja. El tiempo empleado para el desarrollo del presente Trabajo de Titulación es de 480 horas. En la TABLA XIII se da a conocer el costo del talento humano.

TABLA XIII

TALENTO HUMANO

ROL	Número de Horas	Valor por Hora(\$)	Valor Total
Tesista	480.00	10,00	4800,00
Tutor	50.00	20,00	1000,00
Total (\$)			5.800,00

7.2.2.2. Recursos de Hardware y Software

Los recursos de hardware y software empleados en el trabajo de titulación se muestran en la TABLA XIV, representan todos los bienes que serán necesarios adquirir para realizar sin inconvenientes el desarrollo del presente proyecto.

TABLA XIV.

RECURSOS DE HARDWARE Y SOFTWARE.

Recursos	Cantidad	Valor Unitario	Valor Total
HARDWARE			
Laptop	1	1.500,00	1.500,00
Memoria Flash	2	15,00	30,00
Subtotal(\$)			1.530,00
SOFTWARE			
Mendeley	1	00,00	00,00
Word 2016	1	00,00	00,00
Subtotal(\$)			00,00
Total(\$)			1.530,00

7.2.2.3. Servicios

En el transcurso del Desarrollo del presente TT, fue necesario adquirir los servicios de transporte e Internet (Ver TABLA XV) para culminar con éxito las tareas que demanda el presente proyecto.

TABLA XV.

SERVICIOS.

Servicio	Cantidad	Valor Unitario	Valor Total
Transporte	200	0,30	60,00
Internet	400 h	0,75	300,00
ISO/IEC 27001	1	254,10	254,10
Total(\$)			614,10

7.2.2.4. Material de Oficina

Se empleó varios materiales de oficina, los cuales se describen en la TABLA XVI.

TABLA XVI.
MATERIALES DE OFICINA.

Recursos	Cantidad	Valor Unitario	Valor Total
Impresiones	786	0,05	39,3
Copias	786	0,02	15,72
Anillados	3	3,50	10,50
CDs	3	0,50	1,50
Empastados	1	30,00	30,00
Total (\$)			97,02

7.2.2.5. Presupuesto Final

Para imprevisto se tomó el 10% del valor total del presupuesto, los cuales se agregaron al valor total del proyecto y se muestran en la TABLA XVII.

TABLA XVII.
PRESUPUESTO TOTAL DEL TRABAJO DE TITULACIÓN.

RECURSO	SUBTOTAL
Talento Humano	5.800,00
Recursos de hardware y software	1 .530,00
Servicios	6114,10
Materiales de Oficina	97,02
Subtotal (\$)	8.041,12
Imprevistos 10 %	804,12
Total (\$)	8.844,24

7.2.3. Valoración Científica

- El presente TT presenta un aporte mediante una guía para trabajos futuros, teniendo en consideración las fases del modelo propuesto en este proyecto, se puede plantear uno similar para la Gestión de Análisis de Riesgos.

8. Conclusiones

- La Dirección de Tecnología de la Información del GPL no maneja políticas de Seguridad de la Información basadas en estándares internacionales, esto genera el inconveniente de no garantizar la correcta integridad, confiabilidad y disponibilidad de la información.
- La falta de registros históricos sobre los incidentes de Seguridad de la Información ocurridos en la institución y resueltos por la Dirección de Tecnología de la Información es un limitante al momento de identificar la presencia de posibles riesgos y sus soluciones.
- En base a la situación actual y los riesgos con nivel alto y medio; se seleccionó en la Declaración de Aplicabilidad 106 controles para ser implementados; teniendo como referencia los 114 controles del Anexo A de la ISO/IEC 27001:2013.
- La aplicación de la Norma ISO/IEC 27001 mediante los controles del Anexo A, permite cubrir las necesidades más importantes en la gestión de la información a nivel organizacional, esta engloba las mejores prácticas para conservar la confidencialidad, integridad y disponibilidad de la Información y se presentan en los documentos de las diferentes políticas.
- El Modelo de Gestión de Seguridad de la Información permite adoptar de forma efectiva un enfoque basado en procesos y mejora continua para la gestión de procesos, controles, actividades y recursos.
- El Modelo de Gestión de Seguridad de la Información propuesto en el presente Trabajo de Titulación es una herramienta para crear una cultura de Seguridad de la Información a nivel institucional mediante las medidas correctivas socializadas; además que ayuda a fomentar buenas prácticas dentro del personas que labora en el departamento de Tecnología de la Información del GPL.

9. Recomendaciones

- Revisar Constantemente el Apéndice Registro de Incidentes sirve de ayuda para mantener un registro histórico de incidentes y facilitar la gestión de riesgos al momento de valorar la probabilidad y el impacto que tienen los mismos
- El proceso de Análisis de Riesgo se debe realizar constantemente para saber la situación actual y poder implementar controles necesarios en ese momento.
- Considerar el Levantamiento de la Información y la Gestión de Riesgos para aplicar los controles adecuados para mitigar o transferir cada posible riesgo que se presente.
- Contratar Personal técnico especializado en Seguridad de la Información que ayude a implementar y ejecutar por completo el Modelo de Gestión de Seguridad de la Información.
- Cumplir los controles planteados en el modelo mediante seguimientos constantes de cada política para verificar que dichos controles son aplicados adecuadamente y siguiendo el procedimiento correcto.
- Implementar el Modelo de Gestión de Seguridad de la Información en otras Direcciones del Gobierno Provincial de Loja, el proceso para ejecutarlo es el mismo porque el modelo es adaptable a cualquier departamento o empresa.
- Como líneas futuras de investigación se recomienda implementar un Modelo para la Gestión de Continuidad de Negocios, un Modelo para la Gestión de Riesgos y un Modelo para la Gestión de Procesos.
- Como trabajo futuro, se recomienda implementar la fase de Auditoría donde se realizaría todo el proceso de control y auditoría, el cual debe ejecutarse antes de las medidas correctivas.

10 Bibliografía

- [1] D. Espinosa T., J. Martínez P., and S. Amador D., “Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC,” *Ing. USBmed*, vol. 5, no. 2, p. 33, 2014.
- [2] E. Martínez, “Una metodología para la gestión de riesgo aplicada a las MPYMES del Ecuador,” *Enfoque UTE*, vol. 8, p. 15, 2017.
- [3] A. Andrés and L. Gómez, “Guía de aplicación de la Norma UNE-ISO / IEC 27001 sobre seguridad en sistemas de información para pymes,” pp. 1–135, 2009.
- [4] J. Areitio Bertolín, *Seguridad de la información : redes, informática y sistemas de información*. Paraninfo Cengage Learning, 2008.
- [5] V. B. O. Percy Vicanco Muñoz, Augusto Cortez Vásquez, “La seguridad de la información,” vol. 8, no. 1, pp. 25–31, 2011.
- [6] G. Baca Urbina, “Introducción a la seguridad informática.,” Grupo Editorial Patria, México D.F., 2016.
- [7] B. Edber and B. Kelly, “Análisis en Seguridad Informática Y Seguridad de la Información Basado en la Norma Iso/lec 27001- Sistemas De Gestión De Seguridad De La Información Dirigido a Una Empresa De Servicios Financieros.,” UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL, 2015.
- [8] F. N. S. Solarte, E. R. E. Rosero, and M. del C. Benavides, “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001,” *Rev. Tecnológica - ESPOL*, vol. 28, no. 5, pp. 492–507, 2015.
- [9] R. Martha *et al.*, *Introducción a la Seguridad Informática y el Análisis de vulnerabilidades*, Primera. Alicante, 2018.
- [10] M. Soriano, *Seguridad en redes y seguridad de la información*, Primera. Republica Checa, 2014.
- [11] P. Carlos, “Seguridad informática y seguridad de la información en el mundo , como factor de enseñanza en Colombia,” Bogotá, 2018.
- [12] H. Ryan and E. Aguinaga, “Análisis y diseño de un sistema de gestión de

- seguridad de información basado en la norma ISO / IEC 27001 : 2005 para una empresa de producción y comercialización de productos de consumo masivo,” Pontificia Universidad Católica del Perú, 2013.
- [13] J. Areitio Bertolín, *Seguridad de la información : redes, informática y sistemas de información*. Paraninfo Cengage Learning, 2008.
- [14] R. B. José Fabian, *Seguridad informática*, Segunda. Madrid, 2013.
- [15] A. López Neira and J. Ruiz Spohr, “ISO27000.es - Gestión de Seguridad de la Información,” *El portal de ISO 27001 en español.*, 2017. [Online]. Available: <http://www.iso27000.es/sgsi.html>. [Accessed: 17-Feb-2019].
- [16] Organización Internacional de Normalización ISO, “ISO/IEC 27001 Information security management,” 2019. [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html>. [Accessed: 17-Feb-2019].
- [17] Á. M. Parra Giraldo, “Iso 27001 para pymes,” Universidad Internacional de La Rioja, 2014.
- [18] Calidad & Gestión and E. E. Consultoria Ambiental, Calidad, Seguridad, Inocuidad Alimentaria, “Ciclo Pdca - Estrategia Para La Mejora Continua,” *Argentina*, 2015. [Online]. Available: http://www.calidad-gestion.com.ar/boletin/58_ciclo_pdca_estrategia_para_mejora_continua.html. [Accessed: 17-Feb-2019].
- [19] W. A. Gaviria Álvarez, “Propuesta De Actualización De Políticas De Seguridad De La Información Del Sistema De Gestión De La Información De La Empresa Caso De Estudio, En La Sede Medellín De La Iso 27001:2005 A La Iso 27001:2013 Wilber,” UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, 2017.
- [20] A. López Neira and J. Ruiz Spohr, “ISO27000.es-Gestión de Seguridad de la Información,” *El portal de ISO 27001 en español.*, 2017. [Online]. Available: http://www.iso27000.es/sgsi_implantar.html#seccion1. [Accessed: 17-Feb-2019].
- [21] Organización Internacional de Normalización ISO, “ISO/IEC 27001:2013(en), Information technology — Security techniques — Information security management systems — Requirements.” [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>. [Accessed: 17-Feb-2019].
- [22] L. Organización Internacional de Normalización ISO- Barnaby, “Los auditores del

- Sistema de gestión de la seguridad de la información acogen con satisfacción la publicación ISO / IEC 27007,” *17 de octubre*, 2017. [Online]. Available: <https://www.iso.org/news/ref2232.html>. [Accessed: 17-Feb-2019].
- [23] Advisera, “¿Qué es norma ISO 27001?,” *27001Academy*, 2019. [Online]. Available: <https://advisera.com/27001academy/es/que-es-iso-27001/>. [Accessed: 17-Feb-2019].
- [24] ISOTools, “¿Cuál es la estructura de la nueva norma ISO 27001 2013?,” *ISOTools Excellence México*, 2017. [Online]. Available: <https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/>. [Accessed: 17-Feb-2019].
- [25] C. G. del Estado, *Acuerdo034 CG-2014Reglamento seguridad de la informacion.pdf*. 2014.
- [26] A. Brenes, “Gestión del Riesgo.”
- [27] ISOTools, “Etapas y elementos de la Administración de Riesgos Operativos,” *ISOTool, Plataforma Tecnológica para la Gestión de la Excelencia*, 2017. [Online]. Available: <https://www.isotools.com.co/etapas-y-elementos-de-la-administracion-de-riesgos-operativos-saro/>. [Accessed: 18-Feb-2019].
- [28] CES, “Reglamento de Régimen Académico,” no. 289, pp. 1–53, 2013.
- [29] M. G. Genero Bocco, Marcela Cruz Lemus, José A Piattini Velthuis, *Métodos de investigación en ingeniería del software*. Ma, 2014.
- [30] F. Corbalán and Printer Industria Gráfica Newco), *La Proporción áurea: el lenguaje matemático de la belleza y el arte*. RBA Coleccionables, 2010.
- [31] Organización Internacional de Normalizado, “ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements.” [Online]. Available: <https://www.iso.org/standard/54534.html>. [Accessed: 22-Jan-2019].
- [32] I. Rafael and D. Egüez, “Orgánico Funcional del Gobierno Provincial de Loja,” 2018.
- [33] ICETEX, “Manual de Sistema de Administracion de Riesgo Operativo.,” p. 131, 2014.
- [34] C. VALORES, “Manual del Riesgo Operativo,” *J. Chem. Inf. Model.*, vol. 8, no. 9, pp. 1–58, 2017.

- [35] “Beneficios que aporta a las organizaciones la gestión de riesgos operativos con un software (SARO).” [Online]. Available: <https://www.isotools.com.co/beneficios-aporta-las-organizaciones-la-gestion-riesgos-operativos-software-saro/>.
- [36] M. G. P. Cuenca, “Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO / IEC 27001 ,” 2015.
- [37] Precia, “Manual Sistema De Gestion,” 2019.
- [38] E. L. Chaparro Molina, “Diseño Del Sistema De Administracion De Riesgos Operativos (S.A.R.O) Para El Area De Beneficio De Fruta De La Empresa Unipalma De Los Llanos S.A,” Universidad Pedagogica Y Tecnologica De Colombia U.P.T.C, 2016.
- [39] K. G. Cordero Torres, “Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información,” 2015.
- [40] P. Crespo, “Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES,” *Univ. Cuenca*, 2016.
- [41] M. A. Amutio, J. Candau, and J. A. Mañas, “MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método,” *Minist. Hacienda y Adm. Públicas*, vol. 2006, no. 630-12-171–8, p. 127, 2012.
- [42] D. C. Goercke, “Políticas de Seguridad de la Información Aplicadas al Hospital Santa Inés,” Universidad del Azuay, 2013.
- [43] E. Montalban Loyola, E. Arenas Bernal, M. Talavera Ruz, and R. Magaña Iglesias, “Herramienta de mejora AMEF (Análisis del Modo y Efecto de la Falla Potencial) como documento vivo en un área operativa . Experiencia de aplicación en empresa proveedora para Industria Automotriz,” *Rev. Apl. la Ing.*, vol. 2, no. 5, pp. 230–240, 2015.
- [44] F. E. García and D. S. Aldás, “Metodología para el mejoramiento de la calidad a través del análisis de modos y efectos de falla (AMFE).”
- [45] L. R. Sánchez Sánchez, “COSO ERM y la gestión de riesgos,” *Quipukamayoc*, vol. 23, no. 44, pp. 43–50, 2016.
- [46] A. A. de S. P. Dias, “¿Auditoría más efectiva después de COSO ERM 2017 o de ISO 31000:2009?,” *Revista Perspectiva Empresarial*, vol. 4, no. 2, pp. 71–80,

- 2017.
- [47] D. E. Albanese, “Análisis y evaluación de riesgos: aplicación de una matriz de riesgo en el marco de un plan de prevención contra el lavado de activos,” *BASE - Rev. Adm. e Contab. da Unisinos*, vol. 9, no. 3, 2012.
- [48] ISO Tools, “www.isotools.com.co,” 2019. [Online]. Available: <https://www.isotools.com.co/sistema-administracion-del-riesgo-operativo-saro-administrar-los-riesgos/>.
- [49] J. M. F. Mozo, “Análisis del Modo y Efecto de Fallas (AMEF),” Universidad Privada del Norte, 2019.
- [50] C. de A. de F. S.A, “Sistema de Administración de Riesgos Operacionales,” pp. 1–23, 2011.
- [51] G. C. Sulca Córdova and E. R. Becerra Paguay, “Control interno. Matriz de riesgo: Aplicación metodología COSO II.,” *Rev. Publicando*, vol. 12, no. 2, pp. 106–125, 2017.
- [52] CERO, “Cero RiskmentSuite.” [Online]. Available: <https://www.riesgoscero.com/soluciones/risk-orm>. [Accessed: 17-Mar-2020].

11. Anexos

Anexo 1: Acuerdos Actuales



GOBIERNO PROVINCIAL DE LOJA
COORDINACIÓN DE INFRAESTRUCTURA TECNOLÓGICA

fecha: 11 de mayo de 2016

INFORMACIÓN CONFIDENCIAL

su usuario y password de acceso los cuales son de naturaleza confidencial. A fin de garantizar la privacidad de su información y mejorar los servicios, le hacemos conocer los siguientes datos:

INFORMACIÓN
CONFIDENCIAL

Quien recibe será responsable de informar mediante un documento (correo electrónico u oficio) al momento del cese de funciones o comisiones de servicio a la Coordinación de Infraestructura Tecnológica con la finalidad de que esta tome las medidas respectivas.

Quien recibe acuerda poner en conocimiento de la autoridad según corresponda, inmediatamente, cualquier comportamiento o situación sospechosa que puedan poner en peligro la información generada o manejada mediante el uso del acceso a la conexión de bases de datos del GOBIERNO PROVINCIAL DE LOJA.

INFORMACIÓN CONFIDENCIAL

Es de responsabilidad del funcionario quien recibe, dar cumplimiento a las recomendaciones de seguridad de la información antes mencionadas.

INFORMACIÓN CONFIDENCIAL

de Loja y demás procedimientos de seguridad de acceso, de producirse o presumirse el mal uso de la conexión, debe notificar mediante comunicación sea escrita o correo electrónico a la Dirección de Tecnología de la Información.

Quien recibe será responsable de informar mediante un documento (correo electrónico u oficio) al momento del cese de funciones o comisiones de servicio a la Dirección de Tecnología de la Información con la finalidad de que esta tome las medidas respectivas.

Quien recibe acuerda poner en conocimiento de la autoridad según corresponda, inmediatamente, cualquier comportamiento o situación sospechosa que puedan poner en peligro la información generada o manejada mediante el uso del acceso a la conexión ftp del servidor web del GOBIERNO PROVINCIAL DE LOJA.

La utilización de la conexión de acceso ftp del Gobierno Provincial de Loja, es de carácter personal y confidencial, la misma podrá ser utilizada únicamente por el usuario que recibe el mencionado acceso. **Con el objeto de proteger el uso del acceso a la conexión, se recomienda utilizar el equipo donde esta configurada la conexión, únicamente por el funcionario autorizado en este documento.**

Es de responsabilidad del funcionario quien recibe, dar cumplimiento a las recomendaciones de seguridad de la información antes mencionadas.

INFORMACIÓN CONFIDENCIAL

procedimientos de seguridad de acceso, de producirse o presumirse el mal uso de la conexión, debe notificar mediante comunicación sea escrita o correo electrónico a la Dirección de Tecnologías de la Información.

Quien recibe será responsable de informar mediante un documento (correo electrónico u oficio) al momento del cese de funciones o comisiones de servicio a la Dirección de Tecnologías de la Información, con la finalidad de que esta tome las medidas respectivas.

INFORMACIÓN CONFIDENCIAL

Es de responsabilidad del funcionario quien recibe, dar cumplimiento a las recomendaciones de seguridad de la información antes mencionadas.



GOBIERNO PROVINCIAL DE LOJA
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

fecha: 03 de julio de 2018

ACUERDO DE CONFIDENCIALIDAD PARA LA CONEXIÓN A LAS BASES DE DATOS DEL GOBIERNO PROVINCIAL
DE LOJA

INFORMACIÓN CONFIDENCIAL

La institución se los hace conocer por esta única ocasión y pone a su conocimiento el uso ético de los mismos es de su estricta responsabilidad.

INFORMACIÓN CONFIDENCIAL

Quien recibe será responsable de informar mediante un documento (correo electrónico u oficio) al momento del cese de funciones o comisiones de servicio a la Dirección de Tecnologías de la Información, con la finalidad de que esta tome las medidas respectivas.

Quien recibe acuerda poner en conocimiento de la autoridad según corresponda, inmediatamente, cualquier comportamiento o situación sospechosa que puedan poner en peligro la información generada o manejada mediante el uso del acceso a la conexión de bases de datos del GOBIERNO PROVINCIAL DE LOJA.

La utilización de la conexión de acceso a las bases de datos y archivos de la página web del Gobierno Provincial de Loja, es de carácter personal y confidencial, la misma podrá ser utilizada únicamente por el usuario que recibe el mencionado acceso. **Con el objeto de proteger el uso del acceso a la conexión, se recomienda utilizar el equipo donde esta configurada la conexión, únicamente por el funcionario autorizado en este documento.**

Es de responsabilidad del funcionario quien recibe, dar cumplimiento a las recomendaciones de seguridad de la información antes mencionadas.



GOBIERNO PROVINCIAL DE LOJA
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

fecha: 03 de julio de 2018

INFORMACIÓN CONFIDENCIAL

la conexión, debe notificar mediante comunicación sea escrita o vía correo electrónico a la Dirección de Tecnologías de la Información.

Quien recibe será responsable de informar mediante un documento (correo electrónico u oficio) al momento del cese de funciones o comisiones de servicio a la Dirección de Tecnologías de la Información, con la finalidad de que esta tome las medidas respectivas.

Quien recibe acuerda poner en conocimiento de la autoridad según corresponda, inmediatamente, cualquier comportamiento o situación sospechosa que puedan poner en peligro la información generada o manejada mediante el uso del acceso a la conexión de bases de datos del GOBIERNO PROVINCIAL DE LOJA.

La utilización de la conexión de acceso a las bases de datos y archivos de la página web del Gobierno Provincial de Loja, es de carácter personal y confidencial, la misma podrá ser utilizada únicamente por el usuario que recibe el mencionado acceso. **Con el objeto de proteger el uso del acceso a la conexión, se recomienda utilizar el equipo donde esta configurada la conexión, únicamente por el funcionario autorizado en este documento.**

Es de responsabilidad del funcionario quien recibe, dar cumplimiento a las recomendaciones de seguridad de la información antes mencionadas.



GOBIERNO PROVINCIAL DE LOJA
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

fecha: 21-08-2018

INFORMACIÓN CONFIDENCIAL

La institución se los hace conocer por esta única ocasión y pone a su conocimiento el uso ético de los mismos es de su estricta responsabilidad.

Quien recibe reconoce que es responsable por el uso **de la conexión y acceso a los archivos del cloudserver del Gobierno Provincial de Loja** y demás procedimientos de seguridad de acceso, de producirse o presumirse el mal uso de la conexión, debe notificar mediante comunicación sea escrita o vía correo electrónico a la Dirección de Tecnologías de la Información.

Quien recibe será responsable de informar mediante un documento (correo electrónico u oficio) al momento del cese de funciones o comisiones de servicio a la Dirección de Tecnologías de la Información, con la finalidad de que esta tome las medidas respectivas.

La utilización de la conexión de acceso a las bases de datos y archivos de la página web del Gobierno Provincial de Loja, es de carácter personal y confidencial, la misma podrá ser utilizada únicamente por el usuario que recibe el mencionado acceso. Es de responsabilidad del funcionario quien recibe, dar cumplimiento a las recomendaciones de seguridad de la información antes mencionadas.



GOBIERNO PROVINCIAL DE LOJA
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

fecha: 21-08-2018

INFORMACIÓN CONFIDENCIAL

La institución se los hace conocer por esta única ocasión y pone a su conocimiento el uso ético de los mismos es de su estricta responsabilidad.

Quien recibe reconoce que es responsable por el uso **de la conexión y acceso a los archivos del cloudserver del Gobierno Provincial de Loja** y demás procedimientos de seguridad de acceso, de producirse o presumirse el mal uso de la conexión, debe notificar mediante comunicación sea escrita o vía correo electrónico a la Dirección de Tecnologías de la Información.

Quien recibe será responsable de informar mediante un documento (correo electrónico u oficio) al momento del cese de funciones o comisiones de servicio a la Dirección de Tecnologías de la Información, con la finalidad de que esta tome las medidas respectivas.

La utilización de la conexión de acceso a las bases de datos y archivos de la página web del Gobierno Provincial de Loja, es de carácter personal y confidencial, la misma podrá ser utilizada únicamente por el usuario que recibe el mencionado acceso. Es de responsabilidad del funcionario quien recibe, dar cumplimiento a las recomendaciones de seguridad de la información antes mencionadas.

Anexo 2: Controles de la ISO/IEC 27001:2013 del Anexo A

TABLA XVIII.

CONTROLES DE ACUERDO AL ANEXO A.

Controles de Acuerdo con el Anexo A.	
Código	Control
A.5.1.1	Políticas para seguridad de la información.
A.5.1.2	Revisión de las políticas para seguridad de la información.
A.6.1.1	Funciones y responsabilidades de seguridad de la información.
A.6.1.2	Segregación de deberes.
A.6.1.3	Contacto con Autoridades.
A.6.1.4	Contacto con grupos de interés especiales.
A.6.1.5	Seguridad de la información en gestión de proyectos.
A.6.2.1	Política sobre dispositivos móviles.
A.6.2.2	Teletrabajo.
A.7.1.1	Selección.
A.7.1.2	Términos y condiciones de empleo.
A.7.2.1	Gestión de responsabilidades.
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información
A.7.2.3	Proceso disciplinario.
A.7.3.1	Terminación o cambio de condiciones del empleo.
A.8.1.1	Inventario de activos.
A.8.1.2	Propiedad de los activos.
A.8.1.3	Uso aceptable de los activos.
A.8.1.4	Devolución de activos.
A.8.2.1	Clasificación de la información.
A.8.2.2	Etiquetado de la información.
A.8.2.3	Manejo de activos.
A.8.3.1	Gestión de medios removibles.

INFORMACIÓN
CONFIDENCIAL

A.8.3.2	Eliminación de medios.	INFORMACIÓN CONFIDENCIAL
A.8.3.3	Transferencia de medios físicos.	
A.9.1.1	Política de control de acceso.	
A.9.1.2	Acceso a redes y a servicios de red.	
A.9.2.1	Registro y baja de usuarios.	
A.9.2.2	Concesión de acceso de usuarios.	
A.9.2.3	Gestión de derechos de acceso privilegiado.	
A.9.2.4	Gestión de información secreta de autenticación de usuarios.	
A.9.2.5	Revisión de los derechos de acceso del usuario.	
A.9.2.6	Eliminación o ajuste de derechos de acceso.	
A.9.3.1	Uso de información secreta de autenticación.	
A.9.4.1	Restricción al acceso a la información.	
A.9.4.2	Procedimiento de registro en el terminal.	
A.9.4.3	Sistema de gestión de claves.	
A.9.4.4	Uso de programas de utilidad privilegiada.	
A.9.4.5	Control de acceso al código fuente del programa	
A.10.1.1	Política del uso de controles criptográficos	
A.10.1.2	Gestión Clave	
A.11.1.1	Perímetro de seguridad física	
A.11.1.2	Controles físicos de ingreso	
A.11.1.3	Seguridad de oficinas, habitaciones e instalaciones	
A.11.1.4	Protección contra amenazas externas y ambientales	
A.11.1.5	Trabajo en áreas seguras	
A.11.1.6	Áreas de entrega y carga	
A.11.2.1	Ubicación y protección del equipo.	
A.11.2.2	Servicios públicos.	
A.11.2.3	Seguridad en el cableado.	
A.11.2.4	Mantenimiento de equipo.	

A.11.2.5	Eliminación de activos.	INFORMACIÓN CONFIDENCIAL
A.11.2.6	Seguridad de equipamiento y activos fuera de las instalaciones.	
A.11.2.7	Eliminación segura o reutilización del equipo.	
A.11.2.8	Equipo de usuario desatendido.	
A.11.2.9	Política de pantalla y escritorio limpio.	
A.12.1.1	Procedimientos documentados de operación.	
A.12.1.2	Gestión de cambio.	
A.12.1.3	Gestión de capacidad	
A.12.1.4	Separación de ambientes de desarrollo, prueba y operacionales.	
A.12.2.1	Controles contra software malicioso	
A.12.3.1	Copia de seguridad de la información	
A.12.4.1	Registro de eventos	
A.12.4.2	Protección de la información del registro	
A.12.4.3	Registros del administrador y operador	
A.12.4.4	Sincronización de relojes	
A.12.5.1	Instalación de software en sistemas operativos	
A.12.6.1	Gestión de vulnerabilidades técnicas	
A.12.6.2	Restricciones sobre instalación de software	
A.12.7.1	Controles de auditoría sobre los sistemas de información	
A.13.1.1	Controles de red	
A.13.1.2	Seguridad de los servicios de red	
A.13.1.3	Segregación en redes	
A.13.2.1	Procedimientos y políticas sobre transferencia de información	
A.13.2.2	Acuerdos sobre transferencia de información	
A.13.2.3	Mensajes electrónicos	
A.13.2.4	Acuerdos de confidencialidad o no divulgación	

A.14.1.1	Análisis y especificación de los requerimientos de seguridad de la información	INFORMACIÓN CONFIDENCIAL
A.14.1.2	Seguridad de servicios de aplicación en redes públicas	
A.14.1.3	Protección de transacciones de servicios de aplicaciones	
A.14.2.1	Política de desarrollo seguro	
A.14.2.2	Procedimientos para control en cambio de sistema	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma operativa	
A.14.2.4	Restricciones sobre los cambios en los paquetes de software	
A.14.2.5	Principios de ingeniería para sistema seguro	
A.14.2.6	Ambiente de desarrollo seguro	
A.14.2.7	Desarrollo externalizado	
A.14.2.8	Prueba de seguridad del sistema	
A.14.2.9	Prueba de aceptación del sistema	
A.14.3.1	Protección de datos de prueba	
A.15.1.1	Política de seguridad de la información para relaciones con proveedores	
A.15.1.2	Tratamiento de la seguridad en contratos con proveedores	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	
A.15.2.1	Monitoreo y revisión de los servicios de proveedores	
A.15.2.2	Gestión de cambios en los servicios de proveedores	
A.16.1.1	Responsabilidades y procedimientos	
A.16.1.2	Reporte de eventos en la seguridad de la información	

A.16.1.3	Reporte de debilidades en la seguridad de la información	INFORMACIÓN CONFIDENCIAL
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	
A.16.1.5	Respuesta ante incidentes de seguridad de la información	
A.16.1.6	Aprendizaje a partir de los incidentes en la seguridad de la información	
A.16.1.7	Recolección de evidencia	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	
A.18.1.1	Identificación de legislación y requerimientos contractuales aplicables	
A.18.1.2	Derechos de propiedad intelectual	
A.18.1.3	Protección de registros	
A.18.1.4	Privacidad y protección de información personalmente identificable	
A.18.1.5	Regulación de controles criptográficos	
A.18.2.1	Revisión independiente de la seguridad de la información	
A.18.2.2	Cumplimiento con las políticas y estándares de seguridad	
A.18.2.3	Revisión de cumplimiento técnico	

Anexo 3: Documento sobre el Alcance del MGSÍ



Gobierno Provincial de Loja

DOCUMENTO SOBRE EL ALCANCE DEL SGSÍ

Código:	FA01-DOC1
Versión:	0.1
Fecha de la versión:	03/01/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Público

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/01/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA.....	3
3. DEFINICIÓN DEL ALCANCE DEL SGSI	3
3.1. PROCESOS Y SERVICIOS	3
3.2. UNIDADES ORGANIZATIVAS	3
3.3. UBICACIONES	3
3.4. REDES E INFRAESTRUCTURA DE TI	3
3.5. EXCLUSIONES DEL ALCANCE	4
4. VALIDEZ Y GESTIÓN DE DOCUMENTOS	4

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir claramente los límites Modelo de Gestión de Seguridad de la Información en la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

Este documento se aplica a toda la documentación y actividades dentro MGSI.

Los usuarios de este documento son los miembros de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, punto 4,3

3. Definición del alcance del SGSI

La Dirección de Tecnología de la Información del Gobierno Provincial de Loja necesita definir los límites del MGSI para decidir qué información quiere proteger. Este tipo de información deberá ser protegida independientemente de si además es almacenada, procesada o transferida dentro o fuera del alcance del MGSI. El hecho de que determinada información esté disponible fuera del alcance no significa que no se le aplicarán las medidas de seguridad; esto solamente implica que la responsabilidad por la aplicación de las medidas de seguridad será transferida a un tercero que administre esa información.

Tomando en cuenta los requisitos legales, normativos, contractuales y de otra índole, el alcance del MGSI se define de acuerdo con los siguientes aspectos:

3.1. Procesos y servicios

Servicios:

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

Procesos:

INFORMACIÓN CONFIDENCIAL

3.2. Unidades organizativas

- Dirección de Tecnología de la Información
- Área Técnica de Infraestructura.
 - Data Center
- Soporte Técnico

3.3. Ubicaciones

Edificio A, Tercer Piso, Dirección de Tecnología de la Información.

3.4. Redes e infraestructura de TI

- Cortafuegos
- Servidores
- Switches (Todas las marcas y modelos)
- Routers.
- UPS.

3.5. Exclusiones del alcance

Los siguientes elementos no están incluidos en el alcance: los controles a realizarse no aplican para todo el Gobierno Provincial de Loja, son exclusivamente del departamento de Tecnología de la Información del Gobierno Provincial de Loja, se aplica únicamente para el inventario ubicado Edificio A, tercer Piso, Departamento de Tecnología de la Información del GPL.

4. Validez y gestión de documentos


Este documento es válido hasta el enero del 2021.

El propietario de este documento es el Director de Tecnología de la Información del Gobierno Provincial de Loja, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes que surgen por la definición poco clara del alcance del MGSI.
- Cantidad de medidas correctivas que se tomaron a raíz de la ambigua definición del alcance del MGSI.
- Tiempo dedicado por los empleados que implementan el MGSI para solucionar inconvenientes relacionados con el alcance poco claro.

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo

Director de Tecnología de la Información

Anexo 4: Comparativa de Metodologías

A. Evaluar las Metodologías para la Gestión del Análisis de Riesgos

Para evaluar la metodología a utilizar se tendrá en cuenta diversos parámetros que se adapten a las necesidades del proyecto; escoger una metodología en particular es un resultado difícil porque cada metodología ofrece una guía compuesta por etapas y procesos efectivos que permiten obtener resultados de calidad.

Para realizar esta evaluación del desempeño se requiere:

- Realizar un estudio de trabajos similares para tener claro, concepto, ventajas que ofrece cada metodología, fases, factores de riesgo y desventajas.
- Realizar una tabla comparativa con las características principales y más relevantes de cada metodología.

La calificación de evaluación de desempeño será de acuerdo a la TABLA XIX, esto ayudará a la selección de la metodología de gestión de riesgos apropiada para este escenario en particular.

TABLA XIX
CALIFICACIÓN DE EVALUACIÓN DE DESEMPEÑO

Calificación	Descripción
0	Muy Bajo
1	Bajo
2	Aceptable
3	Esperado
4	Destacado

Las metodologías analizar son: SARO (Sistema de Administración del Riesgo Operativo), CRAMM (Metodología para el Análisis y la Gestión de Riesgos) y Magerit (Metodología de Análisis, Gestión de los Sistemas de Información), AMEF (Análisis del Modo y Efecto de Fallas) y COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management).

❖ **SARO (Sistema de Administración del Riesgo Operativo)**

- **Concepto:** “Es un conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales se identifica, mide, controla y monitorea el riesgo operativo” Los riesgos operativos se dan, sobre todo, en 4 ámbitos distintos [33]:
 - Recursos humanos.
 - Procesos internos.
 - Tecnología de la Información.
 - Eventos externos.

- **Objetivos:**
 - Disminuir la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o, por la ocurrencia de acontecimientos externos, incluyendo aquellas situaciones relacionadas con asuntos legales y reputacionales [38].
 - Identificar y gestionar los riesgos que pudieran llegar a generar pérdidas[33].
 - Diseñar e implementar los controles que permitan tratar adecuada y eficientemente los riesgos y las causas identificados y valorados[33].
 - Disminuir la probabilidad de incurrir en pérdidas generadas por eventos[33].

○ **Fases:**

- **Identificación:** Comprende la caracterización de los subprocesos a evaluar, y una vez es conocido el subproceso completamente, se reconocen los riesgos operativos potenciales y/u ocurridos en dicho subproceso, así como las causas que los generan [34].
- **Medición:** se realiza con base en los criterios definidos, la medición de cada uno de los riesgos identificados, de ésta forma es posible cuantificar el nivel de riesgo inherente al cual se encuentra expuesta la Entidad[34].
- **Control:** tiene en cuenta la identificación y calificación de los diferentes controles que mitigan los riesgos operativos. Una vez ha sido realizada la calificación de los mismos se calcula el impacto de éstos sobre los riesgos inherentes encontrados y se encuentra la calificación de riesgo residual para cada uno de los riesgos encontrados [34].
- **Monitoreo:** establece la forma en la cual se va a realizar el seguimiento a la administración de los riesgos operativos, con el fin de mantener los niveles de riesgo en los establecidos por parte de la Junta Directiva de la Entidad. De igual forma en ésta etapa se encuentran establecidos todos los procedimientos relacionados con los cambios realizados al sistema y todo lo relacionado con la divulgación de Información tanto interna, como externa relacionada con el SARO [34].

○ **Ventajas:**

- Compatible con la norma ISO/IEC 27001[37].
- Fácil de implementar por la sencillez de sus fases [34].
- Se adapta a todo tipo de organizaciones [37].
- Busca reducir la cantidad de riesgos ocasionados por las personas [37].

- Ayuda a incrementar la eficiencia de las operaciones de la organización, al aportar un mayor control sobre sus vulnerabilidades[35].
 - Permite a las organizaciones adquirir un amplio conocimiento de manera anticipada y conscientemente de aquellos posibles riesgos que pueden generarse en las operaciones realizadas en el seno de la organización[35].
 - Fomenta una cultura de prevención y autocontrol[35].
- **Desventajas:**
- No cuenta con documentación específica para orientar su aplicación[36].
- **Factor de Riesgo:** Los factores de riesgo son las fuentes generadoras de eventos en las que se originan las pérdidas en los procesos y afectan la consecución de los objetivos estratégicos del Negocio [37]:
- **Recurso Humano:** Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad [38].
 - **Procesos:** Es el conjunto interrelacionado de actividades para transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad[37] [38].
 - **Tecnología:** Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: hardware, software y telecomunicaciones[38].
 - **Infraestructura:** Es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte [37][38].
 - **Relaciones Comerciales:** Corresponde a la fuente de riesgo que existe en las relaciones con otras entidades tales como proveedores, arrendatarios, contratistas, afiliados, clientes, etc. [37].

- **Administración de la Información:** Corresponde a aspectos relacionados con los criterios de Información, confidencialidad, Integridad y disponibilidad [37].
- **Eventos Naturales:** Corresponden a sucesos producidos por la fuerza de la naturaleza tales como terremotos, inundaciones, etc. [37].

❖ **CRAMM (Metodología para el Análisis y la Gestión de Riesgos)**

- **Concepto:** “Es una metodología para el análisis y gestión de riesgos, orientado a proteger la confidencialidad, la integridad y disponibilidad de un sistema y sus activos” [35].
- **Objetivo:**
 - Identificar las Amenazas, vulnerabilidades y evaluar los niveles de riesgos, dando orientación a los responsables de la seguridad para evitar los riesgos individuales, reduciéndolos a un nivel a aceptable [35].
- **Fases:**
 - Identificación y Valoración de Activos: Identificación y valoración de activos físicos[39].
 - Evaluación de los Riesgos y Requisitos de la seguridad: identificación de amenazas y calcular medidas de riesgo[39].
 - Contramedidas: Plan de Seguridad y estrategias [37].
- **Ventajas:**
 - Busca construir planes de continuidad de negocio y recuperación de desastres[36].
 - Compatible con la norma ISO/IEC 27001[36].

- **Desventajas:**
 - No cuenta con documentación específica para orientar su aplicación[36].

- **Factor de Riesgo:** Los factores de riesgo son las fuentes generadoras de eventos[40]:
 - Hardware y Software
 - Procedimientos
 - Elementos físicos
 - Personal
 - Entorno

- ❖ **MAGERIT (Metodología de Análisis y Gestión de los Sistemas de Información)**
 - **Concepto:** “Es un método formal que sirve para investigar los riesgos que soportan los sistemas de información existentes en cada una de las organizaciones para recomendar las medidas apropiadas que poco a poco deberían adoptar todas las organizaciones” [35].

 - **Objetivos:**
 - Concienciar a los responsables de todas las organizaciones de la existencia de riesgos, dando a conocer la necesidad de gestionar los mismo[39].
 - Ayudar a descubrir y planificar el tratamiento oportuno en caso de que los riesgos ataquen los activos de información[39].

 - **Fases:**
 - **Planificación:** La identificación de los riesgos busca una relación de los posibles puntos de peligro, para empezar a planificar el proyecto. Lo que se identifique será analizado en la siguiente etapa. Lo que no se identifique quedará como riesgo oculto o ignorado[41].

- **Análisis de Riesgos:** busca calificar los riesgos identificados, bien cuantificando sus consecuencias (análisis cuantitativo), bien ordenando su importancia relativa (análisis cualitativo). De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante [41].
 - **Gestión de Riesgos:** va un paso más allá del análisis técnico y traduce las consecuencias a términos de negocio. Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no, así como de en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento[41].
 - **Selección de Salvaguardas:** recopila las actividades encaminadas a modificar la situación de riesgo[41].

- **Ventajas:**
 - Ayuda a que las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles[42].
 - Se acopla a los requerimientos de la Norma ISO/IEC 27001 [36].
 - Se adapta a cualquier tipo de Organización[36].

- **Desventajas:**
 - Traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea costosa. [42]
 - El software desarrollado para esta metodología es de uso privativo y necesitamos comprar una licencia para utilizarla[36].

- **Factor de Riesgo:** Los factores de riesgo son las fuentes generadoras de eventos:
 - Hardware y Software [41].
 - Información Electrónica[41].

- Personas [41].
- Instalaciones [41].
- Medios de Soporte [41].

❖ AMEF (Análisis del Modo y Efecto de Fallas)

- **Concepto:** “es la identificación y evaluación de fallas potenciales de un producto o proceso, junto con el efecto que provocan éstas, con el fin de establecer prioridades y decidir acciones para reducir las posibilidades de rechazo y, por el contrario, favorecer la confiabilidad del producto o proceso”[43].
- **Objetivos:**
 - Identificar las posibles fallas en un producto, proceso o sistema [43].
 - Conocer a fondo el producto, el proceso o el sistema [43].
 - Identificar los efectos que puede generar cada falla posible [43].
 - Evaluar el nivel de criticidad (gravedad) de los efectos [43].
 - Identificar las causas posibles de las fallas [43].
- **Fases:**
 - **Determinar los modos de falla:** en esta fase se identifica la forma en la que una pieza o conjuntos pudiera fallar potencialmente a la hora de satisfacer el propósito de diseño/proceso, los requisitos de rendimiento y/o expectativas del cliente [44].
 - **Identificar las causas de los modos de falla:** Es la fase donde se identifica los riesgos que pueden ocurrir el modo de falla, en donde un modo de fallo puede tener más de una causa que lo origine[44].
 - **Determinar las prioridades:** Es donde se realiza una estimación de la probabilidad de detectar la falla, suponiendo que ya haya ocurrido. Para la valoración se tiene una escala del 1 al 10, en donde 1 es muy alta y 10 improbable detectar[44].

- **Ventajas:**
 - Ayuda a la evaluación de las exigencias del diseño, impulsando a la búsqueda de alternativas [43].
 - Origina que aumente la probabilidad de considerar los modos de fallos potencial, así como los efectos de estos en funcionamiento del sistema [43].
 - Se obtiene una información adicional, que apoya la mejora en la definición de pruebas y ensayos en el desarrollo del sistema [43].

- **Desventajas:**
 - Se enfoca más en procesos y productos[44].
 - No cuenta con una guía para su aplicación[44].

- **Factor de Riesgo**
 - **Productos:** El AMEF aplicado a un producto sirve como herramienta predictiva para detectar posibles fallas en el diseño, aumentando las probabilidades de anticiparse a los efectos que pueden llegar a tener en el usuario o en el proceso de producción [43].
 - **Procesos:** El AMEF aplicado a los procesos sirve como herramienta predictiva para detectar posibles fallas en las etapas de producción, aumentando las probabilidades de anticiparse a los efectos que puedan llegar a tener en el usuario o en etapas posteriores de cada proceso [43].
 - **Sistemas:** El AMEF aplicado a sistemas sirve como herramienta predictiva para detectar posibles fallas en el diseño del software, aumentando las probabilidades de anticiparse a los efectos que pueden llegar a tener en su funcionamiento [43].

- ❖ **COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management).**
 - **Concepto:** “es un proceso continuo realizado por el personal de todos los niveles de la organización y no únicamente, por un departamento de

riesgos o área similar , no es la mera conjunción de políticas, encuestas y formularios, sino que involucra gente de los distintos niveles de la organización y está diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre la consecución de objetivos”[45].

○ **Objetivos:**

- Mejorar la alineación entre rendimiento y ERM [46].
- Ajustar las expectativas de gobierno y supervisión [46].
- Reconocer la globalización y la necesidad de aplicar un enfoque común pero ajustado a la medida [46].
- Presentar nuevas formas de ver el riesgo al establecer y alcanzar objetivos en un contexto de una mayor complejidad [46].
- Expandir los informes para lograr una mayor transparencia [46] .
- Ajustarse a la evolución de la tecnología [46].

○ **Fases:**

- **Planificación:** se define los objetivos y el alcance del trabajo, los controles que deberían ser aprobados y documentados; se describe los procedimientos a ser ejecutados en la evaluación de controles; se organiza el equipo y/o encargado responsable[45].
- **Evolución de Riesgos:** debe considerarse el contexto mencionado y el riesgo debe ser identificado, analizado y evaluado. El riesgo del contexto se evalúa siguiendo la estructura de la organización. Posteriormente, se analiza su origen y los efectos que se produzcan. Solo cuando se culminen estas fases se puede tener una idea de cuánto importa ese riesgo, es decir, de su importancia o relevancia[46].
- **Tratamiento de Riesgos:** esta es la última fase del proceso y se refiere a todos los procedimientos necesarios para evitar que el riesgo se materialice [46].

- **Ventajas:**
 - Alinea el nivel de riesgo aceptado con la estrategia [45].
 - Une el crecimiento, riesgo y rendimiento [45].
 - Mejora las decisiones de respuesta al riesgo [45].
 - Minimiza sorpresas y pérdidas operativas [45].
 - Identifica y administra riesgos a nivel de la entidad [45].
 - Ayuda a Racionalizar el uso de recursos [45].

- **Desventajas:**
 - Está enfocado internamente y el contexto no está establecido en términos de factores externos e internos ni influencias [46].
 - Se ignoran las partes interesadas y su objetivo en términos de establecer los criterios de riesgo [46].
 - Los riesgos se ven como eventos, no se asocian al efecto de la incertidumbre en los objetivos [46].
 - Los riesgos solo se ven con una luz negativa y el tratamiento del riesgo (respuesta) solo se relaciona con su mitigación [46].
 - Se usa el riesgo inherente, concepto bastante confuso y defectuoso que es innecesario [46].

- **Factor de Riesgo:** Los factores de riesgo son las fuentes generadoras de eventos:
 - ❖ Nivel de Ingresos [47].
 - ❖ Localización Geográfica de las Actividades [47].
 - ❖ Modalidad de Operatoría (habitual, compleja) [47].
 - ❖ Trayectoria en la Actividad [47].

B. Tabla Comparativa de metodologías

Para llevar a cabo este método, se procedió a realizar una revisión de información mediante páginas oficiales [48], artículos científicos [8], tesis [40], manuales [33], etc., información que se tendrá en cuenta para el proceso de selección final (Ver TABLA XIX).

TABLA XX
COMPARATIVA DE METODOLOGÍAS

	SARO	CRAMM	Magerit	AMEF	COSO-ERM
Madurez de Tecnología	Versión 5.0 Año 2012[37]	Versión 5.0 Año 2011[36]	Versión 3.0 Año 2012[36]	Versión 3.0 Año 2015[49]	Versión 4.0 Año 2017[45]
Idioma	Español[50]	Inglés[36]	Español[36]	Español[43]	Español[45]
Ámbitos de Aplicación	Riesgos TIC / Riesgos Operativos [33].	Riesgos TIC para gobiernos/or ganizaciones [40].	Riesgos TIC para gobiernos/or ganizaciones [41].	Riesgos Operativos/ Riesgos para procesos y	Riesgos Operativos [51]

				Productos [49]	
Norma Internacional Compatible	ISO/IEC 27001, OSHAS 18001:2007, ISO/IEC 27002:2005, ISO 31000 [27].	ISO/IEC 27001, 27002, 27005 Y 31000 [39] [8].	ISO/IEC 27001, 27002, 27005 Y 31000 [39].	ISO 9001[49].	ISO 31000[46].
Herramienta Informática	Cero Risk ORM: Para Gestión de Riesgos Operacionales[52]	CRAMM V (Tiene 3 versiones: CRAMM Expert, CRAMM Express y BS7799) [36].	Pilar II: Es una herramienta que soporta el análisis y la gestión de riesgos de un sistema de información, basado en Magerit [36].	No tiene Herramienta [43].	No tiene Herramienta [45].

C. Resultado de Comparativa

Los resultados obtenidos mediante el análisis de las características establecidas para definir cada metodología se establecen los siguientes puntos, descritos en la TABLA XXI.

TABLA XXI
RESULTADO DE COMPARATIVA DE METODOLOGÍA

Características	Metodologías				
	SARO	CRAMM	MARGERIT	AMEF	COSO ERM
Compatible con la norma ISO/IEC 27001	5	5	5	0	0
Madurez de Tecnología (Versión)	5	3	3	3	4
Idioma (Español)	5	3	5	5	5
Herramienta	5	5	5	0	0
Compatible con Riesgos Tecnológicos	5	5	5	2	2
Compatible con Riesgos Operativos	5	2	2	5	5
Madurez de Tecnología (Año)	4	3	4	5	5
TOTAL	34	26	29	20	21

Se puede determinar que SARO cumple con la mayoría de características establecidas, haciendo uso de las características de mayor importancia como son: compatibilidad con la ISO/IEC 27001, idioma, fases simples, aplicables a riesgos tecnológicos, pocas desventajas, mejor oferta de ventajas.

Teniendo como antecedente este análisis se considera a SARO como la metodología apta para este proyecto de titulación

Anexo 5: Matriz de Riesgos

Matriz de Riesgos											
Proyecto:		Modelo de Seguridad de la Información									
ID:		F1.1									
Fecha de inicio:		22/11/2018									
Fecha de fin:		25/11/2018									
No. de Riesgo	Riesgo	Tipo de riesgo	Riesgo		Síntoma	Impacto (A/M/B)	Probabilidad (A/M/B)	Evaluación		Respuesta	Responsable de la acción de respuesta
			Fuente	Consecuencia				Valor (1 al 9)	Nivel (A/M/B)		
1	INFORMACIÓN CONFIDENCIAL					M	B	2	Bajo	Realizar una correcta comunicación y participación del usuario final para el levantamiento de requerimientos.	Ing. Fabian Calle
2						M	M	4	Medio	Pruebas del producto final basadas en casos de usos. Aprobación del Análisis y Diseño antes de empezar a desarrollar.	Ing. Fabian Calle
3						B	B	1	Bajo	Establecer un plan para estandarizar las versiones de software y actualizaciones.	Ing. Fabian Calle
4						B	B	1	Bajo	Supervisión constante de los productos desarrollados. Comunicación entre el Usuario que utilizará el software y el programador.	Ing. Pablo Vallejo
5						B	M	2	Bajo	Desarrollar conjuntamente el software y el manual, ofrecer información en línea sobre el manejo del mismo.	Ing. Fabian Calle
6						A	M	6	Alto	Mayor Comunicación entre el proveedor y el comprador, establecer compromisos de entrega y garantías.	Ing. Pablo Vallejo
7						M	M	6	Alto	Adquisición de productos con arquitectura abierta.	Ing. Pablo Vallejo
8						M	M	6	Alto	Software para gestionar solicitudes de servicios y establecer niveles de soporte, con tiempo de espera e importancia de la incidencia.	Cristian Lalangui Ing. Fabian Calle

INFORMACIÓN CONFIDENCIAL

9	M	B	2	Bajo	Planificación del POA tomando en cuenta materiales y recursos humanos para hacer más fácil el soporte. Firmar convenios con universidades para que mediante prácticas profesionales los estudiantes ayuden en el área de soporte	Ing. Pablo Vallejo
10	A	M	6	Alto	Se analizan las cláusulas de las políticas y se giran las instrucciones de cada caso.	Ing Pablo Vallejo
11	B	A	3	Medio	Información constante a los usuarios de las políticas para reportar incidentes, por correo electrónico o mediante capacitaciones.	Ing. Rafael Almeida
12	B	M	2	Bajo	Realizar un análisis de indicadores de desempeño y realizar una definición de métricas relevante a evaluar.	Ing. Rafael Almeida
13	A	M	6	Alto	Controlar continuamente el avance del proyecto. Balancear las tareas de los colaboradores.	Ing. Pablo Vallejo
14	A	B	3	Medio	Verificar que se sigue la metodología correcta en los proyectos. Validar que se cumplen con los estándares establecidos.	Ing. Pablo Vallejo
15	A	M	6	Alto	Desarrollar un software exclusivamente para el control de licencias.	Ing. Pablo Vallejo
16	A	M	6	Alto	El usuario final no tiene privilegios para la instalación de software.	Cristian Lalangui
17	A	B	3	Medio	Realizar un esquema de seguridad para restringir accesos y establecer prioridades de los usuarios.	Ing. Paulina Vidal
18	A	B	3	Medio	Controlar el acceso al Data Center mediante cámaras de seguridad y biométrica. Sensores de Temperatura y Humedad	Ing. Paulina Vidal
19	B	B	1	Bajo	Llevar un control de los cambios de versiones de software.	Ing. Fabian Calle
20	A	B	3	Medio	Revisar documentación del proveedor. Aplicar primero en equipos de pruebas. Autorizar cada parche que será utilizado.	Cristian Lalangui Ing Pablo Vallejo
21	A	B	3	Medio	Capacitación a los técnicos en productos nuevos. Se solicita al usuario una firma para aprobar la solución implementada.	Cristian Lalangui

INFORMACIÓN CONFIDENCIAL

22	M	M	4	Medio	Documentar cada problema con la solución implementada.	Cristian Lalangui
23	M	M	4	Bajo	Monitoreo constantes de los cambios tecnológicos implementados.	Ing. Rafael Almeida
24	A	M	6	Alto	Definir procedimientos e instruido al personal. Bitácora de suspensión de servicios.	Ing Pablo Vallejo Ing. Rafael Almeida
25	A	M	6		Tener un servidor de respaldo con la misma información y programas que el principal.	Ing Pablo Vallejo Ing. Rafael Almeida
26	A	M	6	Alto	Comunicar mediante correo electrónico a los usuarios sobre el personal autorizado para instalar software.	Ing. Pablo Vallejo
27	A	M	6	Alto	Implementar sistema para que el usuario cambie la contraseña cada seis meses.	Ing. Rafael Almeida Ing. Fabian Calle
28	M	M	4	Medio	Implementar una red interna moderna y segura que tenga en cuenta estándares internacionales.	Ing. Paulina Vidal
29	M	M	4	Medio	Adquirir Generadores Electricos.	Ing. Pablo Vallejo
30	B	M	2	Bajo	Establecer un plan para levantar una topología de red y reaccionar las etiquetas de los cables.	Ing. Paulina Vidal
31	A	B	3	Medio	Plan de mantenimiento de los servidores, equipos de contingencia en caso de fallar el principal.	Ing Pablo Vallejo Ing. Paulina Vidal
32	A	B	3	Medio	Adecuar el ambiente del data center teniendo como referencia estándares internacionales.	Ing. Paulina Vidal
33	A	B	3	Medio	Tener en cuenta en el POA el presupuesto para sistemas contra incendios.	Ing. Pablo Vallejo

INFORMACIÓN CONFIDENCIAL

34	A	M	6	Alto	Definición de políticas con responsabilidad a los usuarios.	Ing. Pablo Vallejo
35	A	M	6	Alto	Establecer perfiles limitados para modificación de equipos finales.	Cristian Lalangui
36	A	M	6	Alto	Definir roles y una descripción de cada uno.	Ing. Rafael Almeida
37	A	M	6	Alto	Control en el cumplimiento de las políticas de seguridad de la información.	Ing. Pablo Vallejo
38	A	M	6	Alto	Implementar mas controles de seguridad para ingresar, guella didital, contraseñas personalizadas.	Ing. Pablo Vallejo
39	A	M	6	Alto	Privilegios de Usuario Limitados, adquirir licencias.	Ing. Pablo Vallejo Cristian Lalangui.
40	M	A	6	Media	Capacitaciones al personal con dificultades técnicas.	Cristian Lalangui.
41	B	M	2	Baja	Motivación de acuerdo al personal.	Ing. Pablo Vallejo
42	A	B	3	Medio	Revisión del perfil de contratación.	Ing. Pablo Vallejo

Anexo 6: Informe Situación Actual



Gobierno Provincial de Loja

Informe Situación Actual

Código:	INF01
Versión:	Versión 0.1
Fecha de la versión:	04/02/2019
Creado por:	Karla Correa
Aprobado por:	Pablo Vallejo
Nivel de confidencialidad:	Restringido

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
04/02/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

OBJETIVO, ALCANCE Y USUARIOS	3
1. DOCUMENTOS DE REFERENCIA	3
2. PROCESO PARA RECOGER INFORMACIÓN	3
2.1. OBJETIVO DE RECOLECTAR INFORMACIÓN	3
2.2. ACERCA DE LOS CONTROLES	3
2.3. ACERCA DE LOS ACTIVOS	3
2.4. ACERCA DE LOS PROCESOS	3
2.5. ACERCA DE LOS ROLES Y ACTIVIDADES DEL PERSONAL	4
2.6. BREVE RESUMEN DEL PROCESO DE EVALUACIÓN DE RIESGO Y TRATAMIENTO DE RIESGOS.	4
3. VALIDEZ Y GESTIÓN DE DOCUMENTOS	5

Objetivo, alcance y usuarios

El objetivo del presente documento es presentar un resumen detallado situación actual y análisis de riesgos en la Dirección de Tecnología de la Información en el período septiembre 2018 a abril 2019.

La evaluación de riesgos se aplicó a todo el Modelo de Gestión de Seguridad de la Información (MGSI).

El presente documento está dirigido a la dirección de tecnología de la Información del Gobierno Provincial de Loja, a los propietarios de activos de información y a todas las personas involucradas en la planificación, implementación, supervisión y mejora del MGSI.

1. Documentos de referencia

- Norma ISO/IEC 27001.
- Documento sobre el alcance del SGSI
- Política de Seguridad de la Información
- Metodología de evaluación y tratamiento de riesgos.

2. Proceso para recoger información

El proceso para recolectar información ayuda a tener una visión general de la situación actual de la dirección de tecnología de la información en relación con la seguridad de la información, el proceso consiste en recolectar información de los controles, activos, roles del personal y procesos.

2.1. Objetivo de recolectar información

El objetivo del presente documento es definir la situación actual de la seguridad de la información en la dirección de tecnologías de la información.

2.2. Acerca de los Controles

INFORMACIÓN
CONFIDENCIAL

2.3. Acerca de los Activos

Cada Activo es entregado a un funcionario con un acta de recepción y donde se compromete a cuidar dicho activo, también existe un software denominado Sistema de Control de Bienes para dar seguimiento de esos bienes de forma

2.4. Acerca de los Procesos

La Dirección de Tecnología de la Información realiza procesos propios de las entidades gubernamentales a nivel de apoyo, como por ejemplo actividades de soporte humano, materiales y servicios; y, logísticos requeridos por otros departamentos o por el mismo para

la ejecución de planes, programas, proyectos y directrices para el buen desempeño de la gestión de la institución.

2.5. Acerca de los Roles y Actividades del Personal

En la Figura 1 se presenta a cada departamento, sus funciones van acordes al servicio que brinda a los demás departamentos; cada departamento tiene la responsabilidad de preservar los activos entregados a cada colaborador para mantener la integridad de la información. Dentro de cada departamento no cuentan con documentos formales para la gestión de incidentes, y delegación de funciones, por tal motivo los colaboradores realizan diferentes actividades de acuerdo con las necesidades que se presenta día a día.

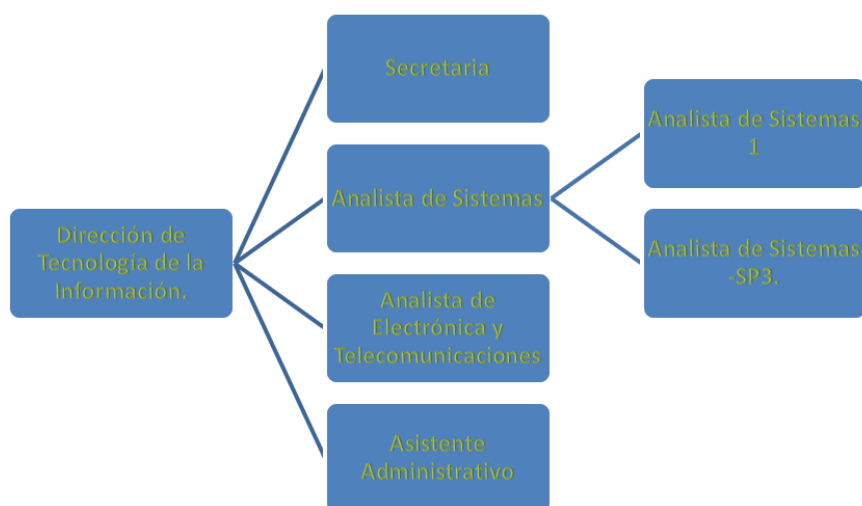


Figura 1 Funciones de la Dirección de Tecnología de la Información

2.6. Breve resumen del Proceso de Evaluación de Riesgo y Tratamiento de Riesgos.

En la evaluación de Riesgos, se seleccionó SARO como metodología para realizar el proceso de gestión de riesgos, para un mejor control de los riesgos se los categorizó en Gestión (riesgos relacionados a la aplicación incorrecta de gestión de TI), Operación (Incumplimiento de Directrices, Procedimientos, Estándares en los Procesos Operativos), Infraestructura (Riesgos Relacionados con las Fallas Potenciales de la Infraestructura Tecnológica), Seguridad (Eventos que Atentan Contra la Confidencialidad, Integridad y Disponibilidad de la información); y, Recurso Humano (Relacionados con el Desempeño de los Colaboradores).

Se identificaron 42 posibles riesgos que puedan presentarse en la Dirección de Tecnología de la Información, se los valoro con valores del 1 al 9, de acuerdo al criterio de aceptación de riesgos. Los riesgos que tenían valores medios y altos, fueron seleccionados para realizar los controles de seguridad para mitigar dichos riesgos, obteniendo el siguiente mapa de calor:

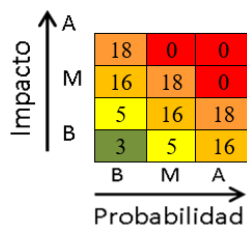


Figura 2 Mapa Térmico

De acuerdo al Mapa de Calor (Ver Figura 2), se puede concluir que existen 34 riesgos con un nivel de criticidad alto y medio y 8 riesgos con un nivel bajo.

3. Validez y Gestión de Documentos

Este documento es válido hasta el enero 2021.

El propietario de este documento es el Director de Tecnología de la Información, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

PABLO
RAMIRO
VALLEJO
ZUNIGA

Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 7: Documento de Políticas de Seguridad de la Información



Gobierno Provincial de Loja

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código:	FA03-DOC1.
Versión:	Versión 0.1
Fecha de la versión:	15/02/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Privada

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
15/02/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA	3
3. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN*	3
4. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	4
4.1. OBJETIVOS Y MEDICIÓN	4
4.2. REQUISITOS PARA LA SEGURIDAD DE LA INFORMACIÓN	4
4.3. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	4
4.4. CONTINUIDAD DEL NEGOCIO	4
4.5. RESPONSABILIDADES	4
4.6. COMUNICACIÓN DE LA POLÍTICA	5
5. APOYO PARA LA IMPLEMENTACIÓN DEL SGSI	5
6. VALIDEZ Y GESTIÓN DE DOCUMENTOS	5

1. Objetivo, alcance y usuarios

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Esta Política se aplica a todo el Modelo de Gestión de Seguridad de la Información (MGSI), según se define en el Documento del Alcance del MGSI.

Los usuarios de este documento son todos los empleados de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja, como también terceros externos a la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Documento sobre el alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Política de la Continuidad del Negocio
- Reglamento de Seguridad de la Información, Bueno Uso de Internet, Correo Electrónico, Control de Recursos Informáticos y de Telecomunicaciones de la Contraloría General del Estado.
- Procedimiento para gestión de incidentes

3. Terminología básica sobre seguridad de la información*

Confidencialidad: característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Integridad: característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.

Disponibilidad: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Modelo de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. Gestión de la seguridad de la información

4.1. Objetivos y medición

Los objetivos generales para el Modelo de Gestión de Seguridad de la Información son los siguientes:

- Cumplir las metas están en línea con los objetivos institucionales, con la estrategia y los planes de negocio de la organización.
- Cumplir con las normas establecidas por Contraloría General del Estado.
- Satisfacer las necesidades de los usuarios.

Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por la tesista Karla Correa y son aprobados por el Director de Tecnología de la Información del GPL en la Declaración de aplicabilidad.

Todos los objetivos deben ser revisados al menos una vez al año.

La Dirección de Tecnología de la Información del Gobierno Provincial de Loja medirá el cumplimiento de todos los objetivos. El Director de Tecnología de la Información del GPL es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos una vez al año y el Director de Tecnología de la Información del GPL, los Analistas de Sistemas y el Analista de Electrónica y Telecomunicaciones analizarán y evaluarán los resultados y los reportarán al Prefecto Provincial de Loja como material para la revisión por parte de la Dirección.

4.2. Requisitos para la seguridad de la información

INFORMACIÓN
CONFIDENCIAL

4.3. Controles de seguridad de la información

El proceso de escoger los controles (protección) está definido en la metodología de evaluación y tratamiento de riesgos.

Los controles seleccionados y su estado de implementación se detallan en la Declaración de aplicabilidad.

4.4. Continuidad del negocio

La Gestión de la continuidad del negocio está reglamentada en la Política de Gestión de la Continuidad del Negocio.

4.5. Responsabilidades

INFORMACIÓN CONFIDENCIAL

4.6. Comunicación de la Política

El Director de Tecnología de la Información del GPL debe asegurarse de que todos los empleados de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja como también los participantes externos correspondientes, estén familiarizados con esta Política.

5. Apoyo para la implementación del MGSÍ

A través del presente, el Director de Tecnología de la Información del GPL declara que en la implementación y mejora continua del MGSÍ se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

6. Validez y gestión de documentos


Este documento es válido hasta el enero del 2021.

El propietario de este documento es el Director de Tecnología de la Información del GPL, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de empleados y participantes externos que cumplen una función en el MGSÍ pero que no están familiarizados con el presente documento.
- No cumplimiento del MGSÍ con las leyes y normas, las obligaciones contractuales de Contraloría General del Estado y con los demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del MGSÍ.
- Responsabilidades ambiguas para la implementación del MGSÍ.

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo

Director de Tecnología de la Información

Anexo 8: Declaración de Aplicabilidad



Gobierno Provincial de Loja

DECLARACIÓN DE APLICABILIDAD

Código:	FA03-DOC2
Versión:	Versión 0.1
Fecha de la versión:	28/03/2019
Creado por:	Karla Correa
Aprobado por:	Pablo Vallejo
Nivel de confidencialidad:	Privado

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
28/03/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA	3
3. APLICABILIDAD DE LOS CONTROLES	3
4. ACEPTACIÓN DE LOS RIESGOS RESIDUALES	24
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS	24

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir qué controles son adecuados para implementar en la Dirección de Tecnología de la Información del GPL, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.

Este documento incluye todos los controles detallados en el Anexo A de la norma ISO 27001. Los controles se aplican a todo el alcance del Modelo de gestión de seguridad de la información (MGSI).

Los usuarios de este documento son todos empleados de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja que cumplen una función dentro del MGSI.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulo 6.1.3 d)
- Política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos

3. Aplicabilidad de los controles

Son aplicables los siguientes controles del Anexo A de la norma ISO 27001:

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.5	Políticas de seguridad de la información					
A.5.1	Dirección de la gerencia para la seguridad de la información	Si	INFORMACIÓN CONFIDENCIAL			Por Planificar.

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.5.1.1	Políticas para seguridad de la información	SI	INFORMACIÓN CONFIDENCIAL			Por planificar.
A.5.1.2	Revisión de políticas para seguridad de la información	SI				Por planificar.
A.6	Organización de la seguridad de la información					
A.6.1	Organización interna					
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	SI	INFORMACIÓN CONFIDENCIAL			Por planificar.

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.6.1.2	Segregación de deberes	SI	INFORMACIÓN CONFIDENCIAL			Por planificar.
A.6.1.3	Contacto con autoridades	SI				Por planificar
A.6.1.4	Contacto con grupos de interés especial	NO				
A.6.1.5	Seguridad de la información en gestión de proyectos	SI				Por planificar
A.6.2	Dispositivos móviles y teletrabajo					

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.6.2.1	Política sobre dispositivos móviles	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.6.2.2	Teletrabajo	SI				Por planificar
A.7	Seguridad relacionada con el personal					
A.7.1	Antes del empleo					

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado		
		SI	INFORMACIÓN CONFIDENCIAL			Por planificar		
A.7.1.1	Selección							
		SI						
A.7.1.2	Términos y condiciones de empleo					Por planificar		
A.7.2	Durante el empleo							
		SI	INFORMACIÓN CONFIDENCIAL			Por planificar		
A.7.2.1	Gestión de responsabilidades							

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.7.2.2	Concienciación, educación y capacitación sobre Seguridad de la información	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.7.2.3	Proceso disciplinario	SI				Por planificar
A.7.3	Terminación o cambio del empleo					
A.7.3.1	Terminación o cambio de responsabilidades del empleo	SI				Por planificar
A.8	Gestión de activos					
A.8.1	Responsabilidad sobre los activos					
A.8.1.1	Inventario de activos	SI	INFORMACIÓN CONFIDENCIAL			Por planificar

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
		SI				Por planificar
A.8.1.2	Propiedad de los activos					
		SI				Por Planificar
A.8.1.3	Uso aceptable de los activos					

INFORMACIÓN
CONFIDENCIAL

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado		
A.8.1.4	Devolución de activos	SI	INFORMACIÓN CONFIDENCIAL			Por Planificar		
A.8.2	Clasificación de la información							
A.8.2.1	Clasificación de la información	SI						Por Planificar.
A.8.2.2	Etiquetado de la información	SI				Por Planificar.		

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
		SI	INFORMACIÓN CONFIDENCIAL			Por Planificar.
A.8.2.3	Manejo de activos					
A.8.3	Gestión de medios					
		SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.8.3.1	Gestión de medios removibles					
		SI	INFORMACIÓN CONFIDENCIAL			Por Planificar
A.8.3.2	Eliminación de medios					

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.8.3.3	Transferencia de medios físicos	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.9	Control de acceso					
A.9.1	Requisitos comerciales para el control de acceso					
A.9.1.1	Política de control de acceso	SI	INFORMACIÓN CONFIDENCIAL			Por planificar.
A.9.1.2	Acceso a redes y a servicios de red	SI				
A.9.2	Gestión de acceso del usuario					
A.9.2.1	Registro de usuarios y baja	SI	INFORMACIÓN CONFIDENCIAL			Por planificar.
A.9.2.2	Concesión de acceso de usuarios	SI				

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.9.2.3	Gestión de derechos de acceso privilegiado	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.9.2.4	Gestión de información secreta de autenticación de usuarios	SI				Por planificar
A.9.2.5	Revisión derechos de acceso del usuario	SI				Por planificar
A.9.2.6	Eliminación o ajuste de derechos de acceso	SI				Por planificar
A.9.3	Responsabilidades del usuario					

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado	
A.9.3.1	Uso de información secreta de autenticación	SI	INFORMACIÓN CONFIDENCIAL			Por Planificar	
A.9.4	Control de acceso a aplicaciones y sistemas						
A.9.4.1	Restricción al acceso a la información	SI		INFORMACIÓN CONFIDENCIAL			Por planificar.
A.9.4.2	Procedimientos de registro en el terminal	NO					
A.9.4.3	Sistema de gestión de claves	SI				Por planificar.	

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.9.4.4	Uso de programas de utilidad privilegiada	No	INFORMACIÓN CONFIDENCIAL			En proceso
A.9.4.5	Control de acceso al código fuente del programa	SI				
A.10	Criptografía					
A.10.1	Controles criptográficos					
A.10.1.1	Política del uso de controles criptográficos	SI	INFORMACIÓN CONFIDENCIAL			Por planificar

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado		
A.10.1.2	Gestión clave	SI	INFORMACIÓN CONFIDENCIAL					
A.11	Seguridad física y del entorno							
A.11.1	Áreas seguras							
A.11.1.1	Perímetro de seguridad física	SI						En proceso
A.11.1.2	Controles de entrada físicos	SI	INFORMACIÓN CONFIDENCIAL			En proceso		

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.11.1.3	Seguridad de oficinas e habitaciones instalaciones	SI	INFORMACIÓN CONFIDENCIAL			En proceso
A.11.1.4	Protección ante amenazas externas y ambientales	SI				En proceso
A.11.1.5	Trabajo en áreas seguras	NO				
A.11.1.6	Áreas de entrega y carga	NO				
A.11.2	Equipos					

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.2.1	Ubicación y protección del equipo	SI	INFORMACIÓN CONFIDENCIAL			En proceso
A.11.2.2	Servicios públicos	SI				En proceso
A.11.2.3	Seguridad en el cableado	SI				En proceso.
A.11.2.4	Mantenimiento de equipo	SI				En proceso

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.2.5	Eliminación de activos	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI				Por planificar.
A.11.2.7	Eliminación segura o reuso del equipo	SI				Por planificar

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.11.2.8	Equipo de usuario desatendido	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.11.2.9	Política de pantalla y escritorio limpio	SI				Por planificar
A.12	Seguridad operativa					
A.12.1	Procedimientos y responsabilidades operativos					

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.12.1.1	Procedimientos operativos documentados	SI	INFORMACIÓN CONFIDENCIAL			Por Planificar
A.12.1.2	Gestión de cambios	SI				Por Planificar
A.12.1.3	Gestión de capacidad	SI				Por planificar
A.12.1.4	Separación de ambientes de desarrollo, prueba y operativo	No				
A.12.2	Protección contra software malicioso					
A.12.2.1	Controles contra software malicioso	SI				INFORMACIÓN CONFIDENCIAL

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.12.3	Copias de seguridad	SI				Por Planificar.
A.12.3.1	Copia de seguridad de la información					
A.12.4	Registros y supervisión	SI				Por Planificar
A.12.4.1	Registro de eventos	SI				Por planificar
A.12.4.2	Protección de la información del registro	SI				Por Planificar
A.12.4.3	Registros del administrador y operador	SI				Por Planificar

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado			
A.12.4.4	Sincronización de relojes	SI	INFORMACIÓN CONFIDENCIAL			Por planificar.			
A.12.5	Control del software operacional								
A.12.5.1	Instalación de software en sistemas operativos	SI							Por planificar
A.12.6	Gestión de vulnerabilidad técnica								
A.12.6.1	Gestión de vulnerabilidades técnicas	SI	INFORMACIÓN CONFIDENCIAL			Por planificar			

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.12.6.2	Restricciones sobre instalación de software	SI	INFORMACIÓN CONFIDENCIAL			Por planificar.
A.12.7	Consideraciones de auditoría de los sistemas de información					
A.12.7.1	Controles de auditoría sobre sistemas de información	NO	INFORMACIÓN CONFIDENCIAL			
A.13	Seguridad de las comunicaciones					
A.13.1	Gestión de seguridad de red					
A.13.1.1	Controles de red	SI	INFORMACIÓN CONFIDENCIAL			Por Panificar
A.13.1.2	Seguridad de los servicios de red	SI				

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
		SI	INFORMACIÓN CONFIDENCIAL			Por Planificar
A.13.1.3	Segregación en redes					
A.13.2	Políticas y procedimientos para					
		SI	INFORMACIÓN CONFIDENCIAL			Por Planificar.
A.13.2.1	Políticas y procedimientos para transferencia de la información					
		SI	INFORMACIÓN CONFIDENCIAL			Por Planificar
A.13.2.2	Acuerdos sobre transferencia de información					

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.13.2.3	Mensajes electrónicos	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.13.2.4	Acuerdos de confidencialidad y no divulgación	SI				Por Planificar.
A.14	Adquisición, desarrollo y mantenimiento de sistemas					
A.14.1	Requisitos de seguridad de los sistemas de la información					
A.14.1.1	Análisis de requerimientos y especificaciones para seguridad de la información	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.14.1.2	Seguridad de servicios de aplicación en redes públicas	NO				

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.14.1.3	Protección de transacciones de servicios de aplicaciones	NO	INFORMACIÓN CONFIDENCIAL			Por planificar
A.14.2	Seguridad en procesos de desarrollo y soporte					
A.14.2.1	Política de desarrollo seguro	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.14.2.2	Procedimientos para control de cambios	SI				Por planificar
A.14.2.3	Revisión técnica de aplicaciones luego de cambios en la plataforma operativa	SI				Por planificar
A.14.2.4	Restricciones sobre cambios a paquetes de software	SI				Por planificar

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección	Objetivos del control	Método de implementación	Estado
A.14.2.5	Principios de ingeniería para sistema seguro	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.14.2.6	Ambiente de desarrollo seguro	No				
A.14.2.7	Desarrollo externalizado	SI				Por planificar
A.14.2.8	Prueba de seguridad del sistema	SI				Por planificar
A.14.2.9	Prueba de aceptación del sistema	SI				Por planificar
A.14.3	Datos de prueba					

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.14.3.1	Protección de datos de prueba	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.15	Relaciones con proveedores					
A.15.1	Seguridad de la información en las relaciones con proveedores					
A.15.1.1	Política de seguridad de la información para relaciones con proveedores	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.15.1.2	Tratamiento de la seguridad en contratos con proveedores	SI				Por planificar
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	SI				Por planificar
A.15.2	Gestión de servicio de entrega de proveedores					
A.15.2.1	Supervisión y revisión de servicios de proveedores	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.15.2.2	Gestión de cambios en los servicios de proveedores	SI				Por planificar
A.16	Gestión de los incidentes de seguridad de la información					

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.16.1	Gestión de los incidentes y mejoras en la seguridad de la información					
A.16.1.1	Responsabilidades y procedimientos	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.16.1.2	Reporte de eventos de seguridad	SI				Por planificar

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.16.1.3	Reporte de debilidades de seguridad de la información	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	SI				Por planificar
A.16.1.5	Respuesta a incidentes de seguridad de la información	SI				Por planificar

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.16.1.6	Aprendizaje a partir de los incidentes en seguridad de la información	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.16.1.7	Recolección de evidencia	SI				Por planificar
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio					
A.17.1	Continuidad de seguridad de la información					
A.17.1.1	Planificación de continuidad de seguridad de la información	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.17.1.2	Implementación de continuidad de seguridad de la información	SI				Por planificar

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.17.2	Redundancias					
A.17.2.1	Disponibilidad de instalaciones para proceso de información	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.18	Cumplimiento					
A.18.1	Cumplimiento de requerimientos legales y contractuales					
A.18.1.1	Identificación de la legislación aplicable y de requerimientos contractuales	SI	INFORMACIÓN CONFIDENCIAL			Por planificar
A.18.1.2	Derechos de propiedad intelectual	SI				

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado		
A.18.1.3	Protección de registros	SI	INFORMACIÓN CONFIDENCIAL			Por planificar		
A.18.1.4	Privacidad y protección de información personal identificable	SI				Por planificar		
A.18.1.5	Regulación de controles criptográficos	SI				Por planificar		
A.18.2	Revisiones de seguridad de la información							
A.18.2.1	Revisión independiente de seguridad de la información	NO				INFORMACIÓN CONFIDENCIAL		

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/no elección	Objetivos del control	Método de implementación	Estado
A.18.2.2	Cumplimiento de políticas y normas de seguridad	SI	INFORMACIÓN CONFIDENCIAL			Por planificar.
A.18.2.3	Revisión del cumplimiento técnico	SI				Por planificar.

4. Aceptación de los riesgos residuales

Debido a que no se han podido reducir todos los riesgos en el proceso de gestión de riesgos, por medio de la presente se aceptan todos los siguientes riesgos residuales:

1. Todos los riesgos con valor 0, 1 ó 2.

Nro.	Nombre del activo	Propietario del activo	Amenaza	Vulnerabilidad	Nueva consecuencia	Nueva probabilidad	Riesgo residual

5. Validez y gestión de documentos

Este documento es válido hasta enero 2021.

INFORMACIÓN CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo

Director de Tecnología de la Información

Anexo 9: Política sobre Dispositivos Móviles y Teletrabajo



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

POLÍTICA SOBRE DISPOSITIVOS MÓVILES Y TELETRABAJO

Código:	FA03-DOC3
Versión:	Versión 0.1
Fecha de la versión:	14/03/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
14/03/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA	3
3. COMPUTACIÓN MÓVIL.....	3
3.1. INTRODUCCIÓN	3
3.2. REGLAS BÁSICAS	3
4. TELE-TRABAJO.....	4
5. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....	5
6. VALIDEZ Y GESTIÓN DE DOCUMENTOS.....	5

1. Objetivo, alcance y usuarios

El objetivo del presente documento es evitar el acceso no autorizado a dispositivos ubicados tanto dentro como fuera de las instalaciones de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

Este documento se aplica a todo el alcance Modelo de Gestión de Seguridad de la Información; es decir, a todas las personas, datos y equipos incluidos en el alcance del Modelo de Gestión de Seguridad de la Información.

Los usuarios de este documento son todos los empleados de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.6.2.1, A.6.2.2 y A.11.2.6
- Política de seguridad de la información
- Política de Uso aceptable

3. Computación móvil

3.1. Introducción

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

El equipamiento mencionado precedentemente puede ser llevado fuera de las instalaciones solamente con autorización, de acuerdo con lo establecido en la Política de uso aceptable.

3.2. Reglas básicas

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN
CONFIDENCIAL

4. Teletrabajo

INFORMACIÓN
CONFIDENCIAL

5. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención

Solamente el Director de Tecnología de la Información puede permitir a otros empleados el acceso a cualquiera de los documentos mencionados precedentemente.

6. Validez y gestión de documentos

Este documento es válido hasta el enero del 2021.

El propietario de este documento es el Director de Tecnología de la información del Gobierno Provincial de Loja, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

INFORMACIÓN
CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA

Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo

Director de Tecnología de la Información

Anexo 10: Trae tu Propio Dispositivo BYOD



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

Política Trae tu propio dispositivo (BYOD)

Código:	FA03-DOC4
Versión:	Versión 0.1
Fecha de la versión:	28/03/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
28/03/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA.....	3
3. REGLAS DE SEGURIDAD PARA EL USO DE BOYD	3
3.1. POLÍTICA DE LA EMPRESA	3
3.2. QUIÉNES PUEDEN UTILIZAR BOYD Y PARA QUÉ	3
3.3. QUÉ DISPOSITIVOS ESTÁN PERMITIDOS.....	4
3.4. USO ACEPTABLE	4
3.5. DERECHOS ESPECIALES	4
3.6. REEMBOLSO	5
3.7. VIOLACIONES DE SEGURIDAD	5
3.8. CAPACITACIÓN Y CONCIENCIACIÓN.....	5
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO	5
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS	5

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir cómo la Dirección de Tecnología de la Información del Gobierno Provincial de Loja retendrá el control sobre su información mientras se accede a dicha información a través de dispositivos que no pertenecen a la organización.

Este documento se aplica a todos los dispositivos personales que tienen la capacidad de almacenar, transferir o procesar cualquier tipo de información sensible dentro del alcance del Modelo de Gestión de Seguridad de la Información. Entre estos dispositivos se incluye a los ordenadores personales, teléfonos inteligentes, unidades de memoria USB, cámaras digitales, etc. En esta política se identificará a estos dispositivos como BOYD.

Los usuarios de este documento son todos los empleados de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.6.2.1, A.6.2.2, A.13.2.1

3. Reglas de seguridad para el uso de BOYD

Las reglas de la presente Política aplican para todos los BOYD, ya sea de uso personal o que se utilicen para trabajar, dentro o fuera de las instalaciones de la organización.

3.1. Política de la empresa

La Dirección de Tecnología de la Información del Gobierno Provincial de Loja adhiere al uso generalizado de BOYD para actividades laborales; por ejemplo, para realizar trabajos para la Dirección de Tecnología de la Información del GPL.

Los datos de la empresa que se almacenan transfieren o procesan en BOYD siguen perteneciendo a la Dirección de Tecnología de la Información del GPL, y la Dirección mantiene el derecho a controlar esos datos, aunque no sea propietaria del dispositivo.

3.2. Quiénes pueden utilizar BOYD y para qué

INFORMACIÓN
CONFIDENCIAL

3.3. Qué dispositivos están permitidos

El Analista de Electrónica y Telecomunicaciones creará una Lista de dispositivos aceptados que pueden ser utilizados como BOYD, junto con configuraciones obligatorias para cada dispositivo, antes de aplicar esta lista de BOYD tendrá que ser aprobada por el Director de tecnología de la Información.

3.4. Uso aceptable

Lo siguiente es obligatorio para todos los BOYD:

INFORMACIÓN
CONFIDENCIAL

No se permite hacer lo siguiente con los BOYD:

INFORMACIÓN
CONFIDENCIAL

3.5. Derechos especiales

INFORMACIÓN
CONFIDENCIAL

3.6. Reembolso

INFORMACIÓN
CONFIDENCIAL

3.7. Violaciones de seguridad

INFORMACIÓN
CONFIDENCIAL

3.8. Capacitación y concienciación

Director de Tecnología de la Información está a cargo de la capacitación de los empleados nuevos y existentes sobre el uso adecuado de los BOYD, como también de concientizar sobre las amenazas más comunes.

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención

5. Validez y gestión de documentos

Este documento es válido hasta el enero del 2021.

El propietario de este documento es el Director de Tecnología de la Información, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

INFORMACIÓN CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA

Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo

Director de Tecnología de la Información

Anexo 11: Declaración de Aceptación de Documentos

Declaración de aceptación de los documentos del modelo de gestión de seguridad de la información

Por medio de la presente, declaro que conozco plenamente la Política de Seguridad de la Información de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja y los demás documentos publicados o que serán publicados como parte del Modelo de Gestión de Seguridad de la Información:

- Políticas de dispositivos móviles y teletrabajo.
- Política de Trae tu Propio Dispositivo BYOD.
- Política de Clasificación de la Información.
- Política de Uso Aceptable.
- Política de Control de Acceso.
- Política de Uso de Controles Criptográficos.
- Política de Pantalla y Escritorio Limpio.
- Política de Creación de Copias de Seguridad.
- Política de Gestión de Cambios.
- Procedimientos Operativos para TI y Comunicación.
- Política de Transferencia de la Información.
- Política de Desarrollo Seguro.
- Política de Seguridad Para Proveedores.
- Apéndice Clausulas de Seguridad para Proveedores.
- Procedimiento Para la Gestión de Incidentes.
- Registro de Incidentes.
- Política de la Continuidad del Negocio.
- Política de Cumplimiento.

Por medio de la presente, declaro que cumpliré la Política y los demás documentos mencionados. Tomo conocimiento que el no cumplimiento de cualquier parte de esta Declaración será considerado

como incumplimiento de deberes y que, ante cada falta de este tipo, se aplicarán medidas disciplinarias.

Nombre: _____

Fecha: _____

Firma: _____

Anexo 12: Declaración de Confidencialidad

Declaración de confidencialidad

Por medio de la presente, declaro que a toda la información recibida durante la duración de mi contrato del [fecha del contrato] (en adelante, "el Contrato") le daré un tratamiento confidencial y no la revelaré a terceros, excepto hasta lo establecido en esta Declaración, en documentos de la Dirección de Tecnología de la Información o en las leyes correspondientes.

INFORMACIÓN
CONFIDENCIAL

Cargo: _____

Nombre: _____

Fecha: _____

Firma: _____

Anexo 13: Política de Clasificación de la Información



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Código:	FA03-DOC5
Versión:	Versión 0.1
Fecha de la versión:	01/05/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Restringida

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
01/05/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS.....	3
2. DOCUMENTOS DE REFERENCIA	3
3. INFORMACIÓN CLASIFICADA	3
3.1. PASOS Y RESPONSABILIDADES	3
3.2. CLASIFICACIÓN DE LA INFORMACIÓN	4
3.2.1. Criterios de clasificación	4
3.2.2. Niveles de confidencialidad.....	4
3.2.3. Lista de personas autorizadas.....	5
3.2.4. Reclasificación.....	5
3.3. ETIQUETADO DE LA INFORMACIÓN.....	5
3.4. MANEJO DE INFORMACIÓN CLASIFICADA.....	5
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....	9
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS.....	9

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar que se proteja la información en un nivel adecuado.

Este documento se aplica a todo el alcance del Modelo de gestión de seguridad de la información (MGSI); es decir, a todos los tipos de información, independientemente del formato, ya sean documentos en papel o electrónicos, aplicaciones y bases de datos, conocimiento de las personas, etc.

Los usuarios de este documento son todos los empleados de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3
- Política de seguridad de la información
- Declaración de aplicabilidad
- Inventario de activos
- Reglamento de Seguridad de la Información, Bueno Uso de Internet, Correo Electrónico, Control de Recursos Informáticos y de Telecomunicaciones de la Contraloría General del Estado.
- Procedimiento para gestión de incidentes
- Procedimientos operativos para tecnología de la información y de la comunicación
- Política de Uso aceptable
- Acuerdo Ministerial No. 012-2019 del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

3. Información clasificada

3.1. Pasos y responsabilidades

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN
CONFIDENCIAL

1
1

3.2. Clasificación de la información

INFORMACIÓN
CONFIDENCIAL

3.2.2. Niveles de confidencialidad

Toda la información debe ser clasificada en niveles de confidencialidad.

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

3.2.3. Lista de personas autorizadas

INFORMACIÓN CONFIDENCIAL

3.2.4. Reclasificación

Los propietarios de activos deben revisar el nivel confidencialidad de sus activos de información cada dos años y deben evaluar si se puede cambiar dicho nivel. Si es posible, deberían bajarlo.

3.3. Etiquetado de la información

INFORMACIÓN CONFIDENCIAL

3.4. Manejo de información clasificada

Todas las personas que tienen acceso a información clasificada deben seguir las reglas enumeradas en el siguiente cuadro. El Director de Tecnología de la Información debe activar acciones disciplinarias cada vez que se no se cumplan las reglas o si la información se transmite a personas no autorizadas.

Cada incidente relacionado con el manejo de información clasificada debe ser reportado de acuerdo con el Procedimiento para gestión de incidentes.

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL


4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención

5. Validez y gestión de documentos

INFORMACIÓN
CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo

Director de Tecnología de la Información

Anexo 14: Política de Uso Aceptable



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

POLÍTICA DE USO ACEPTABLE

Código:	FA03-DOC6
Versión:	0.1
Fecha de la versión:	15/05/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Restringido

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
15/05/2019.	0.1	Karla Correa	Políticas de Uso aceptable.

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS.....	3
2. DOCUMENTOS DE REFERENCIA	3
3. USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN.....	3
3.1. DEFINICIONES	3
3.2. USO ACEPTABLE.....	3
3.3. RESPONSABILIDAD SOBRE LOS ACTIVOS.....	4
3.4. ACTIVIDADES PROHIBIDAS.....	4
3.5. USO DE ACTIVOS FUERA DE LAS INSTALACIONES.....	4
3.6. DEVOLUCIÓN DE ACTIVOS A LA FINALIZACIÓN DE UN CONTRATO	4
3.7. PROCEDIMIENTO PARA COPIAS DE SEGURIDAD	4
3.8. PROTECCIÓN ANTIVIRUS	4
3.9. FACULTADOS PARA EL USO DE SISTEMAS DE INFORMACIÓN	4
3.10. RESPONSABILIDADES SOBRE LA CUENTA DE USUARIO	5
3.11. RESPONSABILIDADES SOBRE LA CLAVE	5
3.12. USO DE INTERNET	6
3.13. CORREO ELECTRÓNICO Y OTROS MÉTODOS DE INTERCAMBIO DE MENSAJES	6
3.14. DERECHOS DE AUTOR	7
3.15. SUPERVISIÓN DEL USO DE SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN	7
3.16. INCIDENTES	7
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....	7
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS	8

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas claras para el uso de los sistemas y de otros activos de información en la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

Este documento se aplica a todo el alcance del Modelo de Gestión de Seguridad de la Información; es decir, a todos los sistemas y demás activos de información utilizados dentro del alcance del Modelo de Gestión de Seguridad de la Información.

Los usuarios de este documento son todos los empleados de la Dirección de Tecnologías de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2
- Política de seguridad de la información
- Inventario de activos
- Procedimientos operativos para tecnología de la información y de la comunicación
- Política de Transferencia de la Información

3. Uso aceptable de los activos de información

3.1. Definiciones

Sistema de información: incluye todos los servidores y clientes, infraestructura de red, software del sistema y aplicaciones, datos y demás subsistemas y componentes que pertenecen o son utilizados por la dirección de tecnología de la Información, o que se encuentran bajo responsabilidad de la Dirección de Tecnologías de la Información. El uso de un sistema de información también incluye el uso de todos los servicios internos o externos, como el acceso a Internet, correo electrónico, etc.

Activos de información: en el contexto de esta Política, el término activos de información se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, ordenadores portátiles, soportes de almacenamiento de datos, etc.

3.2. Uso aceptable

INFORMACIÓN
CONFIDENCIAL

3.3. Responsabilidad sobre los activos

INFORMACIÓN CONFIDENCIAL

3.4. Actividades prohibidas

INFORMACIÓN CONFIDENCIAL

3.5. Uso de activos fuera de las instalaciones

INFORMACIÓN CONFIDENCIAL

3.6. Devolución de activos a la finalización de un contrato

INFORMACIÓN CONFIDENCIAL

3.7. Procedimiento para copias de seguridad

INFORMACIÓN CONFIDENCIAL

3.8. Protección antivirus

INFORMACIÓN CONFIDENCIAL

3.9. Facultados para el uso de sistemas de información

INFORMACIÓN CONFIDENCIAL

INFORMACIÓN
CONFIDENCIAL

3.10. Responsabilidades sobre la cuenta de usuario

INFORMACIÓN
CONFIDENCIAL

3.11. Responsabilidades sobre la clave

INFORMACIÓN
CONFIDENCIAL

3.12. Uso de Internet

INFORMACIÓN
CONFIDENCIAL

3.13. Correo electrónico y otros métodos de intercambio de mensajes

INFORMACIÓN
CONFIDENCIAL

3.14. Derechos de autor

INFORMACIÓN
CONFIDENCIAL

3.15. Supervisión del uso de sistemas de información y comunicación

INFORMACIÓN
CONFIDENCIAL

3.16. Incidentes

INFORMACIÓN
CONFIDENCIAL

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención


Solamente el Director de Tecnología de la Información puede permitir a otros empleados el acceso a cualquiera de los documentos mencionados precedentemente.

5. Validez y gestión de documentos

Este documento es válido hasta el enero 2021.

INFORMACIÓN
CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 15: Política de Control de Acceso



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

POLÍTICA DE CONTROL DE ACCESO

Código:	FA03-DOC7
Versión:	0.1
Fecha de la versión:	29/05/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Restringido

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
29/05/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA	3
3. CONTROL DE ACCESO	3
3.1. INTRODUCCIÓN	3
3.2. PERFIL DE USUARIO A	3
3.3. PERFIL DE USUARIO B	4
3.4. GESTIÓN DE PRIVILEGIOS	5
3.5. REVISIONES PERIÓDICAS DE LOS DERECHOS DE ACCESO	7
3.6. CAMBIO DE ESTADO O FINALIZACIÓN DE UN CONTRATO	8
3.7. IMPLEMENTACIÓN TÉCNICA.....	8
3.8. GESTIÓN DE LA CLAVE DEL USUARIO.....	9
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO	9
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS	10

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas claras para el uso de los sistemas y de otros activos de información en la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

Este documento se aplica a todo el alcance del Modelo de Gestión de Seguridad de la Información; es decir, a todos los sistemas y demás activos de información utilizados dentro del alcance del Modelo de Gestión de Seguridad de la Información.

Los usuarios de este documento son todos los empleados de la Dirección de Tecnologías de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3
- Política de seguridad de la información
- Declaración de aplicabilidad
- Política de Clasificación de la Información
- Declaración de aceptación de los documentos del Modelo de Gestión de Seguridad de la Información

3. Control de acceso

3.1. Introducción

El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupos de usuarios. Debe existir un procedimiento de registro de usuarios para cada sistema y servicio.

Está permitido el acceso a todos los sectores físicos de la organización, excepto a aquellos para las cuales el privilegio debe ser concedido por una persona autorizada (punto "Gestión de privilegios").

Esta Política determina reglas de acceso a sistemas, servicios e instalaciones, mientras que la Política de clasificación de información define reglas de acceso para documentos y registros individuales.

3.2. Perfil de usuario A

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN
CONFIDENCIAL

3.3. Perfil de usuario B

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN
CONFIDENCIAL

3.4. Gestión de privilegios



INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

INFORMACIÓN
CONFIDENCIAL

3.5. Revisiones periódicas de los derechos de acceso

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN
CONFIDENCIAL

3.6. Cambio de estado o finalización de un contrato

INFORMACIÓN
CONFIDENCIAL

3.7. Implementación técnica

La implementación técnica de la asignación o eliminación de derechos de acceso la realizan las siguientes personas:

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

3.8. Gestión de la clave del usuario

Cuando se asignan y utilizan claves de usuarios, se deben cumplir las siguientes reglas:

INFORMACIÓN CONFIDENCIAL

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención

Solamente el Director de Tecnología de la Información puede permitir a otros empleados el acceso a cualquiera de los documentos mencionados precedentemente.

5. Validez y gestión de documentos

Este documento es válido hasta el enero 2021.

INFORMACIÓN
CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA

Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 16: Política de Uso de Controles Criptográficos



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

POLÍTICA DEL USO DE CONTROLES CRIPTOGRÁFICOS

Código:	FA03-DOC8
Versión:	0.1
Fecha de la versión:	12/06/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Confidencial

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
12/06/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1.	OBJETIVO, ALCANCE Y USUARIOS	3
2.	DOCUMENTOS DE REFERENCIA	3
3.	USO DE CRIPTOGRAFÍA	3
3.1.	CONTROLES CRIPTOGRÁFICOS	3
3.2.	CLAVES CRIPTOGRÁFICAS	4
4.	GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....	5
5.	VALIDEZ Y GESTIÓN DE DOCUMENTOS	5

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas para el uso de los controles y claves criptográficas para proteger la confidencialidad, integridad, autenticidad e inviolabilidad de la información.

Este documento se aplica a todo el alcance del Modelo de gestión de seguridad de la información (MGS); es decir, a todos los sistemas e información utilizados dentro del alcance del MGS.

Los usuarios de este documento son los empleados de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos A.10.1.1, A.10.1.2, A.18.1.5
- Política de seguridad de la información
- Política de Clasificación de la Información
- Reglamento de Seguridad de la Información, Bueno Uso de Internet, Correo Electrónico, Control de Recursos Informáticos y de Telecomunicaciones de la Contraloría General del Estado

3. Uso de criptografía

3.1. Controles criptográficos



INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

3.2. Claves criptográficas

El Analista de Electrónica y Telecomunicaciones, es el responsable de establecer las siguientes reglas sobre la gestión de claves:

INFORMACIÓN CONFIDENCIAL

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención

Solamente el Director de Tecnología de la Información del Gobierno Provincial de Loja, puede permitir a otros empleados el acceso a cualquiera de los registros mencionados precedentemente.

5. Validez y gestión de documentos

Este documento es válido hasta el enero del 2021.

INFORMACIÓN
CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA

Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 17: Política de Pantalla y Escritorio Limpio



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIOS

Código:	FA03-DOC9
Versión:	0.1
Fecha de la versión:	26/06/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
26/06/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS.....	3
2. DOCUMENTOS DE REFERENCIA	3
3. POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIO	3
3.1. PROTECCIÓN DEL PUESTO DE TRABAJO	3
3.1.1. <i>Política de escritorio limpio</i>	3
3.1.2. <i>Política de pantalla limpia</i>	3
3.2. PROTECCIÓN DE INSTALACIONES Y EQUIPOS COMPARTIDOS	4
4. VALIDEZ Y GESTIÓN DE DOCUMENTOS.....	4

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas para evitar el acceso no autorizado a la información en los puestos de trabajo, como también a las instalaciones y a los equipos compartidos.

Este documento se aplica a todo el alcance del Modelo de gestión de seguridad de la información (MGSI); es decir, a todos los puestos de trabajo, instalaciones y equipos ubicados dentro del alcance del MGSI.

Los usuarios de este documento son todos los empleados de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.11.2.8 y A.11.2.9
- Política de seguridad de la información
- Política de Clasificación de la Información

3. Política de pantalla y escritorio limpio

Toda la información clasificada como "Uso interno", "Restringido" y "Confidencial" de acuerdo a lo establecido en la Política de Clasificación de la Información, es considerada sensible en esta Política de pantalla y escritorio limpio.

3.1. Protección del puesto de trabajo

3.1.1. Política de escritorio limpio

INFORMACIÓN
CONFIDENCIAL

3.1.2. Política de pantalla limpia

INFORMACIÓN
CONFIDENCIAL

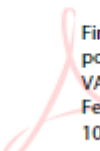
3.2. Protección de instalaciones y equipos compartidos

INFORMACIÓN
CONFIDENCIAL

4. Validez y gestión de documentos

INFORMACIÓN
CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 18: Política de Creación de Copias de Seguridad



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

POLÍTICA DE CREACIÓN DE COPIAS DE SEGURIDAD

Código:	FA03-DOC10
Versión:	Versión 0.1
Fecha de la versión:	12/07/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Confidencial

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
12/07/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA	3
3. COPIAS DE SEGURIDAD	3
3.1. PROCEDIMIENTO PARA COPIAS DE SEGURIDAD	3
3.2. PRUEBA DE LAS COPIAS DE SEGURIDAD	4
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....	4
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS	4

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar que las copias de seguridad sean creadas de acuerdo a intervalos definidos y sean verificadas periódicamente.

Este documento se aplica a todo el alcance del Modelo de gestión de seguridad de la información (MGSI); es decir, a todas las tecnologías de la información y de la comunicación utilizadas dentro del alcance del MGSI.

Los usuarios de este documento son empleados de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, punto A.12.3.1
- Política de seguridad de la información

3. Copias de seguridad

3.1. Procedimiento para copias de seguridad

INFORMACIÓN
CONFIDENCIAL

3.2. Prueba de las copias de seguridad

INFORMACIÓN
CONFIDENCIAL

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención

5. Validez y gestión de documentos

Este documento es válido hasta enero del 2021.

INFORMACIÓN
CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA

Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 19: Política de Gestión de Cambios



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

POLÍTICA DE GESTIÓN DE CAMBIO

Código:	FA03-DOC11
Versión:	0.1
Fecha de la versión:	26/07/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
26/07/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS.....	3
2. DOCUMENTOS DE REFERENCIA	3
3. GESTIÓN DE CAMBIOS.....	3
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....	4
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS.....	4

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir cómo se controlan los cambios en los sistemas de información.

Este documento se aplica a todo el alcance del Modelo de gestión de seguridad de la información (MGSI); es decir, a todas las tecnologías de la información y de la comunicación utilizadas dentro del alcance del MGSI.

Los usuarios de este documento son empleados de la Dirección de Tecnología de la Información.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.12.1.2, A.14.2.4
- Política de seguridad de la información

3. Gestión de cambios

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención

5. Validez y gestión de documentos

INFORMACIÓN CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA

Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 20: Procedimientos Operativos para TI y Comunicación



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

PROCEDIMIENTOS OPERATIVOS PARA TECNOLOGÍA DE LA INFORMACIÓN Y DE LA COMUNICACIÓN

Código:	FA03-DOC12
Versión:	Versión 0.1
Fecha de la versión:	07/08/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Restringida

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
07/08/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS.....	3
2. DOCUMENTOS DE REFERENCIA	3
3. PROCEDIMIENTOS OPERATIVOS PARA TECNOLOGÍA DE LA INFORMACIÓN Y DE LA COMUNICACIÓN	3
3.1. GESTIÓN DE SEGURIDAD DE RED.....	3
3.2. SERVICIOS DE RED	4
3.3. ELIMINACIÓN Y DESTRUCCIÓN DE EQUIPOS Y SOPORTES	4
3.3.1. <i>Equipos</i>	4
3.3.2. <i>Soportes móviles de almacenaje</i>	4
3.3.3. <i>Soportes en papel</i>	4
3.3.4. <i>Borrado y destrucción de registros; comisión para la destrucción de datos</i>	4
3.4. SUPERVISIÓN DEL SISTEMA.....	5
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....	5
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS.....	5

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar el funcionamiento correcto y seguro de la tecnología de la información y de la comunicación.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (MGSI); es decir, a toda la tecnología de la información y de la comunicación, como también a la documentación relacionada dentro del alcance del MGSI.

Los usuarios de este documento son empleados de Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4
- Política de seguridad de la información

3. Procedimientos operativos para tecnología de la información y de la comunicación

3.1. Gestión de seguridad de red

INFORMACIÓN
CONFIDENCIAL

3.2. Servicios de red

INFORMACIÓN
CONFIDENCIAL

3.3. Eliminación y destrucción de equipos y soportes

INFORMACIÓN
CONFIDENCIAL

3.3.1. Equipos

INFORMACIÓN
CONFIDENCIAL

3.3.2. Soportes móviles de almacenaje

INFORMACIÓN
CONFIDENCIAL

3.3.3. Soportes en papel

INFORMACIÓN
CONFIDENCIAL

3.3.4. Borrado y destrucción de registros; comisión para la destrucción de datos

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

3.4. Supervisión del sistema

INFORMACIÓN CONFIDENCIAL

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención

5. Validez y gestión de documentos

INFORMACIÓN CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 21: Política de Transferencia de la Información



Gobierno Provincial de Loja

POLÍTICA DE TRANSFERENCIA DE LA INFORMACIÓN

Código:	FA03-DOC13
Versión:	Versión 0.1
Fecha de la versión:	21/08/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
21/08/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA	3
3. TRANSFERENCIA DE LA INFORMACIÓN	3
3.1. CANALES DE COMUNICACIÓN ELECTRÓNICA	3
3.2. RELACIONES CON ENTIDADES EXTERNAS	3
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO	4
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS	4

1. Objetivo, alcance y usuarios

El objetivo del presente documento es asegurar la seguridad de la información y el software cuando son intercambiados dentro o fuera de la organización.

Este documento se aplica a todo el alcance del Modelo de gestión de seguridad de la información (MGSI); es decir, a toda la información y tecnología de la información y de la comunicación utilizada dentro del alcance del MGSI.

Los usuarios de este documento son empleados de la dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.13.2.1, A.13.2.2
- Política de seguridad de la información
- Política de Clasificación de la Información
- Política de seguridad para proveedores

3. Transferencia de la información

3.1. Canales de comunicación electrónica

INFORMACIÓN
CONFIDENCIAL

3.2. Relaciones con entidades externas

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

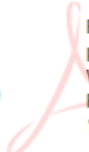
4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención

5. Validez y gestión de documentos

INFORMACIÓN CONFIDENCIAL

**PABLO
RAMIRO
VALLEJO
ZUNIGA**



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 22: Política de Desarrollo Seguro



Gobierno Provincial de Loja

POLÍTICA DE DESARROLLO SEGURO

Código:	FA03-DOC14
Versión:	Versión 0.1
Fecha de la versión:	09/09/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
09/09/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA	3
3. DESARROLLO Y MANTENIMIENTO SEGURO	3
3.1. EVALUACIÓN DE RIESGOS PARA EL PROCESO DE DESARROLLO	3
3.2. PRINCIPIOS DE INGENIERÍA SEGURA.....	3
3.3. REQUERIMIENTOS DE SEGURIDAD.....	4
3.4. VERIFICACIÓN Y PRUEBA DE LA IMPLEMENTACIÓN DE REQUERIMIENTOS DE SEGURIDAD	4
3.5. REPOSITORIO	4
3.6. CONTROL DE VERSIÓN	4
3.7. CONTROL DE CAMBIOS.....	4
3.8. PROTECCIÓN DE DATOS DE PRUEBA.....	4
3.9. CAPACITACIÓN NECESARIA EN SEGURIDAD.....	4
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO	5
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS	5
6. APÉNDICES	5

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir las reglas básicas para desarrollo seguro de software y sistemas.

Este documento se aplica al desarrollo y mantenimiento de todos los servicios, arquitectura, software y sistemas que forman parte del Modelo de gestión de seguridad de la información (MGSÍ).

Los usuarios de este documento son todos los empleados que trabajan en el desarrollo y mantenimiento de Dirección de Tecnología de la Información.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1
- Metodología de evaluación y tratamiento de riesgos
- Política de seguridad para proveedores
- Procedimientos operativos para tecnología de la información y de la comunicación
- Plan de capacitación y concienciación

3. Desarrollo y mantenimiento seguro

3.1. Evaluación de riesgos para el proceso de desarrollo

INFORMACIÓN
CONFIDENCIAL

3.2. Principios de ingeniería segura

INFORMACIÓN
CONFIDENCIAL

3.3. Requerimientos de seguridad

INFORMACIÓN CONFIDENCIAL

3.4. Verificación y prueba de la implementación de requerimientos de seguridad

INFORMACIÓN CONFIDENCIAL

3.5. Repositorio

INFORMACIÓN CONFIDENCIAL

3.6. Control de versión

INFORMACIÓN CONFIDENCIAL

3.7. Control de cambios

INFORMACIÓN CONFIDENCIAL

3.8. Protección de datos de prueba

INFORMACIÓN CONFIDENCIAL

3.9. Capacitación necesaria en seguridad

INFORMACIÓN CONFIDENCIAL

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención


5. Validez y gestión de documentos

INFORMACIÓN
CONFIDENCIAL

6. Apéndices

- Especificaciones de requisitos de los sistemas de información

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'


Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 23: Apéndice Especificación de Requisitos

Apéndice: Especificaciones de requisitos de los sistemas de información

INFORMACIÓN
CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 24: Política de Seguridad para Proveedores



Gobierno Provincial de Loja

POLÍTICA DE SEGURIDAD PARA PROVEEDORES

Código:	FA03-DOC15
Versión:	Versión 0.1
Fecha de la versión:	01/10/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
01/10/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA	3
3. RELACIÓN CON CLIENTES Y SOCIOS	3
3.1. IDENTIFICACIÓN DE RIESGOS	3
3.2. SELECCIÓN	3
3.3. CONTRATOS.....	3
3.4. CAPACITACIÓN Y CONCIENCIACIÓN	4
3.5. SUPERVISIÓN Y REVISIÓN	4
3.6. CAMBIOS O FINALIZACIÓN DE SERVICIOS DEL PROVEEDOR	4
3.7. ELIMINACIÓN DE DERECHO DE ACCESO Y DEVOLUCIÓN DE ACTIVOS.....	4
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....	5
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS	5
6. APÉNDICES	5

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir las reglas básicas para la relación con proveedores.

Este documento se aplica a todos los proveedores que puedan tener influencia sobre la confidencialidad, integridad y disponibilidad de información sensible de la Dirección de Tecnología de la Información.

Los usuarios de este documento son la alta dirección y las personas responsables de proveedores.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
- Metodología de evaluación y tratamiento de riesgos
- Informe de evaluación y tratamiento de riesgos
- Política de control de acceso
- Declaración de confidencialidad

3. Relación con clientes y socios

3.1. Identificación de riesgos

INFORMACIÓN
CONFIDENCIAL

3.2. Selección

INFORMACIÓN
CONFIDENCIAL

3.3. Contratos

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

3.4. Capacitación y concienciación

INFORMACIÓN
CONFIDENCIAL

3.5. Supervisión y revisión

INFORMACIÓN
CONFIDENCIAL

3.6. Cambios o finalización de servicios del proveedor

INFORMACIÓN
CONFIDENCIAL

3.7. Eliminación de derecho de acceso y devolución de activos

INFORMACIÓN
CONFIDENCIAL

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención


5. Validez y gestión de documentos

INFORMACIÓN
CONFIDENCIAL

6. Apéndices

- Cláusula:

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 25: Apéndice Cláusulas de Seguridad para Proveedores

Apéndice: Cláusulas de seguridad para proveedores y socios

Cuando se redacta un contrato con un proveedor, es necesario definir cuáles de las siguientes cláusulas se incluirán en el contrato (la terminología legal del acuerdo debe ser preparada por la persona responsable de asuntos legales):

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

Anexo 26: Procedimiento para Gestión de Incidentes



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

PROCEDIMIENTO PARA GESTIÓN DE INCIDENTES

Código:	FA03-DOC16
Versión:	Versión 0.1
Fecha de la versión:	28/10/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Restringido

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
28/10/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS.....	3
2. DOCUMENTOS DE REFERENCIA	3
3. GESTIÓN DE INCIDENTES	3
3.1. RECEPCIÓN Y CLASIFICACIÓN DE INCIDENTES, DEBILIDADES Y EVENTOS	3
3.2. PROCESO DE TRATAMIENTO PARA DEBILIDADES O EVENTOS DE SEGURIDAD	4
3.3. TRATAMIENTO DE INCIDENTES MENORES	4
3.4. TRATAMIENTO DE INCIDENTES GRAVES	4
3.5. APRENDIZAJE A PARTIR DE LOS INCIDENTES.....	4
3.6. MEDIDAS DISCIPLINARIAS	4
3.7. RECOLECCIÓN DE EVIDENCIA	4
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....	5
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS	5
6. APÉNDICE.....	5

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar la detección temprana de eventos y debilidades de seguridad, como también la rápida reacción y respuesta ante incidentes de seguridad.

Este documento se aplica a todo el alcance del Modelo de gestión de seguridad de la información (MGSI); es decir, a todos los empleados y demás activos que se utilizan dentro del alcance del MGSI, como también a los proveedores y demás personas externas a la organización que entran en contacto con los sistemas y con la información alcanzados por el MGSI.

Los usuarios de este documento son todos los empleados de la Dirección de Tecnología de la Información.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
- Política de seguridad de la información

3. Gestión de incidentes

Un incidente de seguridad de la información es un "evento, o serie de eventos, indeseado e inesperado que tiene una alta probabilidad de poner en riesgo las actividades institucionales y de amenazar la seguridad de la información" (ISO/IEC 27000:2009).

3.1. Recepción y clasificación de incidentes, debilidades y eventos

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

3.2. Proceso de tratamiento para debilidades o eventos de seguridad

INFORMACIÓN CONFIDENCIAL

3.3. Tratamiento de incidentes menores

INFORMACIÓN CONFIDENCIAL

3.4. Tratamiento de incidentes graves

INFORMACIÓN CONFIDENCIAL

3.5. Aprendizaje a partir de los incidentes

INFORMACIÓN CONFIDENCIAL

3.6. Medidas disciplinarias

INFORMACIÓN CONFIDENCIAL

3.7. Recolección de evidencia

INFORMACIÓN CONFIDENCIAL

y

4. Gestión de registros guardados en base a este documento

<i>Nombre del registro</i>	<i>Ubicación de archivo</i>	<i>Persona responsable del archivo</i>	<i>Controles para la protección del registro</i>	<i>Tiempo de retención</i>

Solamente el Director de Tecnología de la Información debe puede permitir el acceso a los registros a otros empleados.


5. Validez y gestión de documentos

INFORMACIÓN
CONFIDENCIAL

6. Apéndice

- Registro de incidentes

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 27: Apéndice Registro de Incidentes

Apéndice: Registro de incidentes

Los incidentes se clasifican dentro de los siguientes tipos:

- relacionados con la información (directamente relacionados con tecnología de la información y comunicación)
- no relacionados con la información (todos los demás incidentes)

Información sobre los incidentes:

INFORMACIÓN
CONFIDENCIAL

Anexo 28: Política de Continuidad del Negocio



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

POLÍTICA DE LA CONTINUIDAD DEL NEGOCIO

Código:	FA03-DOC17
Versión:	0.1
Fecha de la versión:	18/11/2019
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
18/11/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS	3
2. DOCUMENTOS DE REFERENCIA	3
3. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	3
3.1. OBJETIVO DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	3
3.2. RELACIÓN CON LOS OBJETIVOS GENERALES Y OTROS DOCUMENTOS	3
3.3. DEFINICIÓN DE OBJETIVOS DE CONTINUIDAD DEL NEGOCIO	3
3.4. ALCANCE.....	4
3.5. PRODUCTOS Y SERVICIOS CLAVE	4
3.6. RESPONSABILIDADES PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	5
3.7. MEDICIÓN.....	6
3.8. COMUNICACIÓN DE LA POLÍTICA	6
3.9. APOYO PARA LA IMPLEMENTACIÓN DEL SGCN	6
4. VALIDEZ Y GESTIÓN DE DOCUMENTOS	6

1. Objetivo, alcance y usuarios

El propósito de esta Política es definir el objetivo, alcance y reglas básicas para la gestión de la continuidad del negocio.

Esta política contempla todos los aspectos de seguridad de la información relacionados con la gestión de la continuidad del negocio.

Los usuarios de este documento son todos los empleados de Dirección de Tecnología de la Información, como también todos los proveedores y socios que cumplen alguna función en el MGSÍ.

2. Documentos de referencia

- Norma ISO 22301, puntos 4.1, 4.3, 5.3, 6.2 y 9.1.1
- Norma BS 25999-2, puntos 3.2.1, 3.2.2, 3.2.3
- Norma ISO/IEC 27001, sección A.17
- Reglamento de seguridad de la información, buen uso del internet, correo electrónico, control de los recursos informáticos y de telecomunicaciones de la contraloría general del estado.

3. Gestión de la Continuidad del Negocio

3.1. Objetivo de la gestión de la continuidad del negocio

El objetivo de la gestión de la continuidad del negocio es identificar potenciales amenazas en una organización y los impactos que esas amenazas podrían tener sobre las operaciones de negocios; también sirven para proporcionar un marco de referencia para construir resiliencia organizacional con la capacidad de una respuesta efectiva.

3.2. Relación con los objetivos generales y otros documentos

INFORMACIÓN
CONFIDENCIAL

3.3. Definición de objetivos de continuidad del negocio

INFORMACIÓN CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

3.4. Alcance

La política de continuidad del negocio se implementa para toda la Dirección de Tecnología de la Información del Gobierno Provincial de Loja, con especial atención sobre las actividades identificadas durante el Análisis de Riesgos.

Las ubicaciones de negocios de la organización incluidas en el alcance:

- Dirección de Tecnología de la Información
- Área Técnica de Infraestructura.
 - Data Center
- Soporte Técnico

Unidades organizativas incluidas en el alcance:

- Dirección de Tecnología de la Información.

3.5. Productos y servicios clave

INFORMACIÓN CONFIDENCIAL

INFORMACIÓN
CONFIDENCIAL

3.6. Responsabilidades para la gestión de la continuidad del negocio

INFORMACIÓN
CONFIDENCIAL

3.7. Medición

INFORMACIÓN
CONFIDENCIAL

3.8. Comunicación de la Política

INFORMACIÓN
CONFIDENCIAL

3.9. Apoyo para la implementación del SGCN

INFORMACIÓN
CONFIDENCIAL

4. Validez y gestión de documentos

INFORMACIÓN
CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA

Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 29: Declaración de Cumplimiento

Declaración de Cumplimiento

Por medio de la presente, me comprometo a evitar el incumplimiento de las obligaciones legales, de reglamentación o contractuales relacionadas con el modelo de seguridad de la información, y de cualquier requisito de seguridad es importante para no incurrir en demandas, multas u otra clase de afectación a la imagen o a las finanzas de la Dirección de Tecnología de la Información.

Ayudar a definir procesos y controles apropiados para asegurar el cumplimiento de los requisitos legales, de reglamentación y contractuales con base a la Normativa general del estado sobre la seguridad de la información, buen uso de internet, correo electrónico, control de los recursos informáticos y de telecomunicaciones

Cargo: _____
Nombre: _____
Fecha: _____
Firma: _____

Anexo 30: Informe de Pruebas



Dirección de Tecnología de la Información del Gobierno Provincial de Loja

INFORME DE PRUEBAS

Código:	F004-DOC1
Versión:	Versión 0.1
Fecha de la versión:	03/02/2020
Creado por:	Karla Correa
Aprobado por:	Ing. Pablo Vallejo
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/02/2019	0.1	Karla Correa	Descripción básica del documento

Tabla de contenido

ANEXO 30: INFORME DE PRUEBAS	1
1. OBJETIVO, ALCANCE Y USUARIOS.....	3
2. DOCUMENTOS DE REFERENCIA	3
3. DEFINICIÓN DEL PLAN DE PRUEBAS.....	3
4. DEFINICIÓN DEL ENTORNO O ESCENARIOS DE PRUEBAS.....	3
5. MAPA DE RIESGOS DESPUÉS DE LA EJECUCIÓN DEL MODELO	5
6. MAPA DE CALOR	8
7. VALIDEZ Y GESTIÓN DE DOCUMENTOS	8

1. Objetivo, alcance y usuarios

El objetivo del presente documento es Desarrollar un Plan de Pruebas para registrar el proceso de planificación y ejecución de pruebas para ayudar a validar el Modelo de Seguridad de la Información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

Este documento se aplica a todo el alcance Modelo de Gestión de Seguridad de la Información; es decir, a todas las personas, datos y equipos incluidos en el alcance del Modelo de Gestión de Seguridad de la Información.

Los usuarios de este documento son todos los empleados de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

2. Documentos de referencia

- Documentos Anexo A de la ISO/IEC 27001:2013
- Política de Seguridad de la Información.
- Política de Organización de la Seguridad de la Información.
- Política de Seguridad de Recurso Humanos.
- Política de Gestión de Recursos (Activos).
- Política de Control de Acceso.
- Política de Criptografía.
- Política de Seguridad Física y Ambiental.
- Política de Seguridad Operativa.
- Política de Seguridad de las Comunicaciones.
- Política de Adquisición, Desarrollo y Mantenimiento
- Política de Relación con Proveedores.
- Política de Gestión de Incidentes de Seguridad de la Información.
- Política de Gestión de Continuidad de Negocio.

3. Definición del Plan de Pruebas.

Se ejecutaron 18 pruebas de manera exitosa, validando los controles propuestos en el Plan de Pruebas en la fase de diseño. En el plan se elaboró posibles casos de pruebas; los mismos que constan de dos fases, la de planificación y ejecución; la fase de planificación consta de: ID, prueba realizada, sistema, opción de acceso, caso de prueba, pasos de caso, pre-requisito, restricciones, resultado esperado; y, la fase de ejecución consta de: fecha de ejecución, control aplicado, ejecutado por, resultados obtenidos y observaciones, además en la parte final tendrá un resumen de las pruebas ejecutadas

4. Definición del Entorno o Escenarios de Pruebas

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

5. Mapa de Riesgos Después de la Ejecución del Modelo

Después de la puesta en marcha del modelo se puede observar que el nivel de riesgos altos bajo a una totalidad de cero riesgos, mientras que los riesgos con criticidad media, bajo a un total de 23 riesgos y los demás son riesgos con criticidad baja.

Matriz de Riesgos											
Proyecto: Modelo de Seguridad de la Información											
ID: F.1.1											
Fecha de Inicio: 17/02/2020											
Fecha de fin: 24/02/2020											
No. de Riesgo	Riesgo	Tipo de riesgo	Riesgo		Sistema	Impacto (A/M/B)	Probabilidad (A/M/B)	Evaluación		Control Aplicado	Responsable de la acción de respuesta
			Fuente	Consecuencia				Valor (1 al 9)	Nivel (A/M/B)		
1						M	B	2	Bajo	Política de Seguridad con Proveedores Apéndice: Cláusulas de seguridad para proveedores y socios	Ing. Pablo Vallejo Ing. Fabian Calle
2						M	B	2	Bajo	Política de Desarrollo Seguro	Ing. Fabian Calle
3						B	B	1	Bajo	Política de Seguridad con Proveedores Apéndice: Cláusulas de seguridad para proveedores y socios	Ing. Pablo Vallejo Ing. Fabian Calle
4						B	B	1	Bajo	Política de Desarrollo Seguro	Ing. Pablo Vallejo
5						B	M	2	Bajo	Política de Desarrollo Seguro	Ing. Fabian Calle
6						A	B	3	Medio	Política de Seguridad con Proveedores Apéndice: Cláusulas de seguridad para proveedores y socios	Ing. Pablo Vallejo Ing. Fabian Calle
7						A	B	3	Medio	Política de Seguridad con Proveedores Apéndice: Cláusulas de seguridad para proveedores y socios	Ing. Pablo Vallejo
8						A	B	3	Medio	Política de Seguridad con Proveedores	Ing. Pablo Vallejo Ing. Fabian Calle
9						M	B	2	Bajo	Declaración de Aplicabilidad (Controles A.7.1.1 y A.7.1.2)	Ing. Pablo Vallejo
10						A	B	3	Medio	Declaración de aceptación de los documentos del modelo de gestión de seguridad de la información	Ing. Pablo Vallejo

INFORMACIÓN
CONFIDENCIAL

11	<p>INFORMACIÓN CONFIDENCIAL</p>	B	B	1	Bajo	<i>Procedimiento para Gestión de Incidentes Apéndice: Registro de Incidentes</i>	Cristian Lalanguí
12		B	M	2	Bajo	<i>N/A</i>	<i>Ing. Rafael Almeida</i>
13		A	B	3	Medio	<i>Política de Desarrollo Seguro Apéndice: Especificaciones de requisitos de los sistemas de información</i>	Ing. Fabian Calle
14		A	B	3	Medio	<i>Política de Desarrollo Seguro Apéndice: Especificaciones de requisitos de los sistemas de información</i>	Ing. Fabian Calle
15		A	B	3	Medio	<i>Política de Desarrollo Seguro</i>	Ing. Fabian Calle
16		A	B	3	Medio	<i>Política de Seguridad con Proveedores Apéndice: Cláusulas de seguridad para proveedores y socios</i>	Cristian Lalanguí
17		A	B	3	Medio	<i>Política de Control de Acceso Política de Uso de Controles Criptográficos</i>	Ing. Paulina Vidal
18		A	B	3	Medio	<i>Política de Pantalla y Escritorio Limpio</i>	Ing. Paulina Vidal
19		B	B	1	Bajo	<i>Política de Desarrollo Seguro</i>	Ing. Fabian Calle
20		A	B	3	Medio	<i>Política de Uso Aceptable Política de Control de Acceso</i>	Ing. Rafael Almeida Ing. Pablo Vallejo
21		A	B	3	Medio	<i>Procedimiento para Gestión de Incidentes Apéndice: Registro de Incidentes</i>	Cristian Lalanguí
22		M	B	2	Bajo	<i>Apéndice: Registro de Incidentes</i>	Cristian Lalanguí
23		M	B	2	Bajo	<i>Apéndice: Registro de Incidentes</i>	Ing. Rafael Almeida
24		A	B	3	Medio	<i>Procedimientos Operativos para II y Comunicación</i>	Ing. Pablo Vallejo Ing. Rafael Almeida
25		A	B	3	Medio	<i>Política de Continuidad del Negocio</i>	Ing. Pablo Vallejo Ing. Rafael Almeida
26		A	B	3	Medio	<i>Política de Uso Aceptable Política de Control de Acceso</i>	Ing. Pablo Vallejo
27		A	B	3	Medio	<i>Declaración de confidencialidad Política de Uso Aceptable</i>	Ing. Rafael Almeida Ing. Fabian Calle

28	INFORMACIÓN CONFIDENCIAL	M	B	2	Bajo	Política de Continuidad del Negocio	Ing. Paulina Vidal
29		M	B	2	Bajo	Política de Continuidad del Negocio	Ing. Pablo Vallejo
30		B	B	1	Bajo	Política de Pantalla y Escritorio Limpio	Ing. Paulina Vidal
31		A	B	3	Medio	Política de Continuidad del Negocio	Ing. Pablo Vallejo Ing. Paulina Vidal
32		A	B	3	Medio	Política de Continuidad del Negocio	Ing. Paulina Vidal
33		A	B	3	Medio	Política de Continuidad del Negocio	Ing. Pablo Vallejo
34		A	B	3	Medio	Declaración de confidencialidad Política de Uso Aceptable	Ing. Pablo Vallejo
35		A	B	3	Medio	Política de Uso de Controles Criptográficos	Ing. Rafael Almeida
36		A	B	3	Medio	Política de Control de Acceso	Ing. Rafael Almeida
37		A	B	3	Medio	Declaración de confidencialidad Declaración de Cumplimiento	Ing. Pablo Vallejo
38		A	B	3	Medio	Política de Pantalla y Escritorio Limpio	Ing. Paulina Vidal
39		A	B	3	Medio	Política de Control de Acceso	Ing. Rafael Almeida Ing. Jairo Silva
40		M	B	2	Medio	Declaración de Aplicabilidad (Controles A.7.1.1 y A.7.1.2)	Ing. Pablo Vallejo
41		B	B	1	Baja	N/A	Ing. Pablo Vallejo
42	A	B	3	Medio	Declaración de Aplicabilidad (Controles A.7.1.1 y A.7.1.2)	Ing. Pablo Vallejo	

6. Mapa de Calor

El mapa de calor que se presenta una vez finalizadas las pruebas del modelo, se puede observar que no se presentan riesgos con nivel de criticidad alta, riesgos con criticidad media pasaron de 16 a 26, y con criticidad baja de 8 a 14. Es decir, ahora tenemos menor probabilidad que se presente un riesgo que pueda ocasionar daños económicos.

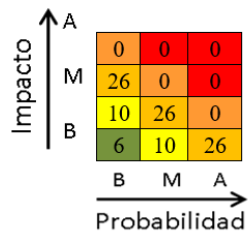


Figura 1 Mapa Térmico

7. Validez y gestión de documentos

Este documento es válido hasta el enero del 2021.

El propietario de este documento es el Director de Tecnología de la información del Gobierno Provincial de Loja, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

**PABLO
RAMIRO
VALLEJO
ZUNIGA**

Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

Anexo 32: Certificado de la Dirección de Tecnología de la Información del Gobierno Provincial de Loja




Ing. Pablo Ramiro Vallejo

**DIRECTOR DE TECNOLOGÍA DE LA INFORMACIÓN DEL GOBIERNO
PROVINCIAL DE LOJA**

CERTIFICA:

Que la egresada **KARLA ANDREA CORREA CUMBICUS**, realizó el Trabajo de Titulación denominado **"Diseño de un Modelo de Gestión de Seguridad de la Información bajo el Estándar ISO/IEC 27001:2013 para la Dirección de la Tecnología de la Información del Gobierno Provincial de Loja"**, bajo mi supervisión y colaboración en la Dirección de Tecnologías de la Información del Gobierno Provincial de Loja. En virtud que el Trabajo de Titulación reúne, a satisfacción las cualidades de fondo y forma exigidas para un trabajo de su nivel, legalizo la aceptación y aprobación del Modelo de Seguridad de la Información, el mismo que fue probado en la institución.

Es todo cuando puedo certificar en honor a la verdad, y autorizo a la propietaria del mismo hacer uso del mismo para trámites pertinentes.


Ing. Pablo Vallejo Zúñiga

Director de Tecnología de la Información

Anexo 33: Carta de Compromiso



CARTA COMPROMISO DE COOPERACIÓN INTERINSTITUCIONAL ENTRE LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN DEL GOBIERNO PROVINCIAL DE LOJA Y LA FACULTAD DE LA ENERGÍA LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES DE LA UNIVERSIDAD NACIONAL DE LOJA

COMPARECIENTES:

Comparecen a la celebración de la presente Carta Compromiso, por una parte, La Dirección de Tecnología de la Información del Gobierno Provincial de Loja, representada por el ingeniero Pablo Ramiro Vallejo Zuñiga, a quien en adelante podrá llamársele **“Dirección de Tecnología de la Información”**; y, por otra, el Área de la Energía, las Industrias y los Recursos Naturales No Renovables de la Universidad Nacional de Loja, legalmente representada por el Ingeniero Thuesman Estuardo Montaña Peralta, en calidad de **DECANO DE LA FACULTAD DE LA ENERGÍA, INDUSTRIAS Y RECURSOS NATURALES NO RENOVABLES DE LA UNIVERSIDAD NACIONAL DE LOJA**, que en adelante y para efectos del presente instrumento se denominará la **“LA FACULTAD LA ENERGÍA”**, quienes con la capacidad legal que en derecho se requiere para este tipo de actos, acuerdan celebrar la presente Carta Compromiso.

Los representantes de las instituciones intervinientes declaran su voluntad para suscribir el presente instrumento, cuyo objeto es concertar acciones específicas de cooperación interinstitucional, que permitan el desarrollo del trabajo de Titulación denominado: **“Diseño de un modelo de Gestión de Seguridad de la Información, bajo el estándar ISO/IEC 27001:2013 para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja”** que en adelante podrá llamársele **“Proyecto de Titulación”**; y cuyo marco regulador se rige por las cláusulas que a continuación se detallan:

PRIMERA: ANTECEDENTES

DIRECCIÓN DE TECNOLOGÍA E INFORMACIÓN:

El Gobierno Provincial de Loja, es una persona jurídica de derecho público, con autonomía política, administrativa y financiera.

Estará integrada por las funciones de participación ciudadana y control social; legislación, normalización y fiscalización; y, ejecución y administración previstas en el Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD), para el ejercicio de las funciones y competencias que le corresponden.

La Dirección de Tecnología de la Información tiene como misión planificar, dirigir, implementar, mantener y administrar los sistemas de información y tecnologías de información y comunicación de la institución, de acuerdo a sus necesidades, objetivos y bajo estándares que garanticen la confiabilidad y



seguridad de la información.

DE LA UNIVERSIDAD NACIONAL DE LOJA

La Universidad Nacional de Loja, es una Institución de Educación Superior, laica, autónoma, de derecho público, con personería jurídica y sin fines de lucro, se rige por la Constitución de la República del Ecuador, la Ley de Educación Superior, su Reglamento de Aplicación y Leyes Conexas, los Reglamentos del Consejo de Educación Superior (CES) y sus Resoluciones, la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), el Estatuto Orgánico y Reglamento General de la Universidad, Los Reglamentos, Normativos e Instructivos; y, las resoluciones que adopten sus organismos de Gobierno y las Autoridades Universitarias, en el ámbito de su competencia.

El Área de la energía, tiene como misión la de sistematizar los conocimientos científico-técnico universales y confrontar su aplicación a la realidad regional y nacional; generar conocimientos, pautas y referentes propios, para enfrentar los problemas del entorno, a través de la investigación, suscitar análisis, debates y construcción de alternativas de los relevantes problemas regionales y nacionales, con la participación de los actores sociales involucrados

SEGUNDA: OBJETO

La presente carta de compromiso tiene como objetivo establecer las condiciones institucional recíprocas entre la Dirección de Tecnología de la Información del Gobierno Provincial de Loja y la Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables de la Universidad Nacional de Loja, para desarrollar acciones conjuntas que permitan el desarrollo del Proyecto de Titulación.

TERCERA: COMPROMISO DE LAS PARTES

DE LA DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN DEL GOBIERNO PROVINCIAL DE LOJA:

- Información sobre los controles de seguridad aplicados actualmente en la dirección de tecnología de la información gobierno provincial de Loja.
- Información de los activos tecnológicos existentes en la dirección de tecnología de la información gobierno provincial de Loja.
- Información sobre las actividades y roles del personal de la dirección de tecnología de la información.



- Información sobre los procesos que llevan a cabo en la dirección de tecnología de la información.

Además, en caso de requerirse información adicional que sea relevante para la ejecución del proyecto, se debe brindar dicha información cuando el responsable del proyecto de titulación así lo solicite, siempre y cuando no comprometa la seguridad de la dirección de la tecnología de la información.

DE LA FACULTAD DE ENERGÍA:

Diseñar un modelo de Gestión de Seguridad de la Información, bajo el estándar ISO/IEC 27001:2013 para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

Para una correcta ejecución del proyecto, se cumplirán las siguientes 4 fases:

FASE 1: Realizar un diagnóstico de la situación actual de la seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja por medio de los procesos descritos en la norma ISO/IEC 27001:2013.

- Recolectar información sobre los controles de seguridad aplicados actualmente en la dirección de tecnología de la información gobierno provincial de Loja.
- Recolectar Información de los activos tecnológicos existentes en la dirección de tecnología de la información gobierno provincial de Loja.
- Recolectar información sobre las actividades y roles del personal.
- Recolectar información sobre los procesos que llevan a cabo.
- Realizar la evaluación de los riesgos.
- Establecer criterios para aceptación de riesgos.
- Identificar los riesgos, amenazas y vulnerabilidades que presentan los activos de información del GP.
- Analizar la información y elaborar un informe de la situación actual de la dirección de tecnología de la información del gobierno provincial de Loja.

FASE 2: Definir políticas de seguridad bajo el estándar ISO/IEC 27001:2013. Anexo A (controles) necesarios para gestionar la seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial.



-
- Definir Políticas de Organización de la Seguridad de la Información.
 - Definir Políticas de Seguridad de Recursos Humanos.
 - Definir Políticas de Gestión de Recursos.
 - Definir Políticas de Control de Acceso.
 - Definir Políticas de Criptografía.
 - Definir Políticas de Seguridad Física y ambiental.
 - Definir Políticas de Seguridad Operacional.
 - Definir Políticas de Seguridad de las Comunicaciones.
 - Definir Políticas de Adquisición, desarrollo y mantenimiento de Sistemas.
 - Definir Políticas de Relaciones con los proveedores.
 - Definir Políticas de Gestión de Incidentes en Seguridad de la Información.
 - Definir Políticas de Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio.
 - Definir Políticas de Cumplimiento.

FASE 3: Definir un modelo para gestión de seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja bajo la norma ISO/IEC 27001:2013.

- Definir las fases del modelo de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013.
- Elaborar la documentación necesaria para la elaboración del modelo gestión de la seguridad de la Información bajo la norma ISO/IEC 27001:2013.

FASE 4: Valorar el modelo mediante la implementación del mismo para la gestión de seguridad de la información para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja.

- Definir el plan de pruebas.
- Definir el escenario de pruebas.
- Ejecutar el modelo de acuerdo con el plan de pruebas.



La responsable del proyecto de titulación se compromete a no utilizar un plan de pruebas crítico que ponga en riesgo el correcto funcionamiento de la dirección de tecnología de la información. Posteriormente queda a criterio de la dirección de tecnología de la información la implementación del modelo.

CUARTA: PROCEDIMIENTOS DE EJECUCIÓN

Para la ejecución de la presente carta de compromiso, en cuanto sea posible y conveniente, las partes observarán los siguientes lineamientos:

- Se mantendrán reuniones ordinarias de acuerdo al calendario de reuniones entre los técnicos de la dirección de tecnología de la información del gobierno provincial de Loja y el responsable del Proyecto de Titulación.
- De ser necesario se convocará a reuniones extraordinarias para tratar asuntos inherentes a la valoración del Proyecto.
- La dirección de tecnología de la información designará un recurso humano para contacto directo con la responsable del proyecto de titulación.
- Se adjunta el cronograma de actividades a desarrollarse en el proyecto de titulación.
- Las reuniones se llevarán a cabo de acuerdo al siguiente calendario.

Calendario de Reuniones Fase 1:

Acción	Julio		Agosto		Responsable
Recolectar Información para conocer la situación actual de la dirección de tecnología de la información del GPL.	27/07/2018	30/07/2018			Karla Correa
Establecer criterios para aceptación de los riesgos			13/07/2018		Karla Correa
Aceptación del informe de la situación actual				24/07/2018	Karla Correa



Calendario de Reuniones Fase 2:

Acción	Septiembre	Octubre	Noviembre	Diciembre	Enero	Febrero	Responsable
Socializar políticas de organización de la seguridad.	03/09/2018.						Karla Correa
Socializar políticas de seguridad de recursos humanos.	17/09/2018.						Karla Correa
Socializar políticas de gestión de recursos.		01/10/2018					Karla Correa
Socializar políticas de control de acceso		15/10/2018					Karla Correa
Socializar políticas de criptografía		29/10/2018					Karla Correa
Socializar políticas de Seguridad Física y ambiental			12/11/2018				Karla Correa
Socializar políticas de seguridad operacional			26/11/2018				Karla Correa
Socializar políticas de seguridad de las comunicaciones.				10/12/2018			Karla Correa
Socializar políticas de Adquisición, desarrollo y mantenimiento de Sistemas				21/12/2018			Karla Correa



Socializar políticas de Relaciones con los proveedores.					07/01/2019		Karla Correa
Socializar políticas de Gestión de Incidentes en Seguridad de la Información.					21/01/2019		Karla Correa
Socializar políticas de Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio.						04/02/2019	Karla Correa
Socializar políticas de Cumplimiento						18/02/2019	Karla Correa
Socializar todas las políticas.						22/02/2019	Karla Correa

Calendario de Reuniones Fase 3:

Acción	Marzo	Responsable
Reunión con el encargo de la dirección de tecnología de la información para exponer el modelo y la documentación necesaria que esta requiere.	29/03/2019	Karla Correa



Calendario de Reuniones Fase 3:

Acción	Marzo	Responsable
Reunión con el encargo de la dirección de tecnología de la información para exponer los resultados del proyecto de titulación	22/04/2019	Karla Correa

QUINTA: RECIPROCIDAD

Las instituciones participantes en el Proyecto de Titulación se comprometen a reconocer su colaboración en el desarrollo del proyecto de titulación en publicaciones, informes, material informativo, mensajes y cualquier otro medio de difusión, previo acuerdo específico, también el responsable del proyecto entregará una copia del modelo diseñado, como resultado final del proyecto de titulación.

SEXTA: DURACIÓN

La presente carta entrará en vigor a la fecha de su firma y tendrá validez durante (un año y medio), a menos que una de las partes comunique por anticipado su deseo de finalizar su participación, o el deseo de incrementar el plazo de participación.

Los términos de la presente carta podrán ser modificados por acuerdo expreso de las partes, anexando al mismo las actas conjuntas correspondientes.



SÉPTIMA: CONTROVERSIAS

Basándose en la buena voluntad como base fundamental de la presente carta, para el caso de controversias derivadas de esta, las partes aceptan solucionarlas de manera directa a través del diálogo entre ellas.

Las partes se ratifican íntegramente en el contenido de la presente carta y para constancia firman en unidad del acto, los comparecientes en original y tres copias del mismo tenor y efecto legal, en la ciudad de Loja a los 5 días del mes de Julio del 2018.

OCTAVA: CONFIDENCIALIDAD

El responsable del proyecto de titulación se compromete a manejar la información obtenida con total discreción y responsabilidad, comprometiéndose a no divulgar información manejada por el gobierno provincial de Loja.



**Ing. Thuesman Montaña
DECANO DE LA FACULTAD DE LA
ENERGÍA, LAS INDUSTRIAS Y LOS
RECURSOS NATURALES NO
RENOVABLES**



**Ing. Pablo Vallejo
RESPONSABLE DE LA DIRECCIÓN DE
TECNOLOGÍA DE LA INFORMACIÓN
DEL GOBIERNO PROVINCIAL DE
LOJA.**

Anexo 34: Permiso de Advisera

The screenshot shows a Gmail interface with a search bar containing 'TESIS'. The email is titled 'Precio y Términos Legales' and is from Aleksandar Bozovic (aleksandar@advisera.com) to Karla Andrea. The email content includes a greeting, a thank you for a message, and information about a document permission for 'tesis' documents, with a note that the documents are from Advisera. It also mentions that a finance team will send a purchase link. A contact card for Aleksandar Bozovic is visible, listing his email, phone number, and role as Sales coordinator. Below the email, there are promotional banners for 'Academy' and a webinar about ISO 27001 & ISO 22301.

Anexo 35: Comprobante de compra ISO27001

The screenshot shows a Gmail interface with a search bar containing 'Purchased templates / Advisera'. The email is from Olivera Stojanovic (olivera@advisera.com) to Aida. The email content includes a greeting, a request to find the purchased templates, and a note that if anything else is needed, the sender should be contacted directly. The email ends with 'Best regards, Olivera'. A contact card for Olivera Stojanovic is visible, listing her email, phone number, and role as Customer/Conformio support.

LATEST BLOG POSTS

[Can ISO 27001 help your organization in a DDoS attack?](#)

[4 crucial techniques to convince your top management about ISO 9001 implementation](#)

[Using AS9100 Rev D for variation management of key characteristics](#)

[Production and Service Provision Process in ISO 13485](#)

[How can ISO 14001 help improve a company's total quality management?](#)

[How to Create an OHSAS 18001 Internal Audit Plan](#)

[What is the Information Security Policy according to ITIL/ISO 20000?](#)

[How to choose the right online ISO management software](#)

9 archivos adjuntos



Anexo 36: Apéndice Plan de capacitación y concienciación

Plan de capacitación y concienciación


Con el objetivo de preparar a los colaboradores de la Dirección de Tecnología de la Información para que pueda cumplir una función en la seguridad de la información, se debe llevar a cabo la siguiente capacitación:

INFORMACIÓN
CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

INFORMACIÓN CONFIDENCIAL

PABLO
RAMIRO
VALLEJO
ZUNIGA



Firmado digitalmente
por PABLO RAMIRO
VALLEJO ZUNIGA
Fecha: 2020.07.28
10:40:38 -05'00'

Ing. Pablo Vallejo
Director de Tecnología de la Información

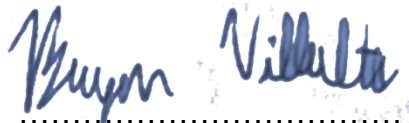
Anexo 37: Certificación Traducción Summary

Newark, viernes 23 de julio de 2020

Ciudad

Yo, Bryan Andrés Villalta Correa con NIF: 581416603, estudiante de Ingeniería en Stevens Institute of Technology; y, americano de nacimiento respaldo que el resumen del Trabajo de Titulación denominado “Diseño de un modelo de Gestión de Seguridad de la Información, bajo el estándar ISO/IEC 27001:2013 para la Dirección de Tecnología de la Información del Gobierno Provincial de Loja” es fiel traducción de su original en español y su contenido en inglés puede ser interpretado de forma correcta.

Atentamente,



.....
Bryan Andrés Villalta Correa
NIF: 581416603