Título del Trabajo Final

Nombre Estudiante: Mayerly Sáenz Casallas

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Antonio José Segovia Henares
Profesor responsable de la asignatura: Carles Garrigues Olivella

Centro: Universitat Oberta de Catalunya

Fecha entrega: 28 de diciembre de 2020

Dedicatoria:

A Dios, mi madre, mi esposo y mis hermanas

Agradecimientos:

Primero que todo a Dios, que me ha acompañado en todo momento, y me ha protegido junto con toda mi familia.

A mi mami Edith, por apoyarme toda la vida en cada logro que he conseguido. Eres mi mejor ejemplo de mujer guerrera y luchadora, la mejor madre del mundo. Para ti mi mayor respeto y toda mi admiración.

A mi esposo Darwin, por tu apoyo incondicional en absolutamente todo. Eres mi más grande inspiración y agradezco a la vida que te haya puesto en mi camino. Primer logro de muchos que nos esperan mi compañerito de vida.

A mis hermanas Marilyn y Maryory, réplicas de mi mami, mujeres excepcionales con las que siempre puedo contar.

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013 para una ISP*
Nombre del autor:	*Mayerly Sáenz Casallas*
Nombre del consultor/a:	*José Segovia Henares*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	12/2020
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Español*
Palabras clave	*SGSI, Plan director, ISO/IEC 27001:2013, ISO 27002, ISP, Análisis de riesgos.*

Resumen del Trabajo:

En este trabajo de fin de máster se presenta la propuesta para implementar el plan director a la empresa ISP ubicada en Imbabura Ecuador, siguiendo las especificaciones para la implantación del Sistema de Gestión de la Seguridad de la Información de la norma ISO/IEC 27001:2013 y la guía de buenas prácticas de la ISO 27002:2013.

Como punto de partida, se realizó un análisis de la situación actual de la empresa con respecto a los requisitos de seguridad de la información para analizar su grado de cumplimiento. Posterior a esto se hizo un análisis de riesgos sobre los activos relevantes en términos de seguridad, con el fin de determinar el impacto potencial que sufrirían al verse materializada cualquier amenaza a la que se encuentran expuestos. A partir de esta información se logra determinar el nivel de riesgo aceptable y proponer proyectos para reducir aquellos riesgos que son tratables. Cada uno de estos proyectos están diseñados con la planificación para ejecutarse y el coste económico que le representará a la organización, el cual no supondrá un gasto mayor al de asumir el riesgo. Finalmente se presentan los resultados esperados, luego de poner en marcha cada uno de los proyectos propuestos, en cuanto al cumplimiento normativo de la ISO/IEC 27002:2013 y cada uno de sus 14 dominios.

Abstract

This master's thesis proposes to implement the master plan to ISP Company located in Imbabura Ecuador. Following the specifications for the implementation of the information security management according to the International Organization for Standardization ISO/IEC 27001: 2013, and the standards on the best practice recommendations in ISO 27002: 2013.

As a starting point, a diagnosis of the company's current situation with respect to information security requirements was carried out to analyze its degree of compliance. Subsequently, a risk analysis was made on the relevant assets in terms of safety, to determine the potential impact, they would suffer in any case exposed to threat. Indeed, with this information it is possible to determine the acceptable level of risk and propose projects to reduce those risks that are treatable. Each of these projects is designed with the planning to be executed, and the estimated cost that the Company would have to assume. Which will not be more costly than taking the risk. Finally, the expected results are presented, after starting each of the proposed projects, regarding the compliance conforming to ISO/IEC 27002:2013, and each of its fourteen domains.

Índice

1. Introducción 1
1.1 Historia de la ISO/IEC 27001 2
1.2 Contexto y justificación 4
1.3 Análisis diferencial entre la organización y la ISO/IEC 27001:2013 y la ISO/IEC 27002 6
1.3.1 Análisis diferencial entre la organización y la ISO/IEC 27001:2013 8
1.3.2 Análisis diferencial entre la organización y la ISO/IEC 27002:2013 9
1.3.3 Presentación de resultados 14
1.4 Objetivos del Plan Director 23
1.5 Enfoque y método seguido 24
1.6 Planificación del Trabajo 25
1.7 Breve descripción de los capítulos de la memoria 26
2. Documentación del Sistema de Gestión de Seguridad de la Información 27
2.1 Política de Seguridad 28
2.2 Procedimiento de Auditorías Internas 28
2.3 Gestión de Indicadores 28
2.4 Procedimiento Revisión por Dirección 29
2.5 Gestión de Roles y Responsabilidades 29
2.6 Metodología de Análisis de Riesgos 29
2.7 Declaración de Aplicabilidad 29
3. Análisis de Riesgos 31
3.1 Introducción 31
3.2 Inventario de activos 32
3.3 Valoración de activos 35
3.4 Dimensiones de Seguridad 38
3.5. Tabla resumen de valoración 40
3.6. Análisis de amenazas 41
3.7. Impacto potencial 48
3.8. Nivel de Riesgo Aceptable y Riesgo Residual 50
4. Propuestas de proyectos 53
4.1 Introducción 53
4.2. Propuestas 54
4.3 Resultados 66
4.3.1 Resultados de comparar el nivel de riesgo potencial con el nivel de riesgo residual 66
4.3.2. Evolución del nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC 27002 68
5. Auditoría de cumplimiento 70
5.1. Introducción 70
5.2. Metodología 70
5.3. Evaluación de la madurez 71
5.3.1. Evaluación de la madurez de la ISO/IEC 27001:2013 71
5.3.2. Evaluación de la madurez de la ISO/IEC 27002:2013 72
5.4. Presentación de resultados 82
5.5 Informe de auditoría interna 86
6. Presentación de resultados y entrega de informes 90

7. Conclusiones 91
8. Glosario 93
9. Bibliografía 95
10. Anexos 96
10.1. Anexo Política de seguridad 96
10.2. Anexo Procedimiento de Auditorías Internas 105
10.3. Anexo Gestión de Indicadores 117
10.4. Anexo Procedimiento Revisión por Dirección 127
10.5. Anexo Gestión de Roles y responsabilidades 132
10.6. Anexo Metodología de Análisis de Riesgos 138
10.7. Anexo Declaración de Aplicabilidad 145

Índice de las ilustraciones

Ilustración 1 Estructura organizacional 5
Ilustración 2 Diagrama de red de la ISP 6
Ilustración 3 CMM de los controles ISO actuales en la ISP 14
Ilustración 4 diagrama de Gantt 26
Ilustración 5 Gráfico de barras de la valoración por tipo de activo 38
Ilustración 6 Relación entre el riesgo y el costo de protección (públicas, 2012) 50
Ilustración 7 Diagrama de Gantt con la planificación de los proyectos parte 1 65
Ilustración 8 Diagrama de Gantt con la planificación de los proyectos parte 2 65
Ilustración 9 Diagrama de Gantt con la planificación de los proyectos parte 3 66
Ilustración 10 Diagrama de Gantt con la planificación de los proyectos parte 4 66
Ilustración 11 Comparación entre el riesgo potencial y la estimación del riesgo residual en los ámbitos [L], [HW] y [SW] 67
Ilustración 12 Comparación entre el riesgo potencial y la estimación del riesgo residual en los ámbitos [D], [COM], [S], [AUX], [P]. 67
Ilustración 13 Comparación entre el riesgo potencial y la estimación del riesgo residual en el ámbito [P]. 68
Ilustración 14 Grafico GAP después de la implementación de los proyectos .. 69
Ilustración 15 Diagrama radar de los requerimientos ISO/IEC 27001:2013 83
Ilustración 16 Diagrama radar de los Dominios ISO/IEC 27002:2013 84
Ilustración 17 Madurez CMM de los controles ISO 85

Índice de las tablas

Tabla 1 Dominios de la ISO/IEC 27001 4
Tabla 2 Modelo de Madurez de la Capacidad (CMM) 7
Tabla 3. Análisis diferencial ISO 27001:2013 8
Tabla 4 Estimación de los controles de la ISO/IEC 27002:2013 con el modelo CMM 9
Tabla 5 Resultados CMM de los controles 14
Tabla 6 Planificación TFM 25
Tabla 7 Clasificación de los activos 32
Tabla 8 Inventario de los activos de la ISP 33
Tabla 9 Escala para valoración de activos 35
Tabla 10 Valoración de cada activo 36
Tabla 11 Valoración total por tipo de activo 37
Tabla 12 Valores de criticidad en las dimensiones de seguridad 39
Tabla 13 Escala de grado de importancia del activo 39
Tabla 14 Valoración de criticidad de las dimensiones de seguridad 39
Tabla 15 Valoración de activos con criticidad en las dimensiones 40
Tabla 16 Clasificación Amenazas MAGERIT 42
Tabla 17 Escala de frecuencia de materialización de una amenaza 42
Tabla 18 Impacto de amenazas en activos de instalaciones 43
Tabla 19 Impacto de amenazas en activos de hardware 43
Tabla 20 Impacto de amenazas en activos de software 43
Tabla 21 Impacto de amenazas en activos de datos 44
Tabla 22 Impacto de amenazas en activos de redes 45
Tabla 23 Impacto de amenazas en activos de Servicios 46
Tabla 24 Impacto de amenazas en activos de Equipamiento auxiliar 46
Tabla 25 Impacto de amenazas en activos de personal 47
Tabla 26 Niveles de impacto 48
Tabla 27 Impacto potencial 49
Tabla 28 Niveles de riesgo analizando la frecuencia de ocurrencia 51
Tabla 29 Nivel de riesgo > 7 51
Tabla 30 Resultados de porcentaje de los 114 controles 68
Tabla 31 Apartados de las normas ISO a evaluar con el CMM 70
Tabla 32 Porcentaje de efectividad de los requerimientos ISO/IEC 27001:2013 final 71
Tabla 33 Controles del dominio Políticas de seguridad de la información 73
Tabla 34 Controles del dominio Organización de la seguridad de la información 73
Tabla 35 Controles del dominio Seguridad relativa a los recursos humanos 74
Tabla 36 Controles del dominio Gestión de activos 74
Tabla 37 Controles del dominio Control de acceso 75
Tabla 38 Controles del dominio Criptografía 76
Tabla 39 Controles del dominio Seguridad física y entorno 76
Tabla 40 Controles del dominio Seguridad de operaciones 78
Tabla 41 Controles del dominio Seguridad de las comunicaciones 79
Tabla 42 Controles del dominio Adquisición, desarrollo y mantenimiento de los sistemas de información 79
Tabla 43 Controles del dominio Relación con proveedores 80

Tabla 44 Controles del dominio Gestión de incidentes de seguridad de la información 81
Tabla 45 Controles del dominio Aspectos de seguridad de la información para la gestión de la continuidad del negocio..... 81
Tabla 46 Controles del dominio Cumplimiento 82
Tabla 47 Porcentaje de efectividad de los requerimientos ISO 27001 inicial y final 83
Tabla 48 Porcentaje de efectividad de los dominios de la ISO 27002 inicial y final 83
Tabla 49 Madurez CMM de los controles ISO..... 85
Tabla 50 No conformidad No.1 86
Tabla 51 No conformidad No.2 87
Tabla 52 No conformidad No.3 87
Tabla 53 No conformidad No.4 88
Tabla 54 Planificación de la revisión anual de los 114 controles 111
Tabla 55 Componentes para un indicador.....120
Tabla 56 Control Política de seguridad 120
Tabla 57 Indicador control Roles y responsabilidades.....121
Tabla 58 Control de capacitaciones del personal en seguridad de la información 121
Tabla 59 Control de Activos devueltos 122
Tabla 60 Control eliminación de soportes 123
Tabla 61 Eliminación de soportes 123
Tabla 62 Puesto de trabajo organizado.....124
Tabla 63 Control en el procedimiento de recopilación de evidencias 124
Tabla 64 Incidentes de seguridad 125
Tabla 65 Política de privacidad 125
Tabla 66 Escala de niveles de riesgo.....143

1. Introducción

La razón de proteger la información de una empresa tiene tanta importancia como su correcto funcionamiento diario, esto debido a que la pérdida de información sensible podría representar una falla en el buen desempeño de los servicios que presta cada organización. La información que trata cualquier empresa o institución tanto pública como privada es un componente indispensable en la dirección y cumplimiento de los objetivos definidos por la estrategia de la organización. Esto representa una razón de vital importancia para que una empresa establezca un marco en el cual se sigan pautas y normas de buenas prácticas que permitan manipular, procesar, transportar y almacenar toda la información sea física o digital asegurando que la información esté protegida de la mejor manera.

Las normativas actuales en Ecuador no cuentan con leyes para la protección de datos ni tampoco se exigen certificaciones que garanticen un Sistema de Gestión de la seguridad de la información, al menos no de carácter obligatorio, por lo que la mayoría de las empresas no disponen de certificaciones que acrediten el correcto desarrollo de las actividades laborales bajo una normativa ISO. Sin embargo, y debido a la situación actual que atraviesa el mundo a raíz de la pandemia, se ha podido observar un incremento en las actividades tales como teletrabajo lo que ha conllevado a un mayor uso de herramientas digitales, y que finalmente nos lleva a valorar la información de las personas y de las empresas en el desarrollo diario de las actividades.

El presente proyecto tiene como finalidad proponer la implantación de un Sistema de Gestión de la seguridad de la información para la empresa proveedora de servicio de internet (ISP) con los lineamientos de la norma ISO/IEC 27001 y con la guía de buenas prácticas de la ISO 27002 que permitan obtener un sistema que contribuya a gestionar de forma adecuada la seguridad de la información de la empresa.

El estándar internacional ISO/IEC 27001 es un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI (Sistema de Gestión de Seguridad de la Información), la revisión más reciente de esta norma fue publicada en 2013 y la primera revisión se publicó en el año 2005, la cual fue desarrollada en base a la norma británica BS 7799-2 (British Standars Institution). (Sánchez, 2017)

Para la ejecución de la propuesta se utilizará el modelo de mejora continua del ciclo Deming que consiste en un proceso iterativo de calidad compuesto por 4 etapas para implantar el SGSI. La primera etapa (Plan) corresponde a la planificación donde se realizará un análisis del estado actual de la ISP que permita trazar los objetivos del proceso de gestión, se definan las políticas de seguridad, alcance, objetivos identificación de los riesgos y selección de las salvaguardas. La segunda etapa Do, en donde se realizará la implantación del plan de gestión de riesgo y además se seleccionarán los controles que generen diferentes

indicadores con el fin de evaluar constantemente la eficacia del plan de gestión. La tercera etapa Check, encargada de evaluar y verificar constantemente la eficacia tanto del plan de gestión como de los controles implementados al igual que los informes de auditorías internas. Finalmente, pero no menos importante se encuentra la etapa Act que basada en los resultados de la evaluación y verificación de la etapa anterior marcará la pauta para mantener o implementar las acciones correctivas necesarias para mejorar.

El trabajo se desarrollará de la siguiente manera: Capitulo 1. Introducción, contextualización de la empresa y situación actual de los sistemas de seguridad. Capítulo 2 y 3 corresponderán a la Etapa de planificación, para lo cual en el segundo se establecerán las políticas de seguridad y políticas de alto nivel, se definirá el alcance y la organización de la seguridad y en el Capítulo 3. se realizará el Análisis de Riesgos con todo lo que esto contempla, análisis de amenazas, vulnerabilidades, impacto potencial y cálculos de riesgo para evaluar aquellos aceptables o críticos. En el Capítulo 4. Se realizará la segunda etapa del modelo de mejora continua realizando una propuesta del plan de gestión de riesgos. El capítulo 5 desarrollará las últimas dos etapas del proceso Deming en donde se establecerán los controles propuestos en la norma ISO 27002 al igual que los planes preventivos y correctivos de mejora continua para el SGSI.

1.1 Historia de la ISO/IEC 27001

ISO/IEC-27001:2013 (Information Technology – Security Techniques – Information Security Management Systems – Requirements) fue aprobado y publicado en 2005 por la International Organization for Standardization y por la International Electrotechnical Commission, especificando los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

La norma ISO/IEC-27001 fue creada basándose en el ciclo de Deming, ciclo de mejora continua o ciclo PDCA, ciclo correspondiente a las iniciales de Planear (Plan), Hacer (Do), Verificar (Check) y Actuar (Act). A partir de lo anterior surge el Sistema de Gestión de la Seguridad de la Información (SGSI) o lo que es lo mismo en inglés: Information Security Management System. (Alvarez, 2016)

Esta norma está dividida en 2 partes, la primera parte donde se establecen los requerimientos de la norma conformada por 10 procesos y la segunda pare donde se encuentran los 14 dominios a su vez conformados por 114 controles. A continuación, se describen los 10 procesos importantes mencionados en la norma y los 14 dominios mencionados.

1. Objeto y campo de aplicación: Especifica los requisitos de aplicación a cualquier organización que pretenda implementar un SGSI.

2. Referencias normativas: en este apartado se establece las normas en las que se basará, en decir la ISO /IEC 27000, Tecnología de la información, Técnicas tecnológicas de seguridad, y Sistemas de Gestión de la Seguridad de la información.

3. Términos y definiciones: Corresponden a todos los usados en la norma ISO/IEC 27000.

4. Contexto de la organización: Conformado por 4 partes importantes: a) aspectos internos y externos relevantes con el correcto funcionamiento de la organización; b) necesidades y expectativas de las partes interesadas; c) determinación del alcance; y d) continua revisión del SGSI.

5. Liderazgo: Corresponde al compromiso que debe tener la alta dirección a lo largo del desarrollo del SGSI, en todos los aspectos relevantes para que cumpla con los objetivos planteados, como lo son establecer la política, así como la asignación de responsabilidades.

6. Planificación: todas aquellas acciones que deben establecerse antes de la ejecución del SGSI, como la gestión, valoración y tratamiento de los riesgos, así como los objetivos y los planes de acción para lograr dichos objetivos.

7. Soporte: Establece los recursos que la organización proporcionará, tanto físicos como respecto al personal competente que trabajará en la ejecución del SGSI, y asegurará que se realicen continuas concientizaciones que comuniquen de manera oportuna la importancia de la implantación del sistema de gestión a todo el personal involucrado con la organización.

8. Operación: Establece los requisitos en cuanto a planificación, implementar y control de los procesos de la organización, así como la gestión de los riegos correspondientes a la evaluación y el tratamiento de estos.

9. Evaluación del desempeño: Corresponde a los métodos y procedimientos que se deben realizar para monitorear, medir, analizar y evaluar la eficacia de la implantación del SGSI, para esto se cuenta con auditorías encargadas de revisar este desempeño además de revisión encargada desde la alta dirección.

10. Mejoras: Es esta sección se tratan las no conformidades, las acciones correctivas y la importancia de la mejora continua.

La segunda parte de la norma está conformada por el anexo A en el cual se incluyen 14 dominios, con 35 objetivos de control y 114 controles se seguridad. La norma ISO 27002:2013, es norma no certificable, considerada como una guía de buenas prácticas que detalla cada uno de los controles que se pueden implantar en cualquier empresa que desee certificarse con la ISO/IEC 27001.

Los dominios mencionados se encuentran descritos a continuación en la tabla 1, con la cantidad de objetivos y controles que los conforman a cada uno.

Tabla 1 Dominios de la ISO/IEC 27001

Dominios	Objetivos	Controles
5. Políticas de Seguridad	1	2
6. Organización de la Seguridad de la Información	2	7
7. Seguridad de los Recursos Humanos.	3	6
8. Gestión de los Activos.	3	10
9. Control de Acceso	4	14
10. Criptografía	1	2
11.Seguridad Física	2	15
12.Seguridad de las Operaciones	7	14
13.Seguridad de las Comunicaciones	2	7
14.Adquisición, desarrollo y mantenimiento de los sistemas de información	3	13
15.Relación con proveedores	2	5
16.Gestión de incidentes de seguridad de la información	1	7
17.Aspectos de seguridad de la información para la gestión de la continuidad del negocio	2	4
18.Cumplimiento	2	8

1.2 Contexto y justificación

He seleccionado una pequeña empresa que se encuentra ubicada en la provincia de Imbabura Ecuador y que se dedica a la prestación de servicios de internet. Ofrece planes de internet con antena con cobertura en las provincias de Imbabura y Carchi y planes de internet con fibra óptica para la provincia de Imbabura. La Ilustración 1 muestra la estructura organizacional de la empresa a la cual se realizará el plan director de seguridad.

Ilustración 1 Estructura organizacional

Gerente General: Representante legal de la empresa
Asistente Administrativo: Puente comunicador entre la gerencia y los demás departamentos
Gerente Técnico: Responsable de asignación de tareas y supervisión de técnicos.
Gerente de Ventas: Responsable de informes y ventas corporativas
Contabilidad y cobranzas: Encargado de la parte financiera de la empresa, declaraciones de impuestos, pagos de salarios cobro de facturas etc.
Servicio al cliente: Responsable de atender los requerimientos de los clientes y canalizar los inconvenientes a quien corresponde.
Técnicos instaladores: Encargados de las instalaciones y de los mantenimientos correctivos
Ejecutivos de Ventas: Contratos pequeños con metas mensuales.
Mensajero: Encargado de cualquier entrega

La empresa no cuenta con ninguna certificación ISO ni para gestión de la seguridad de la información ni para otra relacionada a la prestación de servicios. Actualmente guardan su información de forma física, la cual es toda la relacionada a las órdenes de trabajo tanto de instalaciones como de reparaciones y al mismo tiempo tienen implementado un sistema de base de datos mysql en donde se almacena la información de forma digital. No se tiene ningún documento formal que indiquen procedimientos estándar, aunque si siguen varios procedimientos de prevención y protección de información.

En la ilustración 2 se puede observar el diagrama de red de la infraestructura tecnológica de la ISP.

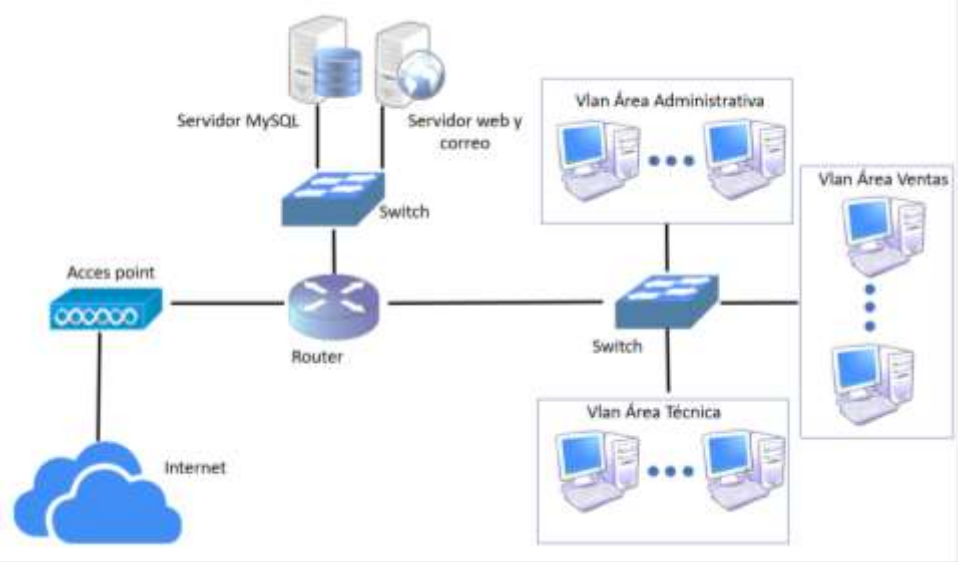

Ilustración 2 Diagrama de red de la ISP

Actualmente la seguridad de la red se encuentra sin protección con respecto a la salida a internet, sin embargo se cuenta con un router que tiene la finalidad de segmentar la red en dos subredes de la siguiente manera: a) Subred para los 2 servidores de los cuales uno es el encargado para el servicio de correo y donde se aloja la página web de la ISP y por otro lado el segundo servidor encargado de la base de datos MySQL; y b) una subred para las computadoras del personal administrativo, personal de ventas y personal técnico.

Una vez realizado un análisis del estado actual del sistema de gestión de la seguridad de la información de la empresa, nos planteamos el siguiente alcance para desarrollar el presente trabajo final de máster:

Implantar el Sistema de Gestión de la seguridad de la información de todas las actividades desarrolladas en el negocio de la proveedora de servicios de internet para la sede de Imbabura.

1.3 Análisis diferencial entre la organización y la ISO/IEC 27001:2013 y la ISO/IEC 27002

Actualmente la organización no cuenta con ninguna medida de seguridad ni normativas debido a que es una empresa relativamente nueva pero que se ha planteado como uno de sus objetivos principales el de posicionarse en el mercado en un lapso menor a dos años y considera que un SGSI lograría poner su nombre a la altura tanto de empresas privadas como Claro y Movistar así como de la empresa pública de telecomunicaciones de CNT. Inicialmente solo prestan el servicio de internet pero ya están realizando las gestiones pertinentes para ofrecer también telefonía móvil.

La Organización tampoco cuenta con algún documento relacionado a políticas de seguridad, ni con procedimientos, sin embargo, en un intento de tener control sobre algunos procedimientos internos,

disponen de documentos no formales donde se registran la salida de los materiales desde la bodega, requeridos por los técnicos para las instalaciones. También se dispone de una bitácora que registra la entrada y salida de las camionetas disponibles tanto para los técnicos como para el mensajero, y un archivo tanto físico como digital con las ordenes de trabajo tanto de instalación como de reparaciones.

Luego de realizar una descripción a grandes rasgos de la situación actual de la ISP, es necesario establecer el cumplimiento actual de la organización para lo cual se realizará en dos partes. La primera se establecerá una comparación entre el estado actual de la empresa con respecto a los requisitos de la norma ISO/IEC 27001 y la segunda parte un análisis de los controles descritos en la guía de buenas prácticas e ISO/IEC 27002.

Para indicar el grado de cumplimiento actual de la organización se realizará una valoración basado en el modelo de madurez de la capacidad (CMM) como se indica en la tabla 2.

Tabla 2 Modelo de Madurez de la Capacidad (CMM)

Efectividad (%)	CMM	Significado	Descripción
0	L0	Inexistente	Carencia completa de cualquier proceso reconocido. No se ha reconocido que exista ningún problema a resolver.
10	L1	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayor parte de las veces en un esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas en nivel corporativo.
50	L2	Reproducible pero intuitivo	Los procesos similares se llevan a cabo de manera similar por diferentes personas con la misma tarea. Se normalizan las “buenas prácticas” en base a la experiencia y al método. No hay comunicación o capacitación formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante capacitación.
95	L4	Gestionado y	Se puede seguir con indicadores numéricos y estadísticos la

		medible	evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, existen herramientas para mejorar la calidad y la eficiencia.
100	L5	Optimizado	Los procesos están en constante mejora basados en los análisis de resultados que se obtienen de los controles implantados. Se pueden determinar desviaciones con respecto a lo esperado y de esa manera optimizar los procesos.

1.3.1 Análisis diferencial entre la organización y la ISO/IEC 27001:2013

En la tabla 3 se presenta el estado de cumplimiento actual de la ISP con respecto a los requerimientos especificados en la ISO 27001:2013.

Tabla 3. Análisis diferencial ISO 27001:2013

	Requerimientos ISO 27001	Efectividad (%)	CMM
4	**Contexto de la organización**	**5**	**L0**
4.1	Comprensión de la organización y de su contexto	10	
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	10	
4.3	Determinación del alcance del SGSI	0	
4.4	Sistema de Gestión de la Seguridad de la Información	0	
5	**Liderazgo**	**6,7**	**L0**
5.1	Liderazgo y compromiso	10	
5.2	Política	0	
5.3	Roles, responsabilidades y autoridades en la organización	10	
6	**Planificación**	**5**	**L0**
6.1	Acciones para tratar los riesgos y oportunidades	0	
6.2	Objetivos de seguridad de la información y planificación para su consecución	10	
7	**Soporte**	**5**	**L0**
7.1	Recursos	0	
7.2	Competencia	10	
7.3	Concienciación	10	
7.4	Comunicación	0	
8	**Operación**	**0**	**L0**
8.1	Planificación y control operacional	0	
8.2	Apreciación de los riesgos de seguridad de la información	0	
8.3	Tratamiento de los riesgos de seguridad de la información	0	
9	**Evaluación del desempeño**	**3,3**	**L0**
9.1	Seguimiento, medición, análisis y evaluación	0	

9.2	Auditoría interna	0	
9.3	Revisión por la dirección	10	
10	**Mejora**	**5**	**L0**
10.1	No conformidad y acciones correctivas	10	
10.2	**Mejora continua**	**0**	

1.3.2 Análisis diferencial entre la organización y la ISO/IEC 27002:2013

En la tabla 4 se listan los 114 controles de seguridad planteados por la norma para cumplir los 35 objetivos de control. Al igual que la estimación de los requisitos de la norma ISO/IEC 27001:2013, se lo realizará de la misma manera, basado en el (CMM).

Tabla 4 Estimación de los controles de la ISO/IEC 27002:2013 con el modelo CMM

Controles	Efectividad	CMM
5. Políticas de seguridad de la información	**0%**	**L0**
5.1 Directrices de gestión de la seguridad de la información	0%	
5.1.1 Políticas para la seguridad de la información	0%	
5.1.2 Revisión de las políticas para la seguridad de la información	0%	
6. Organización de la seguridad de la información	**13.5%**	**L1**
6.1 Organización interna.	2%	
6.1.1 Roles y responsabilidades en seguridad de la información	10%	
6.1.2 Segregación de tareas	0%	
6.1.3 Contacto con las autoridades	0%	
6.1.4 Contacto con grupos de interés especial	0%	
6.1.5 Seguridad de la información en la gestión de proyectos	0%	
6.2 Los dispositivos móviles y el teletrabajo	**25%**	**L1**
6.2.1 Política de dispositivos móviles	0%	
6.2.2 Teletrabajo	50%	
7. Seguridad relativa a los recursos humanos	**16,7%**	**L1**
7.1 Antes del empleo	50%	
7.1.1 Investigación de antecedentes	90%	
7.1.2 Términos y condiciones del empleo	10%	
7.2 Durante el empleo	0%	
7.2.1 Responsabilidades de gestión	0%	
7.2.2 Concienciación, educación y capacitación en seguridad de la información	0%	
7.2.3 Proceso disciplinario	0%	
7.3 Finalización del empleo o cambio en el puesto de trabajo	0%	

7.3.1 Responsabilidades ante la finalización o cambio	0%	
8. Gestión de activos	**20%**	**L1**
8.1 Responsabilidad sobre los activos	40%	
8.1.1 Inventario de activos	50%	
8.1.2 Propiedad de los activos	50%	
8.1.3 Uso aceptable de los activos	10%	
8.1.4 Devolución de activos	50%	
8.2 Clasificación de la información	0%	
8.2.1 Clasificación de la información	0%	
8.2.2 Etiquetado de la información	0%	
8.2.3 Manipulado de la información	0%	
8.3 Manipulación de los soportes	20%	
8.3.1 Gestión de soportes extraíbles	0%	
8.3.2 Eliminación de soportes	10%	
8.3.3 Soportes físicos en tránsito	50%	
9. Control de acceso	**30,3%**	**L1**
9.1 Requisitos de negocio para el control de acceso	25%	
9.1.1 Política de control de acceso	0%	
9.1.2 Acceso a las redes y a los servicios de red	50%	
9.2 Gestión de acceso de usuario	28,3%	
9.2.1 Registro y baja de usuario	50%	
9.2.2 Provisión de acceso de usuario	50%	
9.2.3 Gestión de privilegios de acceso	50%	
9.2.4 Gestión de la información secreta de autenticación de usuarios	10%	
9.2.5 Revisión de los derechos de acceso de usuario	0%	
9.2.6 Retirada o reasignación de los derechos de acceso	10%	
9.3 Responsabilidades del usuario	10%	
9.3.1 Uso de la información secreta de autenticación	10%	
9.4 Control de acceso a sistemas y aplicaciones	58%	
9.4.1 Restricción del acceso a la información	50%	
9.4.2 Procedimientos seguros de inicio de sesión	50%	
9.4.3 Sistema de gestión de contraseñas	50%	
9.4.4 Uso de utilidades con privilegios de sistemas	50%	
9.4.5 Control de acceso al código fuente de los programas	90%	
10. Criptografía	**10%**	**L1**
10.1 Controles criptográficos	10%	
10.1.1 Política de uso de los controles criptográficos	10%	
10.1.2 Gestión de claves	10%	

11. Seguridad física y del entorno	45,5%	L1
11.1 Áreas seguras	36.7%	
11.1.1 Perímetro de seguridad física	50%	
11.1.2 Controles físicos de entrada	10%	
11.1.3 Seguridad de oficinas, despachos y recursos	10%	
11.1.4 Protección contra las amenazas externas y ambientales	50%	
11.1.5 El trabajo en áreas seguras	50%	
11.1.6 Áreas de carga y descarga	50%	
11.2 Seguridad de los equipos	54,4%	
11.2.1 Emplazamiento y protección de equipos	50%	
11.2.2 Instalaciones de suministro	50%	
11.2.3 Seguridad del cableado	50%	
11.2.4 Mantenimiento de los equipos	50%	
11.2.5 Retirada de materiales propiedad de la empresa	90%	
11.2.6 Seguridad de los equipos fuera de las instalaciones	90%	
11.2.7 Reutilización o eliminación segura de equipos	50%	
11.2.8 Equipo de usuario desatendido	10%	
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	50%	
12. Seguridad de las operaciones	35,3%	L1
12.1 Procedimientos y responsabilidades operacionales	40%	
12.1.1 Documentación de procedimientos de operación	50%	
12.1.2 Gestión de cambios	10%	
12.1.3 Gestión de capacidades	50%	
12.1.4 Separación de los recursos de desarrollo, prueba y operación	50%	
12.2 Protección contra el software malicioso (malware)	50%	
12.2.1 Controles contra el código malicioso	50%	
12.3 Copias de seguridad	10%	
12.3.1 Copias de seguridad de la información	10%	
12.4 Registros y supervisión	27,5%	
12.4.1 Registro de eventos	10%	
12.4.2 Protección de la información de registro	50%	
12.4.3 Registros de administración y operación	50%	
12.4.4 Sincronización del reloj	0%	
12.5 Control del software en explotación	90%	
12.5.1 Instalación del software en explotación	90%	
12.6 Gestión de la vulnerabilidad técnica	30%	

12.6.1 Gestión de las vulnerabilidades técnicas	10%	
12.6.2 Restricción en la instalación de software	50%	
12.7 Consideraciones sobre la auditoria de sistemas de información	0%	
12.7.1 Controles de auditoria de sistemas de información	0%	
13. Seguridad de las comunicaciones	**39,1%**	**L1**
13.1 Gestión de la seguridad de las redes	63,3%	
13.1.1 Controles de red	50%	
13.1.2 Seguridad de los servicios de red	50%	
13.1.3 Segregación en redes	90%	
13.2 Intercambio de información	15%	
13.2.1 Políticas y procedimientos de intercambio de información	0%	
13.2.2 Acuerdos de intercambio de información	0%	
13.2.3 Mensajería electrónica	50%	
13.2.4 Acuerdos de confidencialidad o no revelación	10%	
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**35,5%**	**L1**
14.1 Requisitos de seguridad en los sistemas de información	33,3%	
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	0%	
14.1.2 Asegurar los servicios de aplicaciones en redes públicas	50%	
14.1.3 Protección de las transacciones de servicios de aplicaciones	50%	
14.2 Seguridad en el desarrollo y en los procesos de soporte	23,3%	
14.2.1 Política de desarrollo seguro	50%	
14.2.2 Procedimiento de control de cambios en sistemas	10%	
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	50%	
14.2.4 Restricciones a los cambios en los paquetes de software	10%	
14.2.5 Principios de ingeniería de sistemas seguros	10%	
14.2.6 Entorno de desarrollo seguro	50%	
14.2.7 Externalización del desarrollo de software	10%	
14.2.8 Pruebas funcionales de seguridad de sistemas	10%	
14.2.9 Pruebas de aceptación de sistemas	10%	
14.3 Datos de prueba	50%	
14.3.1 Protección de los datos de prueba	50%	
15. Relación con proveedores	**45%**	**L1**
15.1 Seguridad en las relaciones con proveedores	50%	
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	50%	

15.1.2 Requisitos de seguridad en contratos con terceros	50%	
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	50%	
15.2 Gestión de la provisión de servicios del proveedor	40%	
15.2.1 Control y revisión de la provisión de servicios del proveedor	30%	
15.2.2 Gestión de cambios en la provisión del servicio del proveedor	50%	
16. Gestión de incidentes de seguridad de la información	**11,4%**	**L1**
16.1 Gestión de incidentes de seguridad de la información y mejoras	11,4%	
16.1.1 Responsabilidades y procedimientos	10%	
16.1.2 Notificación de los eventos de seguridad de la información	10%	
16.1.3 Notificación de puntos débiles de la seguridad	50%	
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	0%	
16.1.5 Respuesta a incidentes de seguridad de la información	10%	
16.1.6 Aprendizaje de los incidentes de seguridad de la información	0%	
16.1.7 Recopilación de evidencias	0%	
17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	**20%**	**L1**
17.1 Continuidad de la seguridad de la información	10%	
17.1.1 Planificación de la continuidad de la seguridad de la información	10%	
17.1.2 Implementar la continuidad de la seguridad de la información	10%	
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	10%	
17.2 Redundancias	50%	
17.2.1 Disponibilidad de los recursos de tratamiento de la información	50%	
18. Cumplimiento	**9%**	**L1**
18.1 Cumplimiento de los requisitos legales y contractuales	18%	
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	10%	
18.1.2 Derechos de propiedad intelectual (DPI)	10%	
18.1.3 Protección de los registros de la organización	10%	
18.1.4 Protección y privacidad de la información de carácter personal	50%	
18.1.5 Regulación de los controles criptográficos	10%	
18.2 Revisiones de la seguridad de la información	0%	
18.2.1 Revisión independiente de la seguridad de la información	0%	

18.2.2 Cumplimiento de las políticas y normas de seguridad	0%	
18.2.3 Comprobación del cumplimiento técnico	0%	

1.3.3 Presentación de resultados

Como resultados se obtiene un análisis del nivel de madurez porcentual de los diferentes controles en el estado actual de la ISP que se muestran en la ilustración 3.

Ilustración 3 CMM de los controles ISO actuales en la ISP

En la tabla 5 se presentan los resultados de los 114 controles analizados y se puede observar que no hay ninguno de estos en los niveles altos de Gestionado u Optimizado, y sólo un 5,26% se encuentra Definido. El mayor porcentaje de los controles se encuentran en los reproducibles pero intuitivo que se basan en la experiencia y al método de cada persona, en definitiva, depende de la competencia del individuo que ejecuta el proceso y no muy lejano se encuentran los controles en un estado inicial, donde no hay formalización de procedimientos y solo se depende del esfuerzo individual.

Tabla 5 Resultados CMM de los controles

Porcentaje	Significado
24,56%	Inexistente
30,70%	Inicial
39,48%	Reproducible pero intuitivo
5,26%	Definido

A continuación, se hará una breve descripción del estado de cumplimiento actual de la ISP relacionado a cada uno de los controles en los cuales se ha descrito en la tabla anterior tener un porcentaje mínimo de cumplimiento. Para aquellos controles que se marcaron como 0% se entenderán como carencia

completa de cualquier proceso reconocido ya que no se ha reconocido que exista ningún problema a resolver.

Dominio Organización de la seguridad de la información:

6.1.1 Roles y responsabilidades en seguridad de la información: Aunque no se ha determinado formalmente el cargo del responsable de la seguridad de la información, el gerente técnico es la persona delegada por el gerente general para encargarse de supervisar el buen uso de los activos por parte de los empleados de la empresa.

6.2.2 Teletrabajo: Debido a la situación actual de la pandemia por el COVID-19 la empresa se vio forzada a realizar teletrabajo para las áreas administrativas, todo el personal realiza procesos similares al conectarse desde la casa, pero aún no hay un procedimiento establecido ni documentado que indique una política de seguridad del lugar del entorno, únicamente se ha entregado computadores de escritorio con antivirus y con restricciones de acceso a páginas que no son competencia del giro de negocio de la organización.

Dominio Seguridad relativa a los recursos humanos

7.1.1 Investigación de antecedentes: Antes de realizar de contratación, se hace una investigación previa de los candidatos con el fin seleccionar un grupo de personas que cumplan con el perfil solicitado. Luego se realiza una entrevista directamente con el gerente técnico, quien evalúa a través de una prueba escrita los conocimientos teóricos respectos a redes y telecomunicaciones. Una vez aprobado este paso, la asistente administrativa es la encargada de corroborar las experiencias laborales, así como la verificación de los estudios realizados, por ejemplo, la verificación del título de grado de Ingeniería a través de la página del SENECYT donde se comprueba el registro del título. Finalmente, al tener la o las personas seleccionadas, se realizan las comprobaciones respectivas del récord policial en el caso de ciudadanos ecuatorianos o de los antecedentes penales en el caso de ser extranjeros. El mismo procedimiento se lleva a cabo para los puestos administrativos con la diferencia de que el proceso se realiza con el gerente general.

7.1.2 Términos y condiciones del empleo: Únicamente se informa de manera verbal los activos de los que será responsable, este es el caso de un computador, y para el caso de la parte técnica el acceso a los materiales de instalación.

Dominio Gestión de activos

8.1.1 Inventario de activos: Existe un inventario de los activos de la empresa en el computador del gerente técnico, sin embargo, ningún activo está marcado con alguna etiqueta que lo identifique. Tampoco tiene formalmente asignado un propietario, solo está implícito los equipos a los que cada persona tiene acceso

y en el caso de los ordenadores, se tiene una clave de acceso para que solo pueda ser utilizado el equipo a quien se le designó.

8.1.3 Uso aceptable de los activos: se tiene conocimiento de lo que se puede o no hacer con los activos, simplemente con lo que cada persona considera correcto hacer.

8.1.4 Devolución de activos: Se tiene conciencia del procedimiento que se debe realizar al salir de la empresa, aunque no es formal a través de un documento, cada empleado sabe que debe devolver todo en buen estado ya que de no ser así se verá afectada su liquidación al finalizar el contrato.

8.3.2 Eliminación de soportes: Solo se tiene conocimiento de que se debe realizar este proceso, aunque hasta la fecha no ha sido necesario eliminar ningún soporte.

8.3.3 Soportes físicos en tránsito: Se tiene un mensajero en la empresa exclusivo para transportar de manera segura en cualquiera de las 3 camionetas de la empresa que esté disponible en el momento que se requiera hacer un envío, así como de ir a retirar los paquetes.

Dominio Control de acceso

9.1.2 Acceso a las redes y a los servicios de red: Se tienen reglas de acceso solo en los ordenadores de la empresa, con restricción de acceso a la red en dispositivos móviles. El gerente técnico quien también realiza el papel de jefe técnico debido al pequeño tamaño de la empresa es el encargado de administrar la red y configurarla con las restricciones de acceso a solo el personal autorizado.

9.2.1 Registro y baja de usuario: se asignan identificadores a cada usuario.

9.2.2 Provisión de acceso de usuario: se adaptan identificadores a los empleados, y en cuanto finalizan la relación con la empresa son eliminados y asignados nuevos identificadores al personal que ingresa.

9.2.3 Gestión de privilegios de acceso: Aunque no hay una política de acceso si se asigna derechos a las bases de datos solo al personal que lo requiere, en este caso solo el personal técnico y la persona encargada de servicio al cliente quien es la encargada de canalizar los nuevos ingresos o los inconvenientes que surgen.

9.2.4 Gestión de la información secreta de autenticación de los usuarios: se firma un compromiso de confidencialidad en la información secreta.

9.2.6 Retirada o reasignación de los derechos de acceso: No está establecida la política a seguir y no se revisa de forma periódica si ha habido cambios en los puestos que ocupan los empleados, por lo que lo que algunos empleados aún mantienen permisos de roles anteriores. Sin embargo, para quienes

finalizan contrato si se les retira inmediatamente cualquier acceso al que tenía derecho.

9.4.1 Restricción del acceso a la información: Los empleados tiene control de acceso a todo lo relacionado a la información lógica sin embargo los datos físicos, aunque no deberían si están al alcance de todos los empleados ya que no hay seguridad física con respecto a los documentos.

9.4.2 Procedimientos seguros de inicio de sesión: Se tiene un inicio de sesión seguro para cada empleado. Solo acceden a los ordenadores el personal autorizado y al introducir la contraseña no se tiene la opción de poder ver lo que se ingresa sino solo el caracter especial (*) por cada caracter de la contraseña.

9.4.3 Sistema de gestión de contraseñas: El sistema obliga a introducir contraseñas seguras con extensión de 8 caracteres entre números letras mayúsculas y minúsculas y caracteres especiales.

9.4.4 Uso de utilidades con privilegios del sistema: Se registra el uso de antivirus.

9.4.5 Control de acceso al código fuente de los programas: solo tiene acceso y control el gerente técnico, todas las librerías de programas se gestionan por la misma persona quien es la única autorizada.

Dominio Criptografía

10.1.1 Política de uso de los controles criptográficos: No hay una política definida y solo existe el conocimiento en algunos de los técnicos con respecto a aplicaciones criptográficas, pero no las aplican.

10.1.2 Gestión de claves: no se tiene control sobre la información que algún empleado cifrara a través de una clave, aunque esto solo depende del conocimiento que tuviera el empleado.

Dominio Seguridad física y entorno

11.1.1 Perímetro de seguridad física: Las oficinas se encuentran adaptadas en una casa de dos pisos, en el primer piso se encuentra el área técnica junto a la bodega y en el segundo piso tres oficinas, la primera oficina es la de gerencia general, la segunda oficina en la que está el asistente administrativo junto al contador y la persona de servicio al cliente, y en la tercera oficina el gerente de ventas junto a los dos comerciales. La casa solo cuenta con una alarma sencilla con sensores de movimiento que se activa en el caso de detectar movimiento una vez se activa. Además, se encuentra instalado un sensor biométrico de huella digital para el ingreso de los empleados, pero se encuentra en el segundo piso, fuera de las oficinas.

11.1.2 Controles físicos de entrada: Al ser una casa adaptada a oficinas no tiene áreas seguras protegidas, únicamente en la entrada que pasa cerrada la

puerta y solo la abre la persona que está en la bodega o la persona de servicio al cliente que pude ver desde la ventana de oficina. Pero no tiene cámaras ni internas si externas para tener una mejor percepción de quien ingresa.

11.1.3 Seguridad de oficinas, despachos y recursos: La única seguridad física que aplica la empresa es tener una bodega externa en la casa del gerente, la misma persona que es dueño de la empresa, donde se archivan todos los documentos de contabilidad pasado 1 año. Los archivos físicos de las órdenes de trabajo se encuentran en las mismas instalaciones acomodados en un archivador que se encuentra bajo llave en la misma oficina del gerente.

11.1.4 Protección contra las amenazas externas y ambientales: Se tienen instalado reguladores de voltaje que protegen todas las conexiones de las oficinas. Además, procedimientos no formales de cómo realizar las instalaciones de los equipos y los u archivo digital de los manuales técnicos de algunos equipos.

11.1.5 El trabajo en áreas seguras: Existe un área, en la planta baja de las oficinas, destinada para el área técnica, sin embargo, no está cerrada ni están prohibidos los equipos móviles que contienen cámara para realizar grabación o fotografías de los equipos o del lugar de trabajo.

11.1.6 Áreas de carga y descarga: Existe un área de carga y descarga, pero no tiene ninguna restricción de acceso. se dispone de una bitácora en el cual se registra la salida y entrada de las 3 camionetas a la zona de carga además se registra el kilometraje después de cada uso.

11.2.1 Emplazamiento y protección de equipos: Todos los ordenadores están ubicados en cubículos evitando así que la información se pueda ver por personas no autorizadas.

11.2.2 Instalaciones de suministro: Los equipos cuentan con reguladores de voltajes para los cortes de energía inesperados.

11.2.3 Seguridad del cableado: Los cables de energía están separados de los que corresponden a telecomunicaciones.

11.2.4 Mantenimiento de los equipos: El personal del área técnica es el único autorizado a da mantenimiento a los equipos o de resolver algún inconveniente que se presente en los ordenadores administrativos.

11.2.5 Retirada de materiales propiedad de la empresa: Todos los empleados disponen del procedimiento que se debe realizar para poder sacar algún equipo de la empresa, con previa autorización escrita, la cual se debe llenar en un formato que ya está establecido por la organización en el cual se especifica el tiempo que estará fuera de las instalaciones.

11.2.6 Seguridad de los equipos fuera de las instalaciones: Los equipos que salen de las oficinas tienen autorización de salida siempre y cuando esté disponible alguna de las camionetas que garantice la seguridad en el

transporte, además solo pueden ser llevados a sitios cerrados y se llena un registro con las fechas de salida y regreso de cada equipo.

11.2.7 Reutilización o eliminación segura de equipos: El personal técnico está encargado de realizar las comprobaciones en los equipos antes de retirarlos, sin embargo, hay desconocimiento con respecto a cualquier proceso de cifrado.

11.2.8 Equipo de usuario desatendido: los usuarios administrativos solo conocen, por su propia experiencia, como cerrar las sesiones, pero no tienen conocimiento de salidas de las aplicaciones.

11.2.9 Política de puesto de trabajo despejado y pantalla limpia: el área técnica se deja despejada al finalizar la jornada laboral diaria, y se tiene conciencia de dejar todo apagado y desconectado cada día.

Dominio Seguridad de las operaciones

12.1.1 Documentación de procedimientos de operación: no se tiene nada documentado, pero si se realiza el mismo proceso en la mitad de las áreas de trabajo, es decir solo en el área técnica se sabe lo que debe hacerse al momento d presentarse algún menaje en las computadoras, y ene l área administrativa que no tiene ese conocimiento conocen que deben llamar al área técnica en caso de ocurrir cualquier problema. Se tiene en una agenda física los contactos de personal externo, como los técnicos que realizan el mantenimiento preventivo y correctivo de los dispositivos de impresión, en caso de necesitarse.

12.1.2 Gestión de cambios: Se tiene un registro para los cambios que surjan, que no se llena con la debida rigurosidad que requiere.

12.1.3 Gestión de capacidades: El gerente técnico realiza una proyección al inicio del año de lo que se requerirá trimestralmente, con la posibilidad de ir modificando en el trascurso del tiempo si lo requieren los equipos.

12.1.4 Separación de los recursos de desarrollo, prueba y operación: La red está segregada, además las pruebas son realizadas en equipos por separado.

12.2.1 Controles contra el código malicioso: Todos los equipos están con el antivirus Norton instalado y el jefe técnico ha realizado dos capacitaciones creado conciencia para no ingresar a páginas sospechosas ni abrir correos de fuentes dudosas. Además, él se mantiene informado revisando información en internet de nuevo códigos maliciosos.

12.3.1 Copias de seguridad de la información: Cada persona realiza sus copias de seguridad usando el correo o el drive como soporte de información y solo en algunas ocasiones, cuando la información es considerada muy importante.

12.4.1 Registro de eventos: Solo se tiene el formato del documento, pero no se le da la importancia por lo tanto está vacío.

12.4.2 Protección de la información del registro: Al tener claves de acceso a los recursos se evita modificaciones en los ficheros.

12.4.3 Registros de administración y operación: El jefe técnico delega a una persona en lapsos de 6 meses para que revise todos los sistemas de la organización.

12.5.1 Instalación del software en explotación: El jefe técnico es el único autorizado para realizar el manejo de instalación y mantenimiento del software que adquiere la ISP, pero se mantiene guardado las versiones anteriores en caso de ser necesarias.

12.6.1 Gestión de las vulnerabilidades técnicas: Solo se tiene el conocimiento de las vulnerabilidades y no de manera frecuente, solo cuando el personal técnico consulta en ultimas noticias.

12.6.2 Restricción en la instalación de software: Se tienen los privilegios respecto a la instalación de software con claves de restricción en los equipos para que solo el personal técnico sea quien realice las instalaciones.

Dominio Seguridad de las comunicaciones

13.1.1 Controles de red: La responsabilidad de la gestión de los equipos de la red es del jefe técnico. Los sistemas de la red están autenticados y la conexión es restringida.

13.1.3 Segregación en redes: Toda la empresa se encuentra informada y capacitada del funcionamiento de la segregación de la red. Se encuentra segregada en 3 VLan, una para cada área: administrativa, técnica y de ventas.

13.2.3 Mensajería electrónica: Cada empleado cuenta con un correo empresarial por medio del cual es informado de cualquier dato relevante de la empresa además de servir como medio de comunicación con clientes o proveedores según sea el cargo que ocupa.

13.2.4 Acuerdos de confidencialidad o no revelación: Al formalizar el contrato de dependencia con la empresa también se firma un acuerdo de confidencialidad.

Dominio Adquisición, desarrollo y mantenimiento de los sistemas de información

14.1.2 Asegurar los servicios de aplicaciones en redes públicas: Se tienen niveles de confianza mediante autenticación y se dispone de selección de pagos seguros.

14.1.3 Protección de las transacciones de servicios de aplicaciones: El gerente cuenta con firma electrónica, y disponen de protocolos de seguridad para la comunicación

14.2.2 Procedimiento de control de cambios en sistemas: Se informa a las personas correspondientes cuando se realiza un cambio.

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo: Se tiene planificado los cambios en los sistemas operativos teniendo en cuenta el tiempo que requerirá las pruebas antes de regresar al trabajo normal.

14.2.4 Restricciones a los cambios en los paquetes de software: No se tiene control sobre las modificaciones del software

14.2.5 Principios de ingeniería de sistemas seguros: Se tiene conocimiento de que debería diseñarse la seguridad en todas las capas de la arquitectura, pero no se realiza nada respecto a este control.

14.2.6 Entorno de desarrollo seguro: Se tiene la confianza en el personal que trabaja para la empresa por el tiempo que llevan laborando además por las recomendaciones y el currículo con el que se aceptaron. Los diferentes entornos de trabajo están segregados garantizando seguridad.

14.2.7 Externalización del desarrollo de software 14.2.8 Pruebas funcionales de seguridad de sistemas y 14.2.9 Pruebas de aceptación de sistemas: Se supervisa el software externo y se realizan pruebas exhaustivas en los sistemas nuevos.

Dominio Relación con proveedores

15.1.1 Política de seguridad de la información en las relaciones con los proveedores: Existe un procedimiento para la gestión con los proveedores con las obligaciones que deben cumplir cada una de las partes.

15.1.2 Requisitos de seguridad en contratos con terceros: Se tiene un procedimiento con los acuerdos y obligaciones respecto a la seguridad de la información que se firma con los proveedores antes de entablar la relación laboral.

15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones: Dentro del acuerdo con los proveedores está especificado que las fuentes de donde se adquiere cualquier componente o los mismos equipos deben asegurar que todas las terceras partes también cumplan con las prácticas de seguridad. Se especifica que debe garantizar la calidad en los servicios prestados con el fin de prevenir futuros incidentes.

15.2.1 Control y revisión de la provisión de servicios del proveedor se conoce y se revisa el servicio de los proveedores, sin embargo, no se realiza ninguna auditoría para verificar la provisión de los servicios, aunque si se tiene conocimiento de quien provee a los proveedores.

15.2.2 Gestión de cambios en la provisión del servicio del proveedor: se especifican acuerdos con los proveedores en los que si se realizan cambios

deben ser a favor de la ISP y pueden estar dentro de cambios como nuevas aplicaciones o herramientas que beneficien siempre el servicio.

Dominio Gestión de incidentes de seguridad de la información

16.1.1 Responsabilidades y procedimientos. Solo se ha designado la persona responsable de la seguridad de la información, sin embargo, no hay especificado nada relacionado a los incidentes.

16.1.2 Notificación de los eventos de seguridad de la información: Se informa de manera verbal cuando ocurre algún evento que corresponde a errores humanos.

16.1.3 Notificación de puntos débiles de la seguridad: cuando se detecta se informa a través de correo, pero no se lleva un registro ordenado, los respaldos son solo los correos.

16.1.5 Respuesta a incidentes de seguridad de la información: solo se informa el evento que ocurre, pero no hay el conocimiento ni siquiera del término análisis forense por lo que se requiere capacitación al personal técnico de conceptos básicos con respecto a la seguridad de la información.

Dominio Aspectos de seguridad de la información para la gestión de la continuidad del negocio

17.1.1 Planificación de la continuidad de la seguridad de la información: No existe un documento que indique los procedimientos a seguir en caso de situaciones adversas, aunque si se ha hablado del tema en reuniones no formales y se tiene planificado empezar a realizar el estudio.

17.1.2 Implementar la continuidad de la seguridad de la información: solo se tiene conocimiento que debe haber un documento con el procedimiento a realizar, pero debe ser luego de realizar el estudio de las situaciones adversas para poder implementar los documentos.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información: Aun no se tienen descritos los controles que se deben implementar para responder ante un evento, solo el conocimiento de que es un problema el no contar con estos documentos porque no se saben la acciones que tiene que tomarse en el caso de presentase alguna emergencia.

17.2.1 Disponibilidad de los recursos de tratamiento de la información: Todos los empleados tienen sus formas redundantes de tener la información, aunque no es la mejor y tampoco asegura que un equipo funcione en lugar de otro en caso de necesitarse, aunque la información si puede obtenerse porque se encuentra en la nube.

Dominio Cumplimiento

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales: Los directivos conocen algunas leyes, pero no hay nada documentado ni informado a los empleados.

18.1.2 Derechos de propiedad intelectual (DPI): La empresa adquiere software y hardware únicamente de fuentes conocidas con garantía de que no infringen ninguna ley.

18.1.3 Protección de los registros de la organización: los registros solo están protegidos contra accesos no autorizados, pero nada está asegurado contra robos u otro tipo de destrucción.

18.1.4 Protección y privacidad de la información de carácter personal: todas las áreas conocen de la importancia de proteger los datos personales, aunque no hay la capacitación formal si se ha entregado el reglamento que rige a Europa en relación con este tema, Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. y que en Ecuador aún no hay conocimiento de este tipo de leyes y tampoco se aplican sanciones cuando se incurre en este tipo de faltas.

18.1.5 Regulación de los controles criptográficos: No se tiene el conocimiento de que leyes rigen la regulación en los controles criptográficos.

Por parte de la compañía se tiene identificada la legislación aplicable en materia de seguridad, de propiedad intelectual y protección de datos.

La empresa se ha adaptado al actual Reglamente de Protección de Datos de Carácter Personal, por lo que protege los datos de acuerdo con la normativa vigente.

1.4 Objetivos del Plan Director

- Establecer los lineamientos de seguridad de la información que garanticen los principios básicos de confidencialidad integridad y disponibilidad en la ISP.

- Evaluar y valorar los activos para proveer los servicios de internet, así como los activos para el desarrollo de las actividades en torno al giro del negocio para seleccionar los aspectos de seguridad más críticos.

- Analizar las amenazas y vulnerabilidades a las que se encuentran expuestos los activos dispuestos para el tendido de última milla y los activos dispuestos dentro de las instalaciones de la empresa con el fin de proponer un plan de gestión de riesgos.

- Determinar el impacto potencial al que estaría expuesta la empresa en caso de materializarse cualquiera de las amenazas.

- Implementar y gestionar los controles de seguridad sugeridos por la norma ISO/IEC 27002/2013 en cuanto la seguridad de la red de clientes suscriptores y de la red interna que maneja la empresa en el contexto de la información.

- Elaborar los documentos necesarios para la implementación del SGSI tales como las políticas de seguridad, las normativas de requerimientos de seguridad de red, el procedimiento para administrar la seguridad de la red interna de la ISP, instructivos de roles y responsabilidades para la gestión de implantación del sistema de gestión de seguridad de la información guiados por la norma ISO/IEC 27001.

- Reducir los tiempos de instalación del servicio para los nuevos abonados.

- Establecer un protocolo para el buen uso de los suministros en los procesos de instalación.

- Ampliar el catálogo de servicios y la zona de cobertura en toda la región norte del Ecuador.

- Reducir los tiempos de reconexión en caso de presentarse un incidente de seguridad que afecte la prestación del servicio de internet.

1.5 Enfoque y método seguido

Luego de haber realizado un estudio de la situación actual de la empresa, con respecto al cumplimiento de la norma ISO/IEC 27001:2013 y de la ISO/IEC 27002:2013, se concluye que hay muy poco o nada de conocimiento acerca de un SGSI y por lo tanto un estado deficiente con respecto a la seguridad de la información en la ISP.

El método escogido a implementar será el modelo de mejora continua del ciclo Deming el cual garantiza calidad en el proceso del SGSI al desarrollar las 4 etapas: Plan, Do, Check, Act. Se diseñará el presente plan director con el fin de implantar un SGSI alineado a los requisitos especificados en la norma 27001 e implantar controles de seguridad que permitan gestionar los 14 dominios de la guía de buenas prácticas de la norma 27002.

Respecto al análisis de riesgos se seguirá la metodología de MAGERIT, la cual guiará el procedimiento que se desarrollará en el capítulo dos, y que se implementará en el capítulo 3. Esta metodología define los criterios a la hora de valorar cada uno de los activos de la ISP, y define etiquetas para cada uno de

los ámbitos en los cuales se clasifica cada activo, así como las amenazas a considerar de acuerdo con esta misma clasificación.

1.6 Planificación del Trabajo

El trabajo se dividirá en 6 etapas, cada una de estas cumplirá con diferentes propósitos y diferentes tareas pero que una vez ejecutadas refleje el cumplimiento de los objetivos del plan director planteados en el apartado 1.4. Para una mejor percepción de las tareas a realizar en cada una de las etapas se presenta a continuación el diagrama de Gantt.

Tabla 6 Planificación TFM

TAREA	Fecha Inicio	Fecha final
ETAPA 1 SITUACIÓN ACTUAL DE LA ISP	16/09/2020	02/10/2020
Selección de la empresa	18/09/2020	19/09/2020
Descripción del contexto de la empresa	20/09/2020	21/09/2020
Definición del alcance	22/09/2020	22/09/2020
Análisis Diferencial	23/09/2020	30/09/2020
Definición objetivos Plan Director	01/10/2020	01/10/2020
ETAPA 2 GESTION DOCUMENTAL	03/10/2020	16/10/2020
Elaboración de la política de Seguridad	03/10/2020	04/10/2020
Procedimiento de Auditoría interna	05/10/2020	06/10/2020
Elaboración de la Gestión de indicadores	09/10/2020	04/10/2020
Procedimiento Revisión de la dirección	11/10/2020	11/10/2020
Gestión de roles y responsabilidades	12/10/2020	13/10/2020
Metodología de Análisis de riesgos	13/10/2020	15/10/2020
Declaración de aplicabilidad	15/10/2020	16/10/2020
ETAPA 3 ANÁLISIS DE RIESGO	17/10/2020	06/11/2020
Identificación, clasificación de activos	18/10/2020	24/10/2020
Valoración de los activos	25/10/2020	26/10/2020
Identificación de amenazas por cada dimensión de seguridad	27/10/2020	02/11/2020
Cálculo de impacto potencial	03/11/2020	04/11/2020
Cálculo de nivel de riesgo	05/11/2020	06/11/2020
ETAPA 4 PROPUESTAS DE PROYECTOS	07/11/2020	26/11/2020
Propuesta de proyectos con análisis de costes	07/11/2020	18/11/2020
Estimación del nivel de riesgo residual	20/11/2020	22/11/2020
Comparación entre impacto potencial y riesgo residual	23/11/2020	26/11/2020
ETAPA 5 AUDITORIA DE CUMPLIMIENTO	27/11/2020	11/12/2020
Evaluación de los apartados de la norma 27001	27/11/2020	28/11/2020
Evaluación de los 114 controles de la norma 27002	29/11/2020	06/12/2020
Análisis de resultados del nivel de madurez	07/12/2020	09/12/2020
Informe de auditoria	10/12/2020	11/12/2020

ETAPA 6 PRESENTACIÓN DE RESULTADOS	12/12/2020	28/12/2020
Conclusiones y Revisión memoria del TFM	12/12/2020	15/12/2020
Presentación ante la alta dirección	16/12/2020	20/12/2020
Presentación Análisis de Riesgos	21/12/2020	24/12/2020
Elaboración de video explicativo	25/12/2020	28/12/2020

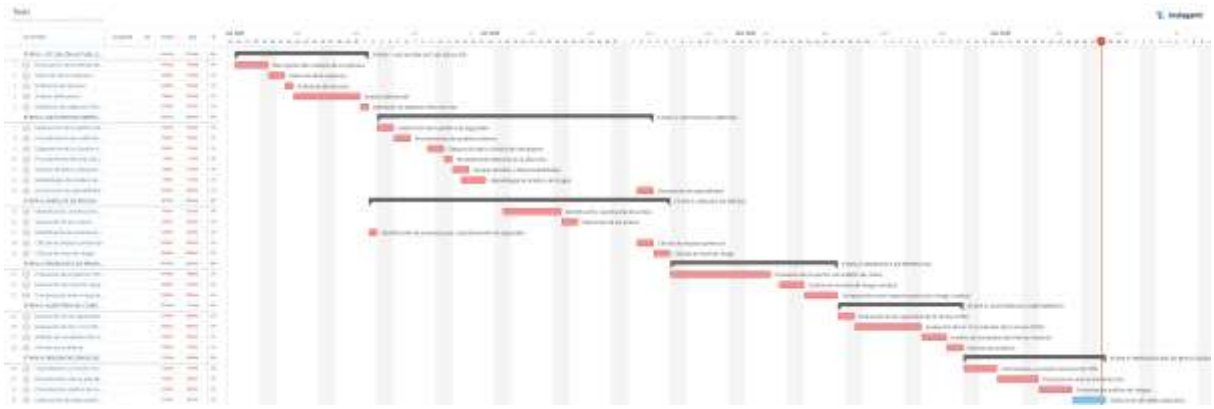

Ilustración 4 diagrama de Gantt

1.7 Breve descripción de los capítulos de la memoria

En el capítulo 1 se definió la empresa a la cual se realizará el plan director para implementar el SGSI. Se definió el alcance, los objetivos y un análisis actual de la ISP con respecto a cada uno de los requerimientos de la norma ISO/IEC 27001/2013 y con respecto a cada uno de los 114 controles de la guía de buenas prácticas ISO/IEC 27002/2013. En el capítulo 2 se desarrollará los documentos necesarios tales como normativas, procedimientos, políticas y metodologías necesarias para la ejecución del plan director. En el capítulo 3 tendremos un análisis de riesgos completo de los activos de la ISP, en el cual se valorará cada activo desde cada una de las 5 dimensiones de seguridad con las respectivas amenazas, el impacto potencial que representaría la materialización de cualquiera de ellas y el nivel de riesgo que determinará el plan de acción de la siguiente etapa. En el capítulo 4 se plantearán diferentes proyectos que permitan llevar a un nivel de cumplimiento óptimo, cada uno de los 114 controles analizados en la primera etapa. Además, se presentarán los resultados gráficamente de tal forma que se pueda apreciar el impacto potencial y una estimación del nivel de riesgo una vez se implementen los proyectos. En el capítulo 5 se aplicará la metodología de auditoría interna elaborada en el capítulo dos, con el fin de revisar el cumplimiento de cada uno de los dominios una vez implementados los proyectos. En el capítulo 6 se presentarán los resultados desarrollados a lo largo de todo el proyecto, los cuales serán a) Una presentación para la alta dirección de la ISP, b) Una presentación del análisis de riesgos y un video con la explicación de lo desarrollado a lo largo de todo el proyecto.

2. Documentación del Sistema de Gestión de Seguridad de la Información

El desarrollo de un marco normativo nos permite respaldar el sistema de gestión implementado, además de que forma parte de los requerimientos principales establecidos por la norma ISOIEC 27001 para la certificación. Todos los documentos normativos, o también llamados estándar, deben tener un lineamiento común de seguridad para que toda la empresa la aplique en su trabajo diario y deben contar con la revisión y aprobación de la dirección. Para este proyecto de implantación nos apoyaremos en la Pirámide jerárquica de documentos, estableciendo tanto políticas con directrices más generales, así como procedimientos con información más específica y detallada. Sin embargo, todos los documentos, independientemente de la posición jerárquica que ocupen, compartirán un mismo formato el cual incluirá: a) El tipo de información que contiene el documento; b) Nivel de obligatoriedad en el cumplimiento; c) Responsable en aprobar el documento y d) personal a quien debe hacerse conocer el contenido del documento.

Nos centraremos en la realización de 7 documentos, procedimientos, metodologías, política de seguridad y documentos de gestión, sin embargo, en los 7 documentos se manejará una misma plantilla con el fin de alinear todos los documentos no solo los actuales sino también los procedimientos o normas que se desarrollan en un futuro. Nuestra plantilla contendrá lo siguiente:

1. Encabezado: Estará compuesto por un cuadro con el logo de la empresa (en este caso no se pondrá por reserva del nombre de la empresa) pero para fines del proyecto nos referiremos con el nombre de ISP, se incluirá el tipo de documento, número de página y número total de páginas, número de versión que para este caso será la primera, y la fecha de emisión. Deberá ir en cada hoja de todo el documento.

2. Un cuadro de registro con fechas de elaboración, revisión, aprobación y firmas de los responsables con nombre y cargo dentro de la empresa.

3. Histórico del documento, que será un cuadro de control de las actualizaciones con fecha y cambio realizado.

4. Contenido, donde se mostrará el nombre de cada uno de los elementos incluidos y la página respectiva de su ubicación en el documento.

5. Introducción donde se resalte la importancia del estándar que se realizará.

6. Objetivo, es decir la finalidad del documento.

7. Alcance con el ámbito de aplicación, a quien está dirigido el documento.

8. Cumplimiento legal donde se nombren las normas que se tienen como guía en el desarrollo del documento

9. Descripción del documento, con las medidas de seguridad, procedimientos, normas o recomendaciones necesarias para el documento.

10. Control del cumplimiento del estándar, donde se detalle el tiempo de las revisiones. Dependiendo del tipo de documento se hará con periodos de un año como es para el caso de políticas, o en menor tiempo para los casos en que los documentos se encuentren en niveles inferiores de la pirámide jerárquica.

11. Penalizaciones en caso de no cumplimiento

12. Medios por el cual se divulga la información del documento

Partiendo de esta plantilla se proponen los documentos que se detallan en los siguientes apartados.

2.1 Política de Seguridad

En el sistema de gestión de seguridad, el documento más importante es el que define la política de seguridad de la información, que se ubica en el nivel más alto de la pirámide jerárquica. El propósito de este documento es establecer los parámetros para la seguridad de la información, de tal forma que sean consistentes con los objetivos comerciales y las políticas de regulación. En el Anexo 10.1 Política de seguridad se puede encontrar el desarrollo de la política para la ISP.

2.2 Procedimiento de Auditorías Internas

Este procedimiento determina la consistencia y efectividad del sistema de gestión de seguridad de la información de acuerdo con la planificación, preparación, ejecución y registro de estándares y lineamientos de auditoría de seguridad interna. Del informe generado durante la auditoría, se verifica si se pueden corroborar las regulaciones preestablecidas relacionadas con la norma ISO/IEC 27001 y los objetivos de la empresa. En el Anexo 10.2 Procedimiento de Auditorías Internas se puede encontrar el desarrollo del Procedimiento para la ISP.

2.3 Gestión de Indicadores

Los indicadores son parámetros generales que guían el proceso de evaluación de la eficiencia y eficacia del SGSI. La efectividad del sistema es proporcional a la efectividad de los controles implementados en la

organización, y los indicadores son el medio para obtener la información. En base a los resultados de los indicadores, es posible generar un informe del estado de la gestión de seguridad del sistema de información. En el Anexo 10.3 Gestión de Indicadores se puede encontrar el desarrollo del procedimiento para la ISP.

2.4 Procedimiento Revisión por Dirección

El Procedimiento de Revisión por Dirección permite el establecimiento de estándares y requisitos para su revisión por parte de la alta dirección para determinar si el SGSI cumple con los requisitos de la norma ISO/IEC 27001: 2013 y el marco regulatorio del caso. La dirección de la organización debe comprobar periódicamente los aspectos más importantes relacionados con el SGSI. Además, los gerentes deben ser conscientes de la conveniencia, adecuación y efectividad del sistema para que puedan realizar mejoras o cambios cuando sea necesario. En el Anexo 10.4 Procedimiento Revisión por Dirección se puede encontrar el desarrollo del Procedimiento para la ISP.

2.5 Gestión de Roles y Responsabilidades

La implementación del SGSI y los procesos definidos en él generará la necesidad de establecer roles y responsabilidades. Los cuales son necesarios para evitar riesgos de una gestión y ejecución de tareas de seguridad incorrectas. En este sentido una de las primeras tareas a realizar en la implementación del SGSI es conformar una estructura interna directamente responsable de la seguridad de la información, permitiendo la creación, mantenimiento, supervisión y mejora del sistema. Además, se debe considerar para el funcionamiento adecuado del SGSI el personal interno como externo con acceso a la información de la empresa debe conocer sus funciones y responsabilidades en materia de seguridad. En el Anexo 10.5 Gestión de Roles y Responsabilidades se puede encontrar el desarrollo del Procedimiento para la ISP.

2.6 Metodología de Análisis de Riesgos

Los SGSI implementados según la norma ISO / IEC 27001 requieren un análisis de riesgos, con el fin de obtener una perspectiva objetiva de los riesgos que enfrenta la organización. En este sentido siempre es recomendable utilizar un método que haya sido definido (ahorra tiempo y esfuerzo), reconocido (brinda confiabilidad) y probado. En el Anexo 10.6 Metodología de Análisis de Riesgos se puede encontrar el desarrollo de la metodología para la ISP.

2.7 Declaración de Aplicabilidad

La Declaración de aplicabilidad es un requisito de la norma ISO/IEC 27001: 2013, para las entidades que desean certificarse en la norma. En

el caso que no se busque la certificación no es necesario desarrollar, pero es recomendable utilizarlo como una forma de registrar y controlar las medidas de seguridad aplicadas en el sistema de gestión de seguridad de la información. Esta declaración describe todos los controles aplicables y los controles que no cumplen con los requisitos. Además, permite indicar si estas medidas están implementadas, lo que hace que este documento sea una guía de auditoría muy útil. En el Anexo 10.7 Declaración de Aplicabilidad se puede encontrar la plantilla de la declaración para la ISP.

3. Análisis de Riesgos

3.1 Introducción

La metodología que se usará para realizar tanto el análisis como la gestión de riesgos es la indicada en MAGERIT 3.0. A partir del capítulo 3 “Método de análisis de riesgos” del libro 1 se establecerán los términos y procedimiento a seguir del análisis de riesgos y posterior a esto se continuará con las pautas del “Proceso de gestión de riesgos” del mismo libro.

Se usará los criterios del capítulo dos del libro 2 MAGERIT 3.0 para realizar la clasificación de los activos y agruparlos según su tipo. Luego se definirá el valor por cada activo considerando los criterios del libro 3 MAGERIT 3.0 con una estimación cuantitativa y cualitativa. Y finamente se analizará el árbol de dependencias entre activos para identificar y valorar el grado de perjuicio que causaría sobre un activo superior la materialización de una amenaza de un activo inferior.

Para completar la valoración de los activos también se considerarán las dimensiones básicas de la seguridad de la información con el fin de definir el grado de criticidad de las 5 dimensiones: a) Disponibilidad, b) Integridad, y c) Confidencialidad, d) Autenticidad y e) Trazabilidad.

Una vez identificado cada activo con su valoración cuantitativa y su valoración de criticidad respecto a los principios básicos, procedemos a identificar las diferentes amenazas a las que están expuestos cada activo, considerando que puede haber más de una amenaza por cada uno. Se agruparán los activos según su tipo y se analizará la frecuencia con la que se produciría la amenaza, así como su impacto en las distintas dimensiones.

Antes de determinar el nivel de riesgo, y clasificarlo entre aceptable o residual, se debe realizar un análisis del impacto potencial, el cual corresponde a determinar el impacto que puede suponer la materialización de una amenaza sobre determinado activo. Cabe recalcar que el impacto que se determinará en este punto corresponde al calculado sin despliegue de salvaguardas y será muy importante para determinar las acciones necesarias a implantar, además que será parte fundamental de la evaluación de desempeño de las medidas de control al poder comparar el impacto potencial con respecto al impacto residual.

Como último paso pautado en el análisis de riesgos de la metodología de MAGERIT, se procederá a realizar la estimación del riesgo considerando el análisis del impacto potencial y el impacto residual. Basados en este análisis se podrá determinar si se asume el riesgo o se implementan medidas que ayuden a gestionarlo con el fin de reducirlo.

Es importante determinar una escala de niveles de riesgo que permitan decidir si la organización puede asumirlos, es decir aceptarlos, o si por el contrario se implementarán medidas de salvaguardas que, aunque no logren desaparecer el riesgo, sí que lo reducirá, haciendo que se encuentre en un nivel aceptable para la organización.

3.2 Inventario de activos

El primer paso en el método de análisis de riesgos de la metodología MAGERIT 3.0 es el identificar todos los activos relevantes para la organización y agruparlos en una columna utilizando los tipos que indica MAGERIT en sus buenas prácticas. Debemos diferenciar entre dos grandes tipos de activos que hacen parte de un sistema de información, estos son: 1. La información que maneja y aquellos activos considerados por los servicios que presta.

El primer grupo de activos su vez está compuesto por 3 subtipos: a) los imprescindibles que sin estos activos se vería afectada la existencia de la organización; b) los activos que se refieren a los datos personales y c) aquellos activos que están relacionados a la normativa de control de acceso y que son importantes debido a su grado de confidencialidad.

No obstante, se pueden identificar otros tipos de activos de igual importancia y en los que se centrará este inventario e identificados cada uno con una etiqueta que será utilizada en la tabla de resumen de inventarios. Esta clasificación se puede observar en la tabla 7.

Tabla 7 Clasificación de los activos

Etiqueta	Tipo de activo	Descripción
[L]	Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.
[HW]	Hardware	Materiales físicos que soportan los servicios que presta la organización. Guardan temporal o permanentemente los datos y las aplicaciones informáticas responsables del procesado o transmisión de datos.
[SW]	Software-Aplicaciones informáticas	Programas, aplicaciones que se desempeñan por un equipo informático
[D]	Datos/Información	Permiten a una organización prestar sus servicios y son almacenados en equipos o soportes de información.
[COM]	Redes de comunicación	Medios de transporte que llevan datos de un sitio a otro. Incluyen

		instalaciones como servicios de comunicaciones contratados a terceros.
[S]	Servicios	Servicios prestados por el sistema que atienden las necesidades de los usuarios.
[AUX]	Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información sin estar directamente relacionados con los datos.
[P]	Personal	Personas relacionadas con los sistemas de información.

Una vez identificados los tipos de activos según la clasificación dada por el libro de MAGERIT se describen en la siguiente tabla 8 el inventario de los activos de la ISP

Tabla 8 Inventario de los activos de la ISP

Tipo	Cantidad	Activo	Descripción
[L] Instalaciones			
[L] [site]	1	Oficina	Casa de dos pisos, primer piso para el área técnica y segundo piso para las oficinas administrativas
[HW] Hardware			
[HW][Host]	2	Servidor Correo y web, MySQL	Server Dell Poweredge R340 Intel Xeon E-2224 8gb 2tb Sata Hd Idrac9 Basic Perc H330plus
[HW] [mobile]	13	Smartphones	Celulares Huawei Y5p
[HW] [pc]	13	Portátiles	9 Lenovo flex 11 4 Dell inspirion 5567
[HW] [print]	4	Impresoras	Epson L210
[HW] [router]	1	Router	Router Linksys Cisco E900 N300 Mimo Vpn
[HW] [switch]	2	Switch	Switch Cisco Smb Sg110-24hp De 24 Puertos
[HW] [modem]	1	Modem	Huawei EchoLife HG8245H
[SW] [Software]			
[SW] [os]	13	S0 WINDOWS 10	WINDOWS 10 Home
[SW][av]	13	Antivirus	Norton
[SW] [office]	13	HerramientasOfimáticas	Office 365
[SW][os]	2	Windows 2019 Server	Windows Server 2019 Inside Out
[SW] [email_server]	1	SoftwareCorreo	ArgoSoft Mail Server 1.8.9.1 para Windows
[SW][www]	1	SoftwareWeb	Wix plataforma de

			desarrollo web basado en la nube
[SW][dbms]	1	SoftwareMySQL	MySQL Database Service
[D] Datos/Información			
[D] [int]		Datos Gerente General	Datos guardados en el computador, celular y correos.
[D] [int]		Datos de asistente administrativo	Datos guardados en el computador, celular y correos.
[D] [int]		Datos contabilidad y contratación	Datos guardados en el computador, celular y correos.
[D] [int]		Datos Gerente de ventas	Datos guardados en el computador, celular y correos.
[D] [int]		Datos de ejecutivos de ventas	Datos guardados en el computador, celular y correos.
[D] [int]		Datos de servicio al cliente	Datos guardados en el computador, celular y correos.
[D][int]		Datos Gerente Técnico	Datos guardados en el computador, celular y correos.
[D] [int]		Datos de los técnicos instaladores	Datos guardados en el computador, celular y correos.
[D] [int]		Datos mensajero	Datos guardados ene l celular y correo.
[COM] Redes de comunicación			
[COM] [Internet]	1	Línea a Internet	Contrato con Corporación Nacional de Telecomunicaciones
[COM] [LAN]	1	Red local	Red de la empresa
[S] Servicios			
[S] [email]	13	Correo electrónico de la empresa	
[S]		Protocolo para acceso a servidores	
[AUX] Equipamiento auxiliar			
[AUX] [fiber]	1	Fibra Óptica	Fibra multimodo
[P] Personal			
[P] [ui]	1	Gerente General	Ingeniero Electrónico en telecomunicaciones
[P] [ui]	1	Gerente de Ventas	Ingeniera comercial
[P] [adm]	1	Gerente Técnico	Ingeniero Electrónico en telecomunicaciones

[P] [ui]	1	Asistente administrativo	Administrador de empresas
[P] [ui]	3	Ejecutivos de ventas	Bachiller
[P] [ui]	4	Técnicos instaladores	4 técnicos superior
[P] [ui]	1	Servicio al cliente	Bachiller
[P] [ui]	1	Contador	Contador público autorizado
[P] [ui]	1	mensajero	Bachiller

3.3 Valoración de activos

A partir de la selección de los activos relevantes para la ISP, se puede continuar con la valoración de cada uno de los activos. La metodología MAGERIT, en su "Libro III nos indica un análisis mediante tablas y "dispone de una escala útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:". (públicas, 2012).

MB: muy bajo
B: bajo
M: medio
A: alto
MA: muy alto

Además de esta escala se completará con una estimación cuantitativa, con rangos que se correspondan a cada uno de los niveles sugeridos por MAGERIT. En base a los rangos establecidos en la tabla 9 se procederá a dar una valoración a cada uno de los activos detallados en el primer anterior

Tabla 9 Escala para valoración de activos

Valor	Rango económico
Muy alto (MA)	Activo > 100.000 $USD
Alto (A)	50.000 $USD < activo<100.000 $USD
Medio(M)	10.000 $USD < activo < 50.000 $USD
Bajo (B)	1000 $USD < activo < 10.000 $USD
Muy bajo (MB)	activo < 1000 $USD

Antes de asignar un valor a cada activo, se deberá considerar el árbol de jerarquización, el cual define el valor de un activo por su dependencia con activos de niveles inferiores. Su valor se verá afectado e incrementará debido al impacto que tendría la materialización de una amenaza que afectará en cadena a los activos superiores con los que se encuentre directamente relacionado.

De esta manera podemos llegar al valor del activo teniendo en cuenta el factor de dependencia, el valor del uso del activo que en definitiva sería el valor de lo que representa para la organización prescindir del recurso por hora, el valor de reponer el activo en caso de perdida y el valor de

configuración que se ve afectado por el tiempo que se demora en regresar al estado anterior de la pérdida.

Tabla 10 Valoración de cada activo

Tipo	Cantidad	Activo	Valor	Rango económico $USD
[L] Instalaciones			**B**	**3.000**
[L] [site]	1	Oficina	B	3.000
[HW] Hardware			**MA**	**27.700**
[HW][Host]	2	Servidor Correo y web, MySQL	MA	10.000
[HW] [mobile]	13	Smartphones	B	2.000
[HW] [pc]	13	Portátiles	M	13.000
[HW] [print]	4	Impresoras	MB	400
[HW] [router]	1	Router	MB	200
[HW] [switch]	2	Switch	B	2.000
[HW] [modem]	1	Modem	MB	100
[SW] [Software]			**M**	**14.600**
[SW] [os]	13	S0 WINDOWS 10	B	2.600
[SW][av]	13	Antivirus	B	2.000
[SW] [office]	13	HerramientasOfimáticas	B	2.000
[SW][os]	2	Windows 2019 Server	B	5.000
[SW] [email_server]	1	SoftwareCorreo	B	1.000
[SW][www]	1	SoftwareWeb	B	1.000
[SW][dbms]	1	SoftwareMySQL	B	1.000
[D] Datos/Información			**A**	**67.300**
[D] [int]		Datos Gerente General	B	5.000
[D] [int]		Datos de asistente administrativo	B	5.000
[D] [int]		Datos contabilidad y contratación	B	10.000
[D] [int]		Datos Gerente de ventas	B	10.000
[D] [int]		Datos de ejecutivos de ventas	B	5.000
[D] [int]		Datos de servicio al cliente	B	5.000
[D][int]		Datos Gerente Técnico	B	11.000
[D] [int]		Datos de los técnicos instaladores	B	5.000
[D] [int]		Datos mensajero	B	1300
[COM] Redes de comunicación			**B**	**4.000**

[COM] [Internet]	1	Línea a Internet	B	2.000
[COM] [LAN]	1	Red local	B	2.000
[S] Servicios			**B**	**3.000**
[S] [email]	13	Correo electrónico de la empresa	B	1.500
[S]		Protocolo para acceso a servidores	B	1.500
[AUX] Equipamiento auxiliar			**B**	**3.000**
[AUX] [fiber]	1	Fibra Óptica	B	3.000
[P] Personal			**A**	**83.000**
[P] [ui]	1	Gerente General	M	15.000
[P] [ui]	1	Gerente de Ventas	M	15.000
[P] [adm]	1	Gerente Técnico	M	15.000
[P] [ui]	1	Asistente administrativo	B	3.000
[P] [ui]	2	Ejecutivos de ventas	B	8.000
[P] [ui]	4	Técnicos instaladores	M	12.000
[P] [ui]	1	Servicio al cliente	B	3.000
[P] [ui]	1	Contador	M	10.000
[P] [ui]	1	Mensajero	B	2.000

En la tabla 11 se presentan los resultados que corresponden a cada tipo de activo, se ha puesto el resultado total de la valoración por uno, los cuales también se representan mediante gráfico de barras junto con la tabla resumen.

Tabla 11 Valoración total por tipo de activo

Tipo	Rango económico $USD	Valor
[L] Instalaciones	3000	B
[HW] Hardware	27000	MA
[SW] [Software]	14600	M
[D] Datos/Información	67300	A
[COM] Redes de comunicación	4000	B
[S] Servicios	3000	B
[AUX] Equipamiento auxiliar	3000	B
[P] Personal	83000	A

La representación de la valoración se puede observar en la ilustración 5 del diagrama de barras

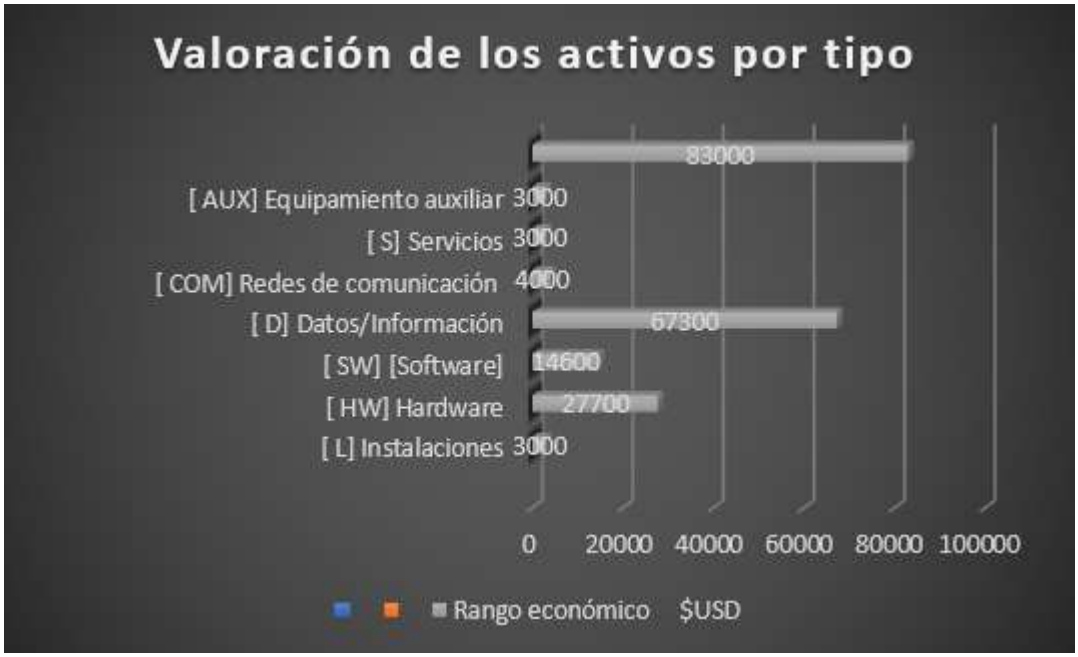

Ilustración 5 Gráfico de barras de la valoración por tipo de activo

Como puede observarse, el valor más alto corresponde al Hardware seguido del personal y los datos de información.

3.4 Dimensiones de Seguridad

Una vez realizada la valoración por cada activo tanto en un rango cualitativo como cuantitativamente en un rango económico establecido por la escala de valores, se analiza un atributo muy importante que determinará finalmente el grado de criticidad de cada activo para valorar cuales son las consecuencias de darse la materialización de una amenaza y de esta manera calificar valorar también cuantas dimensiones de seguridad se verían afectadas

Existen 5 dimensiones de seguridad cada una con una propiedad sobre los activos y etiquetada al igual que la clasificación de los activos. Las primeras 3 dimensiones son consideradas como principios básicos de seguridad, y las últimas dos un complemento que permiten completar las 3 primeras. A continuación, se presenta el concepto de cada una de estas dimensiones haciendo hincapié en la propiedad que representa sobre cada activo

1. Disponibilidad [D]: Característica de los activos para poder ser accedidos a ellos en el cualquier momento de ser necesitado.

2. Integridad [I]: Característica de los activos que determina la seguridad de que no ha sido alterado o modificado por personal no autorizado.

3. Confidencialidad [C]: Característica de los activos que asegura que la información que contiene solo es conocida por el personal autorizado.

4. Autenticidad [A]: Característica de los activos en la que se determina que el personal que accede a la información está autorizado y es quien dice ser.

5. Trazabilidad [T]: Característica de los activos en la que se puede obtener un registro de las acciones sobre cada activo, así como el registro de quienes realizaron dichas acciones.

A partir de la escala dividida en 5 niveles de la tabla 8, se estimará el nivel de daño que podría causar el verse afectada alguna de las dimensiones de seguridad, tanto cuantitativamente como cualitativamente. Además, se representará el valor de cada activo de acuerdo con la importancia en el desarrollo del giro del negocio de la ISP como se puede observar en la tabla 12.

Tabla 12 Valores de criticidad en las dimensiones de seguridad

Valor dimensión	Criterio
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Daño irrelevante a la organización

En la tabla 13 se especifican los niveles de importancia de cada activo.

Tabla 13 Escala de grado de importancia del activo

Importancia del activo	Descripción
(MA)	Muy alta
(A)	Alta
(M)	Media
(B)	Baja
(MB)	Despreciable

Se considerará el criterio de perjuicio a partir de ciertas condiciones como se describirán a continuación en la tabla 14.

Tabla 14 Valoración de criticidad de las dimensiones de seguridad

Criterio	Descripción
Daño muy grave	Interrupción de las actividades para el buen funcionamiento de la organización, con daños irreparables en los activos, afectar a quien ejecuta los procesos de manera irreparable
Daño grave	Interrupción de las actividades para el buen funcionamiento de la organización, sin que conlleve a daños irreparables, con daños graves en los activos difícil de repararlos en un corto tiempo afectando a quien ejecuta los procesos de manera grave.
Daño importante	Interrupciones parciales de las actividades que

	ralenticen su correcto funcionamiento en la organización, con daños importantes en los activos y con cierto grado de complejidad en su reparación que requiera un poco de tiempo y afecte de manera no tan grave a quien ejecuta los procesos
Daño menor	Interrupciones cortas que produzcan un bajo decremento en el correcto funcionamiento de las actividades de la organización, con daños leves en los activos y facilidad en su recuperación. En su reparación requiere un poco de tiempo y afecta de manera no tan grave a quien ejecuta los procesos.
Daño irrelevante	Breve interrupción, sin importancia en el correcto funcionamiento de las actividades de la organización, sin afectar a los activos ni a quien ejecuta los procesos.

3.5. Tabla resumen de valoración

En este apartado se presentará la valoración de cada activo y la criticidad de las 5 dimensiones de seguridad que afectaría a cada uno de los activos de la ISP basado en la escala de valoración del activo de la tabla 13 y la valoración de criticidad de las dimensiones de seguridad de la tabla 12. Esto nos permitirá priorizar acciones sobre aquellos activos que representen un valor alto y muy alto, ya que al verse afectada las dimensiones de estos activos representaría un daño muy grave para el correcto funcionamiento de las funciones de la ISP.

Tabla 15 Valoración de activos con criticidad en las dimensiones

			Criticidad en las dimensiones				
Tipo	**Activo**	**Valor**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[L] Instalaciones							
[L] [site]	Oficina	BAJA	2	6	2	2	2
[HW] Hardware							
[HW] [Host]	Servidor Correo y web, MySQL	MUY ALTA	9	10	10	10	9
[HW] [mobile]	Smartphones	MEDIA	5	5	5	5	5
[HW] [pc]	Portátiles	MEDIA	5	5	5	5	5
[HW] [print]	Impresoras	DESPRECIABLE	0	0	1	1	0
[HW] [router]	Router	ALTA	9	9	8	10	1
[HW] [switch]	Switch	ALTA	9	9	8	10	1
[HW] [modem]	Modem	ALTA	7	9	7	9	1
[SW] [Software]							
[SW] [os]	S0 WINDOWS 10	MEDIA	3	5	5	9	0
[SW][av]	Antivirus	MEDIA	3	4	5	9	0
[SW] [office]	HerramientasOfimáticas	DESPRECIABLE	0	0	0	3	0

[SW][os]	Windows 2019 Server	MUY ALTA	9	9	8	10	9
[SW] [email_server]	SoftwareCorreo	MEDIA	8	8	8	6	4
[SW][www]	SoftwareWeb	ALTA	10	8	10	10	8
[SW][dbms]	SoftwareMySQL	ALTA	5	10	10	10	5
[D] Datos/Información							
[D] [int]	Datos Gerente General	MUY ALTA	9	9	10	10	10
[D] [int]	Datos de asistente administrativo	MEDIA	6	6	7	7	8
[D] [int]	Datos contabilidad y contratación	MUY ALTA	10	8	10	10	9
[D] [int]	Datos Gerente de ventas	MEDIA	7	7	6	7	7
[D] [int]	Datos de ejecutivos de ventas	MEDIA	6	6	6	7	6
[D] [int]	Datos de servicio al cliente	MUY ALTA	9	8	10	9	9
[D][int]	Datos Gerente Técnico	MUY ALTA	9	9	10	8	10
[D] [int]	Datos de los técnicos instaladores	MEDIA	7	7	7	9	7
[D] [int]	Datos mensajero	BAJA	1	1	2	3	3
[COM] Redes de comunicación							
[COM] [Internet]	Línea a Internet	MEDIA	2	6	5	5	4
[COM] [LAN]	Red local	MEDIA	3	7	5	6	5
[S] Servicios							
[S] [email]	Correo electrónico de la empresa	MEDIA	6	9	2	3	2
[S]	Protocolo para acceso a servidores	MEDIA	8	7	8	5	3
[AUX] Equipamiento auxiliar							
[AUX] [fiber]	Fibra Óptica	MEDIA	0	0	9	9	0
[P] Personal							
[P] [ui]	Gerente General	MUY ALTA	10	10	9	8	8
[P] [ui]	Gerente de Ventas	MUY ALTA	10	9	8	7	8
[P] [adm]	Gerente Técnico	MUY ALTA	10	10	9	10	8
[P] [ui]	Asistente administrativo	MEDIA	5	9	9	9	6
[P] [ui]	Ejecutivos de ventas	MEDIA	5	6	8	6	6
[P] [ui]	Técnicos instaladores	ALTA	8	7	8	9	6
[P] [ui]	Servicio al cliente	MEDIA	7	6	8	9	6
[P] [ui]	Contador	ALTA	10	9	8	7	6
[P] [ui]	mensajero	BAJA	1	3	8	2	3

3.6. Análisis de amenazas

Según la clasificación de MAGERIT en su libro 2, las amenazas pueden clasificarse en 4 grandes grupos. Al igual que la clasificación de los activos están etiquetadas y compuestas cada una por subcategorías. Dentro de la descripción de cada una de las amenazas, se especifica a qué tipo de activos afectaría y en que dimensión de seguridad se encuentra su criticidad, además de una pequeña descripción de la

amenaza y el origen que podría causarla. En la siguiente tabla 16 se resumen los 4 grandes grupos de amenazas con la cantidad de subcategorías y etiquetas dadas por MAGERIT:

Tabla 16 Clasificación Amenazas MAGERIT

Tipo de amenaza	Subcategorías	
	Cantidad	Intervalo de subcategorías
Desastres naturales [N]	3	Desde [N1] a [N. *]
De origen industrial [I]	12	Desde [I1] a [I.11]
Errores y fallos no intencionados [E]	18	Desde [E1] a [I.28]
Ataques intencionados [A]	24	Desde [E1] a [I.28]

Es importante reconocer que no todas las amenazas afectan a todos los activos, tal y como se indicó anteriormente, cada amenaza describe al tipo de activo que afectaría. Así mismo se analizará la frecuencia con la que podría presentarse la amenaza, para lo cual se contará con la siguiente escala de frecuencias indicada en la tabla 17:

Tabla 17 Escala de frecuencia de materialización de una amenaza

	Frecuencia	Valor
Muy alto	1 vez al día	**5**
Alto	1 vez cada dos semanas	**4**
Normal	1 vez cada dos meses	**3**
Bajo	1 cada 6 meses	**2**
Muy bajo	1 vez al año	**1**
Extremadamente bajo	**1 vez en varios años**	**0**

Finalmente, en las tablas 18,19,20,21,22,23,24 y 25 se presenta el análisis de las posibles amenazas que afectan a cada activo con el impacto en cada una de las dimensiones de seguridad, además se considerará también una estimación de la frecuencia con la que podría presentarse cada una de las amenazas. Esta escala de frecuencia se hace con respecto a la escala de tabla 17.

Tabla 18 Impacto de amenazas en activos de instalaciones

Amenazas a Activos Instalaciones [L]	Frecuencia	[A]	[C]	[I]	[D]	[T]
Oficina					20%	
[I.1]Fuego	1				20%	
[I.2]Daños por agua	0				20%	
[I.7]Condiciones inadecuadas de temperatura o humedad	1				20%	

Tabla 19 Impacto de amenazas en activos de hardware

Amenazas a Activos Hardware [Hw]	Frecuencia	[A]	[C]	[I]	[D]	[T]
Servidor Correo y web, MySQL			100%	100%	100%	
Smartphones			100%	100%	100%	
Portátiles			100%	100%	100%	
Impresoras			100%	100%	100%	
Router			100%	100%	100%	
Switch			100%	100%	100%	
Modem			100%	100%	100%	
[I.1]Fuego	1				100%	
[I.5]Avería de origen físico o lógico	1				50%	
[E.2]Errores del administrador	1		50%	50%	50%	
[E.21]Errores de mantenimiento/actualización (hardware)	1				50%	
[E.25]pérdida de equipos.	0		10%		10%	
[A.23]Manipulación de equipos.	0		50%		100%	
[A.25]Robo	1		100%		100%	

Tabla 20 Impacto de amenazas en activos de software

Amenazas a Activos Software [SW]	Frecuencia	[A]	[C]	[I]	[D]	[T]
S0 WINDOWS 10		100%	100%	100%	100%	
Antivirus		100%	100%	100%	100%	
Herramientas Ofimáticas		100%	100%	100%	100%	
Windows 2019 Server		100%	100%	100%	100%	
Software Correo		100%	100%	100%	100%	
Software Web		100%	100%	100%	100%	
Software MySQL		100%	100%	100%	100%	
[I.5]Avería de origen	1				50%	

físico o lógico						
[E.1]Errores de los usuarios	2		20%	20%	20%	
[E.2]Errores del administrador	1					
[E.8] Difusión de software dañino	0		50%	50%	50%	
[E.15] Alteración accidental de la información	0			20%		
[E.18] Destrucción de información	0				50%	
[E.19] Fugas de información	0		20%			
[E.20] Vulnerabilidad de los programas (software)	1		50%	50%	50%	
[E.21] Errores de mantenimiento/ actualización de programas (software)	1			50%	100%	
[A.5] Suplantación de la identidad del usuario	0	100%	100%	100%		
[A.8] Difusión de software dañino	0		100%	100%	100%	
[A.11] Acceso no autorizado	1		100%	50%		
[A.15] Modificación deliberada de la información	0			100%		
[A.18] Destrucción de información	1			100%	100%	
[A.19] Divulgación de información	0		100%			

Tabla 21 Impacto de amenazas en activos de datos

Amenazas a Activos Datos [D]	Frecuencia	[A]	[C]	[I]	[D]	[T]
Datos Gerente General		100%	100%	100%	100%	100%
Datos de asistente administrativo		100%	100%	100%	100%	100%
Datos contabilidad y contratación		100%	100%	100%	100%	100%
Datos Gerente de ventas		100%	100%	100%	100%	100%
Datos de ejecutivos de ventas		100%	100%	100%	100%	100%
Datos de servicio al cliente		100%	100%	100%	100%	100%

Datos Gerente Técnico		100%	100%	100%	100%	100%
Datos de los técnicos instaladores		100%	100%	100%	100%	100%
Datos mensajero		100%	100%	100%	100%	100%
[E.1] Errores de los usuarios	1		10%	10%	10%	
[E.2] Errores del administrador	1		50%	50%	50%	
[E.3] Errores de monitorización (log)	2				50%	20%
[E.4] Errores de configuración	1			20%	10%	
[E.15] Alteración accidental de la información	1			100%		
[E.18] Destrucción de información	0			10%	10%	
[E.19] Fugas de información	1		50%			
[A.5] Suplantación de la identidad del usuario	0	100%	100%	100%		
[A.6] Abuso de privilegios de acceso	0		100%	100%	100%	
[A.11] Acceso no autorizado	1		100%	50%	100%	
[A.15] Modificación deliberada de la información	0			100%		
[A.18] Destrucción de información	0				100%	
[A.19] Divulgación de información	1		100%			

Tabla 22 Impacto de amenazas en activos de redes

Amenazas a Activos Redes [COM]	Frecuencia	[A]	[C]	[I]	[D]	[T]
Línea a Internet		50%	50%	50%	50%	
Red local		50%	50%	50%	50%	
[I.8] Fallo de servicios de comunicaciones	1				100%	
[E.2] Errores del administrador	1		10%	10%	10%	
[E.15] Alteración accidental de la información	1			50%		
[E.18] Destrucción de información	0				20%	
[E.19] Fugas de información	0		50%			
[E.24] Caída del sistema por agotamiento de recursos	1				50%	
[A.5] Suplantación de la identidad del usuario	0	50%	50%	50%		

[A.6] Abuso de privilegios de acceso	0		20%	20%	20%	
[A.10] Alteración de secuencia	0			10%		
[A.11] Acceso no autorizado	1		50%	20%		
[A.12] Análisis de tráfico	1		10%			
[A.14] Interceptación de información (escucha)	0		50%			
[A.15] Modificación deliberada de la información	0			10%		
[A.19] Divulgación de información	1		10%			
[A.24] Denegación de servicio	1				100%	

Tabla 23 Impacto de amenazas en activos de Servicios

Amenazas a Activos Servicios [S]	Frecuencia	[A]	[C]	[I]	[D]	[T]
Correo electrónico de la empresa		100%	100%	100%	100%	100%
Protocolo para acceso a servidores		100%	100%	100%	100%	100%
[E.1] Errores de los usuarios	1		50%	50%	50%	
[E.2] Errores del administrador	1		100%	100%	100%	
[E.18] Destrucción de información	1				50%	
[E.24] Caída del sistema por agotamiento de recursos	2				20%	
[A.5] Suplantación de la identidad del usuario	0	100%	20%	50%		
[A.10] Alteración de secuencia	0			100%		
[A.11] Acceso no autorizado	0		100%	50%		
[A.15] Modificación deliberada de la información	0			100%		
[A.18] Destrucción de información	0				100%	
[A.19] Divulgación de información	0		50%			
[A.24] Denegación de servicio	0				100%	

Tabla 24 Impacto de amenazas en activos de Equipamiento auxiliar

Amenazas a Activos Equipamiento auxiliar [AUX]	Frecuencia	[A]	[C]	[I]	[D]	[T]
Fibra Óptica					100%	
[N.1] Fuego (accidental	0				20%	

natural)						
[N.2] Daños por agua (accidental natural)	0				20%	
[N.*] Desastres naturales (rayo, terremoto)	0				20%	
[I.1]Fuego (industrial accidental o provocado)	0				20%	
[I.2] Daños por agua (industrial accidental o provocado)	0				20%	
[I.3] Contaminación mecánica (polvo, suciedad)	0			10%	20%	
[I.5] Avería de origen físico	0			10%	20%	
[I.6] Corte del suministro eléctrico	2				20%	
[I.7] Condiciones de temperatura o humedad	2			50%	20%	
[A.23] Manipulación de los equipos	1			10%	20%	
[A.26] Ataque destructivo (vandalismo)	1				20%	

Tabla 25 Impacto de amenazas en activos de personal

Amenazas a Activos Personal [P]	Frecuencia	[A]	[C]	[I]	[D]	[T]
Gerente General			100%	100%	100%	
Gerente de Ventas			100%	100%	100%	
Gerente Técnico			100%	100%	100%	
Asistente administrativo			100%	100%	100%	
Ejecutivos de ventas			100%	100%	100%	
Técnicos instaladores			100%	100%	100%	
Servicio al cliente			100%	100%	100%	
Contador			100%	100%	100%	
Mensajero			100%	100%	100%	
[E.7] Deficiencias en la organización	1				10%	
[E.19] Fugas de información	0		100%			
[E.28] Indisponibilidad del personal (ausencia por enfermedad, altercados públicos)	2				50%	
[A.28] Indisponibilidad del personal (deliberado, huelgas, bajas no justificadas,	0				10%	

absentismo laboral, ...)						
[A.29] Extorsión	0		100%	100%	100%	
[A.30] Ingeniería social	2		100%	100%	100%	

3.7. Impacto potencial

Hasta este punto se tiene la siguiente información: a)Determinación de los activos de la ISP, b) Clasificación por tipo de activo, c) Valoración tanto económica como cualitativa d) Determinación de la criticidad de las dimensiones que afecta a cada uno de los activos de la organización, e) Análisis detallado de las posibles amenazas por cada tipo de activo con la frecuencia en la que podría materializar una de estas amenazas y f) cálculo del impacto sobre cada una de las dimensiones de seguridad.

Con este análisis hecho hasta el momento se puede realizar el cálculo del impacto potencial, teniendo en cuenta que a partir de este valor se podrán tomar las medidas necesarias para minimizar el riesgo, y poder tomar decisiones con respecto al grado de aceptación de este. Es importante recordar que este valor que se encontrará corresponde al impacto que se generaría sin desplegar ninguna salvaguarda.

El cálculo del impacto potencial dependerá del valor del activo y el porcentaje del impacto

$$Impacto\ potencial = Valor\ activo \times porcentaje\ de\ impacto$$

Al igual que en las estimaciones anteriores se detalla a continuación una escala para calificar los niveles de impacto en la tabla 26.

Tabla 26 Niveles de impacto

Impacto	Porcentaje	Valor
Muy alto	100%	5
Alto	75%	4
Normal	50%	3
Bajo	20%	2
Muy bajo	10%	1
Sin impacto	0%	0

Los impactos potenciales calculados han sido registrados en la tabla 27 detallando el valor activo según cada una de las dimensiones de seguridad y el valor del impacto en porcentaje para finalmente obtener el valor del impacto potencial haciendo uso de la fórmula descrita anteriormente.

Tabla 27 Impacto potencial

	Valor activo					Impacto %					Impacto potencial				
Activo	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Oficina	2	6	2	2	2				20		0	0	0	0,4	0
Servidor Correo y web, MySQL	9	10	10	10	9		100	100	100		0	10	10	10	0
Smartphones	5	5	5	5	5		100	100	100		0	5	5	5	0
Portátiles	5	5	5	5	5		100	100	100		0	5	5	5	0
Impresoras	0	0	1	1	0		100	100	100		0	0	1	1	0
Router	9	9	8	10	1		100	100	100		0	9	8	10	0
Switch	9	9	8	10	1		100	100	100		0	9	8	10	0
Modem	7	9	7	9	1		100	100	100		0	9	7	9	0
S0 WINDOWS 10	3	5	5	9	0	100	100	100	100		3	5	5	9	0
Antivirus	3	4	5	9	0	100	100	100	100		3	4	5	9	0
HerramientasOfimáticas	0	0	0	3	0	100	100	100	100		0	0	0	3	0
Windows 2019 Server	9	9	8	10	9	100	100	100	100		9	9	8	10	0
SoftwareCorreo	8	8	8	6	4	100	100	100	100		8	8	8	6	0
SoftwareWeb	10	8	10	10	8	100	100	100	100		10	8	10	10	0
SoftwareMySQL	5	10	10	10	5	100	100	100	100		5	10	10	10	0
Datos Gerente General	9	9	10	10	10	100	100	100	100	100	9	9	10	10	10
Datos de asistente administrativo	6	6	7	7	8	100	100	100	100	100	6	6	7	7	8
Datos contabilidad y contratación	10	8	10	10	9	100	100	100	100	100	10	8	10	10	9
Datos Gerente de ventas	7	7	6	7	7	100	100	100	100	100	7	7	6	7	7
Datos de ejecutivos de ventas	6	6	6	7	6	100	100	100	100	100	6	6	6	7	6
Datos de servicio al cliente	9	8	10	9	9	100	100	100	100	100	9	8	10	9	9
Datos Gerente Técnico	9	9	10	8	10	100	100	100	100	100	9	9	10	8	10
Datos de los técnicos instaladores	7	7	7	9	7	100	100	100	100	100	7	7	7	9	7
Datos del mensajero	1	1	2	3	3	100	100	100	100	100	1	1	2	3	3
Línea a Internet	2	6	5	5	4	50	50	50	50		1	3	2,5	2,5	0
Red local	3	7	5	6	5	50	50	50	50		1,5	3,5	2,5	3	0
Correo electrónico de la empresa	6	9	2	3	2	100	100	100	100	100	6	9	2	3	2
Protocolo para acceso a servidores	8	7	8	5	3	100	100	100	100	100	8	7	8	5	3
Fibra Óptica	0	0	9	9	0				100		0	0	0	9	0
Gerente General	10	10	9	8	8		100	100	100		0	10	9	8	0
Gerente de Ventas	10	9	8	7	8		100	100	100		0	9	8	7	0
Gerente Técnico	10	10	9	10	8		100	100	100		0	10	9	10	0
Asistente administrativo	5	9	9	9	6		100	100	100		0	9	9	9	0
Ejecutivos de ventas	5	6	8	6	6		100	100	100		0	6	8	6	0
Técnicos instaladores	8	7	8	9	6		100	100	100		0	7	8	9	0
Servicio al cliente	7	6	8	9	6		100	100	100		0	6	8	9	0
Contador	10	9	8	7	6		100	100	100		0	9	8	7	0
mensajero	1	3	8	2	3		100	100	100		0	3	8	2	0

3.8. Nivel de Riesgo Aceptable y Riesgo Residual

Para determinar el nivel de riesgo que asumirá la ISP es necesario establecer una escala de valores de nivel con el fin de determinar la criticidad del riesgo y determinar si se asume o no.

El “umbral de riesgo aceptable” es el nivel máximo de riesgo que la empresa decide aceptar, todos los valores que estén por encima de este nivel serán tratados con una de las 4 siguientes opciones:

a. Asumir el riesgo: no se implementa algún control y la empresa corre el riesgo de que se materialice la amenaza porque consideran que es muy costoso y poco probable de que ocurra, aunque no imposible asumirán resolverlo si se llega a presentar.
b. Eliminar o evitar el riesgo: Que requiere utilizar recursos que permitan eliminar el riesgo, sin embargo, en esta opción puede resultar costoso el realizar estas acciones.
c. Transferir el riesgo: en el caso de que la organización no tenga la capacidad de afrontar con soluciones la probabilidad de que se materialice la amenaza
d. Finalmente, la opción de reducir el riesgo, opción que se aplicará en la mayoría de los casos del presente plan director, que consiste en implantar controles de seguridad que permitan reducir el impacto en el caso de que se materialice una amenaza. Se realizará un análisis de las salvaguardas que ayuden a minimizar el impacto y llevar aquellos riesgos que se han señalado como niveles altos y muy altos, a un nivel medio que pueda ser aceptado por la organización.

El nivel de tolerancia del riesgo debe mantenerse en un equilibrio entre el coste de implementación de protecciones y el de recuperación en el caso de quedar expuesta. Basados en la metodología de MAGERIT tendremos una guía tanto para este equilibrio el cual puede observase en la ilustración 6.

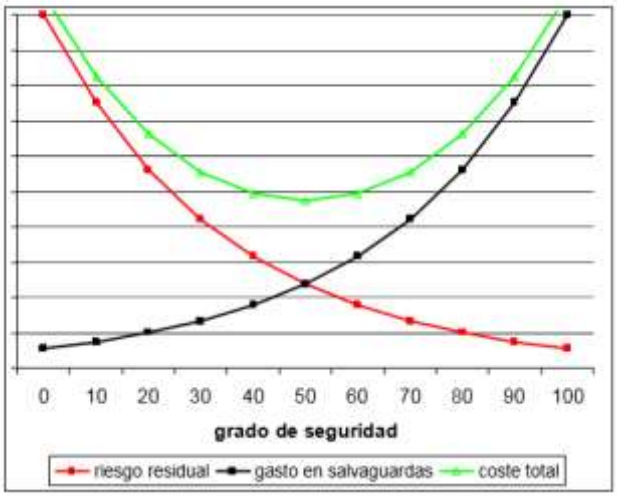

Ilustración 6 Relación entre el riesgo y el costo de protección (públicas, 2012)

Luego de realizar el análisis de riesgos, y obtener los resultados del impacto potencial sobe los activos se puede obtener el nivel de riesgo analizando su frecuencia de ocurrencia sobre cada activo relevante en la empresa. Este resultado se obtuvo a partir de la siguiente formula:

Riesgo = Impacto potencial x Probabilidad de Frecuencia de ocurrencia

Partiendo del cálculo del riesgo tendremos los siguientes niveles de riesgo descritos en la tabla 28, en la cual se resaltan los niveles alto y muy alto como los que requerirán de atención urgente haciendo uso de salvaguardas.

Tabla 28 Niveles de riesgo analizando la frecuencia de ocurrencia

Valor	Rango nivel de riesgo
Muy alto (MA)	9 y 10
Alto (A)	8
Medio(M)	5, 6 y 7
Bajo (B)	2, 3 y 4
Muy bajo (MB)	1

Se ha acordado con la ISP aceptar cualquier riesgo ≤7 y proceder a implantar salvaguardas y controles que permitan reducir el nivel de riesgos de los activos que se encuentren en los niveles > 7. Para una mejor observación de los resultados se resaltarán en rojo todos aquellos que superan este nivel

A partir de los resultados encontrados en la sección anterior del impacto potencial y basados en los niveles asignados de frecuencia de la *Tabla 16. Escala de frecuencia de materialización de una amenaza,* se presentan a continuación en la tabla 29 los resultados de los niveles de riesgos de cada activo resaltando aquellos que se encuentran por encima del nivel aceptable para la organización.

Tabla 29 Nivel de riesgo > 7

	Impacto potencial					Frecuencia de ocurrencia	Riesgo				
Activo	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Oficina	0	0	0	0,4	0	0	0	0	0	0	0
Servidor Correo y web, MySQL	0	10	10	10	0	0	0	0	0	0	0
Smartphones	0	5	5	5	0	1	0	5	5	5	0
Portátiles	0	5	5	5	0	1	0	5	5	5	0
Impresoras	0	0	1	1	0	1	0	0	1	1	0
Router	0	9	8	10	0	1	0	9	8	10	0
Switch	0	9	8	10	0	1	0	9	8	10	0
Modem	0	9	7	9	0	1	0	9	7	9	0
S0 WINDOWS 10	3	5	5	9	0	1	3	5	5	9	0
Antivirus	3	4	5	9	0	1	3	4	5	9	0

Herramientas Ofimáticas	0	0	0	3	0	1	0	0	0	3	0
Windows 2019 Server	9	9	8	10	0	1	9	9	8	10	0
Software Correo	8	8	8	6	0	1	8	8	8	6	0
Software Web	10	8	10	10	0	1	10	8	10	10	0
Software MySQL	5	10	10	10	0	1	5	10	10	10	0
Datos Gerente General	9	9	10	10	10	1	9	9	10	10	10
Datos de asistente administrativo	6	6	7	7	8	1	6	6	7	7	8
Datos contabilidad y contratación	10	8	10	10	9	1	10	8	10	10	9
Datos Gerente de ventas	7	7	6	7	7	1	7	7	6	7	7
Datos de ejecutivos de ventas	6	6	6	7	6	1	6	6	6	7	6
Datos de servicio al cliente	9	8	10	9	9	1	9	8	10	9	9
Datos Gerente Técnico	9	9	10	8	10	1	9	9	10	8	10
Datos de los técnicos instaladores	7	7	7	9	7	1	7	7	7	9	7
Datos mensajero	1	1	2	3	3	1	1	1	2	3	3
Línea a Internet	1	3	2,5	2,5	0	1	1	3	2,5	2,5	0
Red local	1,5	3,5	2,5	3	0	1	1,5	3,5	2,5	3	0
Correo electrónico de la empresa	6	9	2	3	2	1	6	9	2	3	2
Protocolo para acceso a servidores	8	7	8	5	3	1	8	7	8	5	3
Fibra Óptica	0	0	0	9	0	1	0	0	0	9	0
Gerente General	0	10	9	8	0	1	0	10	9	8	0
Gerente de Ventas	0	9	8	7	0	1	0	9	8	7	0
Gerente Técnico	0	10	9	10	0	1	0	10	9	10	0
Asistente administrativo	0	9	9	9	0	1	0	9	9	9	0
Ejecutivos de ventas	0	6	8	6	0	1	0	6	8	6	0
Técnicos instaladores	0	7	8	9	0	1	0	7	8	9	0
Servicio al cliente	0	6	8	9	0	1	0	6	8	9	0
Contador	0	9	8	7	0	1	0	9	8	7	0
mensajero	0	3	8	2	0	1	0	3	8	2	0

Según los resultados del análisis de riesgos, de los 38 activos descritos como relevantes en cuanto seguridad de la información, 11 activos se encuentran bajo el umbral de riesgo, 8 activos se encuentran con al menos un principio de seguridad en alto riesgo, 6 activos se ven afectados en dos de sus dimensiones, 7 activos se ven afectados en 3 dimensiones, 3 activos con cuatro dimensiones y 3 activos con las 5 dimensiones en un alto nivel de riesgo.

4. Propuestas de proyectos

4.1 Introducción

Llegados a este punto, se tienen los resultados del análisis detallado de todos los activos importantes para la empresa ya que se han valorado no solo desde el punto de vista de costos sino del valor agregado que representaría la pérdida de cualquiera de ellos. A partir de esa información se completó el análisis de riesgos destacando las posibles amenazas, el impacto potencial que se generaría al versen materializadas y el nivel de riesgo en el que se encuentran actualmente cada uno de los activos.

En este capítulo se propondrá los diferentes proyectos que contribuirán a reducir los riesgos en los niveles alto y muy alto para situarlos en el nivel aceptable para la organización. Estos proyectos no solo servirán para reducir los riesgos, sino que encaminará el plan director hacia el cumplimiento de la ISO con el fin de mejorar todos los procesos que realiza la organización para su correcto funcionamiento.

Como se indicaba en un inicio, la ISP es una empresa relativamente nueva y pequeña, con pocos integrantes y como es de suponerse no se cuenta con demasiados recursos que generen gastos fuera de la planificación inicial. Por esta razón se pretenderá mejorar en lo posible los procedimientos esperando no incurrir en gastos importantes que no pudiera solventar la empresa.

La idea de encaminar la empresa hacia el cumplimiento de los controles de la ISO 27002 y los requerimientos de la ISO 27001 se hace con el fin de aplicar a la certificación, para esto se planteará la ejecución de estos proyectos en un lapso máximo de 3 años, esperando la colaboración de cada uno de los empleados y con el objetivo de realizar la implantación de los 114 controles de seguridad de la información los cuales se han dividido de manera equitativa a lo largo de este periodo.

Al final de esta etapa se espera reconocer las mejoras en cuanto a los dominios de la seguridad a través de una comparación con el análisis diferencial realizado como punto de partida, y la disminución del nivel de riesgo en aquellos activos que se encuentran con un nivel alto actualmente debido a que no se cuenta con ninguna salvaguarda desplegada.

En cada una de las propuestas se detallará la planificación de la ejecución de cada proyecto clasificándolo según se requiera, en tres plazos: corto, mediano y largo plazo, además del coste económico que representará. Es importante destacar que todo el plan de acción no solo afectará al ámbito tecnológico, sino al funcionamiento de todas las áreas que conforman la organización y de las cuales también depende que la atención y servicio que se brida al cliente garantice calidad.

En este puto es importante destacar que no solo las propuestas de proyectos ayudarán a mejorar el sistema de seguridad de la información, el desempeño

tanto del auditor, así como los resultados de las auditorias jugarán un papel muy importante como complemento para cumplir el objetivo de la implantación del SGSI.

4.2. Propuestas

A continuación, se describe cada uno de los proyectos propuestos para implementar en el SGSI, como se indicó en la sección anterior, los proyectos estarán encaminados a mejorar el cumplimiento de los controles de seguridad y además a reducir el nivel de riesgo encontrado en la última fase del análisis de riesgos. Para cada uno de los proyectos relacionados a los controles de la ISO 27002:

Identificador del Proyecto con el dominio afectado

1. Controles de seguridad que se pretende implementar o mejorar.
2. Objetivo
3. Descripción
4. Activos involucrados en el proceso para reducir el riesgo
5. Plazo previsto para consecución de objetivos
6. Presupuesto

En el caso de los riesgos encontrados con un nivel alto, no se atenderán por separado ya que cada proyecto debe asegurar disminuir alguno de los riesgos, lo que quiere decir que en los casos necesarios se resaltará el riesgo que se disminuirá una vez se haya ejecutado el proyecto.

Para todos los cálculos del presupuesto se considerará un pago de 20 dólares la hora.

PR01: POLÍTICA DE SEGURIDAD:

1. **Controles**

6.1.1 Políticas para la seguridad de la información
5.1.2 Revisión de las políticas para la seguridad de la información

2. **Objetivo**

Definir la política de seguridad de la información

3. **Descripción**

La empresa no cuenta ni con el estado inicial del desarrollo de una política de seguridad, así que el primer paso será elaborar una política de seguridad que debe ser aprobada por la dirección y tener al menos una revisión anual y publicada a todos los empleados a través de medios electrónicos como el correo de la empresa. Cabe destacar que al ser un documento que se encuentra en el nivel alto de la pirámide

documental no requerirá más que una revisión al año o cuando se presente algún cambio significativo.
Estas políticas deberán contener mínimo la definición de los objetivos y de la seguridad de la información que orienten todas las actividades de la empresa con relación a los procedimientos que debe seguirse y debe contener la asignación de responsabilidades generales y específicas para identificar los roles. Además, puede haber más documentos donde se especifiquen políticas dedicadas a los procedimientos más relevantes de la empresa

4. Activos involucrados en el proceso para reducir el riesgo

[L], [HW], [SW], [D], [COM], [S], [AUX], [P]. Este control es el que abarca el trabajo en relación con el sistema de seguridad ya que determina las directrices y procedimientos necesarios para obtener resultados positivos colaterales en los demás controles.

5. Plazo previsto para consecución de objetivos

Al ser el documento que define el enfoque de la organización para gestionar los objetivos de seguridad debe realizarse lo más pronto posible, para esto se define un tiempo de 1 mes, con 20 días laborables y un promedio de 8 horas diarias.

6. Presupuesto

Horas de trabajo: 160 horas
Costo estimado: 3200 dólares

PR02: Organización de la seguridad de la información

1. Controles

6.1.1 Roles y responsabilidades en seguridad de la información
6.1.2 Segregación de tareas
6.1.3 Contacto con las autoridades
6.1.4 Contacto con grupos de interés especial
6.1.5 Seguridad de la información en la gestión de proyectos
16.1 Gestión de incidentes de seguridad de la información y mejoras

2. Objetivos

- Definir los roles y responsabilidades de acuerdo con las políticas generadas en el PR02
- Establecer y distribuir las funciones y responsabilidades entre diferentes áreas.
- Elaborar el procedimiento para contactar las autoridades con el fin de reportar los incidentes.

3. **Descripción**

Como se pudo ver en el análisis diferencial inicial, de los 5 controles, solo el primero se tenía conocimiento de la existencia y necesidad de establecer roles dentro de la organización, sin embargo, no hay ni siquiera conocimiento de los demás controles que se encuentran dentro de este dominio. En un proyecto que se describirá más adelante, se abarcará el hecho de la necesidad de capacitaciones a todo el personal.

En este proyecto se identificarán las responsabilidades en materia de seguridad de la información, así mismo se deberán segregar las tareas distribuyendo las responsabilidades de forma equitativa entre las diferentes áreas involucradas. Además, se establecerá el procedimiento que defina cuando y con quien se deben contactar en el caso de presentarse un incidente. Finalmente se incluirá información de los grupos con conocimientos actualizados de información relevante a la seguridad.

4. **Activos involucrados en el proceso para reducir el riesgo**

[P], la finalidad de este proyecto será mitigar tantos los errores del personal actuales y futuros conociendo los procedimientos que deben realizar a la hora de presentarse un incidente de seguridad y poder contactar de manera rápida a quien corresponda el hecho que se presenta.

5. **Plazo previsto para consecución de objetivos**

5 días para recoger toda la información de las personas que tendrán un rol y una responsabilidad dentro del proceso de la seguridad de la información, 10 días para realizar la investigación de los contactos de Ecuador en relación con los SGSI y 15 días para realizar los procedimientos. Tiempo destinado 20 días laborables y un promedio de 8 horas diarias.

6. **Presupuesto**

Horas de trabajo: 160 horas
Costo estimado: 3200 dólares

PR03: Organización de la seguridad de la información

1. **Controles**

6.2.1Política de dispositivos móviles
6.2.2Teletrabajo

2. **Objetivo**

Definir la política de dispositivos móviles y de Teletrabajo.

3. **Descripción**

   Se elaborarán las políticas que establezca las medidas de seguridad en relación con la protección de los dispositivos móviles tanto de celulares como de las computadoras portátiles con el fin de minimizar la perdida de la información que contengan estos dispositivos a la hora de sufrir un robo o un daño irreparable. Además, se elaborará la política de teletrabajo que actualmente se requiere más urgente debido a la situación de la pandemia por el COVID-19, y que, en Ecuador, según las noticias actuales dadas por el presidente del país, se continuará con la modalidad del teletrabajo al menos 11 meses más.

4. **Activos involucrados en el proceso para reducir el riesgo**

   [HW], [SW], [D], [P]. En los 4 ámbitos se debe llevar el riesgo a un nivel aceptable al implementar este proyecto

5. **Plazo previsto para consecución de objetivos**

   Medio mes, con 10 días laborables y un promedio de 8 horas diarias.

6. **Presupuesto**

   Horas de trabajo: 80 horas
   Costo estimado: 1600 dólares

PR04: Seguridad relativa a los recursos humanos

1. **Controles**

7.1 Antes del empleo
7.2 Durante el empleo
7.3 Finalización del empleo o cambio en el puesto de trabajo

2. **Objetivo**

   Verificar que los empleados tomen conciencia de la importancia de la seguridad de la información en la empresa junto con sus responsabilidades y funciones necesarias para el desarrollo del SGSI.

3. **Descripción**

   Como se indicó en el análisis diferencial solo el control relacionado a la investigación de antecedentes se implementa casi al 100%, sin embargo, los otros 4 controles se desconocen totalmente. Durante la ejecución de este proyecto se establecerá un documento aparte del contrato, que indique las condiciones respecto a la seguridad.

Se realizará un formato de compromiso de confidencialidad que deberán firmar todos los empleados de la empresa, incluso que deben cumplir al finalizar la dependencia con la empresa. Además, se diseñarán cursos de capacitación informando las políticas que deben cumplir todos, también se planificarán capacitaciones de concienciación en seguridad de la información de manera periódica y actualizada.

4. Activos involucrados en el proceso para reducir el riesgo

[P], la mayoría de los riesgos, o al menos los más importantes se deben a desconocimiento, con este proyecto se espera reducir el riesgo en relación con estas fallas que se encuentran actualmente presentes.

5. Plazo previsto para consecución de objetivos

Estos cursos se diseñarán en 45 días ya que su ejecución será de manera virtual, a través de la plataforma gratuita Moodle, con un plazo para que los empleados lo realicen en una semana cada curso. Se impartirán 6 cursos en un lapso de 6 meses, y cada año se realizarán dos cursos de actualización con respecto a nuevos incidentes a nivel internacional con el fin de mantener el personal actualizado.

6. Presupuesto

Horas de trabajo en el diseño de los cursos: 240 horas
Costo estimado: 4800 dólares

PR06: Gestión de activos

1. Controles

8.1 Responsabilidad sobre los activos
8.2 Clasificación de la información
8.3 Manipulación de los soportes

2. Objetivo

Gestionar los activos de manera que todos se encuentren inventariados, clasificados y etiquetados.

3. Descripción

En relación con los 3 objetivos de este dominio, la ISP tiene la mitad del proceso solo en el primero respecto al inventario de activos. Sin embargo, no hay nada gestionado respecto a la clasificación de los activos ni de los procedimientos respecto a la manipulación de los soportes.

En este proyecto se procederá a realizar el inventario completo de todos los activos referentes a seguridad de la empresa, se describirá el ciclo

de vida de cada uno identificando la fecha de creación, el procedimiento para tratar, almacenar, transmitir borrar y destruir cada activo. La información estará actualizada, de manera digital para el acceso del personal autorizado, y finalmente dentro de la documentación estará el propietario del activo quien también será responsable del riesgo para gestionarlo en el caso de presentarse.

Se realizará un formato de entrega recepción, que se entregará al momento de firmar el contrato recibiendo los activos asignados por la empresa a cada responsable y una vez finalizado el contrato se deberá devolver en el mismo estado todos los activos, donde el área de recursos humanos será el responsable de recibir todo para poder firmar el acta de entrega recepción de salida de la empresa. Este documento será necesario para todos los empleados que salgan de la empresa y quieran retirar el cheque de liquidación sin ningún descuento.

Se realizará la clasificación de los activos con ID de identificación y se asignará grupos de activos por áreas en donde los propietarios de los activos serán los responsables de realizar la clasificación siguiendo el procedimiento de etiquetación diseñado por el departamento de seguridad de la información.

Finalmente, para la manipulación de soportes respecto a los soportes extraíbles físicos en tránsito y eliminación de soportes. Se presentará un procedimiento que contenga las indicaciones y pasos a seguir en la gestión de soportes extraíbles y en la eliminación de soportes basados en las directrices de los controles de la ISO 27002.

4. Activos involucrados en el proceso para reducir el riesgo

Todos los ámbitos.

5. Plazo previsto para consecución de objetivos

Todo el proceso llevará 20 días

6. Presupuesto

Horas de trabajo en el diseño de los procedimientos: 50 horas
Horas que corresponden a levantar la información de todos los activos incluyendo el tiempo de clasificación y etiquetado: 110 horas
Costo estimado: 3200 dólares.

PR07: Gestión control de acceso

1. Controles

9.1 Política de control de acceso

9.2 Gestión de acceso de usuario
9.3 Responsabilidades del usuario
9.4 Control de acceso a sistemas y aplicaciones

2. Objetivo

Gestionar el control de acceso solo a personal autorizado

3. Descripción

Se establecerá la política de control de acceso basada en los requisitos de la ISP y de seguridad de la información, además se especificarán las reglas de control de acceso en procedimientos específicos que ayuden de soporte a la política. Se establecerá además la política de acceso a las redes y a os servicio de red solo a personal autorizado.

Se realizarán los procedimientos formales correspondientes a la asignación y revocación de los derechos de acceso a los usuarios autorizados, así como el proceso de acuerdo con la política de control de acceso aplicable y se realizará el formato de confidencialidad en cuanto a la autenticación secreta.

Con respecto al control de acceso a sistemas y aplicaciones la empresa tiene ya procesos que realizan todos los empleados de manera similar, pero sin seguir algún procedimiento por lo que en este proyecto también se realizará los procedimientos seguros para inicio de sesión gestionando de manera segura contraseñas que restrinjan el acceso a personal no autorizado.

4. Activos involucrados en el proceso para reducir el riesgo

[HW], [SW], [S], y [P], se espera reducir el riesgo a los que se encuentran los servidores, router, Switch y al personal de la empresa

5. Plazo previsto para consecución de objetivos

1 mes para el diseño tanto de las políticas como de los procedimientos y la gestión segura de contraseñas para cada uno de los usuarios.

6. Presupuesto

Horas de trabajo al mes 160
Costo estimado: 3200 dólares

PR08: Criptografía

1. Controles

10.1.1 Política de uso de los controles criptográficos
10.1.2 Gestión de claves

13.1 Gestión de la seguridad de redes
13.2 Intercambio de información
18.1.3 Protección de los registros de la organización
18.1.4 Protección y privacidad de la información de carácter personal
18.1.5 Regulación de los controles criptográficos

2. Objetivo

- Establecer una política sobre el uso de los controles criptográficos para garantizar la protección de los principios básicos de la seguridad de la información.
- Definir las políticas tanto para los controles criptográficos como para la gestión de claves de cifrado a lo largo de todo su ciclo de vida.
- Definir los procedimientos para todo el ciclo de vida de las claves criptográficas es decir la generación, mantenimiento archivo, recuperación y destrucción.

3. Descripción

El proyecto consiste en elaborar las políticas de seguridad y todos los procedimientos requeridos para proteger la información a través de controles criptográficos.

En la política de controles criptográficos se especificarán el enfoque de la organización, los principios que se desean proteger: confidencialidad, autenticidad y/o integridad. Se especificarán los métodos y procedimientos para la protección de las claves criptográficas y recuperación de esta información cifrada en caso de pérdida o daños.

En la política de gestión de claves se describirán las directrices respecto a la generación distribución, almacenamiento, cambio o actualización, revocaciones, recuperaciones, y destrucción de las claves criptográficas.

4. Activos involucrados en el proceso para reducir el riesgo

[SW], [D], [S], con este proyecto se espera reducir el riesgo en los ámbitos de alto riesgo que se detectaron en cuanto todos los activos de software que son los más críticos detectados en el análisis

5. Plazo previsto para consecución de objetivos

1 mes con 160 horas en la elaboración de todos los procedimientos y políticas.

6. Presupuesto

3200 dólares

PR09: Seguridad física y de entorno

1. **Controles**

11.1 Áreas seguras
11.2 Seguridad de los equipos

2. **Objetivo**

- Prevenir el acceso a personal no autorizado.

3. **Descripción**

El proyecto consiste en establecer medidas de seguridad en el perímetro para proteger la información implementando un mejor sistema de vigilancia con cámaras que mejoren el reconocimiento de las personas que acceden a las instalaciones. Una vez se identifiquen se deberán implementar controles de acceso a las instalaciones en el cual se deberá dejar un documento a la hora de ingresar para retirarlo una vez se dejen las instalaciones.

Se debe mejorar la distribución de las oficinas internamente con el fin evitar que el público pueda ver la información incluso desde lejos. Todas las áreas deben contar con protecciones y seguir los procedimientos establecidos para áreas segura de trabajo, así como para las áreas de carga y descarga. Algunos de los equipos de la ISP se encuentran protegidos contra fallos de alimentación, pero no existe el procedimiento ni los equipos cumplen con total seguridad para lo que se desarrollará un procedimiento con las respectivas recomendaciones

4. **Activos involucrados en el proceso para reducir el riesgo**

[I], [D], [HW]

5. **Plazo previsto para consecución de objetivos**

1 meses con 110 horas

6. **Presupuesto**

2200 dólares

PR010: Seguridad de las operaciones

1. **Controles**

12.1 Procedimientos y responsabilidades operacionales
12.2 Protección contra el software malicioso (malware)

2. **Objetivo**

   - Elaborar los procedimientos de operación
   - Describir controles de seguridad contra software malicioso.

3. **Descripción**

   Se establecerán procedimientos para adquirir protecciones contra el software malicioso y que se pueda detectar a tiempo cualquier intento de aprovechar alguna vulnerabilidad.

4. **Activos involucrados en el proceso para reducir el riesgo**

   [SW], [D]

5. **Plazo previsto para consecución de objetivos**

   1 mes con 160 horas

6. **Presupuesto**

   3200 dólares

PR011: Copias de seguridad

1. **Controles**

   12.3.1 Copias de seguridad de la información

2. **Objetivo**

   - Implementar procedimientos de copias de seguridad

3. **Descripción**

   Se debe mantener una frecuencia adecuada para guardar copias de seguridad y así evitar que se vea afectado el funcionamiento de la empresa. Para esto se seguirán todas las directrices propuestas en la norma.

4. **Activos involucrados en el proceso para reducir el riesgo**

   [SW], [D]

5. **Plazo previsto para consecución de objetivos**

   7 días 56 horas

6. **Presupuesto**

   1120 dólares

PR012: Adquisición, desarrollo y mantenimiento de los sistemas de información

1. **Controles**

14.1 Requisitos de seguridad en los sistemas de información

2. **Objetivo**

   - Implementar procedimientos y políticas para los servicios de aplicaciones que se transmiten a través de redes públicas y para las transacciones

3. **Descripción**

   Se deberán plantear los requisitos de seguridad de la información en base a las revisiones de las políticas realizadas anteriormente, realizar procedimientos seguros para los servicios de aplicaciones que se transmiten a través de redes públicas y para las transacciones siguiendo las directrices de la norma.

4. **Activos involucrados en el proceso para reducir el riesgo**

   [SW]

5. **Plazo previsto para consecución de objetivos**

   15 días 120 horas

6. **Presupuesto**

   2400 dólares

PR013: Relación con proveedores

1. **Controles**

15.1 Seguridad en las relaciones con proveedores
14.3 Datos de prueba

2. **Objetivo**

   - Realizar los procedimientos en el tratamiento de la información con proveedores externos a la ISP

- Elaborar la política de seguridad de la información en las relaciones con los proveedores

3. Descripción

Deben realizarse formatos donde se establezcan los acuerdos con los proveedores en donde se evidencie el compromiso de ambas partes en el cumplimiento de las normas de seguridad de la información. Se deben tener formatos de los acuerdos con los proveedores para tener acceso a la información de la cadena de suministros de los proveedores.

4. Activos involucrados en el proceso para reducir el riesgo

[S], servicios de proveedores

5. Plazo previsto para consecución de objetivos

18 días 144 horas

6. Presupuesto

2880 dólares

Una vez realizado la propuesta de los proyectos podremos ver la planificación para su ejecución en el siguiente diagrama de Gantt

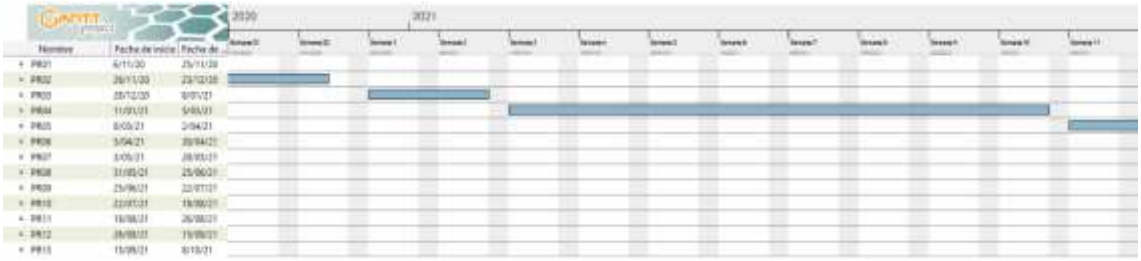

Ilustración 7 Diagrama de Gantt con la planificación de los proyectos parte 1

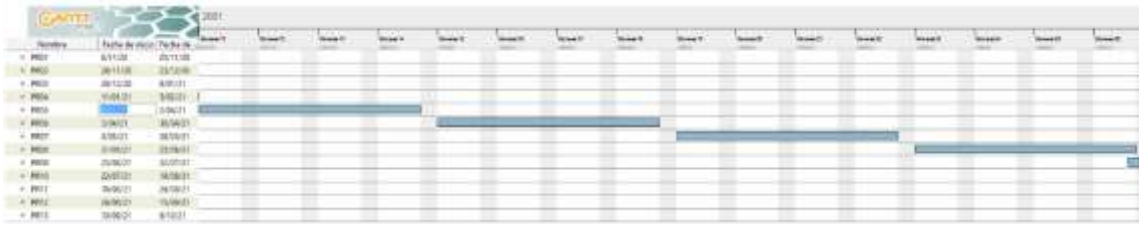

Ilustración 8 Diagrama de Gantt con la planificación de los proyectos parte 2

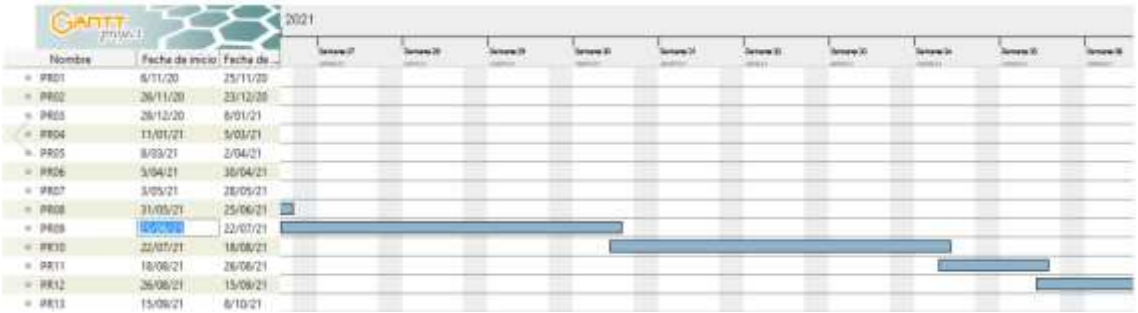

Ilustración 9 Diagrama de Gantt con la planificación de los proyectos parte 3

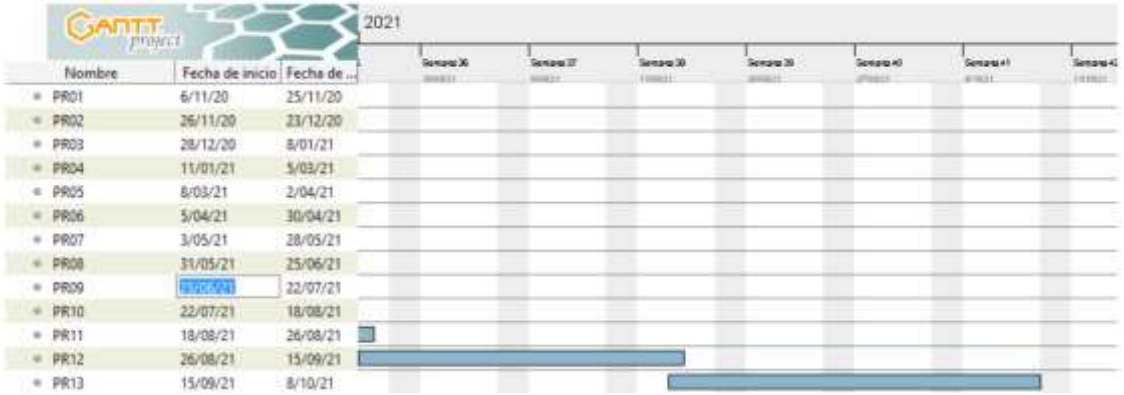

Ilustración 10 Diagrama de Gantt con la planificación de los proyectos parte 4

4.3 Resultados

A continuación, se presentan los resultados de una estimación en el riesgo residual que se obtendrá luego de implementar los proyectos y de cumplir cada uno de los objetivos propuestos. En cada proyecto se ha detallado el procedimiento a realizar no solo con el fin de cumplir los 14 dominios que se requieren para la implantación del SGSI sino también con el fin de mitigar los riesgos hallados en el análisis de riesgos.

Al desarrollar cada uno de los proyectos se ha señalado los activos que forman parte del proceso de implementación del proyecto y por ende la afectación positiva sobre los riesgos identificados por cada uno de los activos. Se ha considerado de suma importancia el desarrollo de políticas y procedimientos que son la base de la implantación en cualquier SGSI además del control con respecto a la concienciación de todo el personal, ya que el capacitar y promover las buenas prácticas disminuye en gran porcentaje los incidentes provocados por la desinformación.

4.3.1 Resultados de comparar el nivel de riesgo potencial con el nivel de riesgo residual

En las siguientes 3 figuras se podrá observar una comparación entre el riesgo potencial hallado en el capítulo 3 del análisis de riesgos, contra la estimación del nivel de riesgo que se obtendrá luego de implementasen las propuestas de

proyectos. En cada una se puede observar que el nivel de riesgo residual quedará por debajo del umbral de riesgo.

Se ha dividido la comparación de los activos en 3 gráficas con el fin de poder apreciar mucho mejor los resultados en los diferentes ámbitos.

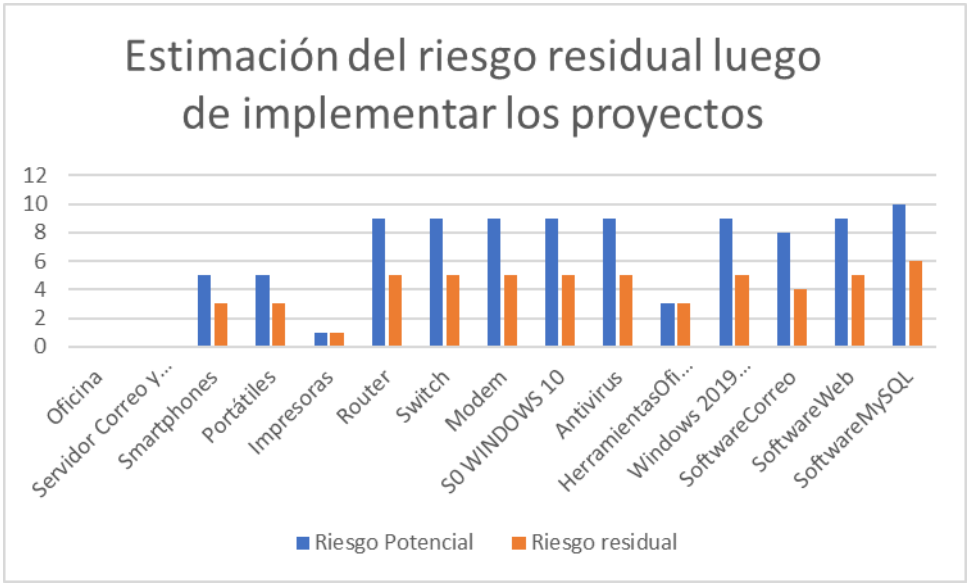

Ilustración 11 Comparación entre el riesgo potencial y la estimación del riesgo residual en los ámbitos [L], [HW] y [SW]

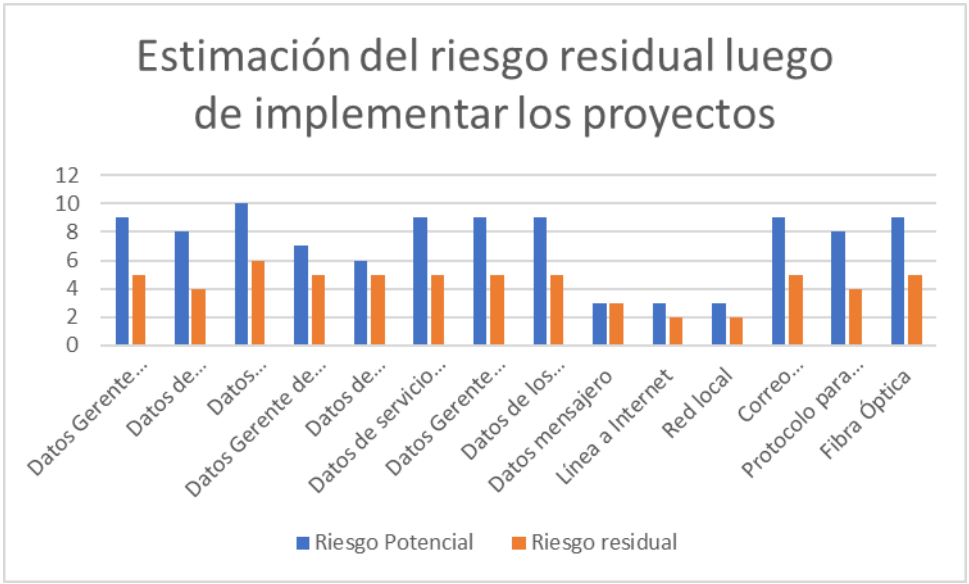

Ilustración 12 Comparación entre el riesgo potencial y la estimación del riesgo residual en los ámbitos [D], [COM], [S], [AUX], [P].

Ilustración 13 Comparación entre el riesgo potencial y la estimación del riesgo residual en el ámbito [P].

4.3.2. Evolución del nivel de cumplimiento de los diferentes dominios de la norma ISO/IEC 27002

En la siguiente figura se indica la comparación entre el porcentaje de cumplimiento de cada uno de los dominios de la norma antes de implementar los proyectos, resultados que se obtuvieron en el análisis diferencial inicial del capítulo 1.

En a tabla 30 presentarán los resultados de porcentaje de los 114 controles en cada dominio.

Tabla 30 Resultados de porcentaje de los 114 controles

Controles	Efectividad inicial	Efectividad luego de implementar los proyectos
5. Políticas de seguridad de la información	**0%**	**100 %**
6. Organización de la seguridad de la información	**13.5%**	**95 %**
7. Seguridad relativa a los recursos humanos	**16,7%**	**95 %**
8. Gestión de activos	**20%**	**90 %**
9. Control de acceso	**30,3%**	**90 %**
10. Criptografía	**10%**	**90 %**
11. Seguridad física y del entorno	**45,5%**	**90 %**
12. Seguridad de las operaciones	**35,3%**	**90 %**
13. Seguridad de las comunicaciones	**39,1%**	**95 %**
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**35,5%**	**90 %**

15. Relación con proveedores	**45%**	**95 %**
16. Gestión de incidentes de seguridad de la información	**11,4%**	**95 %**
17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	**20%**	**95 %**
18. Cumplimiento	**9%**	**95 %**

En el siguiente gráfico se presentan los resultados de la evolución estimada una vez se implementen cada uno de los proyectos y se mantenga un proceso de mejora continua siguiendo la planificación de las auditorías.

Ilustración 14 Grafico GAP después de la implementación de los proyectos

5. Auditoría de cumplimiento

5.1. Introducción

Luego de haber realizado un análisis de riesgos valorando los activos importantes de la ISP, y habiendo determinado las amenazas, el impacto potencial y el nivel de riesgo de cada una de estas, se realizaron diferentes propuestas de proyectos con el fin de llevar todos los niveles de riesgos altos y muy altos a niveles aceptables para la organización. Se ha realizado una estimación de los resultados que se pueden obtener una vez se ejecuten cada uno de los proyectos con los parámetros sugeridos.

En esta quinta fase pasaremos a realizar la verificación del cumplimiento de cada uno de los controles con el fin de mantener el ciclo de mejora continua. A este procedimiento de verificación es al que llamamos auditoria de cumplimiento, el cual nos servirá para poder analizar si se está realizando de manera correcta la ejecución del SGSI y evaluar la madurez de cada uno de los diferentes dominios de control y los 114 controles planteados en las buenas prácticas de la ISO/IEC 27002:2013.

La auditoría estará alineada al procedimiento presentado en el capítulo 2 *Gestión documental,* el cual permitirá analizar el estado de cada uno de los controles y determinar si se deben realizar acciones en caso de encontrar inconformidades importantes.

5.2. Metodología

Como parte del desarrollo de la auditoría, se evaluará la madurez de la seguridad tanto en el cumplimiento de la ISP con respecto a los requerimientos especificados en la ISO 27001:2013 así como lo que respecta a los 114 controles o salvaguardas de cada uno de los 35 objetivos de control correspondientes a los 114 dominios especificados en la ISO 27002. En la tabla 31 se resumen tanto los dominios que serán evaluados, así como los requerimientos de la ISO 27001.

Tabla 31 Apartados de las normas ISO a evaluar con el CMM

Apartados de la ISO 27001:2013	Dominios ISO/IEC 27002:2013
4. Contexto de la organización	**5. Políticas de seguridad de la información**
5. Liderazgo	**6. Organización de la seguridad de la información**
6. Planificación	**7. Seguridad relativa a los recursos humanos**
7. Soporte	**8. Gestión de activos**
8. Operación	**9. Control de acceso**
9. Evaluación del desempeño	**10. Criptografía**
10. Mejora	**11. Seguridad física y del entorno**

	12. Seguridad de las operaciones
	13. Seguridad de las comunicaciones
	14. Adquisición, desarrollo y mantenimiento de los sistemas de información
	15. Relación con proveedores
	16. Gestión de incidentes de seguridad de la información
	17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio
	18. Cumplimiento

Esta estimación se hará de la misma forma que se hizo en el capítulo 1 para el análisis diferencial. Se hará siguiendo los parámetros de la tabla 2 descrito en el punto *1.3 análisis diferencial* que se basa en el Modelo de Madurez de la capacidad (CMM).

5.3. Evaluación de la madurez

En este apartado se realizará el análisis de cada uno de los requerimientos con respecto a los apartados de la ISO/IEC 27001:2013 así como el análisis respecto a los dominios de la ISO 27002.

5.3.1. Evaluación de la madurez de la ISO/IEC 27001:2013

En la siguiente tabla 32 se presentan los resultados de los porcentajes de efectividad finales de los requerimientos de los 7 apartados de la norma ISO luego de haber implementado los controles y gestionado el SGSI en la ISP.

Tabla 32 Porcentaje de efectividad de los requerimientos ISO/IEC 27001:2013 final

	Requerimientos ISO 27001	Efectividad (%)	CMM
4	**Contexto de la organización**	**96,2**	**L4**
4.1	Comprensión de la organización y de su contexto	95	
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	95	
4.3	Determinación del alcance del SGSI	100	
4.4	Sistema de Gestión de la Seguridad de la Información	95	
5	**Liderazgo**	**98,3**	**L4**
5.1	Liderazgo y compromiso	100	
5.2	Política	100	
5.3	Roles, responsabilidades y autoridades en la organización	95	
6	**Planificación**	**95**	**L4**
6.1	Acciones para tratar los riesgos y oportunidades	95	

6.2	Objetivos de seguridad de la información y planificación para su consecución	95	
7	**Soporte**	**92,5**	**L3**
7.1	Recursos	95	
7.2	Competencia	90	
7.3	Concienciación	95	
7.4	Comunicación	90	
8	**Operación**	**93,3**	**L3**
8.1	Planificación y control operacional	90	
8.2	Apreciación de los riesgos de seguridad de la información	95	
8.3	Tratamiento de los riesgos de seguridad de la información	95	
9	**Evaluación del desempeño**	**98,3**	**L4**
9.1	Seguimiento, medición, análisis y evaluación	95	
9.2	Auditoría interna	100	
9.3	Revisión por la dirección	100	
10	**Mejora**	**92,5**	**L3**
10.1	No conformidad y acciones correctivas	95	
10.2	Mejora continua	90	

5.3.2. Evaluación de la madurez de la ISO/IEC 27002:2013

Al igual que se realizó la estimación para los requerimientos de la norma 27001 ahora procederemos a realizar la misma evaluación para cada uno de los 114 controles planteados por la norma para cumplir los 35 objetivos de control correspondientes a cada uno de los 14 dominios.

La información se ha organizado de la misma manera en la que se desarrolló el análisis diferencial inicial, pero además se describirán los objetivos de control por cada uno de los dominios. Una vez analizado los 114 controles, se podrá observar de mejor manera los resultados a través del diagrama radar, en el cual se plasmarán tanto los resultados obtenidos cuando se levantó la información inicial, los resultados actuales obtenidos luego de haber realizado el análisis de riesgos y ejecutado cada uno de los proyectos implementados para reducir los riesgos en cada uno de los activos.

A continuación, se describe el porcentaje de efectividad en cada uno de los 114 controles detallando al dominio que corresponde y os objetivos de control planteados por cada uno de los 14 dominios.

[5] Políticas de seguridad de la información

Objetivo

- Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.

Tabla 33 Controles del dominio Políticas de seguridad de la información

CONTROL	Efectividad	CMM
[5] Políticas de seguridad de la información	**100%**	**L5**
[5.1] Directrices de gestión de la seguridad de la información	100%	
[5.1.1] Políticas para la seguridad de la información	100%	
[5.1.2] Revisión de las políticas para la seguridad de la información	100%	

[6] Organización de la seguridad de la información

Objetivos:

- Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización

- Garantizar la seguridad del teletrabajo y en el uso de los dispositivos móviles.

Tabla 34 Controles del dominio Organización de la seguridad de la información

CONTROL	Efectividad	CMM
[6] Organización de la seguridad de la información	**91,2%**	**L3**
[6.1] Organización interna.	**90%**	**L3**
[6.1.1] Roles y responsabilidades en seguridad de la información	90%	
[6.1.2] Segregación de tareas	90%	
[6.1.3] Contacto con las autoridades	90%	
[6.1.4] Contacto con grupos de interés especial	90%	
[6.1.5] Seguridad de la información en la gestión de proyectos	90%	
[6.2] Los dispositivos móviles y el teletrabajo	**92,5%**	**L3**
[6.2.1] Política de dispositivos móviles	95%	
[6.2.2] Teletrabajo	90%	

[7] Seguridad relativa a los recursos humanos

Objetivos

- Garantizar que los empleados y los contratistas entiendan sus responsabilidades y son las personas idóneas para desempeñar las funciones para las que han sido considerados.

- Garantizar que todos los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.

- Proteger los intereses de la empresa ante el cambio o finalización de un contrato, relaciones laborales o comerciales de empleados y subcontratistas.

Tabla 35 Controles del dominio Seguridad relativa a los recursos humanos

CONTROL	Efectividad	CMM
[7] Seguridad relativa a los recursos humanos	**97,2%**	**L4**
[7.1] Antes del empleo	**100%**	
[7.1.1] Investigación de antecedentes	100%	
[7.1.2] Términos y condiciones del empleo	100%	
[7.2] Durante el empleo	**96,6%**	**L4**
[7.2.1] Responsabilidades de gestión	95%	
[7.2.2] Concienciación, educación y capacitación en seguridad de la información	100%	
[7.2.3] Proceso disciplinario	95%	
[7.3] Finalización del empleo o cambio en el puesto de trabajo	**95%**	**L4**
[7.3.1] Responsabilidades ante la finalización o cambio	95%	

[8] Gestión de activos

Objetivos

- Identificar los activos de la ISP y definir las responsabilidades adecuadas por cada uno de los activos.

- Tratar la información con el nivel más adecuado de protección considerando el grado de relevancia para la ISP

- Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en los diferentes soportes.

Tabla 36 Controles del dominio Gestión de activos

CONTROL	Efectividad	CMM
[8] Gestión de activos	**90,5%**	**L3**
[8.1] Responsabilidad sobre los activos	**90%**	**L3**
[8.1.1] Inventario de activos	90%	
[8.1.2] Propiedad de los activos	90%	
[8.1.3] Uso aceptable de los activos	90%	
[8.1.4] Devolución de activos	95%	
[8.2] Clasificación de la información	**90%**	**L3**

[8.2.1] Clasificación de la información	90%	
[8.2.2] Etiquetado de la información	90%	
[8.2.3] Manipulado de la información	90%	
[8.3] Manipulación de los soportes	**91,6%**	**L3**
[8.3.1] Gestión de soportes extraíbles	90%	
[8.3.2] Eliminación de soportes	95%	
[8.3.3] Soportes físicos en tránsito	90%	

[9] Control de acceso

Objetivos

- Limitar y controlar el acceso a los recursos y a la información.
- Garantizar el acceso solo a los usuarios autorizados, así como la protección de la información, los sistemas y los servicios de usuarios no autorizados
- Disponer responsabilidades a cada uno de los usuarios con el fin de cuidar y salvaguardar la información de autenticación.
- Prevenir el acceso a los sistemas y aplicaciones controlando el acceso al personal autorizado por la ISP.

Tabla 37 Controles del dominio Control de acceso

CONTROL	Efectividad	CMM
[9] Control de acceso	**90%**	**L3**
[9.1] Requisitos de negocio para el control de acceso	**90%**	**L3**
[9.1.1] Política de control de acceso	90%	
[9.1.2] Acceso a las redes y a los servicios de red	90%	
[9.2] Gestión de acceso de usuario	**90%**	**L3**
[9.2.1] Registro y baja de usuario	90%	
[9.2.2] Provisión de acceso de usuario	90%	
[9.2.3] Gestión de privilegios de acceso	90%	
[9.2.4] Gestión de la información secreta de autenticación de usuarios	90%	
[9.2.5] Revisión de los derechos de acceso de usuario	90%	
[9.2.6] Retirada o reasignación de los derechos de acceso	90%	
[9.3] Responsabilidades del usuario	**90%**	**L3**
[9.3.1] Uso de la información secreta de autenticación	90%	

[9.4] Control de acceso a sistemas y aplicaciones	**90%**	**L3**
[9.4.1] Restricción del acceso a la información	90%	
[9.4.2] Procedimientos seguros de inicio de sesión	90%	
[9.4.3] Sistema de gestión de contraseñas	90%	
[9.4.4] Uso de utilidades con privilegios de sistemas	90%	
[9.4.5] Control de acceso al código fuente de los programas	90%	

[10] Criptografía

Objetivo:

- Garantizar un uso adecuado y eficaz de la criptografía para proteger los principios de seguridad: confidencialidad, autenticidad y/o integridad de la información.

Tabla 38 Controles del dominio Criptografía

CONTROL	Efectividad	CMM
[10] Criptografía	**90%**	**L3**
[10.1] Controles criptográficos	**90%**	**L3**
[10.1.1] Política de uso de los controles criptográficos	90%	
[10.1.2] Gestión de claves	90%	

[11] Seguridad física y entorno

Objetivos

- Prevenir el acceso físico no autorizado, así como los daños y la interferencia a la información de la organización y a los recursos de tratamiento de la información.

- Garantizar la seguridad de los activos protegiéndolos contra daños o robo con el fin de evitar interrupciones de la organización.

Tabla 39 Controles del dominio Seguridad física y entorno

CONTROL	Efectividad	CMM
[11] Seguridad física y del entorno	**90,5%**	**L3**
[11.1] Áreas seguras	**90%**	**L3**
[11.1.1] Perímetro de seguridad física	90%	
[11.1.2] Controles físicos de entrada	90%	
[11.1.3] Seguridad de oficinas, despachos y recursos	90%	

[11.1.4] Protección contra las amenazas externas y ambientales	90%	
[11.1.5] El trabajo en áreas seguras	90%	
[11.1.6] Áreas de carga y descarga	90%	
[11.2] Seguridad de los equipos	**91,1%**	**L3**
[11.2.1] Emplazamiento y protección de equipos	90%	
[11.2.2] Instalaciones de suministro	90%	
[11.2.3] Seguridad del cableado	95%	
[11.2.4] Mantenimiento de los equipos	90%	
[11.2.5] Retirada de materiales propiedad de la empresa	90%	
[11.2.6] Seguridad de los equipos fuera de las instalaciones	90%	
[11.2.7] Reutilización o eliminación segura de equipos	90%	
[11.2.8] Equipo de usuario desatendido	90%	
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia	95%	

[12] Seguridad de operaciones

Objetivos

- Asegurar la seguridad de las instalaciones en donde se trata la información, así como el correcto funcionamiento de todos los procedimientos.
- Salvaguardar la información y los recursos de tratamiento de información de software malicioso (malware).
- Evitar la pérdida de datos aplicando copias de seguridad.
- Realizar los registros de eventos y generar las evidencias correspondientes.
- Asegurar la integridad del software en explotación.
- Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.
- Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

Tabla 40 Controles del dominio Seguridad de operaciones

CONTROL	Efectividad	CMM
[12] Seguridad de las operaciones	**87,14%**	**L2**
[12.1] Procedimientos y responsabilidades operacionales	**90%**	
12.1.1 Documentación de procedimientos de operación	90%	
12.1.2 Gestión de cambios	90%	
12.1.3 Gestión de capacidades	90%	
12.1.4 Separación de los recursos de desarrollo, prueba y operación	90%	
[12.2] Protección contra el software malicioso (malware)	**90%**	
12.2.1 Controles contra el código malicioso	90%	
[12.3] Copias de seguridad	**90%**	
12.3.1 Copias de seguridad de la información	90%	
[12.4] Registros y supervisión	**90%**	
12.4.1 Registro de eventos	90%	
12.4.2 Protección de la información de registro	90%	
12.4.3 Registros de administración y operación	90%	
12.4.4 Sincronización del reloj	90%	
[12.5] Control del software en explotación	**90%**	
12.5.1 Instalación del software en explotación	90%	
[12.6] Gestión de la vulnerabilidad técnica	**70%**	
12.6.1 Gestión de las vulnerabilidades técnicas	50%	
12.6.2 Restricción en la instalación de software	90%	
[12.7] Consideraciones sobre la auditoria de sistemas de información	**90%**	
12.7.1 Controles de auditoria de sistemas de información	90%	

[13] Seguridad de las comunicaciones

Objetivos

- Proteger la información en las redes al igual que los recursos de tratamiento de la información.
- El mantener la seguridad de la información que se transfiere dentro de la ISP, así como con entidades externas.

Tabla 41 Controles del dominio Seguridad de las comunicaciones

CONTROL	Efectividad	CMM
[13] Seguridad de las comunicaciones	**90%**	**L3**
[13.1] Gestión de la seguridad de las redes	**90%**	
[13.1.1] Controles de red	90%	
[13.1.2] Seguridad de los servicios de red	90%	
[13.1.3] Segregación en redes	90%	
[13.2] Intercambio de información	**90%**	**L3**
[13.2.1] Políticas y procedimientos de intercambio de información	90%	
[13.2.2] Acuerdos de intercambio de información	90%	
[13.2.3] Mensajería electrónica	90%	
[13.2.4] Acuerdos de confidencialidad o no revelación	90%	

[14] Adquisición, desarrollo y mantenimiento de los sistemas de información

Objetivos

- Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

- Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.

- Garantizar la protección selección y control de los datos de pruebas.

Tabla 42 Controles del dominio Adquisición, desarrollo y mantenimiento de los sistemas de información

CONTROL	Efectividad	CMM
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información	**85,5%**	**L2**
[14.1] Requisitos de seguridad en los sistemas de información	**90%**	
[14.1.1] Análisis de requisitos y especificaciones de seguridad de la información	90%	
[14.1.2] Asegurar los servicios de aplicaciones en redes públicas	90%	
[14.1.3] Protección de las transacciones de servicios de aplicaciones	90%	
[14.2] Seguridad en el desarrollo y en los procesos de soporte	**76,6%**	
[14.2.1] Política de desarrollo seguro	90%	

[14.2.2] Procedimiento de control de cambios en sistemas	90%	
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	90%	
[14.2.4] Restricciones a los cambios en los paquetes de software	90%	
[14.2.5] Principios de ingeniería de sistemas seguros	90%	
[14.2.6] Entorno de desarrollo seguro	50%	
[14.2.7] Externalización del desarrollo de software	50%	
[14.2.8] Pruebas funcionales de seguridad de sistemas	50%	
[14.2.9] Pruebas de aceptación de sistemas	90%	
[14.3] Datos de prueba	**90%**	
[14.3.1] Protección de los datos de prueba	90%	

[15] Relación con proveedores

Objetivos

- Garantizar la protección de los activos disponibles a de los proveedores.
- Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.

Tabla 43 Controles del dominio Relación con proveedores

CONTROL	Efectividad	CMM
[15] Relación con proveedores	**90%**	**L3**
[15.1] Seguridad en las relaciones con proveedores	**90%**	
[15.1.1] Política de seguridad de la información en las relaciones con los proveedores	90%	
[15.1.2] Requisitos de seguridad en contratos con terceros	90%	
[15.1.3] Cadena de suministro de tecnología de la información y de las comunicaciones	90%	
[15.2] Gestión de la provisión de servicios del proveedor	**90%**	
[15.2.1] Control y revisión de la provisión de servicios del proveedor	90%	
[15.2.2] Gestión de cambios en la provisión del servicio del proveedor	90%	

[16] Gestión de incidentes de seguridad de la información

Objetivo

Garantizar eficacia y coherencia en la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

Tabla 44 Controles del dominio Gestión de incidentes de seguridad de la información

CONTROL	Efectividad	CMM
[16] Gestión de incidentes de seguridad de la información	**92,1%**	**L3**
[16.1] Gestión de incidentes de seguridad de la información y mejoras	**92,1%**	
[16.1.1] Responsabilidades y procedimientos	95%	
[16.1.2] Notificación de los eventos de seguridad de la información	90%	
[16.1.3] Notificación de puntos débiles de la seguridad	90%	
[16.1.4] Evaluación y decisión sobre los eventos de seguridad de información	90%	
[16.1.5] Respuesta a incidentes de seguridad de la información	95%	
[16.1.6] Aprendizaje de los incidentes de seguridad de la información	90%	
[16.1.7] Recopilación de evidencias	95%	

[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio

Objetivos

Gestionar la continuidad de la seguridad de la información para que forme parte de los sistemas de gestión de continuidad del negocio de la ISP.

Asegurar los requisitos de disponibilidad de los recursos de tratamiento de la información con la implementación de las redundancias.

Tabla 45 Controles del dominio Aspectos de seguridad de la información para la gestión de la continuidad del negocio

CONTROL	Efectividad	CMM
[17] Aspectos de seguridad de la información para la gestión de la continuidad de negocio	**80%**	**L2**
[17.1] Continuidad de la seguridad de la información	**90%**	
[17.1.1] Planificación de la continuidad de la seguridad de la información	90%	
[17.1.2] Implementar la continuidad de la seguridad de la información	90%	

[17.1.3] Verificación, revisión y evaluación de la continuidad de la seguridad de la información	90%	
[17.2] Redundancias	**70%**	
[17.2.1] Disponibilidad de los recursos de tratamiento de la información	70%	

[18] Cumplimiento

Objetivos

- Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

- Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

Tabla 46 Controles del dominio Cumplimiento

CONTROL	Efectividad	CMM
[18] Cumplimiento	**90,5%**	**L3**
[18.1] Cumplimiento de los requisitos legales y contractuales	**91%**	
[18.1.1] Identificación de la legislación aplicable y de los requisitos contractuales	90%	
[18.1.2] Derechos de propiedad intelectual (DPI)	90%	
[18.1.3]Protección de los registros de la organización	90%	
[18.1.4] Protección y privacidad de la información de carácter personal	95%	
[18.1.5] Regulación de los controles criptográficos	90%	
[18.2] Revisiones de la seguridad de la información	**90%**	
[18.2.1] Revisión independiente de la seguridad de la información	90%	
[18.2.2] Cumplimiento de las políticas y normas de seguridad	90%	
[18.2.3] Comprobación del cumplimiento técnico	90%	

5.4. Presentación de resultados

Se puede observar una comparación entre el estado inicial, el estado actual o final una vez realizado el procedimiento de auditoría y el estado deseado o esperado para el Sistema de Gestión de la Seguridad de la información. Una vez realizada la evaluación de madurez de la seguridad, se recogen los datos en la tabla 47, de los resultados obtenidos al inicio del estudio realizado en la ISP (datos de la tabla 3) y los datos finales analizados (datos de la tabla 32) para poder visualizar de mejor manera la evolución.

Tabla 47 Porcentaje de efectividad de los requerimientos ISO 27001 inicial y final

Requerimientos ISO/IEC 27001:2013	% de efectividad inicial	% de efectividad final
4. Contexto de la organización	5	96,2
5. Liderazgo	6,7	98,3
6. Planificación	5	95
7. Soporte	5	92,5
8. Operación	0	93,3
9. Evaluación del desempeño	3,3	98,3
10. Mejora	5	92,5

La ilustración 15 presenta el diagrama de radar del nivel de cumplimiento de cada uno de los apartados de la norma 27001.

Ilustración 15 Diagrama radar de los requerimientos ISO/IEC 27001:2013

Como se puede observar en el gráfico, inicialmente la ISP no contaba con conocimientos relacionados a la seguridad, solo se seguían algunos procedimientos no formales que los realizaban los empleados por su propia iniciativa. Por esta razón el % de efectividad inicial en todos los dominios estuvo menor al 10% ubicándose en el nivel L0, según la escala del Modelo de Madurez de la Capacidad (CMM) es decir inexistente con carencia total de cualquier proceso reconocible.3

Al igual que se recogieron los datos de la tabla 46, con los resultados iniciales y finales para observar mejor la evolución de los apartados de la norma 27001, en la siguiente tabla 47, se recogen los resultados del análisis inicial por cada uno de los dominios (tabla 4) y los datos por cada dominio finales (tablas de la 33 a la 46) para poder ver la evolución de los controles tanto en porcentaje de efectividad, así como referente al valor CMM.

Tabla 48 Porcentaje de efectividad de los dominios de la ISO 27002 inicial y final

Controles	Resultados iniciales		Resultados finales	
	Efectividad	CMM	Efectividad	CMM
5. Políticas de seguridad de la	0%	L0	100%	L5

información				
6. Organización de la seguridad de la información	**13,5%**	**L1**	**91,2%**	**L3**
7. Seguridad relativa a los recursos humanos	**16,7%**	**L1**	**97,2%**	**L4**
8. Gestión de activos	**20%**	**L1**	**90,5%**	**L3**
9. Control de acceso	**30,3%**	**L1**	**90%**	**L3**
10. Criptografía	**10%**	**L1**	**90%**	**L3**
11. Seguridad física y del entorno	**45,5%**	**L1**	**90,5%**	**L3**
12. Seguridad de las operaciones	**35,3%**	**L1**	**87,14%**	**L2**
13. Seguridad de las comunicaciones	**39,1%**	**L1**	**90%**	**L3**
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**35,5%**	**L1**	**85,5%**	**L2**
15. Relación con proveedores	**45%**	**L1**	**90%**	**L3**
16. Gestión de incidentes de seguridad de la información	**11,4%**	**L1**	**92,1%**	**L3**
17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	**20%**	**L1**	**80%**	**L2**
18. Cumplimiento	**9%**	**L1**	**90,5%**	**L3**

En la ilustración 16 se presentan los resultados de manera gráfica a través del diagrama de radar donde se pueden diferenciar los porcentajes de efectividad por cada uno de los dominios tanto iniciales, finales y deseados.

Ilustración 16 Diagrama radar de los Dominios ISO/IEC 27002:2013

Podemos ver el giro total que dio la ISP en cuanto a la seguridad de la información, luego de no contar con ningún conocimiento ni desarrollo de

documentación de procesos, procedimientos o políticas, en la revisión actual de cumplimiento se puede ver una gran evolución en cada uno de los controles que afecta de manera directa la evolución de los 14 dominios.

En la tabla 49 se encuentra el nivel de madurez con la cantidad de controles que se encuentran dentro de cada nivel. Aunque el 83% se encuentra en el nivel definido, y un pequeño porcentaje entre el gestionado y optimizado; se detectaron 4 controles se encuentran en el nivel de madurez de L2– reproducible, lo que quiere decir que está con un 50% de efectividad y que se catalogaron como no conformidades menores que deben ser corregidas

Tabla 49 Madurez CMM de los controles ISO

L0 - Inexistente	0
L1 - Inicial / Ad-hoc	0
L2 - Reproducible	4
L3 - Definido	95
L4 - Gestionado	10
L5 - Optimizado	5
total	114

En la ilustración 17, se puede observar de manera gráfica la evaluación del nivel de madurez porcentual de cada uno de los 114 controles.

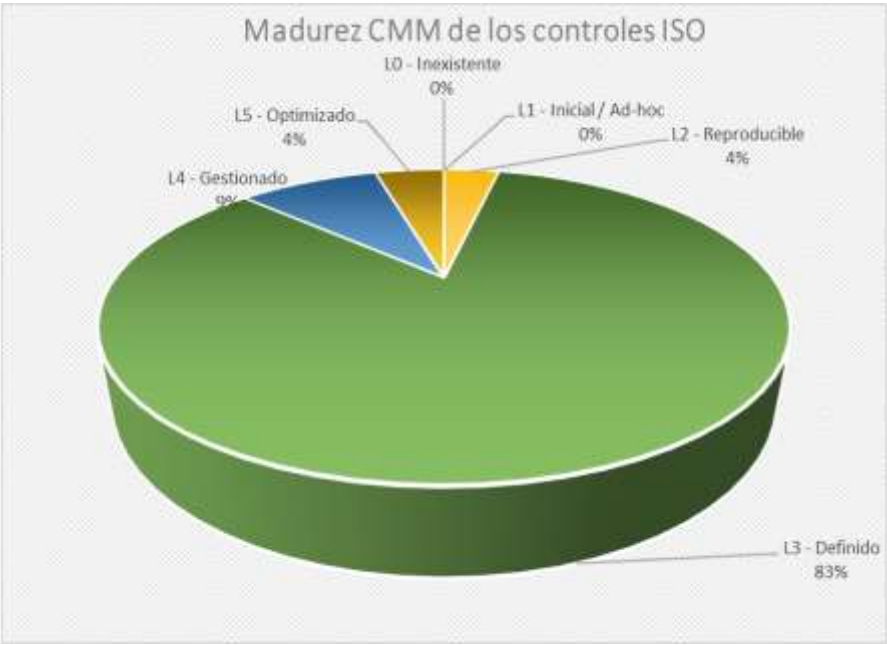

Ilustración 17 Madurez CMM de los controles ISO

5.5 Informe de auditoría interna

A partir de la plantilla propuesta en el punto 5.2 del procedimiento de auditorías internas del anexo 10.2 se realiza el siguiente informe con los resultados obtenidos en la primera auditoría de la ISP.

- Fecha: 30 de noviembre del 2020

- Nombre de los integrantes del equipo Auditor:
  - Auditor jefe: José Ruiz

- Área auditada

  Todas las áreas

- Alcance

  Todos los procedimientos, procesos, indicadores y controles de seguridad que manejan los activos relevantes de la ISP, respecto a la manipulación, transmisión o almacenamiento de la información.

- Objetivo

  Evaluar los 114 controles especificados en las buenas prácticas de la norma ISO 27002:2013 de la ISP con el fin de establecer el nivel de madurez del SGSI.

- Controles auditados

  Los 114 controles de los 14 dominios

  En este apartado se van a exponer los resultados de la auditoría. Se clasificaron los resultados en conformidades y no conformidades. Dentro de las no conformidades también se clasificará en no conformidad mayor o menor dependiendo del grado de incumplimiento alto o menor. Por último, si no se encuentra no conformidades, se realizarán observaciones para mejorar el SGSI

- No conformidades

Tabla 50 No conformidad No.1

ID	001
Tipo	No conformidad menor
Dominio	[12] Seguridad de las operaciones

Control	[12.6.1] Gestión de las vulnerabilidades técnicas
Descripción	No está definida la persona que debe gestionar las vulnerabilidades técnicas, como el grupo de trabajo es muy pequeño y la parte técnica está conformado en su mayoría por personal técnico y tecnólogo, es decir por pocos ingenieros, solo el jefe técnico tiene la formación adecuada, pero está con otras responsabilidades.
Acciones correctivas	Debe contratarse entre el personal técnico una persona mas con el grado de ingeniería o que demuestre experiencia técnica con el fin de no cargar con toda la responsabilidad al jefe técnico.
Responsable	Jefe técnico - jefe de seguridad

Tabla 51 No conformidad No.2

ID	**002**
Tipo	No conformidad menor
Dominio	[14] Adquisición, desarrollo y mantenimiento de los sistemas de información
Control	[14.2.6] Entorno de desarrollo seguro
Descripción	La ISP tiene definida la zona de desarrollo seguro, aunque al momento no es utilizada porque no ofrecen ningún servicio relacionado a este servicio. Sin embargo, por lo que no es utilizada esta pequeña área, puede ser un acceso a personal no autorizado y no hay vigilancia de ningún tipo.
Acciones correctivas	Implementar controles de acceso a esta zona
Responsable	**Gerente general**

Tabla 52 No conformidad No.3

ID	**003**
Tipo	No conformidad menor
Dominio	[14] Adquisición, desarrollo y mantenimiento de los sistemas de información
Control	[14.2.7] Externalización del desarrollo de software
Descripción	No se ha realizado alguna supervisión porque aún no se subcontrata servicios externalizados, sin embargo, tampoco se ha desarrollado ningún procedimiento con el fin de estar preparados en caso de que se empiece con este proceso.

Acciones correctivas	Generar la documentación correspondiente a este proceso siguiendo las directrices de las buenas prácticas de la norma ISO/IEC 27002:2013
Responsable	Jefe de seguridad

Tabla 53 No conformidad No.4

ID	**004**
Tipo	No conformidad menor
Dominio	[14] Adquisición, desarrollo y mantenimiento de los sistemas de información
Control	[14.2.8] Pruebas funcionales de seguridad de sistemas
Descripción	No se dispone de algún programa detallado con las actividades a realizar para comprobar las condiciones ene l caso de probar sistemas nuevos o actualizados.
Acciones correctivas	Realizar los pasos a realizar en el caso de verificar el funcionamiento de los procesos
Responsable	Jefe técnico

- Conclusiones

  - Se está realizando los controles pertinentes sobre cada activo y el nivel encontrado a lo largo de la evaluación de cada uno de los controles ha sido buen.

  - Cabe destacar que las capacitaciones ayudan de manera significativa a la concienciación con respecto a los procedimientos que se deben desarrollar para llegar al nivel máximo de compromiso.

  - Se deben implementar las acciones correctivas para la siguiente auditoría y cumplir con cada uno de los requisitos de los controles con el fin de subir progresivamente al siguiente nivel de gestionado y que al final de los 3 años el nivel de madurez se establezca en el nivel optimizado.

- Recomendaciones

  - Se recomienda implementar más indicadores de control para poder revisar estadísticamente los cambios a favor o en contra de cada proceso implantado.

- Se recomienda capacitar al personal no solo en cursos básicos de seguridad de la información sino también en capacitaciones de más alto nivel como diplomados.

- Se recomienda realizar simulacros de ataques con el fin de evaluar el nivel de respuesta a incidentes y respuesta del personal ante cualquier situación.

6. Presentación de resultados y entrega de informes

En cada capítulo desarrollado a lo largo de este trabajo final se realizó paso a paso las etapas necesarias para el Sistema de Gestión de Seguridad de la Información de la ISP. En esta última fase se presentan los documentos generados con el fin de presentarle a la dirección los resultados del trabajo realizado para una mayor comprensión de los directivos.

Los documentos que complementan la presente memoria del Trabajo Final de Máster realizados se encuentran adjuntos y son: a) Presentación dirigida a la alta dirección de la ISP, b) Video presentación con las fases desarrolladas a lo largo del trabajo y c) presentación de la etapa de análisis de riesgos.

7. Conclusiones

- A través de cada etapa se establecieron todos los lineamientos pertinentes de seguridad de la información que garantizan no solo los principios básicos de confidencialidad integridad y disponibilidad, sino además la trazabilidad y autenticidad por cada uno de los activos de la ISP.

- La etapa del análisis de riesgos permitió valorar y evaluar cada uno de los activos de la ISP tanto los necesarios para proveer los servicios de internet, así como los utilizados en la ejecución de las tareas para el correcto funcionamiento del giro del negocio de la ISP, con un análisis detallado de las amenazas a las que se encuentran expuestos los activos.

- Al finalizar el proceso de análisis de riesgos se evidenció el tipo de amenazas más críticas para poder tomar las decisiones adecuadas que permitieron elaborar cada uno de los proyectos necesarios para reducir el nivel de riesgo.

- La dirección juega un papel muy importante en el desarrollo del SGSI ya que su responsabilidad tanto para la aprobación de la política de seguridad como para la supervisión de la ejecución del SGSI determina el éxito de la implantación.

- Aunque se implementaron controles de seguridad guiados de la norma ISO/IEC 27002/2013 el mayor porcentaje de nivel de madurez al que se llegó fue el L3 de proceso definido, debido a que los niveles más altos de madurez requieren de más indicadores que permitan monitorizar la eficiencia.

- La importancia de la capacitación del personal de la ISP en cuestión a la seguridad de la información permite mayor conciencia y mejor respuesta ante incidentes de seguridad lo que resulta en un incremento tanto en la eficiencia como en la eficacia del SGSI.

- En el caso de querer la certificación de la norma debe mejorarse el proceso de mejora continua a través de la auditoría, ya que es un requisito para realizar el proceso.

- Las auditorias resultan imprescindibles para la mejora continua del sistema de gestión de la seguridad de la información.

- La gestión documental es un proceso muy necesario, no solo como requisito de la norma sino porque el tener desarrolladas normativas y procedimientos con los que puede contar tanto el personal interno como externo permite reducir los tiempos en la gestión del servicio, tanto en la atención que requiere el cliente en instalación como en la solución a los

incidentes que se puedan presentar tanto de seguridad como de prestación como tal del servicio.

- El desarrollo del protocolo para el buen uso de los suministros en los procesos de instalación no se evidencia como tal, sin embargo, se abordó este tema dentro del diseño de las capacitaciones al personal.

- La metodología de MAGERIT resulta ser una guía ideal para el desarrollo del análisis y gestión de riesgos gracias a la clasificación generalizada tanto de los activos como de las amenazas y salvaguardas haciendo que el proceso sea mucho más rápido de realizar, teniendo en cuenta que el factor tiempo es un recurso que debe aprovecharse para dar soluciones a empresas que requieren de servicios de consultoría en Sistemas de Gestión de la Seguridad de la Información.

- Una vez se ejecuten todos los procesos desarrollados a lo largo de este TFM se espera poder ampliar el catálogo de servicios para solicitar los permisos necesarios tanto a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) como al ministerio de telecomunicaciones de Ecuador (MINTEL). Al igual que en un plazo no mayor a dos años cumplir con los requisitos para ampliar la zona de cobertura en toda la región norte del Ecuador.

Como trabajos futuros

- Realizar una propuesta con tantos indicadores como controles hay de la norma, que permitan incrementar el nivel de madurez en cada dominio teniendo como objetivo el nivel L5 (Optimizado).

- Realizar un seguimiento de las 3 auditorías anuales planificadas en el procedimiento de auditorías internas con el fin de evaluar el nivel de madurez de cada uno de los requerimientos de la norma ISO/IEC 27001 y el cumplimiento de cada uno de los 114 controles de la norma ISO/IEC 27002, con el fin de renovar la certificación en caso de que la empresa decida implementar el SGSI propuesto.

.

8. Glosario

Activo: Recurso que genera, procesa, transporta y/o protege datos necesarios para los procedimientos que conllevan al cumplimiento de los objetivos de la organización

Amenazas: Eventos a los que están expuestos los activos que pueden perjudicar a la organización.

Análisis de riesgos: Procedimiento que permite estimar la magnitud de los riesgos a la que se encuentra expuesta una organización

Auditoría: Es un proceso ejecutado por un auditor, que tiene la característica de ser sistemático, independiente y documentado, y que busca obtener a partir de la realización de pruebas de auditoría registros, declaraciones de hechos u otra información conocida como evidencias de auditoría. (Quesada)

Confidencialidad: Propiedad que garantiza que la información no se difunda a personas no autorizadas. (Rubio, 2020)

Declaración de aplicabilidad: Proceso en el cual se indica si a partir de un conjunto de salvaguardas son de aplicación al sistema de información o si por el contrario no se requieren, siempre y cuando se justifique el por qué se necesitan o por qué no.

Disponibilidad: Característica, calidad o condición de la información de encontrarse a disposición de quienes tienen que acceder a ella, sean personas, procesos o aplicaciones. (Rubio, 2020).

Documentos de entrada: Documentos generados en el transcurso de un año de implantación del sistema de gestión de la seguridad.

Documentos de salida: Documentos que se generan con los resultados luego de revisar cada uno de los documentos de entrada.

Equipo auditor: Equipo de personas que estará encargado de ejecutar el proyecto de auditoría, tanto para la revisión de las medidas de seguridad (auditoría de seguridad), como para la revisión de la correcta implantación de la normativa ISO/IEC 27001. (Quesada)

Evaluación de riesgo: Determinación de la importancia del riesgo que se obtiene a partir de la comparación del riesgo estimado con respecto a los criterios de riesgo dados.

Incidente de seguridad: es un acto malintencionado de un atacante cuando intenta evadir las restricciones de seguridad de un sistema informático para obtener información o causar un daño en el funcionamiento de los procesos de una organización.

Indicador: Característica específica, observable y medible que se compara respecto a una referencia.

Información: Activo esencial para el negocio de una organización y que necesita ser protegido adecuadamente. (ISO/IEC17799)

Integridad: Propiedad que garantiza que la información no ha sido modificada. Los sistemas que ofrecen integridad permiten detectar si ha habido una modificación de la información. (Rubio, 2020)

Normativa: Conjunto de reglas establecidas en una organización para el cumplimiento de sus trabajadores.

Política: Conjunto de reglas y principios generales de carácter obligatorio en la ejecución de las actividades desarrolladas por los trabajadores de una organización.

Propietario del riesgo: persona con capacidades de toma de decisiones en relación con la gestión del riesgo.

Riesgos: estimación del grado de exposición al que se encuentra expuesto uno o más activos de que se materialice una amenaza causando un daño a la organización,

Seguridad de la información: Es la protección de la información en un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. (ISO/IEC17799)

Tratamiento del riesgo: proceso de selección y de implantación de medidas para modificar el riesgo.

Vulnerabilidad: debilidad que permite que una persona evada las restricciones de seguridad del sistema al que no tiene permisos de acceso.

9. Bibliografía

2014, N.-I. 2. (2014). *TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de.*

Alvarez, Z. (2016). *ISO/IEC 27001:2013 – SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.*

Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, & Will Robinson. (2008). *NIST Special Publication 800-55 Revision 1.* Gaithersburg.

ISO/IEC17799, E. I. (s.f.). *Tecnologia de la Información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la Información.*

públicas, M. d. (2012). *Magerit 3.0.* Madrid.

Quesada, R. E. (s.f.). *Introducción a la auditoría TIC y de seguridad TI.*

Rubio, J. M. (2020). *Riesgos, vulnerabilidades y amenazas.* Barcelona.

Sánchez, D. J. (2017). *NORMA ISO/IEC 27001 APLICADA A UNA CARRERA UNIVERSITARIA.* Santiago de Chile.

10. Anexos

10.1. Anexo Política de seguridad

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN			Logo ISP
Fecha de emisión: Octubre 2020	Versión: 1	Número de página: Página 1 de 8	

	Nombre/Cargo	Fecha	Firma
Elaborado por			
Revisado por			
Aprobado por			

Versión	Fecha	Ítem modificado	Descripción de la modificación

Contenido

1. Introducción
2. Objetivo
3. Alcance
4. Normativa de referencia
5. Descripción
   - 5.1 Responsabilidades
   - 5.2 Seguridad de la información
   - 5.3 Compromiso de la dirección
   - 5.4 Organización de la seguridad de la información
   - 5.5 Seguridad dad en el personal que se contrata, el que permanece y el desvinculado.
   - 5.6 gestión de activos
   - 5.7 Control de acceso
   - 5.8 Seguridad física
   - 5.9 Protección ante malware
   - 5.10 Copias de respaldo de información
   - 5.11 Gestión de vulnerabilidades
   - 5.12 Gestión de incidentes
   - 5.13 Continuidad del negocio
6. Cumplimiento de la norma
7. Penalización
8. Divulgación

1. Introducción

   La información es componente fundamental en el desarrollo de los objetivos definidos por la estrategia de la empresa, por esta razón resulta es necesario desarrollar una normativa donde se establezcan las reglas que aseguren la protección de los datos que se manejan en la empresa.

   El área asignada como responsable de velar por la seguridad de la información de la empresa se encargará de monitorizar constantemente el cumplimiento de la política y cada miembro de la empresa deberá cumplir con responsabilidad las reglas descritas en el presente documento.

   La política ha sido desarrollada conforme a los requisitos de la norma ISO/IEC 27001 para ser ejecutada en todas las actividades de la empresa por cada uno de los miembros tanto internos como personal externo con quien se mantenga algún tipo de relación comercial, laboral o que hagan uso de los activos de la empresa.

2. Objetivo

   Determinar el marco normativo que permita garantizar y proteger la información de la empresa preservando la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad y confiabilidad.

3. Alcance

   Las políticas definidas en el presente documento se aplican a todo el ámbito de la ISP, trabajadores, proveedores, y cualquier persona que mantenga una relación directa cualquier activo de la empresa.

4. Normativa de referencia

   - ISO/IEC 27001
   - Guía de buenas prácticas ISO/IEC 27001

5. Descripción

5.1 Responsabilidades

El área de seguridad de la información es el responsable de implementar, revisar, actualizar y monitorizar el cumplimiento de las normas, es responsable de cumplir cada regla señalada en este documento al igual que los demás miembros de la empresa.

5.2 Seguridad de la información

Se centra en proteger todos los datos no solo digitales sino también físicos con el fin de asegurar los 3 principios básicos de confidencialidad integridad y disponibilidad, independientemente de la forma en que se trate la información, es decir, como se maneje, procese o almacene. El objetivo principal es el de minimizar y gestionar los riesgos a los que se encuentra expuesta la organización para lo cual se han definido objetivos de seguridad que estén alienados al desarrollo de las actividades de la ISP.

5.3 Compromiso de la dirección

La gerencia general como ente principal de la dirección se compromete a promover el cumplimiento de la política, procedimientos y normativas que aseguran la correcta gestión de la seguridad de la información. Se compromete a asegurar la disponibilidad de los recursos necesarios en la implementación y seguimiento de las políticas, además a promover capacitaciones que conlleven a una conciencia respecto de la seguridad.

5.4 Organización de la seguridad de la información

5.4.1 Estructura organizacional

A través de la gestión de roles y responsabilidades se establecerá el esquema de seguridad, en este caso al ser una empresa pequeña se contará con el mismo comité de dirección para el comité de seguridad de la información.

5.4.2 Uso de dispositivos móviles y portátiles

Se proveerá de estos recursos al personal de la empresa con el fin de mejorar su desempeño en las labores de la empresa y así mismo se hará concienciación del buen uso de los equipos.

5.5 Seguridad en el personal que se contrata, el que permanece y el desvinculado.

La ISP dispondrá de los controles establecidos en la norma ISO/IEC 27001 con respecto a la contratación de nuevo personal asegurando que cumpla los perfiles que se requieran para el cargo solicitado. Con respecto al personal que se encuentra vinculado a la empresa se le proveerá de todos los recursos necesarios para su buen desempeño además de continuas capacitaciones referentes al tratamiento de la información y a la protección en general de los activos. Y por último se seguirá el debido procedimiento a la hora de desvincular algún empleado de la empresa de forma segura.

5.6 Gestión de activos

Cada activo tendrá un responsable y un custodio con el fin de cumplir con las directrices y asegurar el cumplimiento de las normativas y políticas establecidas en la protección de la información. Para realizar un correcto manejo de la información se contará con un sistema de clasificación bajo los lineamientos de la norma ISO/IEC 27001.

5.7 Control de acceso

El acceso a la red de la empresa debe cumplir con los controles respectivos de seguridad para lo cual se delega a cada responsable de área una buena administración de la plataforma tecnológica. Se establecerán usuarios y contraseñas para los equipos de las oficinas y que toda persona que mantenga una relación comercial con la empresa no pueda acceder ni a los equipos ni a la información que maneja cada uno de los miembros de la empresa. De la misma manera solo podrá administrar la red el personal técnico capacitado en este ámbito.

5.8 Seguridad Física

Tanto para la infraestructura como para los equipos utilizados en el desarrollo de las actividades del giro del negocio deberán estar debidamente aseguradas contra posibles amenazas tanto lógicas como físicas.

5.9 Protección ante malware

Se contará con las seguridades necesarias como antivirus, firewall entre otros mecanismos con el fin de asegurar la información de posibles ataques de software maliciosos.

5.10 Copias de respaldo de la información

Se establecerán mecanismos de copias de seguridad de la información más sensible con una periodicidad adecuada asegurando a la disponibilidad de la información.

5.11 Gestión de vulnerabilidades.

Se ejecutará constantemente una revisión y verificación de información respecto a nuevas vulnerabilidades que pudieran afectar los activos de la organización.

5.12 Gestión de incidentes de seguridad

Se proveerá el reporte de incidentes relacionados a la seguridad con responsables asignados para tratar estos eventos encargados de realizar un estudio detallado para dar una solución rápida y que evite la repetición del incidente en un futuro.

5.13 Continuidad del negocio

Se contará con un plan de contingencia en el caso de presentarse incidentes de mayor importancia que afecten la correcta prestación de los servicios de la ISP, de manera que se reestablezcan las operaciones lo más pronto posible y represente un nivel bajo de pérdida.

6. Cumplimiento de la norma

   Al estar en el nivel más alto de la pirámide jerárquica documental, se establecen directrices de manera general y al ser más establece no requerirá constantes revisiones por lo que se harán anualmente.

7. Penalización

   La presente normativa debe cumplirse a cabalidad, de no ser así se puede incurrir en una falta grave que será puesta a disposición del área gerencial.

8. Divulgación

   El conocimiento de esta normativa se divulgará a través del correo de la empresa.

9. Glosario

   Activo: Recurso que genera, procesa, transporta y/o protege datos necesarios para los procedimientos que conllevan al cumplimiento de los objetivos de la organización

   Amenazas: Eventos a los que están expuestos los activos que pueden perjudicar a la organización.

   Análisis de riesgos: Procedimiento que permite estimar la magnitud de los riesgos a la que se encuentra expuesta una organización

   Auditoría: Es un proceso ejecutado por un auditor, que tiene la característica de ser sistemático, independiente y documentado, y que busca obtener a partir de la realización de pruebas de auditoría registros, declaraciones de hechos u otra información conocida como evidencias de auditoría. (Quesada)

   Confidencialidad: Propiedad que garantiza que la información no se difunda a personas no autorizadas. (Rubio, 2020)

   Declaración de aplicabilidad: Proceso en el cual se indica si a partir de un conjunto de salvaguardas son de aplicación al sistema de información o si por el contrario no se requieren, siempre y cuando se justifique el por qué se necesitan o por qué no.

Disponibilidad: Característica, calidad o condición de la información de encontrarse a disposición de quienes tienen que acceder a ella, sean personas, procesos o aplicaciones. (Rubio, 2020).

Documentos de entrada: Documentos generados en el transcurso de un año de implantación del sistema de gestión de la seguridad.

Documentos de salida: Documentos que se generan con los resultados luego de revisar cada uno de los documentos de entrada.

Equipo auditor: Equipo de personas que estará encargado de ejecutar el proyecto de auditoría, tanto para la revisión de las medidas de seguridad (auditoría de seguridad), como para la revisión de la correcta implantación de la normativa ISO/IEC 27001. (Quesada)

Evaluación de riesgo: Determinación de la importancia del riesgo que se obtiene a partir de la comparación del riesgo estimado con respecto a los criterios de riesgo dados.

Incidente de seguridad: es un acto malintencionado de un atacante cuando intenta evadir las restricciones de seguridad de un sistema informático para obtener información o causar un daño en el funcionamiento de los procesos de una organización.

Indicador: Característica específica, observable y medible que se compara respecto a una referencia.

Información: Activo esencial para el negocio de una organización y que necesita ser protegido adecuadamente. (ISO/IEC17799)

Integridad: Propiedad que garantiza que la información no ha sido modificada. Los sistemas que ofrecen integridad permiten detectar si ha habido una modificación de la información. (Rubio, 2020)

Normativa: Conjunto de reglas establecidas en una organización para el cumplimiento de sus trabajadores.

Política: Conjunto de reglas y principios generales de carácter obligatorio en la ejecución de las actividades desarrolladas por los trabajadores de una organización.

Propietario del riesgo: persona con capacidades de toma de decisiones en relación con la gestión del riesgo.

Riesgos: estimación del grado de exposición al que se encuentra expuesto uno o más activos de que se materialice una amenaza causando un daño a la organización,

Seguridad de la información: Es la protección de la información en un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. (ISO/IEC17799)

Tratamiento del riesgo: proceso de selección y de implantación de medidas para modificar el riesgo.

Vulnerabilidad: debilidad que permite que una persona evada las restricciones de seguridad del sistema al que no tiene permisos de acceso.

10.2. Anexo Procedimiento de Auditorías Internas

PROCEDIMIENTO DE AUDITORÍAS INTERNAS			Logo ISP
Fecha de emisión: Octubre 2020	Versión: 1	Número de página: Página 1 de 12	

	Nombre/Cargo	Fecha	Firma
Elaborado por			
Revisado por			
Aprobado por			

Versión	Fecha	Ítem modificado	Descripción de la modificación

Contenido

1. Introducción
2. Objetivo
3. Alcance
4. Normativa de referencia
5. Descripción

5.1 Procedimiento de auditoría

5.1.1 Fase 1. Reunión de inicio

5.1.2 Fase 2. Ejecución de la auditoria

5.2 Modelo de informe

5.3 Requisitos para elección del auditor interno

5.4 Cronograma de auditorías

6. Cumplimiento de la norma
7. Penalización
8. Divulgación

1. Introducción

   Para verificar el correcto funcionamiento del sistema de gestión implantado se dispone de auditorías con el fin de evaluar el desempeño de los controles e indicadores de seguridad, el resultado de este procedimiento nos indicará una serie de resultados que servirán para analizar la situación de la seguridad en la empresa. Para esto se cuenta con un plan de auditoría que incluye auditorías internas y que en definitiva lo que se espera es que sea un procedimiento realizado con personal calificado para poder obtener resultados confiables.

2. Objetivo

   Realizar el procedimiento de auditorías internas siguiendo las directrices y los lineamientos de la norma ISO/IEC 19011, de la ISO/IEC 27001:2013 y la ISO/IEC 27007.

3. Alcance

   El procedimiento se aplica a todas las áreas de la ISP

4. Normativa de referencia

   - ISO/IEC 19011
   - ISO/IEC 27001:2013
   - ISO/IEC 27006

5. Descripción

   El proceso de auditorías internas forma parte de la tercera fase del ciclo Deming que se establece en la norma ISO/IEC 27001:2013. Como parte de la evaluación del desempeño, las auditorías internas forman parte del proceso de verificación del sistema de gestión de la seguridad de la información junto con la revisión de la dirección y el seguimiento, medición del análisis y evaluación.

5.1 Procedimiento de la auditoría

Para la ejecución de la auditoría se tendrá el siguiente procedimiento.

5.1.1 Fase 1. Reunión de inicio

a. Documento de compromiso por parte de la dirección (acuerdo de confidencialidad).

b. Carta de auditoría donde se encontrará lo siguiente

- Objetivo del plan
- Alcance:
- Establecimiento del tipo de pruebas y como se desarrollarán: Fechas con plazos temporales: inicio y fin de periodos de prueba, periodicidad del plan de auditoria.
- Procedimientos de comunicación entre el auditor y auditado, comunicación de inicio y fin de pruebas, informe de descubrimientos críticos de vulnerabilidades o protocolos.
- Material para entregar al finalizar la auditoria: informes, resultados de pruebas técnicas como anexos.
- Nivel de acceso a la información.

5.1.2 Fase 2. Ejecución de la auditoria

1. Recolección de información previa

- Información de los requisitos de la ISP
- Análisis de riesgos
- Leyes y regulaciones
- Estructura organizacional
- Políticas y procedimientos
- Entornos del tratamiento de la información
- Estudio realizado de las vulnerabilidades.
- Descripción de los controles establecidos
- Identificación de roles responsabilidades funciones y cargos

2. Ejecución de las pruebas de auditoría

- Revisión de la documentación de las pruebas: con objetivo de cada prueba siguiendo las políticas de la compañía, el modo en que se realizará cada prueba con su respectivo

procedimiento y técnicas de auditoría para comprobar los requisitos, y definición de las herramientas que se usarán.

- Entrevistas: al responsable de seguridad, responsable de revisión interna y responsable y comité de seguridad.

- Análisis de la información: se realizará paralelamente a la ejecución de las pruebas lo que permite planificar nuevas visitas o entrevistas que sean necesarias.

- Análisis del grado de no conformidad, desde el punto de vista en cuanto a las políticas y en cuanto a la información obtenida durante las pruebas realizadas. El análisis de los resultados estará enfocado en las vulnerabilidades y los controles de seguridad de esta manera el análisis de los resultados nos dará una visión del buen funcionamiento si son efectivos y eficientes los controles que han sido implantados

- Elaboración y presentación del informe: se realizará el informe final de auditoria que entregará las conclusiones obtenidas luego de analizar toda la documentación entregada por la cada área y luego de analizar todas las pruebas,

  Este documento tendrá la siguiente información:

- Un resumen ejecutivo, una visión general de la metodología empleada, fortalezas, debilidades, conclusiones y recomendaciones.
- Breve detalle de la metodología usada durante la auditoría.
- Estarán las entrevistas realizadas, las pruebas realizadas con sus respectivas herramientas y todo con las fechas de ejecución de cada procedimiento.
- Estará el listado detallado de todos los hallazgos con el problema que tienen, la política que incumple y todo lo que sirva para describirlo.
- Una evaluación del impacto
- Resultados de la auditoria
- Anexos con los resultados de las pruebas.

5.2 El modelo del informe de auditoría

Se seguirá la siguiente plantilla para la presentación del informe

a. Fecha
b. Nombre de los integrantes del equipo Auditor
c. Área auditada
d. Alcance
e. Objetivo
f. Controles auditados
g. No conformidades
h. Conclusiones
i. Recomendaciones
j. Anexos:
    - Carta de compromiso con acuerdo de confidencialidad)
    - Carta de auditoría (ítem b del apartado 5.1.1 del presente procedimiento de auditoría)

5.3 Requisitos para elección del auditor interno:

- Demostrar independencia de las actividades a ser auditadas con el fin de evitar conflictos de intereses.
- Tener conocimientos sobre los principios de auditoría, procedimientos y técnicas que aseguren realizar las auditorías de forma correcta
- Debe certificar la formación adecuada que demuestre conocimientos en revisión de la documentación del SGSI y revisión del análisis de riesgos de una organización.
- Certificados donde se demuestre haber auditado la implantación de un SGSI y de haber desarrollado los informes relativos a la auditoría en la que participó.
- Conocimientos específicos en el ámbito de la actividad auditada,
- Conocimientos de documentos de referencia y características de los sistemas de gestión y de control.
- Conocimiento de aspectos técnicos que le permitan entender el alcance de la auditoría y aplicar los criterios de auditoría.
- Capacidad para entender el modelo de negocio del auditado, su sector y las características sociales del mismo.
- Conocimiento de la legislación aplicable, reglamentos y otros requisitos relevantes a la disciplina.
- Acreditar experiencia profesional de cuatro años en el ámbito de las tecnologías de la información.

- Acreditar experiencia profesional por lo menos de dos años en seguridad de las tecnologías de la información.
- Tener capacidad para interactuar eficazmente con el auditado y trabajar conjuntamente.
- Ser perspicaz, ético, imparcial, sincero, honesto y discreto.
- Tener una actitud abierta y estar dispuesto a considerar ideas o puntos de vista alternativos.
- Ser observador, constante y activamente consciente de los entornos físicos y las actividades.
- Capacidad de adaptación a diferentes situaciones.
- Ser tenaz, persistente y orientado sobre la consecución de los objetivos.
- Tener poder de decisión, y utilizar el razonamiento lógico para analizar y llegar a conclusiones acertadas.

5.4 Cronograma de la auditoría

Las auditorías internas se realizarán en intervalos de una vez al año, abarcando la revisión de los 114 controles en el plazo máximo de tres años ya que debe quedar auditado el Sistema de Gestión de la Seguridad de la Información de forma completa. Se realizarán 3 auditorías a lo largo de los 3 años con el fin de cubrir los 114 controles. En la tabla se indica los 38 controles que se revisarán en el primer año, los siguientes 38 en el segundo año y los últimos 38 en el tercer año de modo que cada año se cumpla una revisión del 33,33% de todos los controles.

Tabla 54 Planificación de la revisión anual de los 114 controles

Control	Año 1	Año 2	Año 3
5.1.1 Políticas para la seguridad de la información	✔		
5.1.2 Revisión de las políticas para la seguridad de la información	✔		
6.1.1 Roles y responsabilidades en seguridad de la información	✔		
6.1.2 Segregación de tareas	✔		
6.1.3 Contacto con las autoridades	✔		
6.1.4 Contacto con grupos de interés especial	✔		
6.1.5 Seguridad de la información en la gestión de proyectos	✔		

6.2.1 Política de dispositivos móviles	✔		
6.2.2 Teletrabajo	✔		
7.1.1 Investigación de antecedentes	✔		
7.1.2 Términos y condiciones del empleo	✔		
7.2.1 Responsabilidades de gestión	✔		
7.2.2 Concienciación, educación y capacitación en seguridad de la información	✔		
7.2.3 Proceso disciplinario	✔		
7.3.1 Responsabilidades ante la finalización o cambio	✔		
8.1.1 Inventario de activos	✔		
8.1.2 Propiedad de los activos	✔		
8.1.3 Uso aceptable de los activos	✔		
8.1.4 Devolución de activos	✔		
8.2.1 Clasificación de la información	✔		
8.2.2 Etiquetado de la información	✔		
8.2.3 Manipulado de la información	✔		
8.3.1 Gestión de soportes extraíbles	✔		
8.3.2 Eliminación de soportes	✔		
8.3.3 Soportes físicos en tránsito	✔		
9.1.1 Política de control de acceso	✔		
9.1.2 Acceso a las redes y a los servicios de red	✔		
9.2.1 Registro y baja de usuario	✔		
9.2.2 Provisión de acceso de usuario	✔		
9.2.3 Gestión de privilegios de acceso	✔		
9.2.4 Gestión de la información secreta de autenticación de los usuarios	✔		
9.2.5 Revisión de los derechos de acceso de usuario	✔		
9.2.6 Retirada o reasignación de los derechos de acceso	✔		
9.3.1 Uso de la información secreta de autenticación	✔		
9.4.1 Restricción del acceso a la información	✔		
9.4.2 Procedimientos seguros de inicio de sesión	✔		

9.4.3 Sistema de gestión de contraseñas	✔		
9.4.4 Uso de utilidades con privilegios del sistema	✔		
9.4.5 Control de acceso al código fuente de los programas		✔	
10.1.1 Política de uso de los controles criptográficos		✔	
10.1.2 Gestión de claves		✔	
11.1.1 Perímetro de seguridad física		✔	
11.1.2 Controles físicos de entrada		✔	
11.1.3 Seguridad de oficinas, despachos y recursos		✔	
11.1.4 Protección contra las amenazas externas y ambientales		✔	
11.1.5 El trabajo en áreas seguras		✔	
11.1.6 Áreas de carga y descarga		✔	
11.2.1 Emplazamiento y protección de equipos		✔	
11.2.2 Instalaciones de suministro		✔	
11.2.3 Seguridad del cableado		✔	
11.2.4 Mantenimiento de los equipos		✔	
11.2.5 Retirada de materiales propiedad de la empresa		✔	
11.2.6 Seguridad de los equipos fuera de las instalaciones		✔	
11.2.7 Reutilización o eliminación segura de equipos		✔	
11.2.8 Equipo de usuario desatendido		✔	
11.2.9 Política de puesto de trabajo despejado y pantalla limpia		✔	
12.1.1 Documentación de procedimientos de las operaciones		✔	
12.1.2 Gestión de cambios		✔	
12.1.3 Gestión de capacidades		✔	
12.1.4 Separación de los recursos de desarrollo, prueba y operación		✔	
12.2.1 Controles contra el código malicioso		✔	
12.3.1 Copias de seguridad de la información		✔	
12.4.1 Registro de eventos		✔	

12.4.2 Protección de la información del registro		✔	
12.4.3 Registros de administración y operación		✔	
12.4.4 Sincronización del reloj		✔	
12.5.1 Instalación del software en explotación		✔	
12.6.1 Gestión de las vulnerabilidades técnicas		✔	
12.6.2 Restricción en la instalación de software		✔	
12.7.1 Controles de auditoría de sistemas de información		✔	
13.1.1 Controles de red		✔	
13.1.2 Seguridad de los servicios de red		✔	
13.1.3 Segregación en redes		✔	
13.2.1 Políticas y procedimientos de intercambio de información		✔	
13.2.2 Acuerdos de intercambio de información		✔	
13.2.3 Mensajería electrónica		✔	
13.2.4 Acuerdos de confidencialidad o no revelación			✔
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información			✔
14.1.2 Asegurar los servicios de aplicaciones en redes públicas			✔
14.1.3 Protección de las transacciones de servicios de aplicaciones			✔
14.2.1 Política de desarrollo seguro			✔
14.2.2 Procedimiento de control de cambios en sistemas			✔
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo			✔
14.2.4 Restricciones a los cambios en los paquetes de software			✔
14.2.5 Principios de ingeniería de sistemas seguros			✔

14.2.6 Entorno de desarrollo seguro			✔

PROCEDIMIENTO DE AUDITORÍAS INTERNAS			Logo ISP
Fecha de emisión: Octubre 2020	Versión: 1	Número de página: Página 11 de 12	

14.2.7 Externalización del desarrollo de software			✔
14.2.8 Pruebas funcionales de seguridad de sistemas			✔
14.2.9 Pruebas de aceptación de sistemas			✔
14.3.1 Protección de los datos de prueba			✔
15.1.1 Política de seguridad de la información en las relaciones con los proveedores			✔
15.1.2 Requisitos de seguridad en contratos con terceros			✔
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones			✔
15.2.1 Control y revisión de la provisión de servicios del proveedor			✔
15.2.2 Gestión de cambios en la provisión del servicio del proveedor			✔
16.1.1 Responsabilidades y procedimientos			✔
16.1.2 Notificación de los eventos de seguridad de la información			✔
16.1.3 Notificación de puntos débiles de la seguridad			✔
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información			✔
16.1.5 Respuesta a incidentes de seguridad de la información			✔
16.1.6 Aprendizaje de los incidentes de seguridad de la información			✔
16.1.7 Recopilación de evidencias			✔
17.1.1 Planificación de la continuidad de la seguridad de la información			✔
17.1.2 Implementar la continuidad de la seguridad de la información			✔
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información			✔
17.2.1 Disponibilidad de los recursos de tratamiento de la información			✔
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales			✔

18.1.2 Derechos de propiedad intelectual (DPI)			✔
18.1.3 Protección de los registros de la organización			✔

18.1.4 Protección y privacidad de la información de carácter personal			✔
18.1.5 Regulación de los controles criptográficos			✔
18.2.1 Revisión independiente de la seguridad de la información			✔
18.2.2 Cumplimiento de las políticas y normas de seguridad			✔
18.2.3 Comprobación del cumplimiento técnico			✔

6. Cumplimiento de la norma

   La ISP implementará de forma anual el programa de auditoria del SGSI, con el fin de evaluar los procedimientos, procesos, indicadores y controles de seguridad con el fin de verificar que se encuentren alineados a la norma 27001:2013

7. Penalización

   La presente normativa debe cumplirse a cabalidad, de no ser así se puede incurrir en una falta grave que será puesta a disposición del área gerencial.

8. Divulgación

   El conocimiento de esta normativa se divulgará a través del correo de la empresa.

10.3. Anexo Gestión de Indicadores

GESTIÓN DE INDICADORES			Logo ISP
Fecha de emisión: Octubre 2020	Versión: 1	Número de página: Página 1 de 5	

	Nombre/Cargo	Fecha	Firma
Elaborado por			
Revisado por			
Aprobado por			

Versión	Fecha	Ítem modificado	Descripción de la modificación

Contenido

1. Introducción
2. Objetivo
3. Alcance
4. Normativa de referencia
5. Descripción
6. Cumplimiento de la norma
7. Penalización
8. Divulgación

1. Introducción

   Es necesario definir indicadores que nos ayudan a medir la eficacia de los controles implantados en el sistema de gestión de la seguridad, esto ayuda a que haya una supervisión con datos actualizados acerca del funcionamiento de los controles de seguridad implantados en la empresa.

2. Objetivo

   Establecer los indicadores por cada control que se decida implantar en la organización.

3. Alcance

   Se aplica a todas las áreas en las que se implemente al menos un control de seguridad.

4. Normativa de referencia

   - NIST Special Publication 800-55 Revision 1 - Performance Measurement Guide for Information Security

5. Descripción

   Es importante definir una sistemática de medición de los controles de seguridad implantados en la empresa, ya que esto permitirá controlar el funcionamiento de las medidas de seguridad, la eficiencia y la eficacia de cada uno en periodos de tiempo definidos. El tener un sistema efectivo de controles implantados nos asegurará un sistema de gestión de la seguridad efectivo. A continuación, se describe los 12 componentes que definirán cada indicador implantado a partir de la plantilla propuesta en la norma. (Elizabeth Chew, y otros, 2008)

Tabla 55 Componentes para un indicador

Componente	Descripción
ID del indicador	Será un identificador único siguiendo la convención de nomenclatura definido por la empresa
Nombre del indicador	Será un nombre significativo que represente la medición que se va a realizar.
Descripción	Explicación de la finalidad del indicador.
Control de seguridad	Control de seguridad al cual se le realizara la medición.
Tipo	Clasificación del tipo de medida que pude ser implementación, efectividad / eficiencia o impacto.
Fórmula de medición	Fórmula utilizada para establecer la medición.
Umbral	Límite mínimo para verificar la satisfacción del control evaluado.
Unidades de medida	Unidad estandarizada definida para el cálculo.
Frecuencia de medición	Periodo de tiempo en el que se realiza cada medición del indicador.
Propietario de la Información	Área o persona responsable del reporte de la medida
Recopilador de la información	Persona responsable de recolectar los datos
Formato de la información	Tipo de formato en el que se entregará la medida

Tabla 56 Control Política de seguridad

Componente	Descripción
ID del indicador	I001
Nombre del indicador	Política de seguridad
Descripción	Indica si la política establecida por la organización, aprobada por la dirección y publicada para todos los empleados, se revisa en intervalos de tiempo o cuando ocurre un cambio significativo
Control de seguridad	5.1.2 Revisión de las políticas para la seguridad de la información
Tipo	Implementación
Fórmula de medición	Número de revisiones / 1 año
Unidades de medida	Número de revisiones
Umbral	Número de revisiones < 1
Frecuencia de medición	Anual

Propietario de la Información	Comité de dirección
Recopilador de la información	Auditor interno
Formato de la información	Documento de la política

Tabla 57 Indicador control Roles y responsabilidades

Componente	Descripción
ID del indicador	I002
Nombre del indicador	Custodios
Descripción	Medida de la eficacia del control de seguridad respecto a la asignación de un custodio por cada activo de la empresa
Control de seguridad	6.1.1 Roles y responsabilidades en seguridad de la información
Tipo	Implementación
Fórmula de medición	Número de activos con un responsable asignado sobre Número de activos totales de la empresa
Unidades de medida	Activos con custodio / activos totales
Umbral	90% de activos con custodios
Frecuencia de medición	Trimestral
Propietario de la Información	Responsable de seguridad
Recopilador de la información	Auditor interno
Formato de la información	Documentos de gestión de activos

Tabla 58 Control de capacitaciones del personal en seguridad de la información

Componente	Descripción
ID del indicador	I003
Nombre del indicador	Capacitaciones
Descripción	Indica la cantidad de empleados certificados con capacitaciones respecto a la seguridad de la información.
Control de seguridad	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Tipo	Implementación
Fórmula de medición	Empleados con certificación de haber recibido capacitación / Total empleados

Unidades de medida	Porcentaje de empleados certificados
Umbral	Porcentaje de empleados certificados < 85%
Frecuencia de medición	Semestral
Propietario de la Información	Recursos humanos
Recopilador de la información	Auditor interno
Formato de la información	Gráfico circular

Tabla 59 Control de Activos devueltos

Componente	Descripción
ID del indicador	I004
Nombre del indicador	Activos devueltos
Descripción	Indica las actas de entrega recepción de los activos pertenecientes a los empleados que ya no forman parte de la ISP por finalización de contrato y ya se les pagó la liquidación por la prestación de sus servicios
Control de seguridad	8.1.4 Devolución de activos
Tipo	Implementación
Fórmula de medición	Total, de documentos entrega-recepción de activos / Empleados que ya no trabajan en la empresa
Unidades de medida	Porcentaje de empleados con activos devueltos a la empresa
Umbral	Porcentaje de empleados con activos devueltos a la empresa < 95%
Frecuencia de medición	Trimestral
Propietario de la Información	Recursos humanos
Recopilador de la información	Auditor interno
Formato de la información	Gráfico circular

Tabla 60 Control eliminación de soportes

Componente	Descripción
ID del indicador	I005
Nombre del indicador	Eliminación de soportes
Descripción	Se verifican los procedimientos formales para la eliminación segura de soportes que ya no son necesarios
Control de seguridad	8.3.2 Eliminación de soportes
Tipo	Implementación
Fórmula de medición	Número de revisiones / año
Unidades de medida	Número de revisiones
Umbral	Número de revisiones < 1
Frecuencia de medición	Anual
Propietario de la Información	Responsable de seguridad de la información
Recopilador de la información	Auditor interno
Formato de la información	Documento procedimiento

Tabla 61 Eliminación de soportes

Componente	Descripción
ID del indicador	I006
Nombre del indicador	Cableado seguro
Descripción	Revisión de las protecciones frente a interceptaciones, interferencias o daños en el cableado eléctrico y de telecomunicaciones.
Control de seguridad	11.2.3 Seguridad del cableado
Tipo	Implementación
Fórmula de medición	Revisión de equipos de protección en el cableado
Unidades de medida	Tiene protección o no tiene protección
Umbral	No tiene protección
Frecuencia de medición	Semestral
Propietario de la Información	Responsable de seguridad de la información
Recopilador de la información	Auditor interno
Formato de la información	Inventario de protecciones instaladas

Tabla 62 Puesto de trabajo organizado

Componente	Descripción
ID del indicador	I007
Nombre del indicador	Puesto de trabajo organizado
Descripción	Se revisa si la Organización tiene definida y actualizada una política de puesto de trabajo despejado y pantalla limpia, así como las directrices.
Control de seguridad	11.2.9 Política de puesto de trabajo despejado y pantalla limpia
Tipo	Implementación
Fórmula de medición	Número de revisiones / año
Unidades de medida	Número de revisiones
Umbral	Número de revisiones < 1
Frecuencia de medición	Anual
Propietario de la Información	Comité de seguridad
Recopilador de la información	Auditor interno
Formato de la información	Documento de la Política de puesto de trabajo despejado y pantalla limpia

Tabla 63 Control en el procedimiento de recopilación de evidencias

Componente	Descripción
ID del indicador	I008
Nombre del indicador	Procedimiento recopilación de evidencias
Descripción	Se verifican los procedimientos para la identificación, recogida, adquisición y preservación de información que puede servir de evidencia.
Control de seguridad	16.1.7 Recopilación de evidencias
Tipo	Implementación
Fórmula de medición	Número de revisiones / año
Unidades de medida	Número de revisiones
Umbral	Número de revisiones < 1
Frecuencia de medición	Anual
Propietario de la Información	Responsable de seguridad
Recopilador de la	Auditor interno

información	
Formato de la información	Documentos de procedimientos de recopilación de evidencias.

Tabla 64 Incidentes de seguridad

Componente	Descripción
ID del indicador	I09
Nombre del indicador	Incidentes de seguridad
Descripción	Se revisa la cantidad de incidentes atendidos y solucionados con respecto a los reportados.
Control de seguridad	16.1.1 Responsabilidades y procedimientos 16.1.5 Respuesta a incidentes en seguridad de la información.
Tipo	Implementación
Fórmula de medición	Número de incidentes solucionados / Número de incidentes reportados.
Unidades de medida	Porcentaje de incidentes solucionados
Umbral	Porcentaje de incidentes solucionados < 75%
Frecuencia de medición	Mensual
Propietario de la Información	Responsable de seguridad
Recopilador de la información	Auditor interno
Formato de la información	Gráfico circular

Tabla 65 Política de privacidad

Componente	Descripción
ID del indicador	I010
Nombre del indicador	Política de privacidad
Descripción	Se revisa la política de privacidad y protección de la información de carácter personal.
Control de seguridad	18.1.4 Protección y privacidad de la información de carácter personal
Tipo	Implementación
Fórmula de medición	Número de revisiones / año
Unidades de medida	Número de revisiones
Umbral	Número de revisiones < 1
Frecuencia de medición	Anual
Propietario de la Información	Comité de seguridad
Recopilador de la	Auditor interno

información	
Formato de la información	Documento de política de privacidad y protección

6. Penalización

   La presente normativa debe cumplirse a cabalidad, de no ser así se puede incurrir en una falta grave que será puesta a disposición del área gerencial.

7. Divulgación

   A través de medios físico y digital

10.4. Anexo Procedimiento Revisión por Dirección

PROCEDIMIENTO REVISIÓN POR DIRECCIÓN			Logo ISP
Fecha de emisión: Octubre 2020	Versión: 1	Número de página: Página 1 de 5	

	Nombre/Cargo	Fecha	Firma
Elaborado por			
Revisado por			
Aprobado por			

Versión	Fecha	Ítem modificado	Descripción de la modificación

Contenido

1. Introducción
2. Objetivo
3. Alcance
4. Normativa de referencia
5. Descripción

5.1 Documentos de entrada

5.2 Documentos de salida

6. Control de cumplimiento de la norma
7. Penalización
8. Divulgación

1. Introducción

   En este procedimiento se detallan los documentos que la dirección debe revisar cada año en relación con la implantación y ejecución del Sistema de gestión de la seguridad de la información, una vez terminada esta revisión se registrarán los resultados en un formato para luego archivarse como parte del proceso de la gestión.

2. Objetivo

   Revisar y analizar los documentos que forman parte fundamental en el proceso del Sistema de Gestión de la Seguridad de la Información de la ISP

3. Alcance

   Se aplica a la gerencia general y a la dirección de la organización.

4. Normativa de referencia

   - ISO/ IEC 27001:2013
   - NTP-ISO/IEC 27001:2008
   - NTP-ISO/IEC 27001:20014

5. Descripción

   La revisión de la documentación que pertenece a este procedimiento tiene como fin informar a la dirección acerca del proceso durante el periodo de un año del desarrollo del SGSI implantado.

   5.1 Documentos de entrada

   La revisión gerencial debe disponer de la siguiente información de entrada que será el objeto de revisión:

   a) El estado de las acciones con relación a las revisiones anteriores por parte de la gerencia

   b) Cambios en asuntos externos e internos que son relevantes al sistema de gestión de seguridad de la información

   c) retroalimentación sobre el desempeño de seguridad de la información, incluyendo tendencias en:

1) no conformidades y acciones correctivas;

2) resultados del monitoreo y medición;

3) resultados de auditoría; y

4) cumplimiento de los objetivos de seguridad de la información;

d) retroalimentación de partes interesadas;

e) resultados de la evaluación de riesgo y estado del plan de tratamiento de riesgos; y

f) oportunidades para la mejora continua. (NTP, 2014)

5.2 Documentos de salida

La dirección incluirá la información como resultado del proceso de la revisión junto con cualquier decisión y acción relacionada con lo siguiente:

a) Mejora de la efectividad del SGSI.
b) Actualizaciones de la evaluación de riesgos y del plan de tratamiento de riesgo.
c) Modificación de los procedimientos y controles vinculados con la seguridad de la información, según sea necesario para responder a los eventos internos y externos que pueden impactar en el SGSI, incluyendo cambios a:

1) requisitos de negocio;
2) requisitos de seguridad;
3) procesos de negocio que afectan los requisitos de negocio existentes;
4) marco regulatorio o legal;
5) obligaciones contractuales; y
6) niveles de riesgo y/o criterios de aceptación de riesgos.

d) Necesidades de recursos.
e) Mejoras en cómo se mide la efectividad de los controles.

Todos los resultados de la revisión quedarán registrados como parte del proceso de mejora continua que hace parte del SGSI

6. Cumplimiento de la norma

   Se revisará en periodos anuales

7. Penalización

   La presente normativa debe cumplirse a cabalidad, de no ser así se puede incurrir en una falta grave que será puesta a disposición del área gerencial.

8. Divulgación

   A través del correo empresarial a los miembros de la dirección

10.5. Anexo Gestión de Roles y responsabilidades

NORMATIVA DE ROLES Y RESPONSABILIDADES			Logo ISP
Fecha de emisión: Octubre 2020	Versión: 1	Número de página: Página 1 de 5	

	Nombre/Cargo	Fecha	Firma
Elaborado por			
Revisado por			
Aprobado por			

Versión	Fecha	Ítem modificado	Descripción de la modificación

Contenido

1. Introducción
2. Objetivo
3. Alcance
4. Normativa de referencia
5. Descripción

5.1 Roles y responsabilidades de la organización de la seguridad de la información.

5.1.1 Gerencia General
5.1.2 Comité de seguridad
5.1.3 Auditor interno
5.1.4 Responsable de Seguridad
5.1.5 Delegado de protección de datos personales
5.1.6 Otras responsabilidades
5.1.6.1 Responsables de los activos de información
5.1.4.2 Custodios de la información

6. Control de cumplimiento de la norma
7. Penalización
8. Divulgación

1. Introducción

   El propósito de esta normativa es crear un marco que establezca las responsabilidades que tendrá cada integrante del grupo encargado del cumplimiento de la gestión de la seguridad de la información de la ISP.

2. Objetivo

   Establecer los roles y las responsabilidades de la Seguridad de la Información.

3. Alcance

   La normativa de Roles y Responsabilidades se aplica a todo el ámbito de la ISP y proveedores con quien se mantiene relaciones comerciales.

4. Normativa de referencia

   - ISO/IEC 27001:2013
   - ISO/IEC 27002

5. Descripción

La estructura de seguridad de la información de la ISP se establece en un grupo de roles y responsabilidades que forman parte del ciclo Deming

5.1 Roles y responsabilidades de la organización de la seguridad de la información

5.1.1 Gerencia General

El gerente general es el responsable de la administración de la seguridad de la información y aplicar estratégicamente las directrices de las políticas con el fin de alinearlas a los objetivos de la organización. Sus principales funciones son:

- Aprobar las políticas de seguridad y ponerlas en funcionamiento.
- Indicar el correcto uso de los activos de la empresa.
- Realizar un compromiso en el buen desarrollo de la implementación del sistema de gestión de la seguridad.

- Fomentar la realización de las auditorías internas con el fin de comprobar el cumplimiento de los controles y normativas de seguridad en toda la organización.

5.1.2 Comité de dirección de la compañía CDC

Este comité se definirá en el área designada para la seguridad de la información, conformado por el gerente general quien pertenece a la dirección y los socios de la ISP, las funciones más relevantes de este comité serán:

I. Nombrar a los miembros de un Comité de Seguridad de la Información
II. Aprobar la política, normas y responsabilidades generales relacionadas a la seguridad de la información.
III. Determinar el umbral de riesgo aceptable
IV. Analizar posibles riesgos introducidos por cambios en las funciones o funcionamiento de la compañía para adoptar las medidas de seguridad más adecuadas.
V. Aprobar el Plan de seguridad de la información

5.1.3 Comité de seguridad de la Información CSI

Este comité estará conformado por una persona de cada área, tanto técnica como administrativa y de ventas, además el jefe técnico y el gerente general. Entre sus funciones más destacadas se encuentra:

- Asignar roles y funciones en materia de seguridad.
- Presentar las políticas, normas y responsabilidades ante el Comité de Dirección para su respectiva aprobación
- Validar el mapa de riesgos
- Validar el Plan director de seguridad de la información y presentarlo al Comité de Dirección para su aprobación.
- Velar por el cumplimiento de la legislación que en materia de seguridad sea de aplicación.
- Promover la capacitación de los miembros de la empresa en cuanto a la seguridad de la información.

5.1.3 Auditor interno

Será el gerente técnico, quien cumple con el perfil especificado en el procedimiento de auditorías internas.

5.1.4 Responsable de la seguridad de la información

El personal que cumpla estas funciones será el responsable de coordinar las acciones que garanticen la seguridad de la información, independientemente de su formato, y durante todo su ciclo de vida. Permitiendo que la información esté protegida en su confidencialidad, privacidad, integridad, disponibilidad, autenticidad y trazabilidad. Las funciones que desempeña el personal designado son las siguientes:

- Implementar los lineamientos del Consejo de Seguridad de la Información.
- Formular, promover y mantener políticas de seguridad de la información y proponer metas en el campo de la seguridad de la información.
- Cooperar con todas las instancias de la organización para desarrollar y mantener los documentos de seguridad de la información.
- Desarrollar un marco normativo de seguridad y controlar su cumplimiento con el apoyo de las instancias que correspondan según el caso.
- Servir de soporte en los asuntos internos de seguridad de la información de la empresa, incluyendo la coordinación con todos departamentos.
- Promover y coordinar el análisis de riesgos de los procesos más críticos y de la información más sensible del giro del negocio, y proponer medidas para mejorar y mitigar los riesgos en base al umbral aceptable determinado por los directivos de la organización.
- Comprobar periódicamente el estado de seguridad de la organización, la tecnología y los procesos.
- Coordinar acciones con los departamentos comerciales para desarrollar y gestionar el plan de continuidad del negocio de la empresa.
- Asegurar el cumplimiento de las leyes y regulaciones aplicables y coordinar con las unidades responsables para la toma de decisiones cuando sea necesario.

- Definir la arquitectura de seguridad del sistema de información para monitorear las incidencias de seguridad y reportarlas a los directivos de la organización.
- Cooperar con todos los departamentos para desarrollar y mantener planes de concientización y capacitación del personal en el ámbito de la seguridad de la información.
- Mantener el seguimiento de posibles incidentes e informar a los directivos de la organización.
- Coordinar la implementación de procesos para la seguridad de la información y definir cuadros de mando de seguridad.

5.1.5 Delegado de protección de datos personales

El personal designado para este cargo será el técnico instalador líder del grupo de los técnicos instaladores, quien tiene el grado de Ingeniero y cumple con el perfil. Será el responsable de la normativa de protección de datos en la organización. Este rol puede ser asumido por personas dentro o fuera de la entidad. Sus funciones principales se detallan a continuación:

- Asesoramiento a responsables de la organización y empleados.
- Control de cumplimiento de las normativas.
- Colaborar y actuar de enlace con las autoridades de control y los ciudadanos que deseen ejercer sus derechos.

5.1.6 Otras responsabilidades

5.1.5.1. Responsables de los activos de información
5.1.5.2. Custodios de la información

6. Control de cumplimiento de la norma

El área de seguridad de la información será el responsable de

7. Penalización

La presente normativa debe cumplirse a cabalidad, de no ser así se puede incurrir en una falta grave que será puesta a disposición del área gerencial.

8. Divulgación

A través del correo empresarial.

10.6. Anexo Metodología de Análisis de Riesgos

METODOLOGÍA ANÁLISIS DE RIESGOS			Logo ISP
Fecha de emisión: Octubre 2020	Versión: 1	Número de página: Página 1 de 7	

	Nombre/Cargo	Fecha	Firma
Elaborado por			
Revisado por			
Aprobado por			

Versión	Fecha	Ítem modificado	Descripción de la modificación

1.Introducción
2.Objetivo
3.Alcance
4.Normativa de referencia
5.Descripción
6Control de cumplimiento de la norma
7.Penalización
8.Divulgación

1. Introducción

   La metodología de Análisis de Riesgos describe el proceso que se lleva a cabo para determinar los riesgos ante amenazas que se encuentran expuestos los activos de la empresa. La metodología escogida para realizar este proceso es la de MAGERIT, a partir de la cual se considerarán las directrices que, para establecer paso a paso la obtención de los riesgos, amenazas, impactos, vulnerabilidades y nos conlleve a desarrollar la mejor propuesta para gestionar los riesgos encontrados.

2. Objetivo

   Implementar las directrices de la metodología de Análisis y Gestión de Riesgos propuestos en la herramienta MAGERIT.

3. Alcance

   Esta metodología es de aplicación al área Seguridad de la información quien es la responsable de desarrollar el análisis de Riesgos para luego implementar la gestión de cada uno de estos.

4. Normativa de referencia

   - Metodología de Análisis y Gestión de Riesgos de la herramienta MAGERIT.

5. Descripción

   La metodología de MAGERIT define los pasos fundamentales para el análisis de riesgo, que serán los que se desarrollarán esta metodología y se describen a continuación:

1. Identificar todos los activos relevantes de la ISP, tanto los que pertenecen al grupo de la información como los activos que son utilizados para brindar un servicio.

2. Clasificar los activos, con la etiqueta que sugiere MAGERIT, según corresponda a uno de los siguientes 10 tipos:

- [D]: Datos/Información
- [K]: Claves criptográficas
- [S]: Servicios
- [SW]: Software – Aplicaciones informáticas
- [HW]: Equipamiento informático (hardware)
- [COM]: Redes de comunicaciones
- [Media]: Soportes de información
- [AUX]: Equipamiento auxiliar
- [L]: Instalaciones
- [P]: Personal

3. Obtener la valoración para cada activo luego de haber determinado la dependencia entre los activos. Se debe tener en cuenta que el valor no es lo que cuesta sino lo que representa para la ISP prescindir del activo. Una vez terminado este proceso se puede determinar que dimensiones se verán afectadas al materializarse una amenaza, la confidencialidad, la integridad o la disponibilidad.

4. Determinar a qué amenazas están expuestos los activos seleccionados, para lo cual también se cuenta con 4 grandes grupos de amenazas cada uno con una etiqueta, con una clasificación de posibles amenazas y con los tipos de activos que se consideran pueden ser afectados.

   Los 4 grandes grupos de amenazas se subdividen en unos varios subtipos más, cada uno con su respectiva etiqueta. Las principales amenazas se detallan a continuación:

   1. [N]: Desastres naturales, con 3 subtipos de amenazas
   2. [I]: De origen industrial, con 12 subtipos de amenazas
   3. [E]: Errores y fallos no intencionados, con 28 subtipos de amenazas
   4. [A]: Ataques intencionados, con 24 subtipos de amenazas

Una vez identificadas las amenazas por cada uno de los activos se procederá a estimar con un valor la frecuencia de ocurrencia de cada una de las amenazas junto con una estimación de la degradación que causaría al activo desde el punto de vista de las 3 dimensiones.

5. Determinar las salvaguardas que ayuden a reducir el riesgo. se deben identificar las salvaguardas pertinentes y darle una valoración a cada una y además se debe registrar la descripción de la salvaguarda y su estado de implantación y finalmente determinar su eficacia al desplegarse en el sistema.

6. Determinar el impacto potencial y residual, definido como el daño sobre el activo derivado de la materialización de la amenaza. Se debe hacer un cálculo del impacto potencial considerando el sistema sin implementación de las salvaguardas, así como el cálculo del impacto residual considerando la eficacia de la salvaguarda desplegada.

7. Determinar el riesgo potencial y residual, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza por cada uno de los activos, analizando de la misma manera que con el impacto, sin tener en cuenta el despliegue de las salvaguardas que corresponde al riesgo potencial, así como el riesgo residual calculado con la efectividad de las salvaguardas

8. Una vez realizados los pasos del análisis de riesgos se puede pasar a la gestión de riesgos la cual consiste en seleccionar la mejor solución que permita reducir los riesgos de la organización. Se tendrá en cuenta los costes que le representaría a la ISP proteger los riesgos identificados al igual que los costes a los que estaría dispuesto a asumir si no se protegen los activos y se dejarán expuestos a que se materialicen las amenazas. Sin embargo, se debe analizar que haya un equilibrio entre el coste de protección y el coste de exposición de la organización con el fin de no gastar más en la protección que en lo que costaría recuperarse.

   Antes de tratar los riesgos se debe determinar el umbral de riesgo que ayudará a tomar la decisión para gestionar cada uno de los que se encuentre por encima del riesgo. Para la primera etapa se especificarán los niveles de riesgo y en la segunda etapa se presentarán las opciones del tratamiento de los riesgos.

   - Etapa 1 Niveles de riesgo: Conformado por una escala de 5 niveles como se indica en la tabla, donde deberá atenderse los riesgos de nivel 4 y 5 que son los de prioridad.

Tabla 66 Escala de niveles de riesgo

Valor	Valor numérico	Valor numérico del riesgo teniendo en cuenta la frecuencia
Muy alto (MA)	5	9 y 10
Alto (A)	4	8
Medio(M)	3	5, 6 y 7
Bajo (B)	2	2,3 y 4
Muy bajo (MB)	1	1

- Etapa 2 Tratamiento del riesgo: Una vez identificado los niveles para clasificar los riesgos, y decidido el nivel aceptable, se procederá a tomar la decisión para la estrategia a aplicar en el tratamiento del riesgo, de las cuales se tendrán las 4 opciones:

  1. Aceptar: Consiste en aceptar que existe un riesgo importante, que se encuentra en los niveles 4 (alto) o 5 (muy alto) que de materializarse afectaría el correcto funcionamiento de la organización, sin embargo, la empresa decide no implementar algún control ya que el hacerlo representaría un mayor costo y existe una baja probabilidad de que se presente.

  2. Transferir a terceros: En este punto se ha determinado que existe un riesgo por encima del umbral, pero se decide contratar a una tercera parte para que se haga cargo de la gestión del riesgo porque resulta menos costoso implantar controles que lo reduzcan.

  3. Mitigar: en este punto se toma la decisión de aplicar controles y salvaguardas que ayudan a reducir el riesgo al nivel 3, que es un nivel aceptable para la organización. No se elimina totalmente el riesgo, pero se logra reducir.

  4. Evitar: Se implantan todos los controles necesarios para eliminar el riesgo, aunque es la mejor solución es la más costosa.

Luego de decidir la mejor opción por cada uno de los riesgos se asignará un **propietario del riesgo** quien será el encargado de gestionar todo lo relacionado al tratamiento y control. El dueño del riesgo será el propietario del activo al que se encuentre delegado, de no ser así, por

alguna circunstancia excepcional y valida que se presente, se podrá asignar a otra persona que sea igual de adecuada para gestionar el riesgo.

9. Realizar la documentación de:

    a. Modelo de valor
    b. Mapa de riesgos
    c. Declaración de aplicabilidad
    d. Evaluación de salvaguardas
    e. Informe de vulnerabilidades

6. Cumplimiento de la norma

    Debe realizarse el análisis de riesgos antes de implantar el SGSI

7. Penalización

    La presente normativa debe cumplirse a cabalidad, de no ser así se puede incurrir en una falta grave que será puesta a disposición del área gerencial.

8. Divulgación

    A través del correo empresarial.

10.7. Anexo Declaración de Aplicabilidad

DECLARACIÓN DE APLICABILIDAD			Logo ISP
Fecha de emisión: Octubre 2020	Versión: 1	Número de página: Página 1 de 11	

	Nombre/Cargo	Fecha	Firma
Elaborado por			
Revisado por			
Aprobado por			

Versión	Fecha	Ítem modificado	Descripción de la modificación

Contenido

1. Introducción
2. Objetivo
3. Alcance
4. Normativa de referencia
5. Descripción
6. Cumplimiento de la norma
7. Penalización
8. Divulgación

1. Introducción

Una vez analizados los riesgos a los que se encuentran expuestos los activos, se determinarán cuáles de los 114 controles propuestos en la norma ISO/IEC 27001 se aplican en la empresa de la ISP. Una vez seleccionados con su respetiva justificación del por qué aplica o por qué no aplica deberán ser revisados y aprobados por la dirección de la empresa.

2. Objetivo

Establecer la aplicabilidad de los controles propuestos en ISO/IEC 27001 que se ajusten al desarrollo de la empresa.

3. Alcance

Se aplica a todas las áreas del negocio de la ISP.

4. Normativa de referencia

- UNE-EN ISO/IEC 27002:2017

5. Descripción

En la siguiente tabla se encuentran los 114 controles con su respectivo campo de implantación de si aplica o no aplica y la justificación para haber determinado esta decisión.

Control	Implantación Aplica/No aplica	Justificación
5 políticas de seguridad de la información		
5.1 Directrices de gestión de la seguridad de la información		
5.1.1 Políticas para la seguridad de la información	Aplica	Requisito fundamental para el buen funcionamiento del SGSI
5.1.2 Revisión de las políticas para la seguridad de la información	Aplica	Requisito fundamental para el buen funcionamiento del SGSI
6 organización de la seguridad de la información		
6.1 Organización interna.		
6.1.1 Roles y responsabilidades en seguridad de la información	Aplica	Cumplir con los requisitos de la Política de Seguridad
6.1.2 Segregación de tareas	Aplica	Requisito para el giro del negocio
6.1.3 Contacto con las autoridades	Aplica	Cumplir con los requisitos de la Política de Seguridad
6.1.4 Contacto con grupos de interés especial	Aplica	Requisito en la gestión de incidencias de seguridad
6.1.5 Seguridad de la información en la gestión de proyectos	Aplica	Requisito para el giro del negocio
6.2 Los dispositivos móviles y el teletrabajo		
6.2.1 Política de dispositivos móviles	Aplica	Requisito para el buen funcionamiento del SGSI
6.2.2 Teletrabajo	Aplica	Cumplir con los requisitos de la Política de Seguridad
7 seguridad relativa a los recursos humanos		
7.1 Antes del empleo		
7.1.1 Investigación de antecedentes	Aplica	Requisito para el giro del negocio
7.1.2 Términos y condiciones del empleo	Aplica	Requisito para el giro del negocio
7.2 Durante el empleo		
7.2.1 Responsabilidades de gestión	Aplica	Cumplir con los requisitos de la Política de Seguridad
7.2.2 Concienciación, educación y capacitación en seguridad de la información	Aplica	Cumplir con los requisitos de la Política de Seguridad
7.2.3 Proceso disciplinario	Aplica	Cumplir con los requisitos de la Política de Seguridad

7.3 Finalización del empleo o cambio en el puesto de trabajo		
7.3.1 Responsabilidades ante la finalización o cambio	Aplica	Requisito para el giro del negocio

8 gestión de activos		
8.1 Responsabilidad sobre los activos		
8.1.1 Inventario de activos	Aplica	Requisito en el procedimiento del análisis de riesgos
8.1.2 Propiedad de los activos	Aplica	Requisito en el procedimiento del análisis de riesgos
8.1.3 Uso aceptable de los activos	Aplica	Cumplir con los requisitos de la Política de Seguridad
8.1.4 Devolución de activos	Aplica	Requisito para el giro del negocio
8.2 Clasificación de la información		
8.2.1 Clasificación de la información	Aplica	Requisito para el giro del negocio
8.2.2 Etiquetado de la información	Aplica	Requisito para el giro del negocio
8.2.3 Manipulado de la información	Aplica	Requisito para el giro del negocio
8.3 Manipulación de los soportes		
8.3.1 Gestión de soportes extraíbles	Aplica	Requisito para el giro del negocio
8.3.2 Eliminación de soportes	Aplica	Requisito para el giro del negocio
8.3.3 Soportes físicos en tránsito	Aplica	Requisito para el giro del negocio
9 control de acceso		
9.1 Requisitos de negocio para el control de acceso		
9.1.1 Política de control de acceso	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.1.2 Acceso a las redes y a los servicios de red	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.2 Gestión de acceso de usuario		
9.2.1 Registro y baja de usuario	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.2.2 Provisión de acceso de usuario	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.2.3 Gestión de privilegios de acceso	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.2.4 Gestión de la información secreta de autenticación de los usuarios	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.2.5 Revisión de los	Aplica	Cumplir con los requisitos de

derechos de acceso de usuario		la Política de Seguridad
9.2.6 Retirada o reasignación de los derechos de acceso	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.3 Responsabilidades del usuario		
9.3.1 Uso de la información secreta de autenticación	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.4 Control de acceso a sistemas y aplicaciones		
9.4.1 Restricción del acceso a la información	Aplica	Cumplir con los requisitos de la Política de Seguridad

9.4.2 Procedimientos seguros de inicio de sesión	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.4.3 Sistema de gestión de contraseñas	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.4.4 Uso de utilidades con privilegios del sistema	Aplica	Cumplir con los requisitos de la Política de Seguridad
9.4.5 Control de acceso al código fuente de los programas	Aplica	Cumplir con los requisitos de la Política de Seguridad
10 criptografía		
10.1 Controles criptográficos		
10.1.1 Política de uso de los controles criptográficos	Aplica	Requisito para el giro del negocio
10.1.2 Gestión de claves	Aplica	Requisito para el giro del negocio
11 seguridad física y del entorno		
11.1 Áreas seguras		
11.1.1 Perímetro de seguridad física	Aplica	Requisito para el giro del negocio
11.1.2 Controles físicos de entrada	Aplica	Requisito para el giro del negocio
11.1.3 Seguridad de oficinas, despachos y recursos	Aplica	Requisito para el giro del negocio
11.1.4 Protección contra las amenazas externas y ambientales	Aplica	Requisito para el giro del negocio
11.1.5 El trabajo en áreas seguras	Aplica	Requisito para el giro del negocio
11.1.6 Áreas de carga y descarga	Aplica	Requisito para el giro del negocio
11.2 Seguridad de los equipos		

11.2.1 Emplazamiento y protección de equipos	Aplica	Cumplir con los requisitos de la Política de Seguridad
11.2.2 Instalaciones de suministro	Aplica	Requisito para el giro del negocio
11.2.3 Seguridad del cableado	Aplica	Requisito para el giro del negocio
11.2.4 Mantenimiento de los equipos	Aplica	Cumplir con los requisitos de la Política de Seguridad
11.2.5 Retirada de materiales propiedad de la empresa	Aplica	Cumplir con los requisitos de la Política de Seguridad
11.2.6 Seguridad de los equipos fuera de las instalaciones	Aplica	Cumplir con los requisitos de la Política de Seguridad

11.2.7 Reutilización o eliminación segura de equipos	Aplica	Cumplir con los requisitos de la Política de Seguridad
11.2.8 Equipo de usuario desatendido	Aplica	Cumplir con los requisitos de la Política de Seguridad
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Aplica	Requisito para el buen funcionamiento de la ISP
12 seguridad de las operaciones		
12.1 Procedimientos y responsabilidades operacionales		
12.1.1 Documentación de procedimientos de las operaciones	Aplica	
12.1.2 Gestión de cambios	Aplica	Requisito en el procedimiento del análisis de riesgos
12.1.3 Gestión de capacidades	Aplica	Requisito para el giro del negocio
12.1.4 Separación de los recursos de desarrollo, prueba y operación	Aplica	Cumplir con los requisitos de la Política de Seguridad
12.2 Protección contra el software malicioso (malware)		
12.2.1 Controles contra el código malicioso	Aplica	
12.3 Copias de seguridad		
12.3.1 Copias de seguridad de la información	Aplica	Cumplir con los requisitos de la Política de Seguridad
12.4 Registros y supervisión		
12.4.1 Registro de eventos	Aplica	Requisito en el procedimiento de gestión de incidentes
12.4.2 Protección de la	Aplica	Requisito en el procedimiento

información del registro		de gestión de incidentes
12.4.3 Registros de administración y operación	Aplica	Requisito en el procedimiento de gestión de incidentes
12.4.4 Sincronización del reloj	Aplica	Requisito en el procedimiento de gestión de incidentes
12.5 Control del software en explotación		
12.5.1 Instalación del software en explotación	Aplica	Cumplir con los requisitos de la Política de Seguridad
12.6 Gestión de la vulnerabilidad técnica		
12.6.1 Gestión de las vulnerabilidades técnicas	Aplica	Cumplir con los requisitos de la Política de Seguridad
12.6.2 Restricción en la instalación de software	Aplica	Cumplir con los requisitos de la Política de Seguridad
12.7 Consideraciones sobre la auditoria de sistemas de información		
12.7.1 Controles de auditoría de sistemas de información	Aplica	Requisito en el procedimiento de auditorías internas
13 seguridad de las comunicaciones		
13.1 Gestión de la seguridad de las redes		
13.1.1 Controles de red	Aplica	Cumplir con los requisitos de la Política de Seguridad
13.1.2 Seguridad de los servicios de red	Aplica	Cumplir con los requisitos de la Política de Seguridad
13.1.3 Segregación en redes	Aplica	Cumplir con los requisitos de la Política de Seguridad
13.2 Intercambio de información		
13.2.1 Políticas y procedimientos de intercambio de información	Aplica	Requisito para el giro del negocio

13.2.2 Acuerdos de intercambio de información	Aplica	Requisito para el giro del negocio
13.2.3 Mensajería electrónica	Aplica	Requisito para el giro del negocio
13.2.4 Acuerdos de confidencialidad o no revelación	Aplica	Requisito para el giro del negocio
14 adquisición, desarrollo y mantenimiento de los sistemas de información		
14.1 Requisitos de seguridad en los sistemas de información		
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Aplica	Requisito para el giro del negocio
14.1.2 Asegurar los servicios	Aplica	Requisito para el giro del

de aplicaciones en redes públicas		negocio
14.1.3 Protección de las transacciones de servicios de aplicaciones	Aplica	Requisito para el giro del negocio
14.2 Seguridad en el desarrollo y en los procesos de soporte		
14.2.1 Política de desarrollo seguro	Aplica	Cumplir con los requisitos de la Política de Seguridad
14.2.2 Procedimiento de control de cambios en sistemas	Aplica	Cumplir con los requisitos de la Política de Seguridad
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Aplica	Cumplir con los requisitos de la Política de Seguridad
14.2.4 Restricciones a los cambios en los paquetes de software	Aplica	Cumplir con los requisitos de la Política de Seguridad
14.2.5 Principios de ingeniería de sistemas seguros	No Aplica	La empresa no tiene área de desarrollo
14.2.6 Entorno de desarrollo seguro	No Aplica	La empresa no tiene área de desarrollo
14.2.7 Externalización del desarrollo de software	No Aplica	La empresa no tiene área de desarrollo
14.2.8 Pruebas funcionales de seguridad de sistemas	No Aplica	La empresa no tiene área de desarrollo

14.2.9 Pruebas de aceptación de sistemas	Aplica	Requisito para el giro del negocio
14.3 Datos de prueba		
14.3.1 Protección de los datos de prueba	Aplica	Requisito para el giro del negocio
15 relación con proveedores		
15.1 Seguridad en las relaciones con proveedores		
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Aplica	Cumplir con los requisitos de la Política de Seguridad

15.1.2 Requisitos de seguridad en contratos con terceros	Aplica	Cumplir con los requisitos de la Política de Seguridad
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	Aplica	Requisito para el giro del negocio
15.2 Gestión de la provisión de servicios del proveedor		
15.2.1 Control y revisión de la provisión de servicios del proveedor	Aplica	Requisito para el giro del negocio
15.2.2 Gestión de cambios en la provisión del servicio del proveedor	Aplica	Requisito en el procedimiento del análisis de riesgos
16 gestión de incidentes de seguridad de la información		
16.1 Gestión de incidentes de seguridad de la información y mejoras		
16.1.1 Responsabilidades y procedimientos	Aplica	Cumplir con los requisitos de la Política de Seguridad
16.1.2 Notificación de los eventos de seguridad de la información	Aplica	Cumplir con los requisitos de la Política de Seguridad
16.1.3 Notificación de puntos débiles de la seguridad	Aplica	Cumplir con los requisitos de la Política de Seguridad
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	Aplica	Cumplir con los requisitos de la Política de Seguridad
16.1.5 Respuesta a incidentes de seguridad de la información	Aplica	Cumplir con los requisitos de la Política de Seguridad
16.1.6 Aprendizaje de los incidentes de seguridad de la información	Aplica	Cumplir con los requisitos de la Política de Seguridad
16.1.7 Recopilación de evidencias	Aplica	Cumplir con los requisitos de la Política de Seguridad

17 aspectos de seguridad de la información para la gestión de la continuidad de negocio		
17.1 Continuidad de la seguridad de la información		
17.1.1 Planificación de la continuidad de la seguridad de la información	Aplica	Requisito para el giro del negocio
17.1.2 Implementar la continuidad de la seguridad de la información	Aplica	Requisito para el giro del negocio

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Aplica	Requisito para el giro del negocio
17.2 Redundancias		
17.2.1 Disponibilidad de los recursos de tratamiento de la información	Aplica	Requisito para el giro del negocio para cumplir con las leyes
18 cumplimiento		
18.1 Cumplimiento de los requisitos legales y contractuales		
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Aplica	Requisito para el giro del negocio para cumplir con las leyes
18.1.2 Derechos de propiedad intelectual (DPI)	Aplica	Requisito para el giro del negocio para cumplir con las leyes
18.1.3 Protección de los registros de la organización	Aplica	Requisito para el giro del negocio para cumplir con las leyes
18.1.4 Protección y privacidad de la información de carácter personal	Aplica	Requisito para el giro del negocio para cumplir con las leyes
18.1.5 Regulación de los controles criptográficos	Aplica	Requisito para el giro del negocio para cumplir con las leyes
18.2 Revisiones de la seguridad de la información		
18.2.1 Revisión independiente de la seguridad de la información	Aplica	Requisito para el giro del negocio para cumplir con las leyes
18.2.2 Cumplimiento de las políticas y normas de seguridad	Aplica	Cumplir con los requisitos de la Política de Seguridad
18.2.3 Comprobación del cumplimiento técnico	Aplica	Cumplir con los requisitos de la Política de Seguridad

6. Cumplimiento de la norma

La revisión del cumplimiento de documento debe hacerse de manera continua para su correcto funcionamiento, sin embargo, las actualizaciones de los controles se revisan una vez haya culminado el tiempo de vigencia de la certificación, o de las actualizaciones de los controles de la norma en el proceso de renovación de la certificación

7. Penalización

   La presente normativa debe cumplirse a cabalidad, de no ser así se puede incurrir en una falta grave que será puesta a disposición del área gerencial.

8. Divulgación

   A través del correo empresarial.