UNIVERSIDAD METROPOLITANA DEL ECUADOR

FACULTAD DE INGENIERÍAS

CARRERA DE SISTEMAS DE INFORMACIÓN

SEDE QUITO

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÒN

TEMA: IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA “PINTO SEGUROS”, APLICANDO LA NORMA ISO/IEC 27001

AUTOR: BRYAN ALEXANDER GUANÍN CASTILLO

TUTOR: MSc. TONYSE DE LA ROSA MARTÍN

QUITO-2021

CERTIFICACIÓN DEL TUTOR

MSc. Tonyse de la Rosa como asesor del trabajo de investigación asignado por disposición de Cancillería de UMET (la universidad Metropolitana del Ecuador), certifico que el estudiante BRYAN ALEXANDER GUANÍN CASTILLO con C.C. N° 1104128457 ha completado con el proyecto que se le ha asignado, con el tema: IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA "PINTO SEGUROS", BASADO EN LA NORMA ISO/IEC 27001, quien ha cumplido con todos los requisitos legales exigidos por lo que se aprueba de la misma.

Es todo cuanto puedo decir en honor a la verdad, facultando al interesado hacer uso de la presente, así como también se autoriza la presentación para la evaluación por parte del jurado respectivo.

Atentamente,

_____

MSc. Tonyse de la Rosa

CERTIFICACIÓN DE AUTORÍA DE TRABAJO DE TITULACIÓN

Yo, BRYAN ALEXANDER GUANÍN CASTILLO con Cédula N° 1104128457 estudiante de la Universidad Metropolitana del Ecuador “UMET”, declaro en forma libre y voluntaria que la presente investigación trata sobre IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA “PINTO SEGUROS”, BASADO EN LA NORMA ISO/IEC 27001, así como las expresiones vertidas en la misma son autoría del compareciente, quien ha realizado en base a recopilación bibliográfica, consultas de internet y consultas de campo.

En consecuencia, asumo la responsabilidad de la originalidad de la misma y el cuidado al remitirme a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto.

Atentamente,

Firmado electrónicamente por:
BRYAN ALEXANDER GUANIN CASTILLO

Bryan Alexander Guanín Castillo

1104128457

AUTOR

CESIÓN DE DERECHOS DE AUTOR

Yo, BRYAN ALEXANDER GUANINN CASTILLO, en calidad de autor y titular de los derechos morales y patrimoniales del trabajo de titulación, IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA "PINTO SEGUROS", BASADO EN LA NORMA ISO/IEC 27001, modalidad Proyecto de Investigación de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, cedo a favor de la Universidad Metropolitana del Ecuador una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Metropolitana del Ecuador para que realice la digitalización y publicación de este trabajo de titulación en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Firmado electrónicamente por:
BRYAN ALEXANDER GUANIN CASTILLO

Bryan Alexander Guanín Castillo

1104128457

DEDICATORIA

A mis padres, que estuvieron en todo momento apoyándome y motivándome.

A mi hermana y mi sobrino por su apoyo incondicional en todo momento.

Mi futura Esposa Diana, que ha estado apoyándome a culminar la tesis y motivarme para que siga estudiando y aprendiendo más sobre otras carreras.

AGRADECIMIENTO

A Dios.

Por haber permitido llegar hasta aquí hoy, por darme sabiduría, salud y fuerza para llevar a cabo mis metas y objetivos.

A mis padres Víctor y Efigenia, que desde pequeño me inculcaron la disciplina de estudiar, luchar por los sueños y por haberme dado la oportunidad de tener una excelente educación en el transcurso de mi vida.

A mi hermana y sobrino, que han sido parte en esta trayectoria para alcanzar mi Título profesional.

A mi futura esposa Diana, por creer en mí y apoyarme en la presente tesis, por su paciencia, su amor infinito e incondicional.

A mis abuelitas a las que me dan su apoyo virtualmente y haber creído en mi hasta lo último ya que con sus consejos alentadores me han servido para llegar a ser un profesional.

Mis profesores, por su confianza y conocimientos, gracias por prepararnos para un futuro competitivo no solamente en lo profesional sino también en lo personal; finalmente a mis compañeros, que hemos tenido la dicha de compartir la etapa universitaria.

Gracias a todos por su apoyo.

Tabla de contenidos

CERTIFICACIÓN DEL TUTOR i
CERTIFICACIÓN DE AUTORÍA DE TRABAJO DE TITULACIÓN ii
CESIÓN DE DERECHOS DE AUTOR iii
DEDICATORIA iv
AGRADECIMIENTO v
RESUMEN xii
ABSTRACT xiii
INTRODUCCIÓN 1
Antecedentes y justificación 2
El problema 2
Objetivos 3
Objetivo general 3
Objetivos específicos 3
Planteamiento de hipótesis 3
CAPÍTULO I 5
1. FUNDAMENTACIÓN TEÓRICA 5
1.1 Seguridad de la información 5
1.2 Seguridad informática 6
1.3 Análisis de riesgo 11
1.3.1 Riesgos y amenazas 12
1.4 ISO/ SGSI 14
1.4.1 Anexo SL 15
1.4.2 Fases del sistema de gestión 15
1.5 Historia de la ISO /IEC 27001 17
1.5.1 Norma ISO/IEC 27001 Gestión de la Seguridad de la Información 18
1.5.2 Diferencias entre la ISO/IEC 27001 e ISO/IEC 27002 18
1.6 Anexo A ISO 27001 21
1.7 Teletrabajo 21
CAPÍTULO II 22
2. MARCO METODOLÓGICO 22
2.1. Magerit 23
2.1.1. Objetivos de Magerit. 23
2.1.2. Análisis de metodología de gestión de riesgos 24
2.2. Fases para implementar ISO 27001 24
2.2.1. Fase 1: Auditoría inicial Gap Analysis 24
2.2.1.1. Niveles de Madurez 24
2.2.1.2. Nivel de Cumplimiento 25
2.2.2. Fase 2: Análisis del contexto de la organización y determinación del alcance 25
2.2.2.1. Proceso para el requisito: 25
2.2.2.2. Comprender la Organización y su contexto 26
2.2.2.3. Comunicación y consulta 26

2.2.2.4. Contexto del SGSI 26
2.2.2.5. Contexto de la Gestión de Riesgos 27
2.2.2.6. Definición de criterios de riesgo 28
2.2.2.7. Definir el Alcance de un SGSI 30
2.2.3. Fase 3: elaboración de la política - objetivos del sgsi 30
2.2.3.1. Política de seguridad 30
2.2.3.2. Redactar de acuerdo a las necesidades de cada organización 30
2.2.3.3. Tener en cuenta los objetivos de cada organización 31
2.2.3.4. Demostrar que se tienen en cuenta los requisitos de las partes interesadas 32
2.2.3.5. Comunicación de la política a las partes interesadas 32
2.2.3.6. Propiedad 32
2.2.3.7. Objetivos de seguridad del SGSI 32
2.2.4. Fase 4: Planificación del SGSI 34
2.2.4.1. Inventario de Activos 34
2.2.4.2. Valoración de activos y asignación del nivel de riesgo 36
2.2.4.3. Catálogo de amenazas 36
2.2.4.4. Valoración de las amenazas para la seguridad de la información 36
2.2.4.5. Nivel de Vulnerabilidad 36
2.2.4.6. Análisis de riesgos 36
2.2.4.7. Evaluación de riesgos 37
2.2.4.8. Tratamiento de riesgos 37
2.2.4.9. Responsable del riesgo 37
2.2.4.10. Selección de controles: declaración de aplicabilidad 38
2.2.5. Fase 5: Documentación SGSI 38
2.2.5.1. Información a publicarse 38
2.2.5.2. Niveles de documentación en ISO 27001 39
2.2.5.3. Listado de documentos obligatorios del SGSI 40
2.2.6. Fase 6: Implementación de un SGSI 40
2.2.6.1. Criterios de agrupación y ordenamiento de procesos de seguridad 40
2.2.6.2. Proceso de la seguridad 41
2.2.6.3. Responsabilidades 42
2.2.6.4. Definir indicadores de procesos 43
2.2.6.5. Implementación del proceso 43
2.2.7. Fase 7: Comunicación y sensibilización SGSI 43
2.2.7.1. Plan de comunicación ISO 27001 43
2.2.7.2. Documentación del plan de comunicación del SGSI 44

2.2.7.3. Tener cultura de la seguridad 44
2.2.7.4. Creación de una cultura de la seguridad de la información 45
2.2.7.5. Educación del personal 45
2.2.7.6. Evaluación del cumplimiento 46
2.2.8. Fase 8: Auditoría interna según ISO 27001 46
2.2.8.1. Determinar el objetivo de la auditoría interna ISO 27001 46
2.2.8.2. Identificar los beneficios de la auditoría interna del SGSI 46
2.2.8.3. Establecer quién será el auditor interno del SGSI 47
2.2.8.3.1. Funciones y tareas del Auditor Interno ISO 27001 47
2.2.8.3.2. Definir el equipo auditor 47
2.2.8.3.3. Candidatos a auditores internos 47
2.2.8.3.4. Diferenciar la auditoría interna de la auditoría de certificación 48
2.2.8.3.5. Consejos para una auditoría interna 48
2.2.9. Fase 9: Revisión por la dirección según ISO 27001 50
2.2.9.1. Importancia de la revisión del sistema 50
2.2.9.2. Objetivo de la revisión 50
2.2.9.3. La revisión como parte de la mejora continua 50
2.2.9.4. Ciclo PDCA en la estructura de la norma 50
2.2.9.4.1. Planificar (PLAN) 51
2.2.9.4.2. Hacer (DO) 51
2.2.9.4.3. Check (Monitorear) 52
2.2.9.4.4. Actuar (ACT) 52
2.2.9.5. Consideraciones en la revisión del SGSI 53
2.2.9.6. Frecuencia para la revisión del SGSI 53
2.2.10. Fase 10: Proceso de certificación ISO 27001 53
2.2.10.1. Auditoría de certificación del SGSI 54
2.2.10.2. Auditoria de certificación ISO 27001 Fase 1 54
2.2.10.3. Auditoria de certificación ISO 27001 Fase 2 54
CAPÍTULO III 56
3. RESULTADOS 56
3.1. Entorno actual de la empresa “Pinto Seguros” 56
3.1.2. Visión 56
3.1.3. Valores 56
3.2. Antecedentes de la empresa 56
3.3. Infraestructura de la empresa 57
3.4. Estructura organizacional de la empresa 57
3.5. Modelo de negocio 57

3.6. Diagnóstico de la situación actual de la empresa 58
3.7. Técnicas de investigación 59
3.8. Población 59
3.9. Muestra 59
3.10. Propuesta 59
3.11. Objetivo de la propuesta 59
3.12. Alcance 59
3.13. Fases para implementar ISO 27001 60
3.13.1. Fase 1: Auditoría inicial Gap Análisis 60
3.13.1.1. Nivel de Cumplimiento 60
3.13.2. Fase 2: Análisis del contexto de la organización y determinación del alcance 64
3.13.2.1. Comunicación y consulta 64
3.13.2.2. Contexto del SGSI 65
3.13.2.3. Contexto de la Gestión de Riesgos 66
3.13.2.4. Definición de criterios de riesgo 66
3.13.2.5. Entender las necesidades y expectativas de las partes involucradas 67
3.13.3. Fase 3: Elaboración de la política - objetivos del SGSI 69
3.13.3.1. Política de seguridad 69
3.13.3.2. Auditoría de actividades de seguridad 69
3.13.4. Fase 4: Planificación del SGSI 69
3.13.4.1. Inventario de Activos 69
3.13.4.2. Valoración de activos y asignación del nivel de riesgo 70
3.13.4.3. Catálogo de amenazas 71
3.13.4.4. Valoración de las amenazas para la seguridad de la información 78
3.13.4.5. Nivel de Vulnerabilidad 79
3.13.4.6. Análisis de riesgos 80
3.13.4.7. Cálculo de Valores de impacto de Cada Activo 81
3.13.4.8. Cálculo de Nivel de Impacto 81
3.13.4.9. Evaluación de riesgos 82
3.13.4.10. Tratamiento de riesgos 83
3.13.4.11. Responsable del riesgo 83
3.13.4.12. Selección de controles: declaración de aplicabilidad 84
3.14. Resultados 85
RECOMENDACIONES 89
BIBLIOGRAFÍA 90

Índice de Figuras

Figura 1. Tríada CIA. 5
Figura 2. Diagrama de Vulnerabilidad. 6
Figura 3. Ciclo de vida de Desarrollo Seguro de Software. 8
Figura 4. Defensa en Capas para Reducir el Riesgo. 9
Figura 5. Navegar en Forma Segura por Internet. 10
Figura 6. Seguridad de una Red LAN. 11
Figura 7. Riesgos y Amenazas 12
Figura 8. Análisis de riesgos 13
Figura 9. Defensa en Capas para Reducir el Riesgo 14
Figura 10. Estructura Alineada a Anexo SL 15
Figura 11. Fases del Sistema de Gestión. 16
Figura 12. Historia de la ISO/IEC 27001 18
Figura 13. Metodología 22
Figura 14. ISO 31000 Magerit V3 23
Figura 15. Proceso para Definir el Alcance de un SGSI 31
Figura 16. Clasificación y Valoración de Riesgo. 37
Figura 17. Niveles de Documentación ISO 27001. 39
Figura 18. Orden y Agrupación de Procesos de Seguridad. 41
Figura 19. Proceso de Seguridad de la Información. 42
Figura 20. Niveles de la Cultura de la Seguridad. 44
Figura 21. Comunicación de valores y cultura de la Seguridad de la Información. 44
Figura 22. Creación de Cultura de Seguridad de la Información. 45
Figura 23. Niveles en las Políticas de la Seguridad de la Información. 45
Figura 24. Tareas del Auditor Interno ISO 27001. 47
Figura 25. Ciclo PDCA 50
Figura 26. Fases del proyecto SGSI. 51
Figura 27. Fases de la Implementación 52
Figura 28. Fases del Control. 52
Figura 29. Organigrama “Pinto Seguros” 57
Figura 30. Niveles de riesgo extremo e importante. 71
Figura 31. Niveles de riesgo moderado, menor e incidental. 78
Figura 32. Escala de Probabilidades de Amenazas. 79
Figura 33. Nivel de Vulnerabilidad. 80
Figura 34. Valores de Impacto. 81
Figura 35. Valoración de Amenazas 81
Figura 36. Nivel de impacto. 82
Figura 37. Clasificación y Valoración de Riesgo. 82
Figura 38. Tratamiento de Riesgo. 83
Figura 39. Modelo de Declaración de aplicabilidad ISO 27001. 84
Figura 40. Plan de Trabajo. 94

Índice de tablas

Tabla 1 Familia ISO 17
Tabla 2. Procedimiento para Implementar ISO 27001 19
Tabla 3. Documentación requerida para implementar ISO 27001 20
Tabla 4. Registros requeridos para implementar ISO 27001 20
Tabla 5 Diagnóstico Basado en ISO 27001 58
Tabla 6 Test de Control para determinar el nivel de Madurez en el cumplimiento NormativaISO 27001 60
Tabla 7. Nivel de Cumplimiento de “Pinto Seguros” 63
Tabla 8 Plan de Comunicación 64
Tabla 9 Criterios de Riesgo 66
Tabla 10 Requisitos de Clientes 67
Tabla 11 Requisito de Usuarios Finales 67
Tabla 12 Requisitos de Socios 67
Tabla 13 Requisitos de Empleados 68
Tabla 14 Requisitos de Administración 68
Tabla 15. Riesgos-Inventarios de activos 69
Tabla 16 Catálogo Genérico de Amenazas 71
Tabla 17 Controles Anexo A 98
Tabla 18 Documentos para Aplicabilidad de acuerdo a Anexo A 99

Índice de anexos

Anexo A. Plan de Trabajo 94
Anexo B. Glosario de términos 94
Anexo C. Documentos de Control Anexo A 98
Anexo D. Documentación Específica para Control en Anexo A 99
Anexo E. Bitácora de incidentes de Seguridad 99
Anexo F. Acuerdo Ministerial de teletrabajo 99

RESUMEN

Con el presente trabajo se desea brindar una solución apropiada a la empresa “Pinto Seguros” mediante la implementación de un sistema de gestión de seguridad de la información, y a consecuencia de la pandemia ocasionada por el Covid-19 se han incrementado los riesgos de seguridad y existen vulnerabilidades en el teletrabajo, razón por la cual se utilizará la normativa ISO 27001 que garantice minimizar el riesgo, protegerla información en las computadoras o en los sistemas interconectados, ya que la integridadde los datos es uno de los activos más importantes de las organizaciones y asegurar la confidencialidad de la información de determinados procesos críticos o sensibles ante la pérdida, fuga o no disponibilidad de la información y así evitar problemas a la organización.

Palabras clave: ISO, seguridad, información, proceso, riesgo, gestión.

ABSTRACT

With this work it is desired to provide an appropriate solution to the company “Pinto Seguros” through the implementation of an information security management system, and as a result of the pandemic caused by Covid-19, security risks have increased and there are vulnerabilities in teleworking, which is why the ISO 27001 standard will be usedto guarantee minimizing risk, protecting information on computers or interconnected systems, since data integrity is one of the most important assets of organizations and ensure the confidentiality of the information of certain critical or sensitive processes in the event of the loss, leakage or unavailability of the information and thus avoid problemsfor the organization.

Keywords: ISO, security, information, process, risk, management.

INTRODUCCIÓN

La información es un medio intangible. (García, 2020) menciona: “La inversión en activos intangibles conduce a un gasto con retorno a futuro, contribuyendo a la llamada economía del conocimiento”. Los activos intangibles generar mucho valor económico para las empresas, en la era de los datos, la información tiene mucho valor ya que generan productividad, amplían las ventas y disminuyen los costos por reducir el tiempo de utilidad de dicha información en la producción.

De acuerdo a (Ecuador, Ministerio de Telecomunicaciones, 2020) El Sistema de Gestión de Seguridad de la Información (SGSI) es: “El elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información institucional” . El SGSI pretende salvaguardar la confidencialidad, integridad y disponibilidad de la información.

Toda organización y persona natural valora los datos y toda la información acumulada a lo largo de su trabajo o actividad económica, es por eso que, para su manejo, mal uso o posible pérdida es imprescindible el uso de mejoras continuas y normativas que eviten o restrinjan los riesgos.

Las normativas deben estar al alcance no solo de las organizaciones, sino también de las personas que a diario podemos estar expuestas a riesgos de mal uso de nuestra privacidad, cuentas electrónicas, redes sociales, etc.

La pandemia Covid-19 ha acelerado la transformación digital de las empresas y a la par se han establecido procedimientos que posibilitan la flexibilización laboral por medio del teletrabajo, en elcaso puntual de Ecuador el Ministerio del trabajo ha diseñado las directrices para el teletrabajo. Estacoyuntura ha hecho que a la par las empresas estén expuestas a mayores ciber amenazas, que han tenido un crecimiento exponencial, cada vez más incidentes de seguridad son registrados por empresas públicas y privadas, por lo cual es importante la Implementación de un Sistema de Gestión de Seguridad de la información acorde a la norma ISO 27001.

Este trabajo consta de 3 capítulos; en el capítulo 1 se incluye el marco teórico, en el capítulo 2 marco metodológico, en el capítulo 3 presenta resultados.

Antecedentes y justificación

La empresa “Pinto Seguros”, inició sus operaciones el 28 de noviembre del 2018, se encuentra ubicada en Machachi, esta brinda los servicios de seguros de vida, asistencia médica, transporte, equipos y maquinarias; a su vez está también ofrece seguros de viajes a nivel internacional.

En el área de gestión de la empresa, este establecimiento conserva una gran cantidad de información, mayormente en medios impresos, debido a la documentación necesaria que se maneja al momento de requerir un seguro.

Dicha información que se recolecta es receptada, procesada y almacenada para que puedan utilizar sus empleados y directivos con fines de trabajo, a su vez esta puede ser transmitida por medios digitales dentro y fuera de las instalaciones de la empresa.

La seguridad es un instinto natural (Lucio Vásquez, 2020) menciona: “El deseo de seguridad de los hombres frente a los peligros que representan la naturaleza, sus semejantes, los estados y últimamente la tecnología, han sido una base fundamental en la formación de entidades políticas”. La seguridad en la actualidad necesita ser altamente eficiente, una mayor conciencia sobre los riesgos ayuda en la toma de decisiones, los riesgos pueden ser identificados, evaluados y atenuados. El conocimiento es la clave para mantener políticas de seguridad efectivas y buenas prácticas de prevención de riesgos con enfoques de mejora continua y por ello la implementación un Sistema de Gestión de la Seguridad de la Información es imprescindible en las organizaciones.

Actualmente, para cualquier organización, implementar un SGSI es de suma importancia para la protección de sus activos de información, más aún en caso obtuviesen la certificación le sumaría un valor agregado al servicio que ofrecen a sus clientes ya que alcanzarían un grado de reconocimiento internacional, el cual les dará a sus clientes una mayor garantía sobre la seguridad de la información.

El problema

Los riesgos y los delitos informáticos han evolucionado al mismo ritmo que la tecnología. Sin embargo, la pandemia ocasionada por el Covid-19 ha acelerado éstos incidentes, por lo cual el manejo de seguridad de la información en la flexibilización laboral y teletrabajo es un compromiso de las organizaciones altamente responsables con sus datos y prestigio.

De igual manera, nunca se puede lograr que un sistema sea totalmente seguro, ya que contantemente surgen nuevas amenazas, pero también existen medidas de seguridad que permite evitar daños y problemas que se pueden ocasionar; es por ello que se han creado numerosas leyes, estándares y normas, cuyo propósito es la prevenciónde ataques para poder mitigar los riesgos.

Al momento la empresa no cuenta con un sistema de información adecuado y fuerte para la gestión de riesgos de seguridad, lo que dificulta establecer y visualizar el estado global de su seguridad, en cuanto a personas, procesos, tecnología y otros aspectos, no existe la participación activa de toda la empresa con relación a la definición de procesos adecuados, planeación e identificación de controles de seguridad.

Es por ello que la empresa requiere asegurar y proteger sus procesos con la finalidad de e sean solo accesibles por aquellas personas que estén debidamente autorizadas; a su vez la empresa no cuenta con una metodología para la identificación y clasificación de riesgos, por lo tanto, es indispensable separar las funciones de seguridad de la información y seguridad informática.

Objetivos

Objetivo general

Implementar un Sistema de Gestión de Seguridad de la Información acorde a la normativa ISO 27001 que permita promover las buenas prácticas de mejora continua sobre la disponibilidad, integridad y confidencialidad de la información de la empresa “Pinto Seguros”.

Objetivos específicos

- Recopilar información sobre ISO/ SGSI y estructura estándar internacional ISO/IEC 27001 para determinar los requisitos normativos de implementación de un SGSI (Sistema de Gestión de Seguridad de la información)
- Examinar las probabilidades e impactos de los riesgos identificados en el alcance y deducir los niveles de riesgo mediante la aplicación de la metodología MAGERIT.
- Implementar el plan de acción del tratamiento de riesgos basado en las fases de la norma ISO 27001.

Planteamiento de hipótesis

- La implementación del Sistema de Gestión de Seguridad de la información ha permitido que

la empresa “Pinto Seguros” tenga procesos adecuados en el manejo de los datos acorde a la norma ISO 27001.

- El plan de tratamiento de riesgo se ajusta a las necesidades de los usuarios de la empresa “Pinto Seguros” y han permitido establecer buenas prácticas de seguridad de la información en el manejo de riesgos e incidentes basado en la norma ISO 27001.

CAPÍTULO I

1. FUNDAMENTACIÓN TEÓRICA

1.1 Seguridad de la información

La seguridad de la información de acuerdo a (ISOTools Excellence, 2015) "El Sistema de Gestión de Seguridad ISO 27001 busca proteger la información y de los sistemas de información del acceso, divulgación o destrucción no autorizada".

La seguridad y la privacidad es muy importante y para (Tecon. Soluciones informáticas, 2019) "Por seguridad de la información se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información". El tratamiento adecuado de los datos y de la información es muy imprescindible en la actualidad, ya que la información es un bien inmaterial invaluable y por lo tanto su tratamiento, manejo aseguramiento tiene que ser prioritario en cualquier organización. La tríada de seguridad de la información se muestra en la Figura 1.

Figura 1. Tríada CIA.

Fuente: (Cambio digital, 2020)

Confidencialidad. – De acuerdo a (Cambio digital, 2020) "Solo los usuarios y procesos autorizados pueden acceder y modificar los datos" . La información no debe llegar a personas que no estén autorizadas.

Integridad.- Según (Cambio digital, 2020) "Los datos deben mantenerse en un estado correcto y nadie debe poder modificarlos de manera incorrecta, ya sea accidental o maliciosamente". Proteger la información frente a vulnerabilidades externas o internas o posibles errores humanos.

Disponibilidad. – La disponibilidad es para (Cambio digital, 2020) "Los usuarios autorizados pueden acceder a los datos siempre que lo necesiten". Acceso a la información por personal autorizado, tomando en cuenta la privacidad.

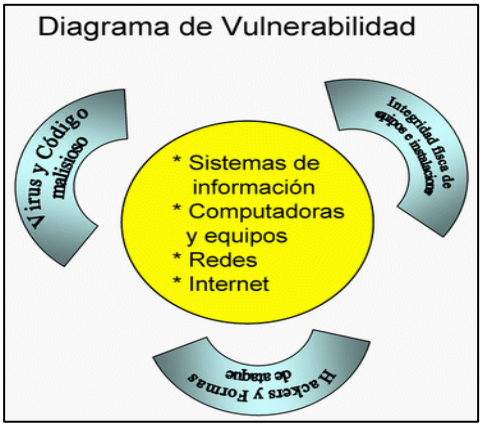
1.2 Seguridad informática

Ciberseguridad.- (Lanz, 2018) "Según los profesionales en seguridad de ISACA (Information Systems Audit and Control Association) la ciberseguridad se define como una capa de protección para los archivos de información". Es la seguridad informática y busca proteger la información digital en los sistemas interconectados.

La seguridad informática como menciona (Universidad Cooperativa de Colombia, 2014) "Asocia temas en un contexto menor tales como: ataques informáticos, virus, Spam, análisis de vulnerabilidad, Firewall, contraseñas, etc.". Este concepto es fundamentalmente técnico, dando importancia a los sistemas de información, las redes y la infraestructura netamente tecnológica, así como a los ordenadores. La vulnerabilidad de un sistema de información, computadoras, redes y equipos se indica en la Figura 2.

Reglas básicas de seguridad informática

Figura 2. Diagrama de Vulnerabilidad.



Fuente: (Seguridad Informática, 2020)

Sistema operativo. - Es importante actualizar el sistema operativo de manera periódica, de acuerdo a (Seguridad Informática, 2020) " se recomienda activar las actualizaciones

automáticas para poder recibir los parches de seguridad de forma automática". Las actualizaciones pueden solucionar pequeños daños o defectos e incluso problemas graves de seguridad.

Antivirus.- (Seguridad Informática, 2020) afirma: "Se recomienda instalar solo un Antivirus así como un Anti-Spam en su ordenador, actualizarlo semanalmente, y analizar las unidades locales y externas periódicamente". Los antivirus protegen los equipos o sistemas informáticos.

Copias de seguridad. – De acuerdo a: (Rouse, 2018) **"**La copia de seguridad, también llamada respaldo o *backup*, se refiere a la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe". La información digital es más valiosa para las empresas, ya que constituyen los respaldos de su actividad e información vital para su razón de ser. Por tal motivo realizar copias de seguridad de manera regular garantiza el resguardo de dicha información. La rapidez de la generación de los respaldos, depende de la información más crítica o relevante.

La frecuencia de pruebas de copias de seguridad (Kirvan, 2019) menciona: "Debe alinear sus pruebas de copia de seguridad con la frecuencia de los respaldos". Entonces la información constituye un activo de TI, el cual estará listo para su utilización en una emergencia.

Seguridad de software. – Según: (Universidad Internacional de Valencia, 2016) **"**La seguridad de software se utiliza para proteger el software contra ataques maliciosos de hackers y otros riesgos, de forma que nuestro software siga funcionando correctamente con este tipo de riesgos potenciales". En el año 2001 los expertos en seguridad recién investigaron de manera ordenada como construir un sistema seguro. Además, existen defectos de software que es importante también evaluar al momento de optar por software, ya que existe mayor riesgo en aplicaciones que tienen salida a internet.

Para: (Intelequia, 2020) es importante aplicar seguridad en el ciclo de vida del desarrollo del software "A nivel de seguridad, debemos considerar a los productos software como entes vivos en constante cambio para corregir vulnerabilidades, añadir controles y adaptarse a las regulaciones y amenazas cambiantes". Actualmente los negocios y actividades digitales generan millones de dólares en ganancias a través del uso de software apropiados para el uso estratégico, pero a la vez también pierden mucho dinero por robos y daños por ataques criminales, por lo tanto, es altamente importante garantizar que el negocio siga siendo rentable. En las distintas fases del ciclo de vida

de desarrollo del software se debe cumplir un marco legal, así como también ciertas políticas de seguridad. El desarrollo de un software también debe ser seguro durante su ciclo de vida, se muestra en la Figura 3.

Figura 3. Ciclo de vida de Desarrollo Seguro de Software.

Fuente: (Intelequia, 2020)

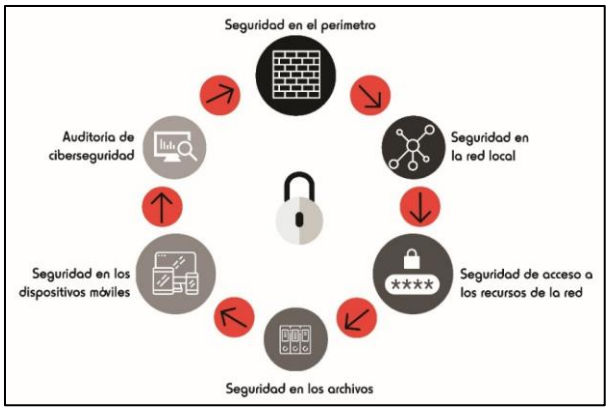
Para desarrollar un software seguro se toma en cuenta 6 fases:

- **Requerimientos. -** considerar los requerimientos de seguridad desde el inicio.
- **Diseño. -** Añadir la seguridad desde la fase de diseño del software para disminuir costos identificando las amenazas mediante threat modeling y diseñar una arquitectura de acuerdo al flujo del negocio.
- **Desarrollo. -** Realizar una codificación segura, tomando en cuenta los entornos de desarrollo integrado.
- **Pruebas. -** Diseñar y ejecutar pruebas manuales específicas para validar los controles implementados y, de esta forma, abordar las amenazas sobre los flujos críticos de negocio.
- **Despliegues. –** Realizar pruebas de intrusión o ethical hacking independientes ejecutadas por un servicio de terceros para asegurar una revisión adecuada.
- **Operaciones. -** Evaluar de manera constante la seguridad mediante pruebas de intrusión y análisis de vulnerabilidades.

Seguridad de red. - De acuerdo a (Cisco, 2020) la seguridad de la red es: "Cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos".

Es importante tener en cuenta la seguridad de la red que permita reducir el riesgo, se indica en la Figura 4.

Figura 4. Defensa en Capas para Reducir el Riesgo.



Fuente: (Fadrell Grupo Tecnológico, 2017)

La seguridad de la red, requiere la seguridad de cada capa y se lo debe hacer tanto en software como en hardware, el software tendrá que ser actualizado de manera frecuente para proteger los datos de diversas amenazas, entonces un sistema de seguridad de red tiene muchos componentes.

Algunos de esos componentes para (Universidad Internacional de Valencia, 2016) son:

- "Antivirus y antispyware
- Cortafuegos, para bloquear el acceso no autorizado a la red
- Sistemas de prevención de intrusiones (IPS)
- Redes privadas virtuales (VPN)". Para mejorar la seguridad, los componentes trabajan de manera conjunta.

Navegación en Internet. – Actualmente la navegación en internet es tan común por cualquier dispositivo y para: (Smile Informática, 2018) "Cuándo navegamos siempre queremos e intentamos en toda medida conservar nuestra privacidad y nuestros datos intactos". Se recomienda evitar sitios web de confiabilidad dudosa, uso de tarjetas en compras por internet, Descargar aplicaciones en sitios oficiales, evitar enlaces poco confiables. Figura 5 muestra la imagen de navegación segura por internet.

Figura 5. Navegar en Forma Segura por Internet.

Fuente: (Smile Informática, 2018)

Contraseñas. - En el ordenador, en las redes sociales y en otros servicios en línea se guarda mucha información personal. (Tecnología Informática, 2018)menciona: "No sólo guardamos fotos y videos de nuestros viajes, sino que también almacenamos allí muchos datos privados de índole comercial, como números de tarjetas de crédito y demás. Es por ello que las contraseñas deben ser seguras y fuertes". Las contraseñas permiten autentificar a los usuarios en cualquier servicio que lo requiera. Entonces se recomienda crear una buena contraseña que contenga letras, números y símbolos.

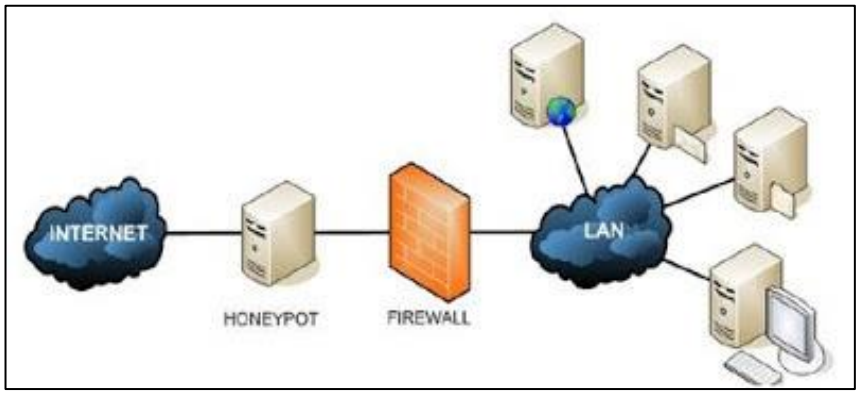
Correo electrónico. – Para: (Digital Guide IONOS, 2020). "Los spambots, o programas "caza-correos", recorren Internet de forma incesante a la búsqueda de direcciones de correo que más tarde podrán utilizar para acciones de publicidad agresiva, para enviar phishing o para distribuir todo tipo de malware". Es evidente que nuestra información cada vez está más expuesta y puede ser utilizada en otros beneficios, entonces será necesario implementar mayores controles de seguridad.

Firewall. – De acuerdo a (Fernández, 2019) un cortafuegos es: "Un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados. También se utilizan en redes de ordenadores, especialmente en intranets o redes locales". Constituye una de las primeras medidas en cuanto a seguridad y su creación e implementación se dio tras el origen del internet, ya que se necesitaba un mayor desarrollo de seguridad de acuerdo a la evolución de la tecnología.

Redes Sociales. – A consecuencia de la pandemia ocasionada por el Covid-19 las redes sociales han tenido un uso masivo y no solamente para pasar el tiempo, sino también para trabajar, estudiar y para impulsar los negocios. “Muchos han descubierto internet a consecuencia de la COVID, para bien o para mal, o bien se han visto obligados a usar la red de redes” (López, 2020). Con el uso global de las redes es necesario estar preparados ante las amenazas y no compartir información confidencial, ya que los fraudes y suplantaciones de identidad son las principales amenazas con las que se puede encontrar.

Red LAN. - Las redes LAN brindan soluciones eficientes en la transmisión de información entre ordenadores. “Las redes inalámbricas son bastante populares en la actualidad, siendo muy atractivas para los atacantes, ya que es muy fácil intentar conectarse silenciosamente” (Seguridad Informática, 2019).En la Figura 6 se muestra la seguridad de una Red LAN.

Figura 6. Seguridad de una Red LAN.



Fuente: (Seguridad Informática, 2019)

1.3 Análisis de riesgo

Luego de haber identificado y clasificado los riesgos, es importante analizarlos según explica: (Análisis de Riesgos, 2019)“Se estudian la posibilidad y las consecuencias de cada factor de riesgo con el fin de establecer el nivel de riesgo de nuestro proyecto”. El análisis del riesgo determina los factores de riesgo potencialmente peligrosos y con mayor efecto en nuestros datos o información, por lo cual deberán ser gestionados de manera prioritaria.

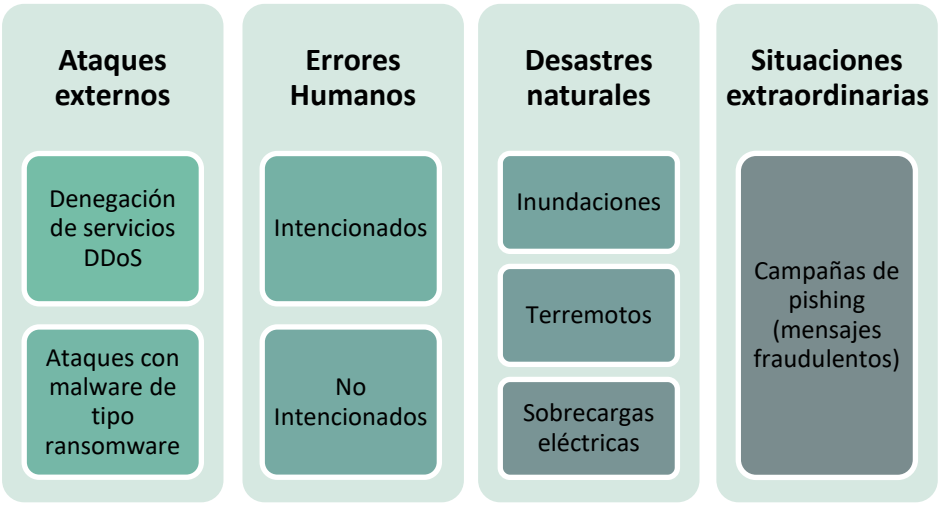
(Rodríguez, 2020) afirma: “El análisis y gestión de los riesgos previene a las empresas de este tipo de situaciones negativas para su actividad y recoge una serie de factores fundamentales para su consecución”. Para eso será indispensable identificar todos los activos de la empresa, en

los cuales se incluyen los recursos afines a la gestión de la información en la empresa (software, hardware, comunicación, documentación digital, manuales y recursos humanos).

1.3.1 Riesgos y amenazas

Cuando se identifican todos los activos de la información que tenga la empresa, es necesario identificar las amenazas a las que se puede estar expuestos como se muestra en la Figura 7.

Figura 7. Riesgos y Amenazas.



Fuente: (Rodríguez, 2020)

Las ventajas de la transformación digital también están acompañadas de amenazas que ponen en riesgo la seguridad y además la privacidad se ve altamente afectada. Los ciberdelincuentes siguen evolucionando con el objetivo de robar información.

Las empresas siempre deben analizar los riesgos informáticos para tomar medidas que logren evitar efectos negativos o a su vez mitigar los efectos. El diagrama de análisis de riesgos se muestra en la Figura 8.

Figura 8. Análisis de riesgos.

Fuente: (Ayudaley, 2017)

Con la globalización y "Con las nuevas tecnologías nuestros datos personales circulan por la red sin ningún tipo de control" (Ayudaley, 2017). Es por eso que en Europa se ha publicado el Reglamento General de Protección de Datos (RGPD), que es una normativa a seguir para el tratamiento de datos personales y cuyo objetivo es proteger el derecho de las personas físicas, con el fin de preservar su información.

Razones para realizar el análisis. – Los avances tecnológicos y los delitos informáticos son cada vez más frecuentes y la información personal, así como los datos empresariales son vulnerables.

Describir flujos de información. – Es el proceso que debe seguirse para establecer las medidas de seguridad.

Identificar los riesgos. - Es el plan de gestión de riesgos, en el cual se pueden incluir: alcance, cronograma, costos, nivel de calidad. En este proceso la identificación puede ser temprana, reiterada, emergente, extensa y proporcionada.

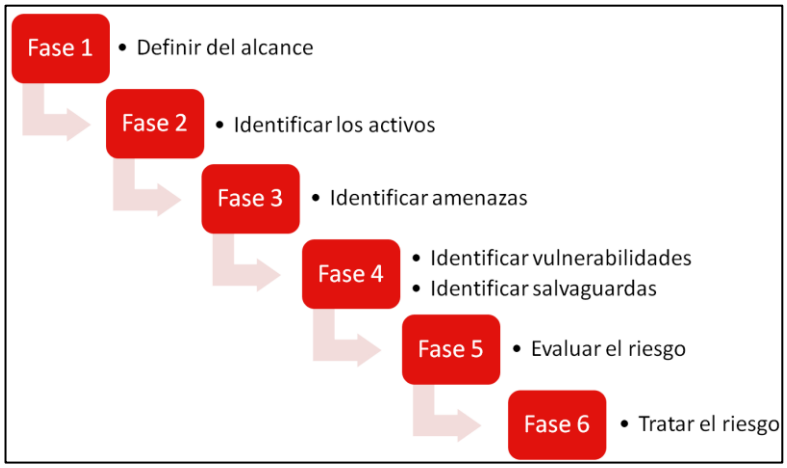
Establecer soluciones. – "Una vez que hemos identificado los riesgos para la privacidad, tal y como hemos descrito en el punto anterior, lo más lógico es desarrollar las medidas correspondientes para eliminar o mitigar dichos riesgos" (Ayudaley, 2017).

Implementar soluciones. – Una vez recogidas las conveniencias necesarias que garanticen la privacidad, es momento de tomar la decisión "cuáles de ellas implementamos, ya que como se ha comentado anteriormente, no necesariamente hay que poner en funcionamiento todas" (Ayudaley, 2017). La empresa puede adjudicarse determinados riesgos, siempre y cuando sean considerados como tolerables. Sin embargo, pueden existir riesgos que no se puedan eliminar.

Participación de los agentes implicados. - En cualquier fase del análisis de riesgos debe fluir la información en todos los niveles de la organización. Interno y externo, para saber la opinión de los afectados y dar transparencia a la información entre usuarios y consumidores.

Integrar análisis de riesgos. – Para garantizar la privacidad de productos y servicios. "Todas las empresas, sin excepción, deben analizar las vulnerabilidades informáticas y potenciales brechas de seguridad lógica con el fin de seleccionar e implementar las mejores soluciones informáticas destinadas a impedir, bloquear o neutralizar los ataques" (Ayudaley, 2017). También se puede implementar un Plan Director de Seguridad (PDS) que consta de 6 fases como indica la Figura 9

Figura 9. Defensa en Capas para Reducir el Riesgo.



Fuente: (Fadrell Grupo Tecnológico, 2017)

1.4 ISO/ SGSI

ISO (International Organization for Standardization), (ISO 2700.ES, 2005) afirma: "Es la Organización Internacional de Normalización, integrada por más de 160 países". La función de ISO es normar productos y servicios, las normas son optativas.

Un SGSI es la abreviatura de un (Sistema de Gestión de Seguridad de la Información), (ISO 2700.ES, 2005) dice: “Un SGSI a través de un enfoque sistémico se busca preservar la confidencialidad, integridad y disponibilidad de la información”.

1.4.1 Anexo SL

(Nqa. Organismo de Certificación Global., 2020) menciona: “El Anexo SL proporciona una nueva estructura, denominada de Alto Nivel, para los sistemas de gestión ISO- sustituye a la histórica Guía 83 de la ISO”. El anexo SL fue creada para implantar un texto base idéntico con cláusulas y definiciones comunes. Con SL permite:

- Optimizar las normas
- Fomentar la certificación
- Facilitar la integración de los sistemas de gestión

La estructura alineada a Anexo SL se muestra en la Figura 10.

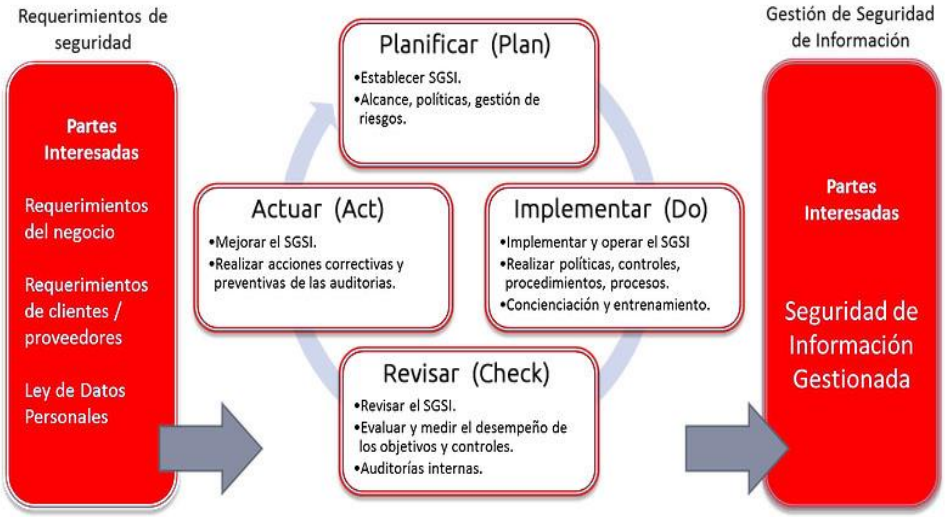
Figura 10. Estructura Alineada a Anexo SL.

Fuente: **(**Buigues, 2015)

1.4.2 Fases del sistema de gestión

De acuerdo al ciclo de mejora continua, un Sistema de Gestión está formado por 4 fases, para reducir al mínimo los riesgos de la información es necesario la implementación de forma constante. En la Figura 11 se muestra las fases del sistema de gestión.

Figura 11. Fases del Sistema de Gestión.



Fuente: (Redser, 2019)

Planificar. – Establecer los objetivos de seguridad de la información, para determinar los controles adecuados (catálogo de posibles controles)

Implementar. – Aplicar todo lo establecido en la fase anterior

Revisar. – Comprobar y verificar si el funcionamiento y los resultados cumplen lo determinado.

Actuar. – Para mejorar los incumplimientos que han sido detectados en la fase de revisión. (Redser, 2019) menciona: "El cumplimiento de esta norma es una **decisión estratégica apoyada por la dirección**, debe existir un compromiso firme para establecer una política y asignar recursos necesarios para su cumplimiento". El principal objetivo es proteger la información para evitar que caiga en las manos equivocadas o se pierda, ya que las amenazas pueden ser externas o internas y pueden ser de maliciosas o accidentales.

La Organización Internacional de Estandarización acopia un número extenso de normas en la familia ISO 27000, como se muestra en la Tabla 1.

Tabla 1 Familia ISO

N°	ISO	Función
1)	27000:2018	Fundamentos y Vocabulario
2)	27001:2013	Norma Principal
3)	27002:2013	Buenas Prácticas
4)	27003:2017	Guía de Implementación
5)	27004:2016	Métricas y Mediciones
6)	27005:2018	Gestión de Riesgos
7)	27006:2015	Esquema de Certificación
8)	27007:2017	Guía de Auditoría al SGSI
9)	27008:2011	Guía de Auditoría a los Controles
10)	27032:2012	Lineamientos de Ciberseguridad

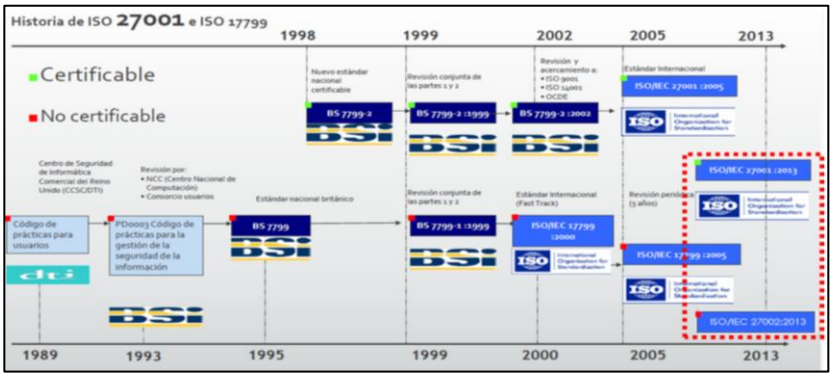
Fuente: (ISOTools Excellence, 2015)

1.5 Historia de la ISO /IEC 27001

La ISO 270001 es la norma ISO que establece los requerimientos para implementar, mantener y mejorar un SGSI y en la actualidad es el único estándar aceptado a nivel internacional para la gestión de la Seguridad de la Información.

La ISO actualmente ha ido evolucionando gracias a normas y buenas prácticas que han permitido a las empresas administrar apropiadamente la seguridad de la información. “La ISO 27001 como la conocemos hoy en día, ha sido resultado de la evolución de otros estándares relacionados con la seguridad de la información” (ISOTools Excellence, 2015). La historia de los ISO 27001 se muestra en la Figura 12.

Figura 12. Historia de la ISO/IEC 27001.



Fuente: (ISOTools Excellence, 2015)

1.5.1 Norma ISO/IEC 27001 Gestión de la Seguridad de la Información

Un sistema de Gestión de Seguridad de la Información (SGSI) constituye "El medio más eficaz de minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización" (BSI, 2020). La estrategia de negocio consiste en adoptar controles y procedimientos eficaces para la empresa.

ISO/IEC 27001:2013 = NTP ISO/IEC 27001:2014. Permite reforzar la seguridad de la información y disminuir los riesgos de fraude, así como la pérdida o filtración de información.

Algunos beneficios de la Norma ISO/IEC 27001.

- Identificar los riesgos y establecer controles para gestionarlos o eliminarlos.
- Confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información.
- Flexibilidad para adaptar los controles a todas las áreas de la empresa o solo a algunas seleccionadas.
- Conseguir que las partes interesadas y los clientes confíen en la protección de los datos
- Demostrar conformidad y conseguir el estatus de proveedor preferente.
- Alcanzar las expectativas demostrando conformidad. (BSI, 2020).

1.5.2 Diferencias entre la ISO/IEC 27001 e ISO/IEC 27002

En las normas para la evaluación de la seguridad de la información se incluye dos partes:

ISO/IEC 27001:2013 Describe los requisitos para la implementación y la documentación necesaria de un Sistema de Gestión de Seguridad de la Información (SGSI). Constituye:

- Tecnología de la Información.
- Técnicas de Seguridad.
- Sistemas de Gestión de Seguridad de la Información.
- Requisitos.

ISO/IEC 27002:2013 es el documento de referencia para las mejores prácticas de un SGSI, en donde contienen las instrucciones para la implementación.

Código de Prácticas para Sistemas de Gestión de Seguridad. Procedimiento para implementar ISO 27001:

Tabla 2. Procedimiento para Implementar ISO 27001

N°	Proceso
1)	Obtener el apoyo de la dirección
2)	Utilizar una metodología para gestión de proyectos
3)	Definir el alcance del SGSI
4)	Redactar una política de alto nivel sobre seguridad de la información
5)	Definir la metodología de evaluación de riesgos
6)	Realizar la evaluación y el tratamiento de riesgos
7)	Redactar la Declaración de aplicabilidad
8)	Redactar el Plan de tratamiento de riesgos
9)	Definir la forma de medir la efectividad de sus controles y del SGSI
10)	Implementar todos los controles y procedimientos necesarios
11)	Implementar programas de capacitación y concienciación
12)	Realizar todas las operaciones diarias establecidas en la documentación del SGSI
13)	Monitorear y medir el SGSI
14)	Realizar la auditoría interna
15)	Realizar la revisión por parte de la dirección
16)	Implementar medidas correctivas

Fuente: (Normaiso 27001, 2020)

Tabla 3. Documentación requerida para implementar ISO 27001

N°	Documentación	Referencias
1)	Alcance del SGSI	(punto 4.3)
2)	Objetivos y política de seguridad de la información	(puntos 5.2 y 6.2)
3)	Metodología de evaluación y tratamiento de riesgos	(punto 6.1.2)
4)	Declaración de aplicabilidad	(punto 6.1.3 d)
5)	Plan de tratamiento de riesgos	(puntos 6.1.3 e y 6.2)
6)	Informe de evaluación de riesgos	(punto 8.2)
7)	Definición de roles y responsabilidades de seguridad	(puntos A.7.1.2 y A.13.2.4)
8)	Inventario de activos	(punto A.8.1.1)
9)	Uso aceptable de los activos	(punto A.8.1.3)
10)	Política de control de acceso	(punto A.9.1.1)
11)	Procedimientos operativos para gestión de TI	(punto A.12.1.1)
12)	Principios de ingeniería para sistema seguro	(punto A.14.2.5)
13)	Política de seguridad para proveedores	(punto A.15.1.1)
14)	Procedimiento para gestión de incidentes	(punto A.16.1.5)
15)	Procedimientos para continuidad del negocio	(punto A.17.1.2)
16)	Requisitos legales, normativos y contractuales	(punto A.18.1.1)

Fuente: (Normaiso 27001, 2020)

Tabla 4. Registros requeridos para implementar ISO 27001

N°	Registros	Referencias
1)	Registros de capacitación, habilidades, experiencia y calificaciones	(punto 7.2)
2)	Monitoreo y resultados de medición	(punto 9.1)
3)	Programa de auditoría interna	(punto 9.2)
4)	Resultados de auditorías internas	(punto 9.2)
5)	Resultados de la revisión por parte de la dirección	(punto 9.3)
6)	Resultados de medidas correctivas	(punto 10.1)
7)	Registros sobre actividades de los usuarios, excepciones y eventos de seguridad	((puntos A.12.4.1 y A.12.4.3)

Fuente: (Normaiso 27001, 2020)

1.6 Anexo A ISO 27001

El Anexo A es una guía para toda organización que desea implementar un Sistema de Gestión de seguridad de la Información. (ISOTools Excellence, 2015) define. “Es un documento normativo que sirve como guía para implementar los controles de seguridad específicos de ISO 27001”. Este documento está compuesto por 114 controles de seguridad, sin embargo, para brindar asesoría en el tema de flexibilización laboral y teletrabajo que permita reactivar la economía frente a la crisis ocasionada por la pandemia del Covid-19 se tomará en cuenta la composición A.6 Organización de la Seguridad de la información, para que mediante los controles se puedan establecer responsables y además el acceso a dispositivos móviles y situaciones como la de teletrabajo, conforme al ACUERDO MDT-2020-076 emitido por el Ministerio de Trabajo del Ecuador el 12 de marzo del 2020.

1.7 Teletrabajo

Un efecto de la pandemia ocasionada por el Covid-19 ha sido la flexibilización laboral, lo que ha permitido la incorporación de nuevas tecnologías y a la par el incremento de delitos informáticos.

Según, (Barrionuevo, 2020) “flexibilidad incorpora, además, posibilidades alineadas con la protección de los derechos laborales”.

CAPÍTULO II

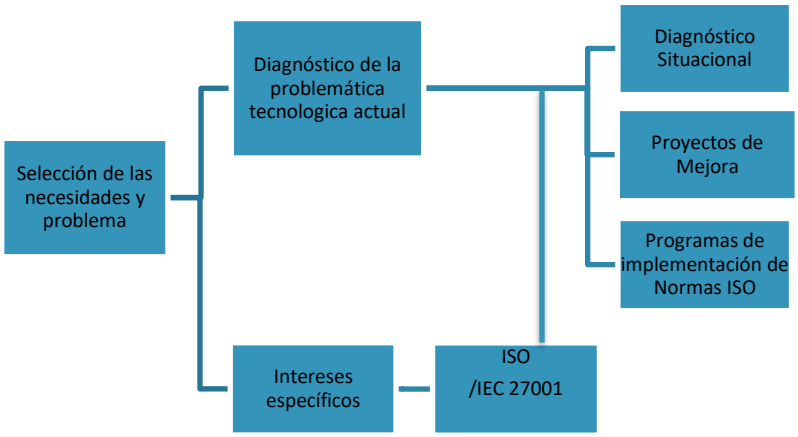
2. MARCO METODOLÓGICO

El presente trabajo es de aplicación sin embargo ha sido necesario recolectar, seleccionar e interpretar datos relevantes al proceso de Gestión de Seguridad de la Información, así como también conocer las necesidades de la empresa.

Con el enfoque metodológico se pretendió coordinar y alcanzar los objetivos propuestos acerca de información ISO/ SGSI y estructura estándar internacional ISO/IEC 27001 para determinar los requisitos y normativas que permitan el establecimiento, implementación, operación, supervisión yrevisión de un SGSI (Sistema de Gestión de Seguridad de la información).

Para el estudio se consideró el área informática, la problemática sobre la vulnerabilidad de la seguridad de la información, los posibles riesgos informáticos, las alternativas tecnológicas de solución y las normativas para la implementación de seguridades de Sistemas de información. La Figura 13 muestra la metodología utilizada.

Figura 13. Metodología.

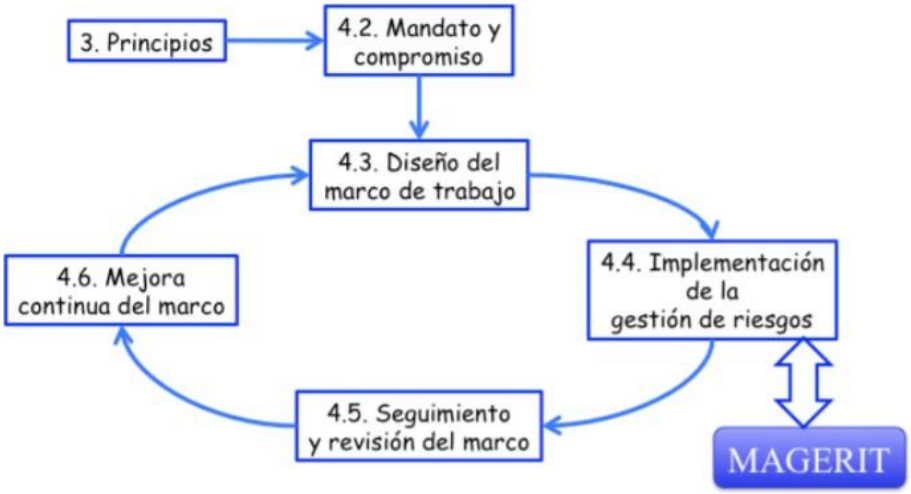


Elaborado por: Bryan Alexander Guanín Castillo

Para el proceso de gestión de riesgos se ha tomado en cuenta la metodología Magerit, porque implementa el proceso de gestión de riesgos enfocado al trabajo, pensado a orientar a los gobiernos a tomar en cuenta riesgos producidos por el uso de tecnologías de la información.

Según (ISOTools Excellence, 2015) “Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista”. Además, Magerit tiene objetivos directos e indirectos para el análisis de riesgos.

Figura 14. ISO 31000 Magerit V3



Fuente: (Normaiso 27001, 2020)

2.1. Magerit

Magerit, es la “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Publicas”, mismo que fue creado por el Consejo Superior de Administración Electrónica (CSAE); cuyo uso de esta metodología es de carácter público.

Está dirigido para los medios electrónicos, informáticos y telemáticos, debido a que su uso en la actualidad es a diario, se ha dado lugar a ciertos riesgos que se deben de evitar con medidas preventivas con la finalidad de lograr tener confianza y así poder utilizarlos.

Magerit, de igual manera es un método formal que permite investigar los riesgos que soportan los Sistemas de Información, para así recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

2.1.1. Objetivos de Magerit.

Directos:

- Concienciar a los responsables de los sistemas de información sobre la existencia de riesgos y de la necesidad de detectarlos a tiempo.

- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las salvaguardas oportunas para mantener los riesgos bajo control.

Indirectos:

- Preparar a la empresa para procesos de evaluación, auditoría, certificación o acreditación, según corresponda cada caso.

2.1.2. Análisis de metodología de gestión de riesgos

- ✓ La metodología COBIT, es de análisis cuantitativo, cualitativo y mixto.
- ✓ COBIT, OCTAVE y MAGERIT, son metodologías que ofrecen un análisis más completo de elementos dentro del proceso u organización.
- ✓ Por otro lado, la metodología MAGERIT, ofrece un análisis completo desde los objetivos de seguridad.

2.2. Fases para implementar ISO 27001

2.2.1. Fase 1: Auditoría inicial Gap Analysis

En la ISO 27001:2013 es necesario realizar un análisis de riesgos que permita determinar el alcance efectivo de los controles a implementar (Normaiso 27001, 2020) .

- Auditoría inicial con la idea clara de nivel de implantación de la norma ISO 27001.
- Establecer el inicio para implantar la norma y evaluar el cuidado indispensable que permita tener una herramienta confiable y así elaborar el plan para la implementación de ISO 27001.
- Durante el proceso de implantación es importante mantener un instrumento de evaluación del nivel de avances del proyecto.

Para la realización del análisis de brechas GAP se conseja la utilización de un modelo de cumplimento o madurez.

2.2.1.1. Niveles de Madurez

- ➢ Nivel 0: En este nivel no existe la necesidad del control o requisito

- Nivel 1: Existe algo de reconocimiento de la necesidad de reconocimiento de requisito o control interno. Se puede aplicar para tareas específicas
- Nivel 2: Existen controles ejecutados, pero no se encuentran documentados.
- Nivel 3: Los controles se encuentran definidos y documentados.
- Nivel 4: Existe un control interno manejable y medible del cumplimiento de los requisitos.
- Nivel 5: Existe un control interno óptimo que mide la eficacia de los controles y que permite determinar objetivos de mejora.

2.2.1.2. Nivel de Cumplimiento

Para determinar el cumplimiento de los niveles de madurez de la organización se puede utilizar un listado de preguntas de acuerdo a los controles estándar ISO 27001 (Normaiso27001, 2020). Además, también se utilizará un listado de preguntas de acuerdo al anexo A de la normativa.

2.2.2. Fase 2: Análisis del contexto de la organización y determinación del alcance

En esta fase permite según (Normaiso 27001, 2020): "establecer el contexto del SGSI en cumplimiento de los requisitos de la norma ISO 27001 recogidos en la cláusula 4 de la Norma". En esta fase enseña cómo emprender el nuevo requisito que proporciona comprensión de la organización y sus necesidades.

Es importante considerar las necesidades y las expectativas que tienen las partes involucradas.

2.2.2.1. Proceso para el requisito:

a) Entender a la organización y su contexto
   - Comunicación y Consultas
   - Contexto del SGSI
   - Contexto de la Gestión de Riesgos
   - Definición de criterios del Riesgo

b) Entender las necesidades y expectativas de las partes involucradas
   - Descripción

c) Determinación del alcance del Sistema de Gestión
   - Propósito del Alcance del SGSI

- Manera para definir los limites el SGSI
- Cuestionario para definir el Alcance del SGSI

2.2.2.2. Comprender la Organización y su contexto

Para identificar y diferenciar el contexto interno y externo de la Organización la Norma ISO 27001 conjuntamente con los estándares ISO 31000 propone determinar la medida de afectación a los propósitos de la Organización mediante los agentes internos y externos (Normaiso 27001, 2020). Para identificar la influencia en la Seguridad de la Información, se recomienda realizar un análisis y evaluación de riesgos, lo que equivale a determinar:

- Cómo se gestiona y gobierna la organización
- Conocimiento y capacidades de la organización
- Cultura organizacional
- Relaciones contractuales
- Influencia de las condiciones ambientales
- Tendencias del mercado y condiciones regulatorias
- Avances tecnológicos
- Relaciones con proveedores externos

2.2.2.3. Comunicación y consulta

Consiste en la elaboración de un plan de comunicación que permita conocer el nivel de efectividad de las medidas determinadas para la seguridad de la información (Normaiso 27001, 2020). Los niveles de efectividad podrían ser para:

- Adquirir respaldos seguros
- Riesgos identificados por distintas áreas de experiencia
- Integrar y comprender los intereses de todas las partes interesadas
- Mejorar la comunicación con los agentes internos y externos

2.2.2.4. Contexto del SGSI

Permite definir los parámetros internos y externos a tener en cuenta cuando se gestiona el riesgo (Normaiso 27001, 2020). A continuación, se detallan los contextos externos e internos.

a) El contexto externo puede incluir:

- Entorno social y cultural, político, legal, regulatorio, financiero, tecnológico, económico, ambiental
- Entorno competitivo, ya sea internacional, nacional, regional o local;
- Factores clave del negocio y las tendencias que tienen impacto en los objetivos de la organización;
- Percepciones y los valores de (contratistas, clientes, administraciones públicas etc.).

b) El contexto interno puede incluir:

- Administración (estructura organizacional, los roles y responsabilidades)
- Políticas, objetivos y estrategias a alcanzar
- Capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías);
- Relaciones con las percepciones y valores de los agentes internos;
- Cultura de la organización;
- Sistemas de información formales como informales (flujos de información y procesos de toma de decisiones)
- Normas, directrices, modelos adoptados por la organización, forma y el alcance de las relaciones contractuales.

2.2.2.5. Contexto de la Gestión de Riesgos

Para (Normaiso 27001, 2020): "El contexto del proceso de gestión de riesgos variará de acuerdo con las necesidades". Sin embargo, para el mismo autor, la organización puede contemplar:

- Definir las metas y objetivos de las actividades de gestión de riesgos;
- Definir responsabilidades dentro del proceso de gestión de riesgos;
- Definir el alcance, así como la profundidad y amplitud de las actividades de gestión de riesgos que se llevarán a cabo, incluidas las exclusiones específicas;

- Definir la actividad, proceso, función, proyecto, producto, servicio o activo en términos de tiempo y ubicación;
- Definir las relaciones entre un proyecto, proceso o actividad particular y otros proyectos, procesos o actividades de la organización;
- Definir las metodologías de evaluación de riesgos;
- Definir la forma en que se evalúa el rendimiento y la efectividad en la gestión del riesgo;
- Identificar y especificar la toma de decisiones;
- Identificar el alcance o los estudios necesarios, su extensión, objetivos, y los recursos requeridos para dichos estudios.

2.2.2.6. Definición de criterios de riesgo

La organización define los criterios a utilizarse al momento de evaluar el nivel de importancia del riesgo, para lo cual se debe considerar:

- Naturaleza, los tipos de causas y consecuencias que pueden ocurrir (medición);
- Forma para definir la probabilidad;
- Marco de tiempo de la probabilidad y / o consecuencia;
- Formas y herramientas para determinar el nivel de riesgo;
- Opiniones de los interesados;
- Determinar el nivel de riesgo (aceptable o tolerable);
- Consideraciones de las combinaciones de riesgos múltiples a tomar en cuenta.

Para facilitar el proceso, tomar en cuenta las siguientes interrogaciones de ejemplo:

- ¿Cómo podría afectarse la (confidencialidad, integridad y disponibilidad) de la información?
- ¿Qué valor agregado tienen los activos de información para la Organización?
- ¿Cuál sería el impacto que tendría una divulgación involuntaria de la información? ¿Qué supondría un evento o incidente?
- ¿Cuál sería el impacto de la pérdida de confianza en la integridad de la información?

- ¿Qué consecuencias tendría una divulgación involuntaria de información en un acuerdo de subcontratación o en el extranjero?
- ¿Cuáles son las fuentes de riesgo?
- ¿Qué amenazas existen?

Al examinar la información para el proceso de identificación de riesgos, es importante tener en cuenta los planes de seguridad (Normaiso 27001, 2020). Las personas u organizaciones constituyen las partes interesadas de acuerdo al contexto SGSI y por lo tanto ellas influyen directamente en la seguridad de la información y determinan la continuidad del negocio, ya que pueden verse afectadas por la seguridad de la información.

Entre las partes interesadas se contemplarían:

- Colaboradores y sus familias
- Accionistas/ propietarios del negocio
- Agencias gubernamentales y entidades reguladoras
- Servicios de emergencia (911, bomberos, policía, ambulancia, etc.)
- Clientes
- Medios de comunicación
- Socios y proveedores
- Personas consideradas importantes para el negocio.

Es significativo que la organización tome en cuenta las peticiones a considerar:

- Las necesidades y/o expectativas importantes la seguridad de la información.
- Incluir requisitos legales y reglamentarios, así como también las obligaciones contractuales de las partes interesadas
- Detectar lo que las partes requieren para satisfacerlos en el SGSI.

Las peticiones de las partes interesadas podrían ser, por ejemplo:

- Las entidades regulatorias pretenden el cumplimiento de las leyes y regulaciones sobre seguridad de la información y protección de datos

- Los accionistas solicitan seguridad en sus inversiones y además utilidad
- Los clientes esperan que se cumplan con las cláusulas de seguridad en los contratos y en los datos personales
- Los medios de comunicación buscan información y noticias de forma ágil y precisa relacionadas con los incidentes en seguridad de información, etc.

Es necesario identificar los requisitos, antes de iniciar el desarrollo del SGSI (Normaiso 27001, 2020).

2.2.2.7. Definir el Alcance de un SGSI

El alcance de un SGSI, es el ámbito de la organización que queda sometido al SGSI, mismo que se debe incluir una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas, prestando especial atención en aquellos casos en los que el ámbito de influencia del SGSI considere una parte menor de la organización como delegaciones, divisiones, áreas, procesos o tareas concretas.

2.2.3. Fase 3: elaboración de la política - objetivos del sgsi

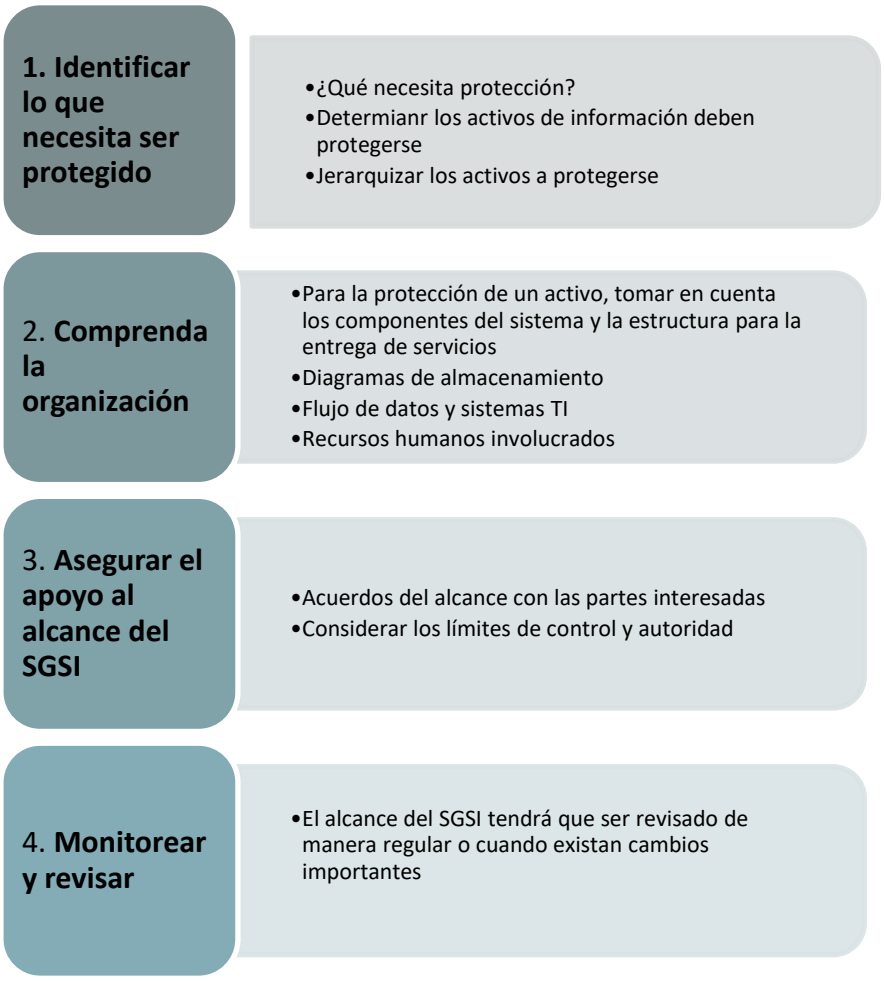
2.2.3.1. Política de seguridad

La Política de Seguridad es un requisito de la norma ISO 27001 y considera los objetivos de la seguridad de la información de la organización (Normaiso 27001, 2020).

2.2.3.2. Redactar de acuerdo a las necesidades de cada organización

Para redactar la política es necesario tomar en cuenta el tamaño, estructura y la actividad de la organización (Normaiso 27001, 2020).

Figura 15. Proceso para Definir el Alcance de un SGSI



Fuente: (Normaiso 27001, 2020)

2.2.3.3. Tener en cuenta los objetivos de cada organización

En la política de seguridad protege a la organización para el logro de los objetivos (Normaiso 27001, 2020).

Los objetivos de la organización se ven desde dos aspectos:

- Objetivos comerciales
- Objetivos de Seguridad de la Información

2.2.3.4. Demostrar que se tienen en cuenta los requisitos de las partes interesadas

Una vez identificadas las expectativas de las partes interesadas, es tiempo de referirse al compromiso que tiene la organización para satisfacerlas (Normaiso 27001, 2020).

2.2.3.5. Comunicación de la política a las partes interesadas

Se recomienda nombrar un responsable que permita el cumplimiento de los procedimientos y con ello garantizar que se cumplan las fechas y la forma de la comunicación (Normaiso 27001, 2020).

2.2.3.6. Propiedad

Establecer el propietario de la política, así como también el proceso de revisión para el cumplimiento de los requisitos de la norma ISO 27001 (Normaiso 27001, 2020).

En la política de la seguridad se puede incluir:

- Alcance del SGSI
- Responsabilidades del SGSI
- Estructura de la organización
- Enfoque y la metodología para el análisis y evaluación de riesgos

2.2.3.7. Objetivos de seguridad del SGSI

Objetivo general: Implementar todas las iniciativas que logren el cumplimiento de los objetivos de seguridad del SGSI (Normaiso 27001, 2020). La política de la Seguridad de la Información constituye una base para la planificación de seguridad aun cuando se amplifican los sistemas o se crean nuevas aplicaciones:

- Al describir las responsabilidades del usuario, como proteger la información confidencial y crear contraseñas no leves.
- Al explicar cómo controlará la efectividad de las medidas de seguridad.
- El control y la monitorización ayuda a detectar intentos de evasión de las protecciones de resguardo de la información.

Es indispensable que los objetivos se definan de forma clara durante el desarrollo de la política (Normaiso 27001, 2020). Los objetivos se pueden clasificar en las siguientes categorías:

1. **Protección de activos de información**

- Garantizar que solo los usuarios autorizados puedan acceder a la información en SGSI.
- Capacidad de asegurar todos los tipos de recursos del sistema.
- Categorizar adecuadamente a los usuarios que pueden acceder al sistema.
- Definir el tipo de autorizaciones de acceso que serán otorgados a los usuarios.

2. **Autenticación**

- Utilizar métodos más sólidos para verificar los accesos al sistema ante posibles falsas identidades.
- Permisos de acuerdo a los niveles de permisos una vez autentificados.

3. **Autorización**

- La autorización de acceso a los diferentes recursos está determinada por la autenticación del SGSI.
- Política para renovar autorizaciones habitualmente y así garantizar el acceso a información sensible.

4. **Integridad de la información**

- Integridad de datos
- Integridad del sistema
- Garantizar pruebas de transmisión de información de manera bilateral entre emisor y receptor.
- Garantizar la confidencialidad de la información
    - Entornos privados para la información sensible y evitar accesos no autorizados y ataques maliciosos.
    - Cifrado de datos mediante el uso de certificados digitales
    - Conexiones Secure Socket Layer (SSL) o red privada virtual (VPN)
    - Garantizar la confidencialidad de la información dentro de la red, sistemas de la organización y también cuando la información abandona la red.

5. Auditoría de actividades de seguridad

- Registrar actividades sospechosas y posibles incidentes para evitar o prevenir eventos no deseados.
- Supervisar eventos relevantes para evaluar y registrar accesos en (exitosos, no exitosos o denegados), con eso determinar la interacción de los usuarios e identificar posibles violaciones de seguridad.

2.2.4. Fase 4: Planificación del SGSI

2.2.4.1. Inventario de Activos

Proceso para identificar activos:

a) Identificar los servicios internos y externos de la organización
b) Información necesaria para desarrollar los servicios
c) Infraestructura incluida en la prestación de los servicios
    - Hardware (computadoras portátiles, servidores, impresoras, teléfonos móviles o memorias USB).
    - Infraestructura (oficinas, electricidad, aire acondicionado etc.)
d) Software (comprado y gratuito) involucrado en la prestación de los servicios.
e) Identificar las actividades subcontratadas (servicios)
    - Legales
    - De Limpieza
    - En la nube
    - De correo, etc.
f) Identificar las personas de las que dependen los servicios o información relevante para el negocio.
g) Determinar los medios de transmisión de la información
h) Identificar los soportes en los que se encuentra la información (digital, papel y otros medios).

De acuerdo a la norma ISO 27001 la recomendación para un Inventario de Activos con tipo de Información y estructura (Normaiso 27001, 2020). El inventario de activos se describe a continuación:

- Nombre del Proceso
- Propietario del proceso
- Nombre del Activo
- Descripción del Activo
- Tipo de activo de información
    - Especificar tipo (Copia impresa, archivo digital)
    - Especificar tipo de dispositivo (extraíble, disco duro, nube)
- Especificar si el activo contiene datos personales sensibles
- Nivel de confidencialidad (Alta – Media – Baja)
- Nivel de disponibilidad (Alta – Media – Baja)
- Nivel de integridad (Alta – Media – Baja)
- Responsable de la custodia del activo
- Periodo de custodia de datos
- Nivel de protección Actual
    - **Para copia impresa:**
        - ✓ Almacenado en (caja fuerte a prueba de fuego, en armario/ archivo sin llave, escritorio, bajo llave en todo momento, se mantiene bajo llave durante la noche, etc.)
    - **Para copia electrónica:**
        - ✓ Almacenado en (unidades locales sin protección o protegidas, unidad de red en portátil sin protección o con protección, PC desprotegido o protegido, computadora portátil cifrado o PC)

Si la información se trasfiere o transmite tiene que detallarse el destino y el nivel de protección en el nuevo destino (Normaiso 27001, 2020).

2.2.4.2. Valoración de activos y asignación del nivel de riesgo

En relación al impacto comercial perjudicial que tendría un posible evento, se asignará a cada activo un nivel de riesgo.

Además, se deberá establecer con la mayor precisión admisible la probabilidad de frecuencia del evento para determinar el perfil de riesgo de cada uno de los activos para determinar el daño supuesto y así definir una escala de valoración aplicable a cada activo para prever la afectación en pérdida de confidencialidad, integridad o disponibilidad (Normaiso 27001, 2020).

2.2.4.3. Catálogo de amenazas

Para identificar las amenazas que podrían afectar la Seguridad de la Información de la organización se tiene que elaborar y diseñar un catálogo de amenazas. Además, se debería identificar la fuente de la amenaza, agentes y motivaciones (Normaiso 27001, 2020).

2.2.4.4. Valoración de las amenazas para la seguridad de la información

Se refiere a la frecuencia de ocurrencia de las amenazas, ante lo cual es necesario identificar la probabilidad que sucedan, determinando una escala de valor para cada amenaza (Normaiso 27001, 2020).

2.2.4.5. Nivel de Vulnerabilidad

Si la amenaza se produce el nivel de vulnerabilidad considera el grado de afectación que tendría la organización con la pérdida de información (Normaiso 27001, 2020). Es importante establecer adecuadamente la escala para el impacto de pérdida y vulnerabilidad, ya que los valores van a variar en los diferentes activos.

2.2.4.6. Análisis de riesgos

Frente a una amenaza potencial podemos ahora establecer un análisis en base a los parámetros de la frecuencia y el valor de la vulnerabilidad (Normaiso 27001, 2020). El análisis de riesgos es un proceso en el cual se tomarán en cuenta los niveles de impacto.

2.2.4.7. Evaluación de riesgos

Cuando se ha determinado un valor de riesgo para cada amenaza que puede afectar a un activo de información, se debe definir los criterios aceptables para el riesgo (Normaiso 27001, 2020). Seleccionar los niveles de riesgo pueden ser asumibles y determinar ante cuales tomar correctivos, como se muestra en la Figura 16.

Figura 16. Clasificación y Valoración de Riesgo.

CALIFICACION DEL RIESGO	DESCRIPCIÓN
Muy alto (7-9)	El riesgo es totalmente inaceptable. Se deben tomar medidas inmediatas para reducir estos riesgos y mitigar los riesgos.
Alto (5-6)	El riesgo es inaceptable. Las medidas para reducir el riesgo y los riesgos de mitigación deberían implementarse lo antes posible.
Medio (3-4)	El riesgo puede ser aceptable en el corto plazo. Los planes para reducir los riesgos y mitigar los peligros deberían incluirse en los planes y presupuestos futuros.
Bajo (0-2)	Los riesgos son aceptables. Se deben implementar medidas para reducir aún más el riesgo o mitigar los peligros junto con otras mejoras de seguridad y mitigación.

Fuente: (Normaiso 27001, 2020)

Los controles de riesgo en la norma ISO 27001 para la seguridad de la información, permiten identificar las medidas que permitan disminuir los distintos niveles de riesgo (Normaiso 27001, 2020). Además, se tiene que considerar la realización de un plan urgente en donde se incluyan las actualizaciones de los controles adicionales sobre los estándares mínimos recomendados por la organización.

2.2.4.8. Tratamiento de riesgos

Consiste en realizar un plan para el tratamiento de los riesgos identificados lo que permite determinar cuáles son los riesgos inaceptables.

2.2.4.9. Responsable del riesgo

Identificar al propietario de los riesgos (Normaiso 27001, 2020). El propietario de los riesgos actuará en la toma de decisiones para el tratamiento que se dará a cada una de las amenazas y también los riesgos identificados. La documentación en el análisis de riesgos será:

- Documentación sobre los criterios utilizados para las valoraciones de los riesgos y las evaluaciones particulares.
- Documentación sobre las valoraciones intrínsecas de cada riesgo

- Inventario de activos de información con la identificación de los propietarios de cada activo
- La definición del riesgo asumible tomada en la evaluación de riesgos

2.2.4.10.Selección de controles: declaración de aplicabilidad

Consiste en identificar los controles de seguridad que se van a aplicar a los activos que se han determinado para el tratamiento de riesgos (Normaiso 27001, 2020). En el inventario de activos es conveniente incluir:

- Categorización de la información (datos personales, nivel de confidencialidad etc.)
- Necesidad de establecer controles de acceso
- Incluida o no en procesos de copia de seguridad
- Soportes de almacenamiento
- Necesidades de comunicación de la información etc.

Luego de esa información es importante definir los controles técnicos y de organización para proteger los activos de las amenazas. Posteriormente será necesario realizar un análisis de aplicabilidad, tomando en cuenta los controles del Anexo A sin dejar ningún control que sea aplicable a la protección del activo.

2.2.5. Fase 5: Documentación SGSI

Es necesario documentar los procesos anteriores. La documentación es importante por dos motivos:

- Garantizar la repetición en el tiempo de un proceso.
- Establecer un proceso de mejora continua.

La documentación es imprescindible para implementar procesos de mejora continua en el Sistema de Gestión (Normaiso 27001, 2020). La documentación permite justificar el cumplimiento de la norma, por lo tanto, son las evidencias del trabajo que se realiza.

2.2.5.1. Información a publicarse

Los requisitos que la norma ISO 27001 solicita son:

- Documentación completa

- Documentación actualizada
- Realización de un control de la documentación adecuado.

Los documentos de análisis y evaluación de riesgos de la seguridad tienen que permanecer protegidos.

2.2.5.2. Niveles de documentación en ISO 27001

Figura 17. Niveles de Documentación ISO 27001.

Fuente: (Normaiso 27001, 2020)

a) Políticas de Seguridad

Las políticas de seguridad tanto específicas como del SGSI proporcionan apoyo para la documentación (Normaiso 27001, 2020). Algunas políticas específicas se detallan:

- Uso permitido del internet dentro de la empresa
- Uso de dispositivos móviles corporativos
- Política de uso de dispositivos móviles no corporativos

b) Procedimientos administrativos

Los procesos específicamente establecidos para la mejora continua, permiten gestionar de una manera responsable los riesgos de seguridad de la información.

Se pueden definir procedimientos para explicar las funciones del propietario de un activo de información.

c) Procedimientos técnicos

Algunos de los procedimientos que se podrían definir serían, por ejemplo:

- Procedimiento de información sensible
- Procedimiento para comunicaciones
- Procedimiento de niveles de acceso a información reservada

d) Procedimientos Físicos

Entre los procedimientos físicos se podrían describir los siguientes:

- Recomendaciones de seguridad de los cuartos fríos de servidores
- Almacenamiento y destrucción de información sensible

Además, los registros también son necesarios, ya que están atados con los documentos.

2.2.5.3. Listado de documentos obligatorios del SGSI

El listado de documentos obligatorios de acuerdo a la norma ISO 27001 se puede observar en el Anexo A de la norma.

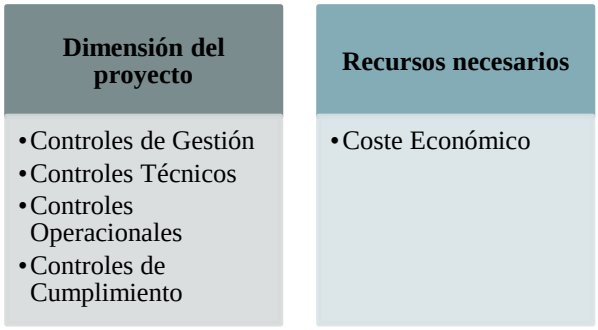
2.2.6. Fase 6: Implementación de un SGSI

Diseñar los procesos de seguridad e integrarlos a los procesos de la organización asumiendo lo que se ha identificado en los procesos anteriores de control para mitigar los riesgos lo que permita garantizar niveles aceptables en la Seguridad de la Información (Normaiso 27001, 2020). Los niveles aceptables se los consideraría en confidencialidad, integridad y disponibilidad de la información.

2.2.6.1. Criterios de agrupación y ordenamiento de procesos de seguridad

Es importante coleccionar todos los proyectos de seguridad (Normaiso 27001, 2020). Esto permitirá priorizar y clasificar adecuadamente la seguridad de la información, lo que a su vez será muy útil para tomar decisiones en el SGSI. El orden y agrupación de los procesos se muestran en la Figura 18.

Figura 18. Orden y Agrupación de Procesos de Seguridad.



Fuente: Bryan Alexander Guanín Castillo.

Controles de Gestión: Los controles que afectan la estructura, responsabilidades y funciones sobre la seguridad de la información, así como también las instrucciones de uso de los dispositivos de seguridad.

Controles Técnicos: Son los controles que toman en cuenta los factores tecnológicos para las medidas de seguridad.

Controles Operacionales: Constituyen las medidas que pretendan eliminar o disminuir los riesgos en la seguridad de la información.

Controles de Cumplimiento: Son los controles que permiten integrar o mejorar las actividades realizadas en la seguridad de la información.

Coste económico: Identificar proyectos con menores costos, que sean asumibles y sin impactos para la empresa. Para lo cual será necesario realizar una planificación temporal y prever los recursos humanos y materiales necesarios.

2.2.6.2. Proceso de la seguridad

La seguridad de la Información es un proceso de mejora continua (Normaiso 27001, 2020). Los procesos de mejora serán acordes a las necesidades de la organización.

De acuerdo al Anexo A los procesos de seguridad se detallan en la Figura 19

Figura 19. Proceso de Seguridad de la Información.

Fuente: (Normaiso 27001, 2020)

2.2.6.3. Responsabilidades

Para la implementación de controles y procesos de seguridad, es importante la asignación de tareas y responsabilidades en el desarrollo del tratamiento de riesgos (Normaiso 27001, 2020). Tareas a asignar responsabilidad en los procesos de seguridad:

- Determinar objetivos de las medidas de seguridad
- Efectivizar las medidas de la organización
- Implantar y ejecutar las tareas técnicas planificadas.
- Supervisar las actividades
- Adquirir y analizar la información de los indicadores.
- Detección y notificación de las incidencias

Los objetivos tienen que ser medibles de acuerdo a la normativa ISO 27001 para determinar las cuantificaciones dentro de cada proceso y evaluar el nivel de implantación, lo que permitirá:

- Comunicar los objetivos al equipo
- Planificar la implementación
- Medir la eficacia de los procesos de control de seguridad
- Efectuar cambios cuando se detectan problemas

- Plantear cambios en la gestión de riesgos para mejorar el sistema SGSI

2.2.6.4. Definir indicadores de procesos

Es conveniente establecer plantillas para recolectar datos como, por ejemplo:

- Descripción del Control
- Criterios de Medición
- Valores Indicativos
- Cálculo de resultados
- Frecuencia de las Medidas
- Registro de Datos

2.2.6.5. Implementación del proceso

Cuando el proceso se ha determinado, con responsables y lo planificado (Normaiso 27001, 2020). La implementación del proceso determina el grado de implantación del Sistema de Gestión.

2.2.7. Fase 7: Comunicación y sensibilización SGSI

La comunicación es muy importante y constituye la base éxito de la implementación del SGSI con normativa ISO 27001.

2.2.7.1. Plan de comunicación ISO 27001

En el plan de comunicación de acuerdo a la norma ISO 27001 se incluyen los requisitos:

- Responsable de la comunicación de los procesos de seguridad
- Receptor de la comunicación
- Contenido del proceso de seguridad
- Determinar el tiempo para realizar la comunicación
- Medios a utilizarse

La comunicación interna en la organización busca definir:

- La necesidad del SGSI.
- Responsabilidades legales de la organización.
- Afectación a los miembros de la organización una vez implantado el SGSI.

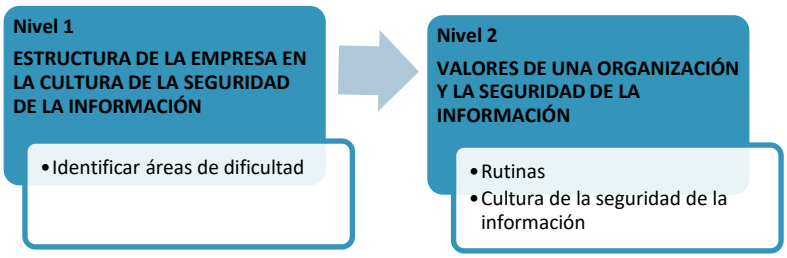
2.2.7.2. Documentación del plan de comunicación del SGSI

El plan de comunicación implica además responsabilidad para evitar problemas de comunicación (Normaiso 27001, 2020). Por lo cual es importante contar con una adecuada estrategia y un plan de comunicación correctamente documentado.

2.2.7.3. Tener cultura de la seguridad

La cultura de la seguridad requiere un análisis en diferentes niveles de la organización (Normaiso 27001, 2020). Los niveles se muestran en la Figura 20. Y los valores de la Cultura de la Seguridad de la Información se pueden observar en la Figura 21.

Figura 20. Niveles de la Cultura de la Seguridad.



Fuente: Bryan Alexander Guanín Castillo.

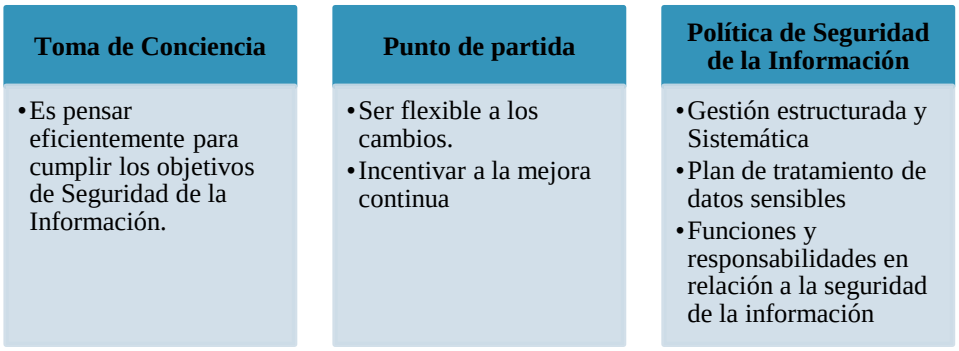
Figura 21. Comunicación de valores y cultura de la Seguridad de la Información.

Fuente: (Normaiso 27001, 2020)

Los colaboradores necesitan contar con los conocimientos que les permitan realizar las tareas cotidianas de una forma segura.

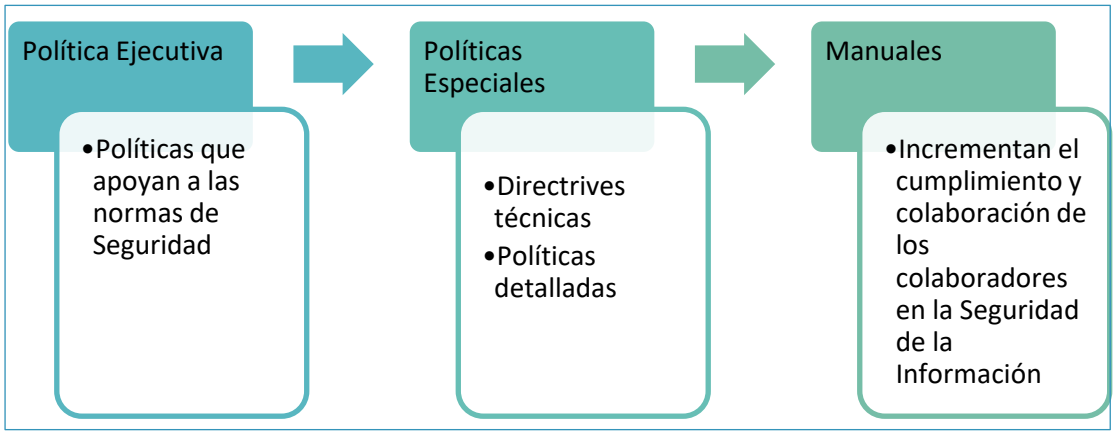
2.2.7.4. Creación de una cultura de la seguridad de la información

Figura 22. Creación de Cultura de Seguridad de la Información.



Fuente: (Normaiso 27001, 2020)

Figura 23. Niveles en las Políticas de la Seguridad de la Información.



Fuente: (Normaiso 27001, 2020)

2.2.7.5. Educación del personal

Es necesario que los colaboradores participen y además estén capacitados apropiadamente, de tal manera que puedan afrontar las amenazas contra el SGSI (Normaiso 27001, 2020).

Nota: Los colaboradores no necesitan dominar todo sobre la seguridad de la información, sin embargo, se espera que conozcan los riesgos de la labor que desempeñan y cómo mitigarlos.

2.2.7.6. Evaluación del cumplimiento

- Garantizar el comportamiento seguro de los colaboradores y procesos dentro de la organización
- Presentar a los colaboradores las consecuencias de acciones poco seguras.
- Concienciar en los beneficios del cumplimiento del Sistema de Seguridad de la Información.

2.2.8. Fase 8: Auditoría interna según ISO 27001

La auditoría interna es un proceso de mejora continua dentro de la organización y constituye un hábito de utilidad, pero para el cumplimiento del requisito de la Norma ISO 27001: 2013 es importante establecer un plan de auditorías internas que permitan la revisión del SGSI (Normaiso 27001, 2020). Las auditorías internas son herramientas que permiten identificar inconsistencias en el SGSI.

2.2.8.1. Determinar el objetivo de la auditoría interna ISO 27001

Con las auditorías internas se pretende:

- Comprobar el cumplimiento de los requisitos de la norma en el SGSI implantado.
- Comprobar que los procesos de la organización han integrado correctamente los requisitos de la seguridad de la información determinados en el SGSI.

2.2.8.2. Identificar los beneficios de la auditoría interna del SGSI

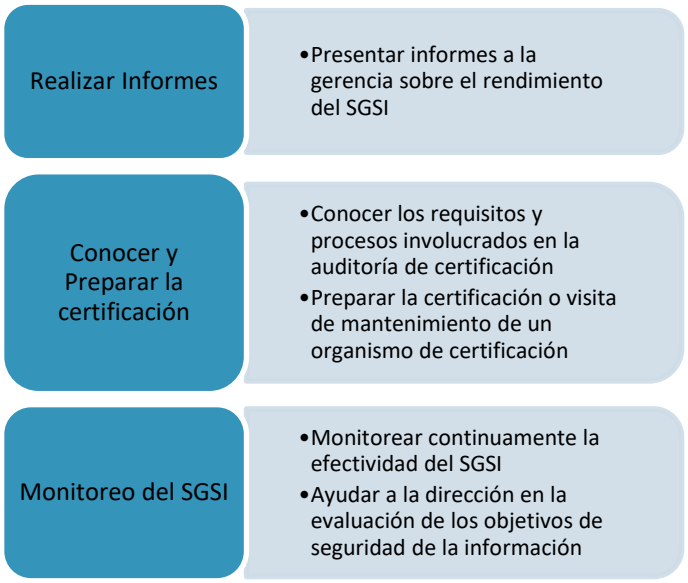
- La auditoría interna orienta para la auditoria de certificación
- Las auditorías internas identifican oportunidades de mejora.
- La realización de auditorías internas periódicas proporciona la evidencia de la revisión continua tanto a la propia organización como a la certificadora del SGSI.
- Las auditorías internas son un recordatorio para los colaboradores de la importancia y prioridad del cumplimiento de los requisitos de la seguridad de la información permiten a la empresa el alcance de los objetivos.

2.2.8.3.Establecer quién será el auditor interno del SGSI

2.2.8.3.1. Funciones y tareas del Auditor Interno ISO 27001

Las principales funciones y tareas del auditor interno se detallan en la Figura 24.

Figura 24. Tareas del Auditor Interno ISO 27001.



Fuente: (Normaiso 27001, 2020)

2.2.8.3.2. Definir el equipo auditor

Dependiendo del tamaño de la empresa es conveniente determinar al menos dos o más personas que desempeñen en conjunto la responsabilidad (Normaiso 27001, 2020). También se puede designar un auditor por cada departamento, lo que incrementa la responsabilidad y a su vez reduce el riesgo de errores y permite realizar el seguimiento de acciones preventivas y correctivas.

2.2.8.3.3. Candidatos a auditores internos

Por lo general los altos ejecutivos de la organización son los candidatos mejor calificados para convertirse en auditores internos (Normaiso 27001, 2020). Formar parte del equipo de implantación del SGSI ISO 27001 permitiría que el trabajo de implantación sea más factible.

Formar auditores internos del SGSI ISO 27001 da a los colaboradores habilidades valiosas para la organización y además garantiza controles adecuados.

2.2.8.3.4. Diferenciar la auditoría interna de la auditoría de certificación

- La auditoría interna prepara para la auditoría de certificación.
- La auditoría interna permite validar la efectividad del SGSI implantado
- La auditoría interna de SGSI incluye pruebas de efectividad del SGSI.
- La auditoría de certificación enfatiza las pruebas de cumplimiento para informar sobre la conformidad del SGSI.
- La auditoría de certificación necesita confiar en la auditoría interna y en la revisión por la dirección de SGSI.

2.2.8.3.5. Consejos para una auditoría interna

Dedicar tiempo necesario: Reservar tiempo adecuado para la completa auditoría de cada área o departamento. Los factores que inciden en la asignación de tiempo para cada tarea:

- El nivel de madurez del SGSI
- El tamaño de la organización
- La cantidad de hallazgos identificados en la auditoría anterior.

Los controles entre los auditores se pueden asignar dependiendo de las habilidades y potencialidades de cada uno.

Preparar las auditorías: Comunicar el plan de auditoría y los objetivos por adelantado.

- Comprender a profundidad los requisitos de Anexo A y de la organización.
- Disponer de la información necesaria para la auditoria
    - Novedades o no conformidades en Seguridad de la información
    - Procedimientos y políticas
    - Declaración de aplicabilidad
- Preparar una lista de verificación de los puntos a tratarse en la auditoria
- Preparar un plan de auditoría incluyendo:
    - Horarios
    - Departamentos y

    - Ubicaciones
- Previo a la auditoría, coordinar con anticipación el plan de auditoria con el área o departamento a auditar.
- Programar tiempo con las áreas a auditar para:
    - Analizar y explicar el informe de auditoria
    - Realizar reuniones de seguimiento con los representantes del área o departamento.

Involucrar a toda la organización: Comunicar y sensibilizar las responsabilidades en el proceso de las auditorías a los colaboradores para que involucren en el logro de los objetivos.

Auditar la comprensión de los objetivos del SGSI y el cumplimiento: Verificar el nivel de comprensión de los colaboradores en la importancia de la seguridad de la información, para lo cual se tienen que revisar los procesos sobre la seguridad de la información:

- Identificar las causas del no cumplimiento de los procedimientos
- Evaluar el grado de comprensión de las políticas y procedimientos

Mejorar el SGSI: La auditoría interna no pretende explorar los incumplimientos, porque es una herramienta informativa de mejora continua. Es importante tomar apuntes de las novedades y mantener reuniones con los responsables de las áreas o departamentos.

Toma de Decisiones: Garantiza que las novedades tengan un tratamiento adecuado a través de algunas acciones:

- Acordar las decisiones con los responsables de las áreas o departamentos
- Las decisiones serán registradas y documentadas
- Identificar las medidas correctivas
- Planificar la implementación
- Establecer responsables
- Programar un seguimiento para comprobar la implementación y efectividad

2.2.9. Fase 9: Revisión por la dirección según ISO 27001

(Normaiso 27001, 2020): “La revisión del sistema por parte de la dirección es un requisito de la norma ISO 27001”.

2.2.9.1. Importancia de la revisión del sistema

La revisión del sistema de gestión es muy importante en la norma ya que constituye una buena práctica en la seguridad de la información.

2.2.9.2. Objetivo de la revisión

El objetivo de la revisión es bidireccional, ya que permite:

- Garantizar que el SGSI y sus objetivos permanezcan convenientes y efectivos
- Revisar la validez de los riesgos de la organización y las novedades identificadas.

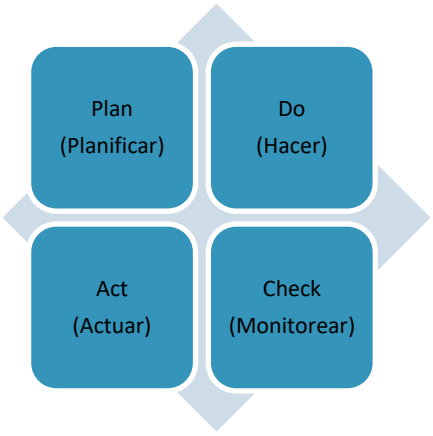
2.2.9.3. La revisión como parte de la mejora continua

La mejora continua en la norma ISO 27001 constituye el eje del SGSI y en la estructura de la norma el ciclo PDCA se encuentra sobreentendido en el punto 10.2.

2.2.9.4. Ciclo PDCA en la estructura de la norma

De acuerdo a las fases del ciclo de mejora continua PDCA se establece una correlación con la estructura de la norma ISO 27001 (Normaiso 27001, 2020). Las fases del proyecto del SGSI se observa en la Figura 25.

Figura 25. Ciclo PDCA

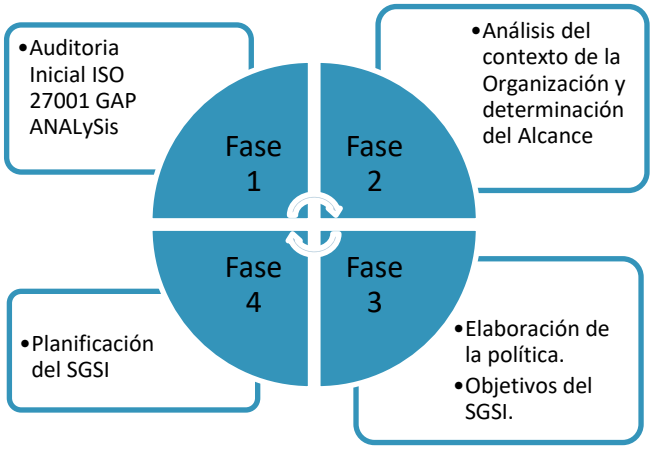


Elaborado por: Bryan Alexander Guanín Castillo.

2.2.9.4.1. Planificar (PLAN)

La planificación del proyecto SGSI se describe en la Figura 26.

Figura 26. Fases del proyecto SGSI.



Fuente: (Normaiso 27001, 2020)

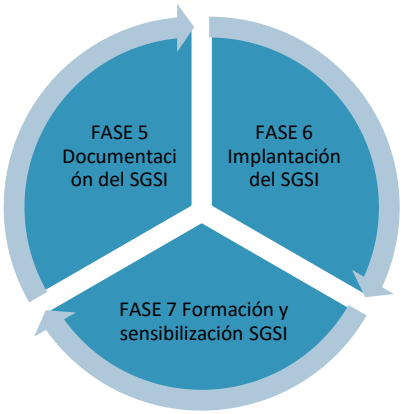
La fase 4 tiene su correspondencia en la norma ISO 27001 en los capitulos:

4. Análisis del contexto de la organización
5. Liderazgo
6. Planificación del Sistema
7. Recursos del Sistema (Soporte)

2.2.9.4.2. Hacer (DO)

Corresponde a la implementación del sistema generando la documentación necesaria, los controles de la seguridad de la información establecidos con el análisis de riesgos (Normaiso 27001, 2020). Las tareas y funciones también deben establecerse. Las fases de la implementación se observan en la Figura 27.

Figura 27. Fases de la Implementación.



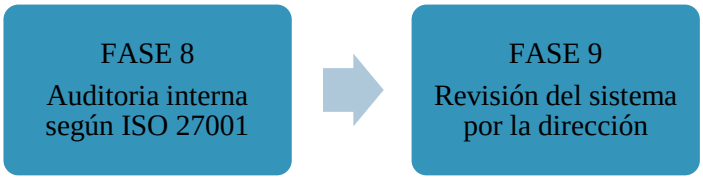
Elaborado por: Bryan Alexander Guanín Castillo.

Estas fases se corresponden en el Capítulo 8 (Operación), de la norma ISO 27001.

2.2.9.4.3. Check (Monitorear)

El control corresponde a la mejora continua. La norma establece los requisitos para determinar el sistema de control de los procesos del SGSI (Normaiso 27001, 2020). Las fases del control se muestran en la Figura 28.

Figura 28. Fases del Control.



Elaborado por: Bryan Alexander Guanín Castillo.

Estas fases tienen su equivalencia en el capítulo 9 de la norma (Evaluación del Desempeño).

2.2.9.4.4. Actuar (ACT)

En la mejora continua son obligatorias las acciones del SGSI y será imprescindible establecer un plan de acciones correctivas sobre las novedades o fallos detectados (Normaiso 27001, 2020). La norma define los requisitos en el capítulo 10 (Mejora).

Un sistema SGSI en las primeras etapas debe tener al menos:

- Políticas sobre la Seguridad de la información y análisis de riesgos.
- Medidas de seguridad mínimas de protección de la información y cumplimiento de los requisitos de la norma.
- Revisión del sistema y seguimiento de los objetivos (acciones correctivas sobre fallos detectados en la seguridad de la información).

2.2.9.5. Consideraciones en la revisión del SGSI

En la revisión del SGSI permite determinar el cumplimiento de los requisitos de la norma ISO 27001 (Normaiso 27001, 2020). Se puede integrar la revisión del SGSI en un informe de alto nivel, en el cual se consideren los requisitos de un sistema de calidad ISO 9001 que son los requisitos de cumplimiento legal en cuanto a la protección de datos.

En una revisión se debe considerar al menos:

- Cumplimiento de los objetivos en el SGSI
- Mejoras necesarias
- Factibilidad de cambios en el alcance
- Aprobación de recursos necesarios para los controles y procesos de la Seguridad de la información
- Factibilidad de modificaciones en los documentos principales (políticas de alto nivel), etc.

2.2.9.6. Frecuencia para la revisión del SGSI

El requisito mínimo de la norma para la revisión del SGSI es al menos una vez al año, si existen cambios o actualizaciones se lo realizará con mayor frecuencia ya que afectan directamente a la seguridad de la información (Normaiso 27001, 2020). La frecuencia más adecuada depende directamente de la dirección de la organización tomando en cuenta los requisitos internos que permitan evaluar efectivamente el SGSI.

2.2.10. Fase 10: Proceso de certificación ISO 27001

La obtención de un certificado de cumplimiento de los requisitos de la norma es el fin del proceso de certificación ISO 27001 (Normaiso 27001, 2020). Las certificaciones emitidas por una

Entidad de Certificación pueden ser o no acreditadas por una entidad de acreditación, pero la acreditación debe pertenecer a la IAF (International Accreditation Forum).

La fase de certificación no es obligatoria, pero los beneficios pueden ser:

- Ventaja competitiva ante otras organizaciones
- Facilita el acceso a un mercado competitivo y exigente
- Mejoramiento de la imagen de la organización
- Favorece la confianza de clientes y usuarios por la protección de los datos en los servicios
- Garantiza una implantación efectiva de la norma

2.2.10.1. Auditoría de certificación del SGSI

Se realiza la auditoría de Certificación luego de la fase de implantación después de 3 meses al menos para verificar su funcionamiento (Normaiso 27001, 2020). La auditoría de la certificación inicia con una solicitud a una entidad certificadora, la cual emite un contrato formal.

La auditoría se realiza en dos fases:

2.2.10.2. Auditoria de certificación ISO 27001 Fase 1

Constituye un proceso de análisis de la documentación mediante el informe del cumplimiento de los requisitos de la norma ISO 27001

Documentación obligatoria:

- Información sobre los controles de Seguridad
- Diagrama de la red
- Instrucciones técnicas
- Políticas especificas
- Procesos de Seguridad
- Listado de documentación vigente, etc.

2.2.10.3. Auditoria de certificación ISO 27001 Fase 2

En esta fase se revisa la implantación del SGSI y se comprueba el cumplimiento de las políticas, la implantación de los controles de seguridad, etc. (Normaiso 27001, 2020). La

organización dispondrá de un plazo adecuado para la corrección de las No Conformidades. La implantación de las acciones correctivas será verificada en las próximas auditorías.

(Normaiso 27001, 2020): “Finalizado el proceso de auditoría de certificación se procede a la emisión del certificado el cual tendrá una validez de 3 años, siendo necesaria una auditoria de renovación para mantener la validez por otro periodo”. Además, es obligatorio realizar una auditoría de seguimiento habitualmente anual para verificar que el SGSI se mantiene de acuerdo a los requisitos de la norma.

Evidencia. - Consiste en la comprobación de la documentación del SGSI con la realidad.

Entrevistas. - Constituyen en una manera de comprobar si la organización está cumpliendo las actividades o procesos con integración del SGSI.

Concienciación. - La concienciación de los colaboradores es muy importante en un SGSI por lo que el auditor realizará una serie de entrevistas de manera aleatoria a diferentes colaboradores para comprobar los documentos que aplican.

Los documentos que los colaboradores suelen aplicar son:

- Política de seguridad de la información
- Cláusulas de confidencialidad
- Uso aceptable de los activos
- Política de control de acceso

La preparación de la auditoria de Certificación ISO 27001 es importante:

- Realizar la Auditoría Interna
- Seleccionar del Auditor
- Revisar del Plan de Auditoría
- Preparar las Entrevistas

CAPÍTULO III

3. RESULTADOS

3.1. Entorno actual de la empresa “Pinto Seguros”

3.1.1. Misión

Somos una empresa que acompaña a las familias y a las empresas, asesorándolas con respecto al resultado de su patrimonio, preservación de sus activos brindando protección y tranquilidad con soluciones sencillas y adecuadas, a través de productos y servicios de calidad, que garantice el desarrollo del país con calidez, responsabilidad social y medio ambiente. (Pinto Seguros, 2018)

3.1.2. Visión

Ser una empresa altamente competitiva, con base en la actualización permanente de las herramientas tecnológicas, la continuidad de los procesos y la cultura de trabajo en equipo; como también ofrecer el apoyo personal y familiar a los empleados como inicio de enfoque de la empresa a la responsabilidad social. (Pinto Seguros, 2018)

3.1.3. Valores

- Disciplina
- Dinamismo
- Confidencialidad
- Confianza
- Responsabilidad
- Innovación” (Pinto Seguros, 2018)

3.2. Antecedentes de la empresa

La empresa “Pinto Seguros”, inició sus operaciones el 28 de noviembre del 2018, se encuentra ubicada en Machachi, esta brinda los servicios de seguros de vida, asistencia médica, transporte, equipos y maquinarias; a su vez está también ofrece seguros de viajes a nivel internacional.

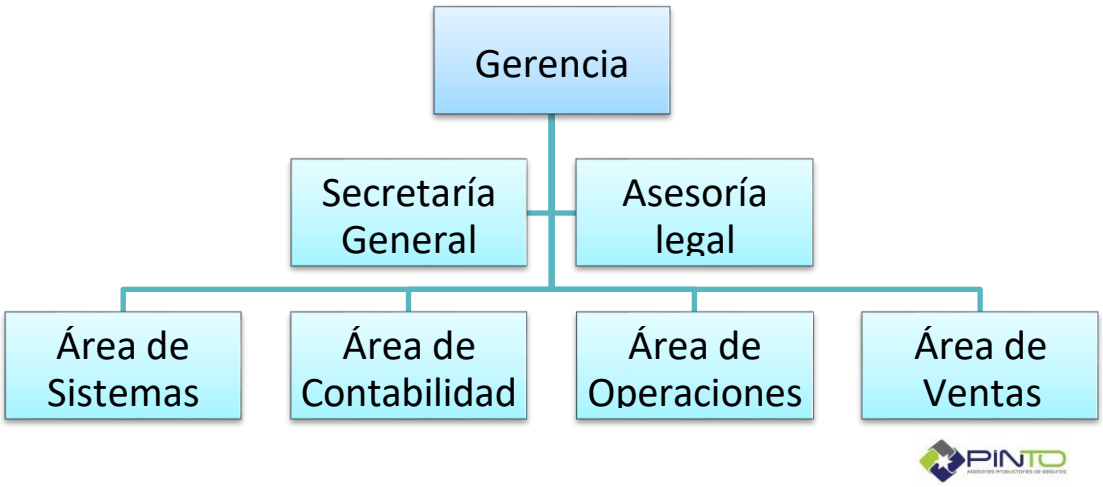
Actualmente, para cualquier organización, implementar un SGSI es de suma importancia para la protección de sus activos de información, más aún en caso obtuviesen la certificación le sumaría un valor agregado al servicio que ofrecen a sus clientes ya que alcanzarían un grado de reconocimiento internacional, el cual les dará a sus clientes una mayor garantía sobre la seguridad de la información.

3.3. Infraestructura de la empresa

La empresa cuenta con una oficina propia, situada en el Catón Mejía.

3.4. Estructura organizacional de la empresa

Figura 29. Organigrama "Pinto Seguros"



Fuente: (Pinto Seguros, 2018)

3.5. Modelo de negocio

Pinto Seguros productores de seguros ofrece seguros de:

- Vehículos livianos y pesados
- Vida individual y colectiva
- Asistencia médica
- Transporte
- Responsabilidad civil
- Equipo y maquinaria

- Todo riesgo contratista
- Obras civiles terminadas

3.6. Diagnóstico de la situación actual de la empresa

La empresa “Pinto Seguros” requiere identificar los riesgos para gestionar los controles pertinentes con el fin de mantener la confidencialidad, integridad y disponibilidad de la información. Por tanto, se ha tomado la decisión estratégica de implementar un SGSI. En la Tabla 5 se presenta el diagnóstico basado en la norma ISO 27001.

Tabla 5 Diagnóstico Basado en ISO 27001

REQUISITO NORMATIVO	PORCENTAJE DE CUMPLIMIENTO
4. SISTEMA DE GESTIÓN DE SEGURIDADDE LA INFORMACIÓN	**22%**
4.1 Requisitos generales	**20**
4.2 Establecimiento y gestión del SGSI	**20**
4.3 Requisitos de la documentación	**25**
5. RESPONSABILIDAD DE LA DIRECCIÓN	**33%**
5.1 Compromiso de la dirección	**35**
5.2 Gestión de los recursos	**30**
7 REVISIÓN POR LA DIRECCIÓN DEL SGSI	**10%**
7.1 Generalidades	**10**
7.2 Elementos de entrada para la revisión	**10**
7.3 Resultados de la revisión	**10**
8 MEJORA DEL SGSI	**10%**
8.1 Mejora continua	**10**
8.2 Acción correctiva	**10**
8.3 Acción preventiva	**10**

PORCENTAJE DE CUMPLIMIENTO GENERAL	**18,54%**

Fuente: (Normaiso 27001, 2020)

3.7. Técnicas de investigación

La técnica de investigación fue documental, tomando en cuenta fuentes de investigación previa e histórica sobre análisis de riesgos informáticos, Sistemas de Gestión de Información, Normas ISO.

3.8. Población

La población comprende los usuarios del Sistema de Gestión de Seguridad de la Información de la empresa “Pinto Seguros”.

3.9. Muestra

El tamaño de la muestra constituye un grupo de 10 personas de los distintos departamentos de la empresa “Pinto Seguros” y 10 personas más como personal de apoyo y proveedores

3.10. Propuesta

Para dar solución a los requerimientos de la empresa “Pinto Seguros” se ha propuesto realizar una implementación de un Sistema de Gestión de Seguridad de la Información, el cual permita garantizar el proceso de gestión de la seguridad dirigido a preservar la disponibilidad, confidencialidad, integridad y la autenticación de la información y así evitar o disminuir los riesgos y amenazas vigentes actualmente. El SGSI será implantado acorde a la normativa del Anexo A ISO 27001.

3.11. Objetivo de la propuesta

Facilitar a la alta gerencia los lineamientos y el soporte para la seguridad de la información basada en la norma ISO 27001, acorde con los requerimientos comerciales del negocio, políticas de la empresa y regulaciones vigentes actuales en el marco legal del Ecuador.

3.12. Alcance

Proteger la información de las bases de datos e información financiera de la empresa, de losclientes y proveedores de acuerdo a la importancia y valor, excluyendo el control previsto en A.10.9.1 Comercio electrónico en nuestro SGSI porque la empresa no realiza

transacciones decomercio electrónico.

3.13. Fases para implementar ISO 27001

3.13.1. Fase 1: Auditoría inicial Gap Análisis

Para la realización del análisis de brechas GAP se utilizó de un modelo de cumplimento o madurez que permita determinar el alcance efectivo de los controles a implementar (Normaiso 27001, 2020).

3.13.1.1. Nivel de Cumplimiento

Para determinar el cumplimiento de los niveles de madurez de la organización se ha utilizado unlistado de preguntas de acuerdo a los controles estándar ISO 27001. Se adjunta listado de control en la Tabla 6.

Tabla 6 Test de Control para determinar el nivel de Madurez en el cumplimiento NormativaISO 27001

Categoría	Subcategoría	Preguntas de Control		Puntuación
4. Contexto de la organización	4.1 Conocimiento de la organización y su contexto	1	¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	1
		2	¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	2
		3	¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	4
	4.2 Expectativas de las partes interesadas	4	¿Se han identificado las partes interesadas?	4
		5	¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	4
		6	¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	2
	4.3 Alcance del SGSI	7	¿Se ha determinado el alcance del SGS y se conserva información documentada?	1
	4.4 SGS Sistema de Gestión de la Seguridad de la información	8	¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	1
5. Liderazgo	5.1 Liderazgo y compromiso	9	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	2

	5.2 Política de la Seguridad de la Información	10	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	2
		11	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	2
		12	¿Se ha definido una Política de la Seguridad de la Información?	2
		13	¿Se ha establecido un marco que permita el establecimiento de objetivos?	2
		14	¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?	2
		15	¿Se mantiene información documentada de la política del SGSI y de sus objetivos?	2
	5.3 Roles y Responsabilidades	16	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?	2
		17	¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?	2
6. Planificación	**6.1 Tratamiento de Riesgos y Oportunidades**	18	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?	2
		19	¿Se identifican y analizan los riesgos mediante un método de evaluacióny aceptación de riesgos?	2
		20	¿Se ha definido un proceso de tratamiento de riesgos?	1
		21	¿Se han establecido criterios para elaborar una declaración de aplicabilidad?	2
		22	¿Se mantiene información documentada de los puntos anteriores?	2
	6.2 Planificación para consecución de objetivos	23	¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?	2
		24	¿Los objetivos de la Seguridad de la Información están planificados mediante: Asignación de responsabilidades, cronograma de ejecución temporal y método de evaluación?	2
		25	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?	2
	7.1 Recursos	26	¿Se identifican y asignan los recursos necesarios para el SGSI?	3
	7.2 Competencia	27	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?	3
		28	¿Se mantiene información actualizada sobre la competencia del personal?	3
		29	¿El personal está involucrado y es consciente de su papel en la	2

7. Soporte			Seguridad de la Información?	
	7.3 Concienciación	30	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?	3
	7.4 Comunicación	31	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?	2
		32	¿Existe un proceso para comunicar las deficiencias o malas prácticas enla seguridad de la Información?	2
	7.5 Información Documentada	33	¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluyendo registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.)	2
		34	¿Existe un óptimo control documental interno?	2
		35	¿Se controlan los documentos de origen externo?	3
8. Operación	**8.1 Control Operacional**	36	¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?	2
		37	¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad?	2
		38	¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados?	3
		39	¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?	2
	8.2 Análisis de riesgos de la Seguridad de la Información	40	¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? (Propietario del riesgo, importancia del riesgo o nivel de impacto, probabilidad de ocurrencia)	1
	8.3 Tratamiento de riesgos de la Seguridad de la Información	41	¿Se ha implementado un plan de tratamiento de riesgos?	1
		42	¿Están informados los propietarios del riesgo y han aprobado el plan?	1
		43	¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?	2
		44	¿Se documenta el nivel de aplicación de todos los controles a aplicar?	2
		45	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?	2

9. Evaluación del desempeño	**9.1 Seguimiento y medición**	46	¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta porlos responsables tanto de los procesos como de la Seguridad de la Información?	2
	9.2 Auditorías Internas	47	¿Se ha establecido una programación de Auditorías Internas y asignado responsables?	3
		48	¿Se ha definido el alcance y los requisitos para el informe de auditoría?	2
		49	¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?	2
	9.3 Informe de Revisión por la Dirección	50	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?	2
		51	¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI?	2
10. Mejora	**10.1 No Conformidades y acciones correctivas**	52	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?	2
		53	¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?	3
	10.2 Mejora continua	54	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?	2

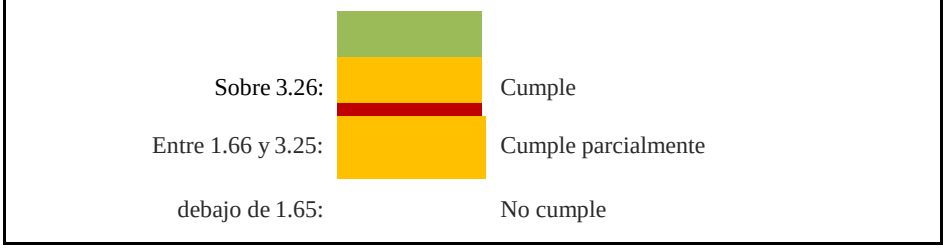
Elaborado por: Bryan Alexander Guanín Castillo.

A continuación, se presentan los resultados con el nivel de cumplimiento en la Tabla 7.

Tabla 7. Nivel de Cumplimiento de “Pinto Seguros”

RESUMEN			
Categoría	**Valor Ideal**	**Valor Obtenido**	**Cumplimiento**
Organización y Contexto	5,00	2,38	Cumple Parcialmente
Liderazgo	5,00	2,00	Cumple Parcialmente
Planificación	5,00	1,88	Cumple Parcialmente
Soporte	5,00	2,50	Cumple Parcialmente
Operación	5,00	1,75	Cumple Parcialmente
Evaluación del desempeño	5,00	2,14	Cumple Parcialmente

Mejora	5,00	2,33	Cumple Parcialmente



Elaborado por: Bryan Alexander Guanín Castillo.

3.13.2. Fase 2: Análisis del contexto de la organización y determinación del alcance

Tomando en cuenta que la empresa "Pinto Seguros" es una empresa joven, se ha determinado elalcance del SGSI, considerando las necesidades y las expectativas de la empresa, por lo tanto, se facilitará a la alta gerencia los lineamientos y el soporte para la seguridad de la información basada en la norma ISO 27001, acorde con los requerimientos comerciales del negocio, políticas de la empresa y regulaciones vigentes actuales en el marco legal del Ecuador.

3.13.2.1. Comunicación y consulta

Para conocer el nivel de efectividad de las medidas que determinadas para la seguridad de lainformación (Normaiso 27001, 2020) se elaboró un plan de comunicación.

Tabla 8 Plan de Comunicación

ETAPA	TEMA	OBJETIVO	PERIODICIDAD	AUDIENCIA	MEDIO	RESPONSABLE
Inicio de Implementación	Presentación del esquema Gestión de Riesgos de Seguridad de la Información	✓ Entender elesquema deriesgos. ✓ Entender elconcepto deriesgos. ✓ Dar a conocer los beneficios de la Gestión de riesgos. ✓ Presentar el organigrama delproyecto de implementación.	Una vez al inicio	Personal interno Proveedores	Presentación	Jefe de seguridad
Durante Implementación	Campaña de concientización	✓ Sensibilizar a los colaboradores sobre los inconvenientes sobre los riesgos de seguridad y su inadecuada gestión. ✓ Difundir los beneficios de laGestión de seguridad de la información.	Mensual	Personal interno Proveedores	Presentación Correo Talleres	Jefe de seguridad Responsables de área

		✓ Lograr que la organización se involucre en las diferentes etapasde la implementación del SGSI. ✓ Fomentar las buenas prácticasen el manejo de riesgos de seguridad de lainformación.				
	Presentación de avances	✓ Establecer acciones preventivas/ correctivas de ser necesario. ✓ Obtener retroalimentación sobre el estado de la implementación.	Quincenal	Equipo de implementación del SGSI	Presentación	Jefe de seguridad
Final Implementación	Presentación cierre de Implementación	✓ Informar del cumplimiento delos objetivos de la implementación. ✓ Formalizar el esquema final delSGSI.	Una vez al cierra	Personal interno Proveedores	Presentación	Jefe de seguridad
Durante Operación	Presentación Indicadores	✓ Informar a la dirección sobreel desempeño del esquema delas acciones a seguir. ✓ Determinar lasacciones preventivas o correctivas frente a los riesgos.	Semestral	Dirección Equipo de Seguridad de la información	Presentación	Jefe de seguridad

Elaborado por: Bryan Alexander Guanín Castillo.

3.13.2.2. Contexto del SGSI

A continuación, se detallan los contextos externos e internos.

a) Contexto externo:

- "Pinto Seguros" es una empresa productora de seguros con responsabilidad civil, presentes en todo riesgo contratista, multiriesgo, seguro de todo tipo de vehículos, salud y vida.
- El entorno competitivo es nacional, pero ofrece seguro de viajes a nivel internacional.

b) Contexto interno:

- La administración de "Pinto Seguros" está conformada por:
  - 1 gerente general

- 1 secretaria de gerencia
- 1 responsable de la asesoría legal
- colaboradores en el área de sistemas
- colaboradores del área de contabilidad
- colaboradores del área de operaciones
- colaboradores en el área de marketing y ventas

- Es compromiso de la dirección formalizar las políticas, las relaciones internas y los flujos de información, así como los procesos para la toma de decisiones en función delmodelo de negocio para fomentar la cultura organizacional en función de normas acordes al alcance de las relaciones contractuales vigentes.

3.13.2.3. Contexto de la Gestión de Riesgos

La empresa "Pinto Seguros" que cuenta con 10 colaboradores ha contemplado la prioridad de gestión de riegos en base a la información de negocio y de los clientes como máxima prioridad.

3.13.2.4. Definición de criterios de riesgo

Los criterios definidos por la organización para evaluar el nivel de importancia del riesgo son:

Tabla 9 Criterios de Riesgo

TIPO DE RIESGO	RANGO	RIESGO INICIAL		RIESGO RESIDUAL	
		Cantidad	%	Cantidad	%
Riesgo Bajo	0 – 10%	0	0	0	0
Riesgo Medio	11 – 30%	2	5%	9	24%
Riesgo Alto	31 – 50%	12	32%	9	24%
Riesgo Muy alto	51 – 100%	23	62%	19	51%
		37	100%	37	100%
Promedio			58%		53%

Elaborado por: Bryan Alexander Guanín Castillo.

3.13.2.5. Entender las necesidades y expectativas de las partes involucradas

Las personas u organizaciones constituyen las partes interesadas de acuerdo al contexto SGSI y por lo tanto ellas influyen directamente en la seguridad de la información y determinan la continuidad del negocio, ya que pueden verse afectadas por la seguridad de la información.

Se han identificado los requisitos, antes de iniciar el desarrollo del SGSI, se muestran en las Tablas 7, Tablas 8, Tablas 9, Tablas 10 y Tabla 11.

Tabla 10 Requisitos de Clientes

N°	Identificación de requisitos de Clientes
1.	Entregar servicios con confidencialidad
1.1.	de acuerdo con los requisitos contractuales.
1.2.	En caso de interrupciones
1.3.	Cumpliendo los requisitos legales aplicables
1.4.	Cumpliendo los requisitos adicionales de los brókeres de seguros
2.	Dar servicio en condiciones (24/7/365)
3.	Cumplir con los requisitos de ISO 27001
4.	Disponibilidad de Sistemas 99,9%
5.	SLA de respuesta a incidentes: 4 horas desde recepción de comunicaciones en centro de contacto
6.	Requisitos PCI DSS v3.2.1

Elaborado por: Bryan Alexander Guanín Castillo.

Tabla 11 Requisito de Usuarios Finales

N°	Identificación de requisitos de Usuarios Finales
1.	Servicios disponibles
1.1.	Sistemas de apoyo ante interrupciones
1.2.	Mantener servicios de soporte ante interrupciones
2.	Protección de datos: Los productos y servicios protegen adecuadamente los datos de los usuarios finales cumpliendo los requisitos legales tanto para los datos de contacto como para los datos confidenciales

Elaborado por: Bryan Alexander Guanín Castillo.

Tabla 12 Requisitos de Socios

N°	Identificación de requisitos de Socios
1.	Cumplir con los requisitos de integridad de información según los acuerdos firmados
2.	Cumplir con los acuerdos de confidencialidad firmados
3.	Proporcionar información técnica y soporte suficiente que les permita mejorar sus aplicaciones
4.	Proporcionar la formación necesaria tanto técnica como comercial enfocada a la venta de los productos y servicios
5.	Cumplir los acuerdos contractuales especialmente en los tiempos de entrega acordados

Elaborado por: Bryan Alexander Guanín Castillo.

Tabla 13 Requisitos de Empleados

N°	Identificación de requisitos de Empleos
1.	Proporcionar un ambiente de trabajo seguro y apropiado.
2.	Recibir capacitación y apoyo requeridos.
3.	La compañía especifica claramente sus requisitos y expectativas de los trabajadores.
4.	Protección de su información personal.
5.	La compañía paga justamente por el trabajo.
6.	Continuidad del empleo
7.	Oportunidades para el avance y desarrollo profesional

Elaborado por: Bryan Alexander Guanín Castillo.

Tabla 14 Requisitos de Administración

N°	Identificación de requisitos de Administración
1.	Cumplir con los requisitos de las leyes de protección de datos
2.	Identificar y cumplir con los requisitos legales propios del negocio emprendido
2.1	Ley de comercio electrónico

2.2	Ley general de telecomunicaciones
2.3	Otras
3.	Información mediante planes de comunicación y procedimientos establecidos para mitigar su impacto

Elaborado por: Bryan Alexander Guanín Castillo.

3.13.3. Fase 3: Elaboración de la política - objetivos del SGSI

3.13.3.1. Política de seguridad

La Política de Seguridad es un requisito de la norma ISO 27001 y considera los objetivos de la seguridad de la información de la organización (Normaiso 27001, 2020). El proceso para definir el alcance de un SGSI se visualiza en el anexo.

3.13.3.2. Auditoría de actividades de seguridad

- Registrar actividades sospechosas y posibles incidentes para evitar o prevenir eventos no deseados.
- Supervisar eventos relevantes para evaluar y registrar accesos en (exitosos, no exitosos o denegados), con eso determinar la interacción de los usuarios e identificar posibles violaciones de seguridad.

3.13.4. Fase 4: Planificación del SGSI

3.13.4.1. Inventario de Activos

Tabla 15. Riesgos-Inventarios de activos

Nombre del Activo	Descripción del Activo	Tipo de Activo	Contiene datos Sensibles	Nivel de Confidencialidad	Nivel de Disponibilidad	Nivel de Integridad	Custodio	Periodo de custodia	Nivel de protección actual
Hardware	1 servidor	Físico	Si	Alta	Media	Alta	Analista de tecnología e Información	4 años	Medio
	11 portátiles	Físico	Si	Media	Alta	Alta	Responsable	3 años	Medio
	4 impresoras	Físico	No	Baja	Alta	Media	Responsable de área	4 años	Medio
	3 teléfonos móviles	Físico	Si	Media	Alta	Media	Contabilidad	3 años	Medio

	2 discos duros externos	Físico	Si	Alta	Alta	Alta	Jefe de Sistemas	2 años	Medio
Infraestructura	1 oficina	Físico	Si	Alta	Media	Media	Gerencia	10 años	Alta
	servicios de electricidad	Físico	No	Baja	Alta	Media	Contabilidad	4 años	Baja
	servicios de agua potable	Físico	No	Baja	Alta	Media	Contabilidad	4 años	Baja
	servicio de internet	Físico	No	Media	Alta	Media	Área de Sistemas	4 años	Medio
Software	Office 2016	Digital	Si	Media	Alta	Media	Área de Sistemas	1 año	Medio
	Ilustrador	Digital	Si	Media	Alta	Media	Área de Sistemas	1 año	Medio
	Antivirus	Digital	Si	Media	Alta	Alta	Área de Sistemas	1 año	Medio
	Safi	Digital	Si	Media	Alta	Alta	Área de Sistemas	1 año	Medio
Servicio subcontratado	Legal	Físico	Si	Alta	Alta	Alta	Gerencia	2 años	Medio
	limpieza	Físico	No	Baja	Media	Baja	Secretaría General	3 años	Baja
	Nube	Digital	Si	Alta	Alta	Alta	Área de Sistemas	1 año	Medio
	Sitio web	Digital	Si	Alta	Alta	Alta	Área de Sistemas	1 año	Medio
Personal	10 administrativos	Físico	Si	Alta	Alta	Media	Gerencia	2 años	Medio
	1 servicios	Físico	No	Baja	Media	Baja	Secretaría	2 años	Baja

Elaborado por: Bryan Alexander Guanín Castillo.

3.13.4.2. Valoración de activos y asignación del nivel de riesgo

En relación al impacto comercial perjudicial que tendría un posible evento, se asignará a cada activo un nivel de riesgo.

De acuerdo al impacto, la valoración de los riesgos se muestran en la Figura 30.

Figura 30. Niveles de riesgo extremo e importante.

Impacto Extremo 5 Puntos	Impacto Importante 4 Puntos
• Pérdida financiera insostenible para el negocio • Cobertura de medios negativa internacional a largo plazo; pérdida totalde la cuota de mercado • Enfrentar juicios con posibilidad deencarcelamiento de directivos • Multas importantes • Litigios que incluyen acciones colectivas, • Lesiones o muertes a empleados o terceros, como clientes o vendedores • Fuga de talentos con consecuencias lesivaspara el negocio	• Pérdida financiera entre un valor 1 y un valor 2 • Impacto nacional negativo a nivel de medios de comunicación a largo plazo • Pérdida significativa de cuota de mercado • Requisito de comunicación a las entidades reguladoras por incidentes con un proyectoimportante como acción correctiva • Se requiere atención hospitalaria limitada para empleados o terceros, como clientes ovendedores • Alta rotación de personal experimentado

Elaborado por: Bryan Alexander Guanín Castillo.

3.13.4.3. Catálogo de amenazas

Para identificar las amenazas que podrían afectar la Seguridad de la Información de la organización se tiene que elaborar y diseñar un catálogo de amenazas. Además, se debería identificar la fuente de la amenaza, agentes y motivaciones (Normaiso 27001, 2020). Existen diferentes catálogos de amenazas, pero también es posible utilizar catálogos genéricos como se muestra en la Tabla 16.

Tabla 16 Catálogo Genérico de Amenazas

Anexo	Riesgo	Descripción
A1	**Fuego**	Aquí podríamos distinguir sobre fuego en CPD (centro proceso de datos) o en oficinas etc.
A2	**Condiciones climáticas desfavorables**	Se trata de analizar las consecuencias para equipos e instalaciones en caso de condiciones adversas. Como ejemplo podríamos evaluar las consecuencias de las altas temperaturas en verano junto con las necesidades de los equipos de climatización. En este caso deberíamos evaluar fallos en equipos por altas temperaturas o des magnetizaciones de soportes de información etc.

A3	**Inundaciones**	Aquí deberíamos evaluar las posibles causas de inundaciones de agua en las instalaciones y oficinas: • Inundaciones por interrupciones de suministro • Sistemas de riesgo • Sistemas de calefacción • Sistemas contra incendios • Sabotajes (grifos bloqueo de desagües etc.)
A4	**Contaminación, polvo, corrosión**	En este punto podríamos tener en cuenta el riesgo de contaminación de salas de equipos especialmente sensibles a niveles de polvo o sustancias en suspensión etc. • Contaminación por obras o reformas en las salas • Polvo derivado de tareas de empaquetado • Instalaciones de nuevos equipos
A5	**Desastres Naturales**	Probabilidad de ser afectado por inundaciones, terremotos, tormentas eléctricas, impactos sobre la disponibilidad de servicios de comunicaciones etc.
A6	**Desastres ambientales**	Probabilidad de ser afectado por desastres ambientales • Incendios • Explosiones • Fugas • Evaluación del entorno (empresas vecinas con actividades peligrosas) • Interrupción de accesos al trabajo
A7	**eventos importantes en el medio ambiente**	Probabilidad de ser afectado por obras realizadas en el entorno, manifestaciones o desordenes públicos etc.

A8	**Interrupción dela fuente de alimentación**	• Probabilidad de interrupciones micro cortes en el suministro eléctrico< • Estabilidad de la red • Subidas de tensión • Afectaciones a sistemas de seguridad, ascensores • Interrupciones prolongadas
A9	**Interrupción delas redes de comunicación**	Como afectan las interrupciones de las comunicaciones a • Comunicación con los clientes • Procesos propios del negocio • Perdidas de datos • Procesos de pedidos • Dependencia de servicios de Internet • Etc.
A10	**Interrupción delsuministro de red**	Sistemas o tareas afectadas por falta de suministro • Climatización o ventilación • Agua y alcantarillado, (Sistema contra incendios) • Gas • Sistemas de alarma y control (por ejemplo, pararobo, incendio, control de limpieza) • Sistemas de comunicación internos
A11	**Fracaso o interrupción delos proveedoresde servicios**	• Interrupciones parciales o totales de serviciossubcontratados • Niveles de calidad de los servicios no aceptables • Indisponibilidad de instalaciones externas
A12	**Interferencias**	Interferencias en servicios inalámbricos (p. ej. RedesWLAN, Bluetooth, GSM, UMTS)
A13	**Emisiones comprometidas**	Riesgo de interceptación de información confidencial por radiaciones emitidas por equipos • Riesgo de exposición de información sobre la compañía, productos y servicios que puedan serutilizados por la competencia o entidades para perjuicio de la actividad de la organización

A14	**Espionaje**	• Escuchas ilegales • Intercepción de señales de transmisión • Intercepción de transmisiones desprotegidas de datos en redes publicas
A15	**Robo de dispositivos, soportes de almacenamiento y documentos**	Robo de soportes de almacenamiento de datos, sistemas deTI, accesorios, software o datos de clientes etc.
A16	**Pérdida de dispositivos, soportes de almacenamiento y documentos**	Pérdidas de equipos portátiles o soportes de almacenamiento de datos (Tarjetas de memoria) Documentos impresos olvidados en restaurantes o en lugares públicos, medios de transporte
A17	**Mala planificación o falta de adaptación**	• Procedimientos inadecuados de mantenimiento • Protocolos de transferencia • Procesos de adquisición de nuevas tecnologías
A18	**Divulgación de información sensible**	• Accesos no autorizados • Reciclaje de equipos y soportes • Destrucción de equipos y soportes • Software malicioso • Difusión de información inadvertida en procesos externos (Ordenes de reparación etc.) • Robo de contraseñas • Etc.
A19	**Información o productos de una fuente no confiable**	• Verificación insuficiente de información o software externo • Apertura de archivos o aplicaciones provenientes de fuentes no verificadas en equipos de trabajo (P. ej. emails) • Instalación de aplicaciones y actualizaciones de software por usuarios finales

A20	**Manipulación de hardware o software**	• Venganzas de empleados • Actuaciones ilícitas para beneficio propio
A21	**Manipulación de información**	• Datos falos en formato electrónico o en papel • Falsificación o modificación de datos y documentos
A22	**Acceso no autorizado a los sistemas de TI**	Accesos no autorizados a aplicaciones o sistemas
A23	**Destrucción de dispositivos o soportes de almacenamiento**	Destrucción de soportes de almacenamiento o sistemas TI por venganzas, negligencias o usos indebidos
A24	**Fallo de dispositivos o sistemas**	• Fallos en dispositivos críticos del sistema • Fallos técnicos por mal funcionamiento • Fallos por uso indebido o errores humanos • Fallos por causas externas (falta de suministro etc.) • Fallos por sabotaje • Fallos por accidentes
A25	**Mal funcionamiento de dispositivos o sistemas**	• Por fatiga o desgaste del material • Falta de mantenimiento • Tolerancias de fabricación • Errores de diseño • Superación de límites máximos de carga o condiciones de uso
A26	**Falta de recursos**	• Congestiones en el servicio (cuellos de botella) • Sobrecargas en sistemas e infraestructuras • Requisitos de nuevas aplicaciones que exceden las capacidades existentes • Falta de recursos económicos
A27	**Vulnerabilidades o errores del software**	• Errores de programación • Fallos en navegadores y aplicaciones WEB

A28	**Violación de leyes o regulaciones**	• Violaciones de leyes sobre procesamientos de información • Incumplimientos de cláusulas contractuales • Incumplimientos legales en el tratamiento de datos personales
A29	**Uso no autorizado o administración de dispositivos y sistemas**	
A30	**Uso incorrecto o administración de dispositivos y sistemas**	
A31	**Abuso de Autorizaciones**	
A32	**Ausencia de personal**	• Bajas prolongadas • Sustituciones por bajas o vacaciones • Bajas masivas por epidemias
A33	**Terrorismo**	• Ataques con explosivos • Incendios premeditados • Ataques con armas de fuego
A34	**Coerción, extorsión o corrupción**	Uso indebido de datos o acceso a datos confidenciales por chantajes, extorsiones o corrupción de personas
A35	**Robo de identidad**	• Robos de datos personales para suplantar identidades (datos bancarios etc.) • Ataques con datos ficticios (Suplantación de identidades por maquinas o robots.
A36	**Comportamientos anti-éticos**	• Negación de recepción de informaciones, mensajes o instrucciones de seguridad (p. ej. negar la recepción de emails o pedidos

		realizados etc.)
A37	**Abuso de datos personales**	• Violaciones a las leyes sobre protección de datos • Recoger datos sin base legal o consentimiento, usa para fines diferentes al objetivo establecido enel momento de la recolección, eliminación de datos personales demasiado tarde • Divulga datos de forma no autorizada • Etc.
A38	**Software malicioso**	Ataques de software malicioso tales como virus, gusanos y caballos de Troya.
A39	**Ataques DoS o denegación de servicio**	Interrupciones de los procesos comerciales (envió masivo de formularios etc.) • Daños a la infraestructura (Bloque de accesos etc.) • Fallos por sobrecarga por ataques por accesos masivos provocados
A40	**Ingeniería Social**	Los ataques típicos de ingeniería social para acceder de forma no autorizada suponen casi siempre una suplantación de identidad basándose en la confianza, miedo o respeto de personas. Normalmente se utilizan llamadas urgentes para reclamar información de contraseñas etc. amparados en la autoridad, la amistad o la confianza.
A41	**Reproducción de mensajes**	Intercepción de transmisiones para introducir datos maliciosos y retransmitir el mensaje
A42	**Entrada no autorizada a las instalaciones**	
A43	**pérdida de datos**	Perdida de la disponibilidad de datos por borrados indebidos o corrupción por Software malicioso, usos indebidos o fallos técnicos

Elaborado por: Bryan Alexander Guanín Castillo.

3.13.4.4. Valoración de las amenazas para la seguridad de la información

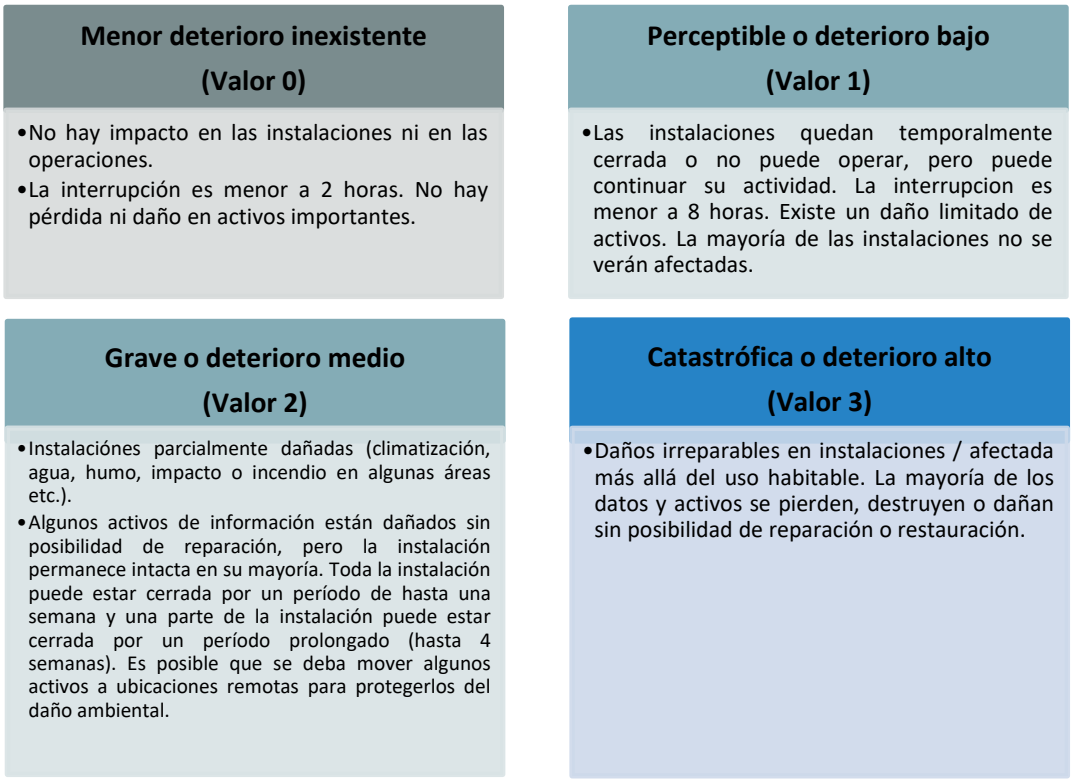
Figura 31. Niveles de riesgo moderado, menor e incidental.

Impacto Moderado3	Impacto Menor2	Impacto Incidental1
• Pérdida financiera entre unvalor 1 y un valor 2 • Impacto en medios de comunicación negativo a nivel nacional a corto plazo • Requisito de comunicacióna las entidades reguladoras por incidentes con una acción correctiva inmediata • Tratamiento médico ambulatorio requerido paraempleados o terceros, clientes o proveedores	• Pérdida financiera entre unvalor 1 y un valor 2 • Daño reputaciones local • Incidente denunciable al regulador, sin seguimiento • Sin lesiones menores a empleados o terceros, comoclientes o proveedores • Problemas generales en el ánimo o moral del personaly aumento en la rotación	• Pérdida financiera insignificante • La atención de los medioslocales se remedia rápidamente • Incidente no reportable alas entidades reguladoras • No hay lesiones para los empleados o terceros, comoclientes o proveedores • Insatisfacción del personal

Elaborado por: Bryan Alexander Guanín Castillo.

Se refiere a la frecuencia de ocurrencia de las amenazas, ante lo cual es necesario identificar la probabilidad que sucedan, determinando una escala de valor para cada amenaza (Normaiso 27001, 2020). La escala se puede representar como se muestra a continuación en la Figura 32.

Figura 32. Escala de Probabilidades de Amenazas.

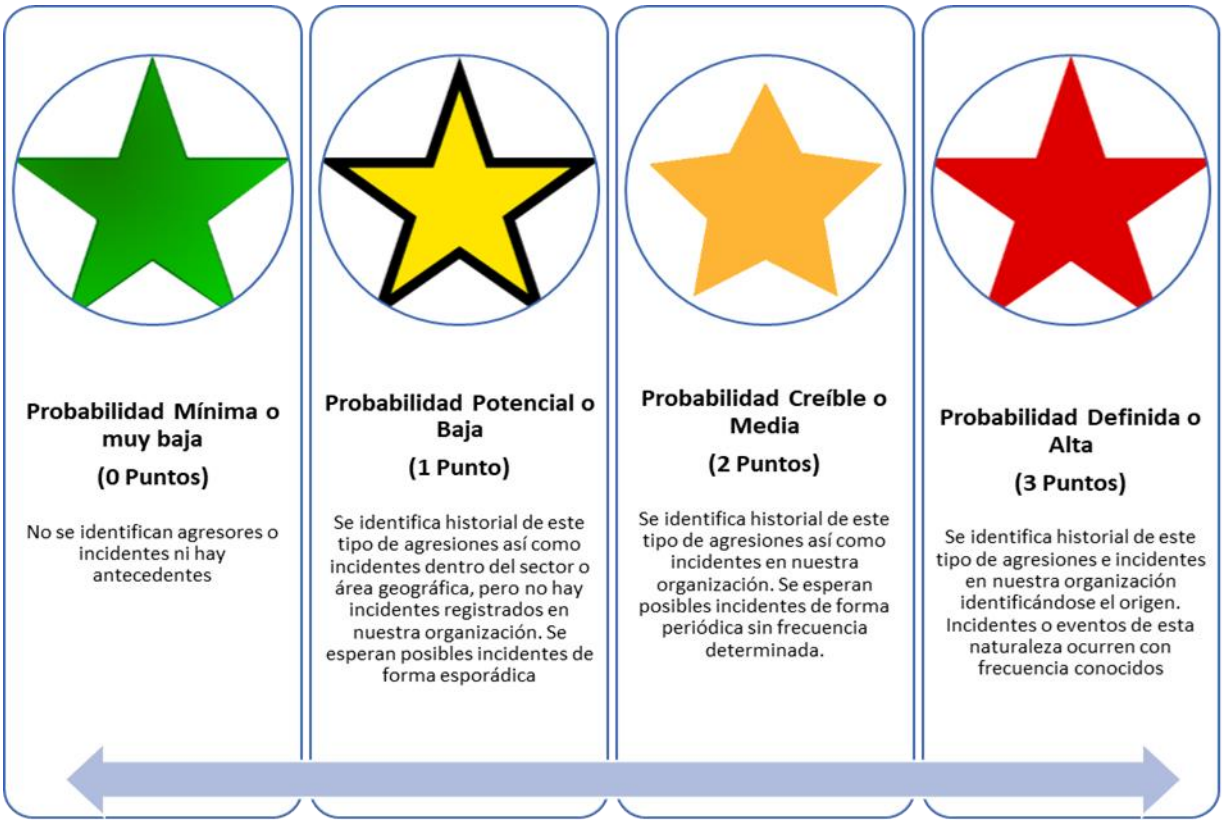


Elaborado por: Bryan Alexander Guanín Castillo.

3.13.4.5.Nivel de Vulnerabilidad

Si la amenaza se produce el nivel de vulnerabilidad considera el grado de afectación que tendríala organización con la pérdida de información (Normaiso 27001, 2020). Es importante establecer adecuadamente la escala para el impacto de pérdida y vulnerabilidad, ya que los valores van a variaren los diferentes activos. La escala de valoración de la vulnerabilidad se muestra en la Figura 33.

Figura 33. Nivel de Vulnerabilidad.



Elaborado por: Bryan Alexander Guanín Castillo

3.13.4.6. Análisis de riesgos

Frente a una amenaza potencial podemos ahora establecer un análisis en base a los parámetros de la frecuencia y el valor de la vulnerabilidad (Normaiso 27001, 2020). El análisis de riesgos es un proceso en el cual se tomarán en cuenta los niveles de impacto.

Niveles de Impacto de las amenazas. La Figura 34 muestra una tabla de valores de impacto.

Figura 34. Valores de Impacto.

Tabla 1 Valores Impacto						
Valor de Vulnerabilidad de la amenaza	VALORES DE DE LAS DIMENSIONES DE LOS ACTIVOS 0 No Aplicable 1 Incidental 2 Menor 3 Moderado 4 Importante 5 Extremo					
	0	1	2	3	4	5
0 - Deterioro Menor / inexistente	0	0	0	0	0	0
1 - Deterioro Perceptible / Bajo	0	1	2	3	4	5
2 - Deterioro Grave / medio	0	2	3	4	5	6
0 - Deterioro Catastrófico / Alto	0	3	4	5	6	7

Fuente: (Normaiso 27001, 2020)

3.13.4.7. Cálculo de Valores de impacto de Cada Activo

Con los valores de probabilidad y la valoración de activos se construirá la tabla de valoración de activos como se muestra en la Figura 35**.**

Figura 35. Valoración de Amenazas

	Tabla 2 de Valoración de Amenazas de Activos				
	ACTIVOS		0 No Aplicable 1 Incidental 2 Menor 3 Moderado 4 Importante 5 Extremo		
	Sistema de Correo Electrónico	Probabilidad / Ocurrencia 0 Minima - 1 Baja - 2 Media - 3 Alta	Deterioro Confidencialidad	Deterioro Integridad	Deterioro Disponibilidad
AMENAZAS	Fuego	1	0	2	5
AMENAZAS	Inundacion	1	0	2	4
AMENAZAS	Interrupcion de suministro Eléctrico	2	1	2	4
AMENAZAS	Robo de dispositivos	3	3	3	0
AMENAZAS	Fallo Comunicaciones	3	3	3	0
	Servidor para la página web corporativa				
AMENAZAS	Fuego	2	0	3	5
AMENAZAS	Inundacion	1	0	3	4
AMENAZAS	Interrupcion de suministro	3	1	2	3
AMENAZAS	Robo de dispositivos	1	3	3	0
AMENAZAS	Fallo Comunicaciones	2	3	3	0

Fuente: (Normaiso 27001, 2020)

3.13.4.8. Cálculo de Nivel de Impacto

De acuerdo a la Figura 35 se construirá la Figura 36.

Figura 36. Nivel de impacto.

	Tabla 3 de Nivel de Impacto			
	Niveles de Impacto			
	Sistema de Correo Electrónico	**Impacto Confidencialidad**	**Impacto Integridad**	**Impacto Disponibilidad**
AMENAZAS	Fuego	0	2	5
	Inundacion	0	2	4
	Interrupcion de suministro Electrico	2	3	5
	Robo de dispositivos	5	5	0
	Fallo Comunicaciones	5	5	0
	Servidor para la página web corporativa			
AMENAZAS	Fuego	0	4	6
	Inundacion	0	3	4
	Interrupcion de suministro	3	4	5
	Robo de dispositivos	3	3	0
	Fallo Comunicaciones	4	4	0

Fuente: (Normaiso 27001, 2020)

3.13.4.9.Evaluación de riesgos

Cuando se ha determinado un valor de riesgo para cada amenaza que puede afectar a un activo de información, se debe definir los criterios aceptables para el riesgo (Normaiso 27001, 2020). Seleccionar los niveles de riesgo pueden ser asumibles y determinar ante cuales tomar correctivos, como se muestra en la Figura 37.

Figura 37. Clasificación y Valoración de Riesgo.

CALIFICACION DEL RIESGO	DESCRIPCIÓN
Muy alto (7-9)	El riesgo es totalmente inaceptable. Se deben tomar medidas inmediatas para reducir estos riesgos y mitigar los riesgos.
Alto (5-6)	El riesgo es inaceptable. Las medidas para reducir el riesgo y los riesgos de mitigación deberían implementarse lo antes posible.
Medio (3-4)	El riesgo puede ser aceptable en el corto plazo. Los planes para reducir los riesgos y mitigar los peligros deberían incluirse en los planes y presupuestos futuros.
Bajo (0-2)	Los riesgos son aceptables. Se deben implementar medidas para reducir aún más el riesgo o mitigar los peligros junto con otras mejoras de seguridad y mitigación.

Fuente: (Normaiso 27001, 2020)

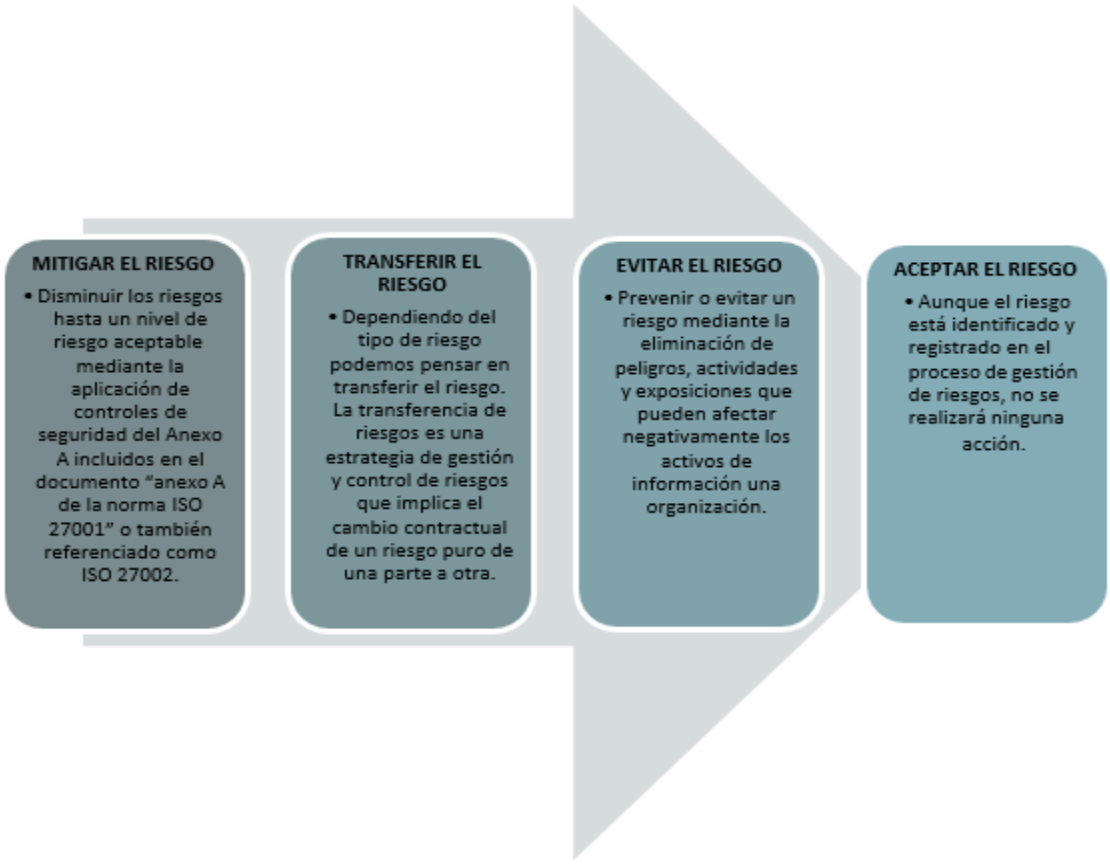
Los controles de riesgo en la norma ISO 27001 para la seguridad de la información, permiten identificar las medidas que permitan disminuir los distintos niveles de riesgo (Normaiso 27001, 2020). Además, se tiene que considerar la realización de un plan urgente en donde

se incluyan las actualizaciones de los controles adicionales sobre los estándares mínimos recomendados por la organización.

3.13.4.10. Tratamiento de riesgos

Consiste en realizar un plan para el tratamiento de los riesgos identificados lo que permite determinar cuáles son los riesgos inaceptables, las opciones de tratamiento de riesgo se muestranen la Figura 38.

Figura 38. Tratamiento de Riesgo.



Fuente: Bryan Alexander Guanín Castillo.

3.13.4.11. Responsable del riesgo

Identificar al propietario de los riesgos (Normaiso 27001, 2020). El propietario de los riesgos actuaráen la toma de decisiones para el tratamiento que se dará a cada una de las amenazas y también los riesgos identificados. La documentación en el análisis de riesgos será:

- Documentación sobre los criterios utilizados para las valoraciones de los riesgos y las evaluaciones particulares.
- Documentación sobre las valoraciones intrínsecas de cada riesgo
- Inventario de activos de información con la identificación de los propietarios de cada activo
- La definición del riesgo asumible tomada en la evaluación de riesgos

3.13.4.12. Selección de controles: declaración de aplicabilidad

Consiste en identificar los controles de seguridad que se van a aplicar a los activos que se han determinado para el tratamiento de riesgos (Normaiso 27001, 2020). En el inventario de activos esconveniente incluir:

- Categorización de la información (datos personales, nivel de confidencialidad etc.)
- Necesidad de establecer controles de acceso
- Incluida o no en procesos de copia de seguridad
- Soportes de almacenamiento
- Necesidades de comunicación de la información etc.

Luego de esa información es importante definir los controles técnicos y de organización para proteger los activos de las amenazas. Posteriormente será necesario realizar un análisis de aplicabilidad, tomando en cuenta los controles del Anexo A sin dejar ningún control que sea aplicable a la protección del activo. En la Figura 39 se muestra un modelo de aplicabilidad ISO 27001.

Figura 39. Modelo de Declaración de aplicabilidad ISO 27001.

		Activo 1				
A9	**Control de Acceso**	Implementado	Aplica a los riesgos del activo	Coste de implementacion Aceptable	Coste de mantenimiento Aceptable	Justificacion o comentarios
9.1.1	Política de control de acceso	SI/NO	SI/NO	SI/NO	SI/NO	
9.1.2	Acceso a las redes y a los servicios de red	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.1	Registro y baja de usuarios	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.2	Provisión de acceso de los usuarios	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.3	Gestión de privilegios de acceso	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.4	Gestión de la información secreta de autentificación de los usuarios	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.5	Revisión de los derechos de acceso de usuario	SI/NO	SI/NO	SI/NO	SI/NO	
9.2.6	Retirada o ajuste de los derechos de acceso	SI/NO	SI/NO	SI/NO	SI/NO	

Fuente: (Normaiso 27001, 2020)

3.14. Resultados

En toda empresa los activos están expuestos a riegos, es por eso la importancia de conocer cuáles son los activos que poseen mayor nivel de riesgo con el fin de implementar protecciones para evitar que las amenazas se materialicen.

A continuación, se establece varias medidas de seguridad para los activos generales de la empresa:

- **Internet**
  - El control que se debe de tomar en cuenta es la restricción de páginas como son redes sociales y descarga de programas; el uso de internet en las máquinas de la empresa debe ser estrictamente para actividades de trabajo.
  - Además, no hay nada que garantiza la protección de los servicios como es el aseguramiento de la disponibilidad para ello se deberían adquirir dispositivos accesibles (cortafuegos, servidores) para soportarla máxima carga prevista.
- **Safi**
  - Debería existir claves confidenciales para acceder al sistema.
  - Mejorar la protección de la aplicación con privilegios de acceso deacuerdo al puesto de trabajo y a la información que maneja.
  - Antivirus.
  - La medida que se debe tomar es la adquisición de software óptimo para evitar la propagación de virus.
  - También es que por lo menos una cuatro veces al mes el antivirus sea actualizado para que pueda contra restar cualquier software dañino o que en lo posible de colocar dispositivos externos en las máquinas para así evitar que pueda ser infectadas.
- **Software ilustrator**
  - La adquisición de software con licencia.
  - Además de la instalación de parches y actualizaciones que son muy necesarios.
  - Control de acceso al sistema operativo: con el uso de claves de usuario.
- **Servidos de bases de datos**

- Es de trasladar el servidor hacia un cuarto donde se toman todas las medidas de seguridad necesarias como es el control de accesos.
- La resguardar la seguridad física para ser frente amenazas como desastres naturales.

- **Computadoras portátiles**
  - Crear cuentas de usuario y administrador para así poder instalar el software adecuado necesario para las jornadas de trabajo.
- **Red LAN**
  - Se deberían implementar protecciones criptográficas para la confidencialidad de los datos intercambiados.
  - Además de implementar algoritmos para este caso sería mejor:
  - Dispositivos Físicos y emplear servicios certificados.
  - Además de realizar mantenimientos regulares del estado de la red LAN.
- **Cableado**
  - Para la protección de cableado se debería tener lo siguiente:
  - Disponer de planos actualizados del cableado.
  - Etiquetar todos los elementos de cableado.
  - Evitar rutas a través de áreas públicas.
  - Controlar todos los accesos al cableado.
  - Separar el cableado de alimentación del de comunicaciones para evitar interferencias.
  - Proteger contra daños o interceptaciones no autorizadas (conductos blindados, cajas o salas cerradas).
- **Oficinas**
  - Se deberían de disponer un mayor número de guardias de seguridad, además de botones de emergencia.
  - Disponer de cámara de vigilancia dentro de la empresa.
- **Personal**
  - Crea una normativa relativa a la gestión de personal (en materia de seguridad).
  - Crear procedimientos relevantes se seguridad: emergencias, incidencias.
  - Prevención y reacción frente a extorción.
  - Prevención y reacción frente ataques de ingeniería social.

El presente trabajo, busca cumplir a su totalidad la de implementación del SGSI mismo que es pertinente señalar que el alcance se vio limitado por los factores de tiempo y recursos, es por ello que la implementación del proyecto se deja como guía para que se pueda desarrollarlo a futuro.

A su vez, el plan de seguridad óptimo pretender eliminar las fallas de seguridad, contando con normativas de seguridad dentro de la empresa y buenas practicas sobre el manejo de la información.

CONCLUSIONES

La empresa “Pinto Seguros” no tiene medidas de seguridad guiados y documentados, por lo cual este estudio será de gran beneficio para minimizar riesgos en el futuro, es por ello que gracias a la metodología Magerit se pudo identificar ciertos riesgos y posibles soluciones para mitigar en cierta parte dichas vulnerabilidades.

Después de haber realizado este proyecto, la empresa podrá encaminase a tener una buena seguridad, mismo que será un punto de partida para la creación de normativas y políticas de seguridad para los recursos informáticos y para los empleados que laboran en la empresa.

Cabe recalcar que este proyecto investigativo presentado, se adapta a los objetivos actuales de la empresa, mismo que al momento de cambiar sus procesos o gestiones este puede variar, ya que tiene riesgos acordes a lo que actualmente conlleva la empresa.

RECOMENDACIONES

Se recomienda que haya una revisión periódica de las amenazas y riesgos, ya que la tecnología está cambiando constantemente y deben ser controlados para evitar futuros problemas, es por eso que se debe dar importancia a la identificación de riesgos, mismo que están expuestos los activos de la empresa con el fin de evitar pérdidas económicas u operacionales.

Es importante que se establezca un sistema de medición, que permita valorar la marcha del SGSI de modo global y particular, detectando desviaciones y cambios en la organización que deban ser tratados para que el SGSI se mantenga operativo.

Se aconseja continuar con el proceso de implementación bajo la norma ISO 27001, mismo que busca completar el análisis de riesgo de los activos involucrados en el manejo de la información, de igual manera es importante que la organización se asegure de crear procedimientos para el monitoreo y revisión del sistema que cubran incidentes de seguridad, auditorías internas y revisiones gerenciales.

BIBLIOGRAFÍA

Análisis de Riesgos. (2019). *Análisis y cuantificación del Riesgo.* Recuperado el 3 de diciembre de 2020, de http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/4AnalisisycuantificaciondelRiesgo%28AR%29_es.pdf

Ayudaley. (18 de noviembre de 2017). *Análisis de riesgos sobre Protección de Datos.* Recuperado el 3 de diciembre de 2020, de https://ayudaleyprotecciondatos.es/2017/11/28/analisis-riesgos-proteccion-datos/

Barrionuevo, J. (14 de abril de 2020). *La flexibilidad laboral como estrategia de competitividad y sus efectos sobre la economía, la empresa y el mercado de trabajo.* Recuperado el 3 de diciembre de 2020, de Instituto Jubones: https://institutojubones.edu.ec/ojs/index.php/societec/article/download/106

BSI. (2020). *Gestión de la Seguridad de la Información ISO/IEC 27001*. Recuperado el 3 de diciembre de 2020, de BSI Group.: https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/

Buigues, M. (18 de junio de 2015). *Iso 27001 actualización versión 2013*. Recuperado el 3 de diciembre de 2020, de Slideshare: https://es.slideshare.net/mariajosebuigues3/iso-27001-actualizacin-versin-2013

Cambio digital. (2020). *La tríada CIA: Definición, componentes y ejemplos*. Recuperado el 3 de diciembre de 2020, de https://cambiodigital-ol.com/2020/03/la-triada-cia-definicion-componentes-y-ejemplos/

Cisco. (28 de septiembre de 2020). *¿Qué es la seguridad de red?* Recuperado el 3 de diciembre de 2020, de https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

Digital Guide IONOS. (12 de noviembre de 2020). *Correo seguro: protege tu email de los spambots*. Recuperado el 3 de diciembre de 2020, de https://www.ionos.es/digitalguide/correo-electronico/seguridad-correo-electronico/correo-seguro-protege-tu-direccion-de-correo-electronico/

Ecuador, Ministerio de Telecomunicaciones. (04 de abril de 2020). *Guía para la implementación del esquema gubernamental de seguridad de la informaciòn.* Recuperado el 3 de diciembre de 2020, de Gobierno Electrónico del Ecuador: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-IMPLEMENTACI%C3%93N-DEL-EGSI-ABRIL2020.pdf

Fadrell Grupo Tecnológico. (28 de junio de 2017). *Ciberseguridad: defensa en capas para reducir el riesgo*. Recuperado el 3 de diciembre de 2020, de http://www.fadrell.com/ciberseguridad-defensa-en-capas-para-reducir-el-riesgo/

Fernández, Y. (1 de octubre de 2019). *Firewall: qué es un cortafuegos, para qué sirve y cómo funciona*. Recuperado el 3 de diciembre de 2020, de Xataka: https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona

García, G. (2020). *Activos intangibles: qué son y cómo ayudan a tu empresa*. Recuperado el 3 de diciembre de 2020, de Sage Advice: https://www.sage.com/es-es/blog/activos-intangibles-ayudar-empresa/

Intelequia. (28 de noviembre de 2020). *Ciclo de vida del software: todolo que necesitas saber*. Recuperado el 3 de diciembre de 2020, de https://www.belatrixsf.com/blog/seguridad-desarrollo-software

ISO 2700.ES. (4 de mayo de 2005). *SGSI*. Recuperado el 3 de diciembre de 2020, de https://www.iso27000.es/sgsi.html

ISOTools Excellence. (21 de mayo de 2015). *ISO 27001: ¿Qué significa la Seguridad de la Información?* Recuperado el 3 de diciembre de 2020, de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

Kirvan, P. (29 de julio de 2019). *¿Cuál es una buena frecuencia de prueba de copias de seguridad?* Recuperado el 3 de diciembre de 2020, de Computerweekly: https://searchdatacenter.techtarget.com/es/respuesta/Cual-es-una-buena-frecuencia-de-prueba-de-copias-de-seguridad

Lanz, L. (22 de mayo de 2018). *¿Qué es la ciberseguridad?* Recuperado el 3 de diciembre de 2020, de OpenWebinars: https://openwebinars.net/blog/que-es-la-ciberseguridad/

López, J. (4 de octubre de 2020). *Tendencias de seguridad para tu vida digital en la internet de la COVID*. Recuperado el 3 de diciembre de 2020, de Hipertextual: https://hipertextual.com/2020/10/amenazas-seguridad-vida-digital-internet-covid

Lucio Vásquez, Á. G. (2020). Evolución del concepto de seguridad en la República del Ecuador: desde una perspectiva de seguridad nacional hacia la seguridad integral. Relaciones Internacionales, 43, 171. *Relaciones Internacionales*(43), 171–188. Recuperado el 3 de diciembre de 2020, de https://revistas.uam.es/relacionesinternacionales/article/view/relacionesinternacionales2020.43.009/11888

Normaiso 27001. (2020). *Implementar ISO 27001 paso a paso - 1 como hacer un Analisis Previo*. Recuperado el 3 de diciembre de 2020, de https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/

Nqa. Organismo de Certificación Global. (10 de julio de 2020). *Anexo SL*. Recuperado el 3 de diciembre de 2020, de https://www.nqa.com/es-es/certification/systems/annex-sl

Pinto Seguros. (2018). *Estatuto.* Machachi: Pinto Seguros.

Redser. (22 de agosto de 2019). *ISO 27001-Sistema de Gestión de Seguridad de Información*. Recuperado el 3 de diciembre de 2020, de https://redser.com/servicios/iso-27001.asp

Rodríguez, P. (7 de mayo de 2020). *Análisis de riesgos informáticos y ciberseguridad*. Recuperado el 3 de diciembre de 2020, de Ambit: https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad

Rouse, M. (28 de septiembre de 2018). *Programas para hacer copias de seguridad.* Recuperado el 3 de diciembre de 2020, de Computerweekly: https://www.computerweekly.com/es/definicion/Copia-de-seguridad-o-respaldo

Seguridad Informática. (19 de marzo de 2019). *Seguridad en Redes LAN*. Recuperado el 3 de diciembre de 2020, de http://seguridadinformatica2406.blogspot.com/2019/03/seguridad-en-redes-lan.html

Seguridad Informática. (2020). *Reglas Básicas de Seguridad Informática*. Recuperado el 3 de diciembre de 2020, de https://sites.google.com/site/seguridadinformaticayweb/reglas-basicas-de-seguridad-informatica

Smile Informática. (12 de abril de 2018). *Cómo navegar de forma segura por la web*. Recuperado el 3 de diciembre de 2020, de https://www.smileinformatica.es/consejos-soporte/como-navegar-de-forma-segura-por-la-web/

Tecnología Informática. (7 de julio de 2018). *Cómo hacer una contraseña segura. Cuáles contraseñas no usar*. Recuperado el 3 de diciembre de 2020, de https://www.tecnologia-informatica.com/contrasenas-seguras-cuales-no-usar/

Tecon. Soluciones informáticas. (2019). *La seguridad de la información*. Recuperado el 3 de diciembre de 2020, de https://www.tecon.es/la-seguridad-de-la-informacion/

Universidad Cooperativa de Colombia. (25 de junio de 2014). *Seguridad de la información y seguridad informática, conceptos que debemos conocer y diferenciar*. Recuperado el 3 de diciembre de 2020, de https://www.ucc.edu.co/prensa/2014/Paginas/seguridad-de-la-informacion-y-seguridad-informatica.aspx

Universidad Internacional de Valencia. (10 de octubre de 2016). *Tres tipos de seguridad informática que debes conocer*. Recuperado el 3 de diciembre de 2020, de https://www.universidadviu.com/es/actualidad/nuestros-expertos/tres-tipos-de-seguridad-informatica-que-debes-conocer

ANEXOS

Anexo A. Plan de Trabajo

Figura 40. Plan de Trabajo.

Nombre de tarea	Responsable	Duración	nov-20	dic-20	ene-21	feb-21	mar-21
Presentación del Tema	Autor	15 días					
Aprobación del Tema	Autor	30 días					
Elaboración de la propuesta	Autor	15 días					
Presentación del 1er borrador	Autor	10 días					
Presentación de borrador final	Autor	15 días					
Elaboración de encuestas	Autor	2 días					
Análisis y tabulación de encuestas	Autor	1 día					
Presentación de la propuesta	Autor	7 días					
Defensa de la propuesta	Autor	1 día					

Fuente: Bryan Alexandre Guanín Castillo.

Anexo B. Glosario de términos

A

- **Acción correctiva:** Acción para eliminar la causa de una no conformidad y prevenir su repetición.
- **Acción preventiva:** Medida de tipo pro-activo orientada a prevenir potenciales no conformidades
- **Aceptación del riesgo:** Decisión informada de asumir un riesgo concreto.
- **Alcance:** Ámbito de la organización que queda sometido al SGSI.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Ataque:** Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.
- **Auditor:** Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.
- **Autenticación:** Provisión de una garantía de que una característica afirmada por una entidad es correcta.

C

- **CIA:** Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Conformidad:** Cumplimiento de un requisito.
- **Control:** Medida por la que se modifica el riesgo.
- **Corrección:** Acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.
- **Criterio del riesgo:** Términos de referencia contra los cuales se estima la importancia del riesgo.

D

- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

E

- **Eficacia:** Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.
- **Estándar de implementación de seguridad:** Documento que especifica formas autorizadas para materializar la seguridad.
- **Estimación de riesgos:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
- **Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos.
- **Evento**
- Ocurrencia o cambio de un conjunto particular de circunstancias.

F

- **Fiabilidad:** Propiedad del comportamiento y de unos resultados consistentes previstos.

G

- **Gestión de claves:** Controles referidos a la gestión de claves criptográficas.
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

I

- **Identificación de riesgos:** Proceso de encontrar, reconocer y describir riesgos.
- **IEC:** International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.
- **Impacto:** El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Indicador:** Medida que proporciona una estimación o evaluación.

- **Información documentada**
- Información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).
- **ISO/IEC 27001:** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.
- **ISO/IEC 27002:** Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

M

- **Mejora continua:** Actividad recurrente para aumentar el rendimiento.
- **Método de medida:** Secuencia lógica de operaciones, descrita genéricamente, utilizada para cuantificar un atributo con respecto a una escala específica.
- **Monitoreo:** Determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente.

N

- **Necesidad de información:** Conocimiento requerido para gestionar objetivos, metas, riesgos y problemas.
- **Nivel de riesgo:** Magnitud de un riesgo expresado en relación a la combinación de consecuencias y su probabilidad.
- **No conformidad:** Incumplimiento de un requisito.

O

- **Objetivo de control:** Declaración que describe lo que se debe lograr como resultado de la implementación de los controles.
- **Organización:** Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

P

- **PDCA:** Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Política:** Intenciones y dirección de una organización, expresada formalmente por su alta dirección.
- **Probabilidad:** Posibilidad de que ocurra algo.
- **Proceso:** Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

- **Proceso de gestión del riesgo:** Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicación, consultoría, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos.
- **Propietario del riesgo:** Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

R

- **Recursos de tratamiento de información:** Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.
- **Rendimiento:** Resultado medible.
- **Requisito:** Necesidad o expectativa que es establecida, generalmente de forma implícita u obligatoria.
- **Revisión:** Actividad realizada para determinar la idoneidad, adecuación y efectividad del objeto de estudio para lograr los objetivos establecidos
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.

S

- **Salvaguarda:** Control.
- **Segregación de tareas:** Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Selección de controles:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **Sistema de Gestión:** Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos.
- **Sistema de Gestión de la Seguridad de la Información:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **Sistema de Información:** Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información.
- **SoA:** Declaración de aplicabilidad.
- **Startup:** Es una empresa que se encuentra en la etapa inicial de su operación y que debe desarrollar su producto para generar ingresos que le permitan crecer.

T

- **TIC:** Tecnología de la Información y las Comunicaciones
- **Tratamiento de riesgos:** Proceso para modificar el riesgo.
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

V

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Fuente: Bryan Alexander Guanín Castillo.

Anexo C. Documentos de Control Anexo A

Tabla 57 Controles Anexo A

Referencia	Controles
4.3	El alcance del SGSI
5.2	Política de seguridad de la información
6.1.2	Proceso de evaluación de riesgos de seguridad de la información
6.1.3	Proceso de tratamiento de riesgos de seguridad de la información
6. 1.3	d) La declaración de aplicabilidad
6.2	Objetivos de seguridad de la información
7.2	d) Prueba de competencia
7.5.1	b) Información documentada determinada por la organización como necesaria para la efectividad del SGSI
8.1	Planificación y control operacional
8.2	Resultados de la evaluación de riesgos de seguridad de la información
8.3	Resultados del tratamiento de riesgo de seguridad de la información
9.1	Evidencia del monitoreo y medición de resultados
9.2	Un proceso de auditoría interna documentado
9.2	g) Evidencia de los programas de auditoría y los resultados de la auditoría
9.3	Evidencia de los resultados de las revisiones de la administración
10.1	f) Evidencia de la naturaleza de las no conformidades y cualquier acción posterior tomada10. 1 g) Evidencia de los resultados de cualquier acción correctiva tomada

b

Fuente: Bryan Alexander Guanín Castillo.

Anexo D. Documentación Específica para Control en Anexo A

Tabla 68 Documentos para Aplicabilidad de acuerdo a Anexo A

Referencia	Controles
A 7.1.2 y A.13.2.4	Definición de funciones y responsabilidades de seguridad
A 8.1.1	Un inventario de activos
A 8.1.3	Reglas para el uso aceptable de los activos
A.8.2.1	Esquema de clasificación de la información
A.9.1.1	Política de control de acceso
A 12.1.1	Procedimientos de operación para la administración de TI
A 12.4.1 y A.12.4.3	Registros de actividades del usuario, excepciones y eventos de seguridad
A 14.2.5	Principios de ingeniería de sistemas seguros
A 15.1.1	Política de seguridad del proveedor
A 16.1.5	Procedimiento de gestión de incidentes
A 17.1.2	Procedimientos de continuidad del negocio
A 18.1.1	Requisitos legales, reglamentarios y contractuales

Fuente: Bryan Alexander Guanín Castillo.

Anexo E. Bitácora de incidentes de Seguridad

Bitacora_de_Incidentes_de_Seguridad.xlsx

Anexo F. Acuerdo Ministerial de teletrabajo

ACUERDO MDT-2020-076 TELET