ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2017, PARA EL PROCESO DE VIÁTICOS DEL INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA¨

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGÍSTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

AUTOR

MARÍA FERNANDA FERNÁNDEZ NOLIVOS

GUAYAQUIL, AGOSTO 2020

AGRADECIMIENTO

Gracias infinitas, Dios por darme la fuerza y la sabiduría para poder vencer cada uno de los obstáculos que se presentaron, a mi familia, pilar fundamental que estuvo siempre empujándome y apoyándome con amor y confianza, a todos los docentes que con su profesionalismo, carisma y dedicación permitieron culminar con éxito un objetivo más propuesto.

DEDICATORIA

Dedico el presente trabajo a mi familia, empezando por mi esposo Sergio, mis hijos Sergio Luis y Kerly Fernanda y a mi madre Luisa Nolivos quien me inculcó los principios y valores que rigen mi vida familiar, laboral y profesional.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenin Freire Cobo

COORDINADOR DEL PROGRAMA

MSIG. Juan Carlos García

PROFESOR DELEGADO

RESUMEN

El presente trabajo, describe el alcance y la expectativa de aplicar el diseño del Plan de Implementación de un Sistema de Gestión de Seguridad de Información, basado en la Norma ISO/IEC 27001:2017, considerando la Base Legal, situación actual del contexto, estado real frente a la seguridad de información, roles y responsabilidades, dirigido al proceso de viáticos del personal de Servidores y Trabajadores Públicos del Instituto Oceanográfico y Antártico de la Armada, que por necesidad Institucional deben desplazarse fuera de su domicilio y/o lugar habitual del trabajo, a cumplir tareas oficiales o desempeñar actividades inherentes a sus puestos.

Con la metodología de análisis, evaluación y tratamiento de riesgos, se gestionó los posibles riesgos al proceso de viáticos, empleando la Guía para la Gestión de Riesgos ISO/IEC 27005:2008, identificando los activos de información que intervienen, por lo que, a través de un diagnóstico, se consideró su valoración en cuanto al impacto en la pérdida de la confiabilidad, integridad y disponibilidad de la información, así mismo se identificó las amenazas y vulnerabilidades que causan daño a los activos o a la Institución y revisión de los controles existentes para la seguridad de la información.

El tratamiento de los riesgos es tomar decisiones frente a los riesgos existentes de acuerdo a la estrategia de la Institución, que deben ser aprobadas por la Máxima Autoridad, por lo que el Comité y Oficial de Seguridad evalúa y realiza

la selección de controles, que se encuentran incluidos en el Guía de la Norma ISO/IEC 27002:2017, en los niveles de riesgo alto, medio y bajo por la probabilidad de ocurrencia de las amenazas y vulnerabilidades, con la finalidad de administrar y gestionar ciertos criterios de contingencia y evaluación de riesgos para reducir, aceptar/retener, evitar o transferir los riesgos.

Gracias a la implementación del Plan, se logrará brindar a los funcionarios y clientes, niveles apropiados de protección, procesamiento y almacenamiento, preservando la calidad, eficiencia y seguridad de la Información.

ÍNDICE GENERAL

AGRADECIMIENTO i
DEDICATORIA ii
TRIBUNAL DE SUSTENTACIÓN iii
RESUMEN iv
ÍNDICE GENERAL vi
ABREVIATURAS Y SIMBOLOGÍA ix
ÍNDICE DE FIGURAS 1
ÍNDICE DE TABLAS 3
INTRODUCCIÓN 5
CAPÍTULO 1 7
1. GENERALIDADES 7
1.1. DESCRIPCIÓN DEL PROBLEMA 1
1.2. SOLUCIÓN PROPUESTA 2
CAPÍTULO 2 1
2. DESARROLLO DE LA SOLUCIÓN 1
2.1. BASE LEGAL Y METODOLOGIA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) 5
2.1.1. ESTADO ACTUAL FRENTE A LA SEGURIDAD 12
2.2. SITUACIÓN ACTUAL CONTEXTO 16
2.3. DESCRIPCIÓN DEL PROCESO DE VIÁTICOS 19
2.4. ALCANCE DEL PLAN 22
2.5. OBJETIVOS DEL PLAN 23
2.5.1. NIVEL DE CUMPLIMIENTO 24
2.6. SISTEMA DE GESTIÓN DOCUMENTAL 26

2.7. POLÍTICAS DE SEGURIDAD 26
2.8. GESTIÓN DE ROLES Y RESPONSABILIDADES 27
2.9. METODOLOGÍA Y GUÍA PARA LA GESTIÓN DE RIESGO 30
2.9.1. ESTABLECIMIENTO DE CONTEXTO 33
2.9.2. VALORACIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN 35
2.9.3. ANALISIS DEL RIESGO 36
2.9.3.1. IDENTIFICACIÓN DEL RIESGO. 36
2.9.3.1.1. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN 37
2.9.3.1.2. VALORACIÓN DE LOS ACTIVOS / PONDERACIÓN DE LA CRITICIDAD DE ACTIVOS 40
2.9.3.1.3. IDENTIFICACIÓN DE LAS AMENAZAS 44
2.9.3.1.4. IDENTIFICACIÓN DE VULNERABILIDADES 47
2.9.3.2. ESTIMACIÓN DE RIESGO 50
2.9.3.2.1. CRITERIOS DE PROBABILIDAD DE OCURRENCIA DE AMENAZAS: 51
2.9.3.2.2. CRITERIO DE PROBABILIDAD DE OCURRENCIA DE VULNERABILIDADES: 52
2.9.4. EVALUACIÓN DEL RIESGO 53
2.9.4.1. CRITERIO DE LA EVALUACIÓN DE RIESGOS: 54
2.9.5. TRATAMIENTO DE RIESGO 54
2.9.6. REDUCCIÓN DEL RIESGO 57
2.9.7. RETENCIÓN/ACEPTACIÓN DEL RIESGO 57
2.9.8. EVITACIÓN DEL RIESGO 57
2.9.9. TRANSFERENCIA DEL RIESGO 58
2.9.9.1. MATRIZ DE TRATAMIENTO DE RIESGO 58

2.9.10. COMUNICACIÓN DE LOS RIESGOS DE LA SEGURIDAD DE INFORMACIÓN 58
2.9.11. MONITOREO Y REVISIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN 60
CAPÍTULO 3 63
3. ANALISIS DE RESULTADOS 63
3.1. HOJA DE RUTA DE IMPLEMENTACIÓN DEL PLAN 64
3.2. IMPACTO DEL CUMPLIMIENTO ACTUAL VS. CUMPLIMIENTO CON LA IMPLEMENTACIÓN DEL PLAN 65
3.3. BENEFICIOS POR LA IMPLEMENTACIÓN DEL PLAN 68
4. CONCLUSIONES 69
5. RECOMENDACIONES 72
6. BIBLIOGRAFÍAS 73
7. ANEXOS 76

ABREVIATURAS Y SIMBOLOGÍAS

APC Administración Pública Central

CMM (Capability Maturity Model) Modelo de Madurez de Capacidades

COA Código Orgánico Administrativo

COVID 19

CSI Comité de Seguridad de la información

ESGI Esquema Gubernamental de Seguridad de la Información

INOCAR Instituto Oceanográfico y Antártico de la Armada

ISO /IEC 27000 Information Technology. Security techniques. Information Security Management Systems. Overview and Vocabulary

LAN Red de Área Local

MINTEL Ministerio de Telecomunicaciones y Sociedad de la Información

MSIG Magíster en Sistemas de Información Gerencial

OSI Oficial de Seguridad

PDCA Planificar, Hacer, Chequear y Actuar

SGSI Sistema de Gestión de Seguridad de la Información

SI Sistemas de Información

TIC Tecnologías de Información y Comunicación

ÍNDICE DE FIGURAS

Figura 2.1 Estructura PDCA-ISO 27001:2013 Fuente: [5, p. 14] 11

Figura 2. 2 Funcionamiento del proceso de SGSI bajo estándar ISO 27001:2013 [9] 12

Figura 2. 3 Organigrama del Instituto Oceanográfico Antártico de la Armada Fuente: [14] 18

Figura 2.4 Mapa de Proceso Área Financiera Fuente: [14] 20

Figura 2. 5 Proceso de Viáticos Fuente: [14] 21

Figura 2. 6 Esquema del Comité de Seguridad Fuente: Elaboración propia 28

Figura 2. 7 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18] 34

Figura 2. 8 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18] 36

Figura 2. 9 Activos de Información Fuente: [16] 38

Figura 2. 10 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18] 53

Figura 2. 11 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18] 55

Figura 2. 12 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18] 56

Figura 2. 13 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18] 59

Figura 2. 14 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18] 61

Figura 3. 1 Hoja de Ruta de implementación del Plan, Fuente: Elaboración propia. 64

Figura 3. 2 Cumplimiento actual vs. Cumplimiento con la implementación del plan 67

ÍNDICE DE TABLAS

Tabla 2. 1 Proceso, Subproceso y Procedimientos de Viáticos Fuente: elaboración propia. 22

Tabla 2. 2 Valoración de Criterios de Madurez CMM vrs % actual de cumplimiento, Fuente: elaboración propia 25

Tabla 2. 3 Identificación de Activos de Información, Fuente: Elaboración propia..... 38

Tabla 2. 4 Valoración del impacto en términos Pérdida de la confidencialidad Fuente: [5, p. 22]..... 41

Tabla 2. 5 Valoración del impacto en términos Pérdida de la integridad Fuente: [5, p. 22]..... 41

Tabla 2. 6 Valoración del impacto en términos Pérdida de la disponibilidad Fuente: [5, p. 22]..... 41

Tabla 2. 7 Valoración de activos de información, Fuente: Elaboración propia 42

Tabla 2. 8 Identificación de amenazas de los activos de información, Fuente: Elaboración propia..... 45

Tabla 2. 9 Identificación de las vulnerabilidades de los activos de información; Fuente: Elaboración propia..... 47

Tabla 2. 10 Valoración al criterio de probabilidad de ocurrencia amenaza Fuente: [5, p. 26]..... 51

Tabla 2. 11 Valoración al criterio de probabilidad de ocurrencia de vulnerabilidades Fuente: [5, p. 26] 52
Tabla 2. 12 Valoración al criterio de probabilidad de ocurrencia de vulnerabilidades Fuente: [5, p. 26] 54
Tabla 2. 13 Cumplimiento actual vs. Cumplimiento con la implementación del plan 66

INTRODUCCIÓN

La información del Instituto Oceanográfico y Antártico de la Armada constituye uno de los activos de mayor valor e importancia, que se deriva de estudios e investigaciones, y actualmente es de mucho interés, proporcionando así herramientas y conocimientos a los interesados, dicha información debe ser utilizada dentro de un entorno de seguridad, cualquiera que sea el medio en el que se encuentre: físico, lógico, así también el ambiente en que se procese.

La seguridad de la información es importante en un proceso administrativo, relacionado y depende de los aspectos tecnológicos. Por tal razón, se establece un compromiso Institucional el diseño y aprobación de un Plan de soporte para la gestión y la promoción de una cultura de seguridad al proceso de viáticos, defendiendo los roles y responsabilidades, por parte del Comité y Oficial de seguridad de la información, usuarios y clientes.

Para la Institución es una decisión estratégica, el “Plan del Implementación del Sistema de Gestión de Seguridad Información, basado en la Norma ISO/IEC 27001:2017, para el proceso de viáticos”, proporcionado los requisitos para implementar y mantener el mejoramiento continuo del Plan, así también analizando y evaluando los riesgos y posibles consecuencias mediante la Guía Gestión de Riesgos ISO/IEC 27005:2008 y para el tratamiento de riesgos la selección de controles de la Guía de Controles ISO/IEC 27002:2017, para reducir, aceptar/retener, evitar o transferir los riesgos de tal manera se pueda

prever, hacer, corregir y actuar ante un evento que podría poner en peligro la confidencialidad, integridad y disponibilidad de la seguridad de la información.

CAPÍTULO 1

GENERALIDADES

1.1. DESCRIPCIÓN DEL PROBLEMA

El personal de Servidores y Trabajadores Públicos, por necesidad institucional de acuerdo con los servicios que brindan a la ciudadanía, deben desplazarse fuera de su domicilio y/o lugar habitual del trabajo, a cumplir tareas oficiales o desempeñar actividades inherentes a sus puestos, por el tiempo que dure, desde la fecha y hora de salida hasta su retorno. Por el cual, debe seguir el procedimiento correspondiente para justificar la salida y el regreso a la Institución o a su domicilio.

Para que la Institución tome decisiones acertadas, se necesita contar con las tareas bien definidas y establecidas en cada área correspondiente, de acuerdo con el proceso de viáticos, por comisiones institucionales al interior y exterior del país.

Pero, en el cumplimiento del proceso y procedimiento establecido, existen problemáticas presentadas en la realización y liquidación de las comisiones que se ejecutan, detalladas a continuación:

a) La falta de políticas de seguridad en cuanto al acceso de la información.
b) Definición de roles y responsabilidades para el proceso de viáticos.
c) Aplicación del teletrabajo.
d) Control de las redes.

e) Falta de la protección de los equipos en cuanto a las amenazas, vulnerabilidades y riesgos ambientales.

Así es como las Tecnologías de Información y Comunicación (TIC) son el apoyo principal en la organización para manejar los procesos e información en una sociedad cada día más competitiva, es lo que con lleva al buen uso de un Sistema de Gestión de Seguridad de la Información, preservando la confidencialidad, la integridad y la disponibilidad de la información institucional.

1.2. SOLUCIÓN PROPUESTA

Una vez identificado el problema, se evidencia la necesidad de diseñar un Plan de Implementación de un Sistema de Gestión de Seguridad de Información, basado en la Norma ISO/IEC 27001:2017, para el proceso de Viáticos del Instituto Oceanográfico y Antártico de la Armada, información que debe ser utilizada dentro de un adecuado entorno de seguridad cualquiera que sea el medio en el que se encuentre físico, lógico así también el ambiente físico y tecnológico en que se procese.

Para la Institución es una decisión estratégica, ejecutar el Plan, que permita brindar a sus funcionarios niveles apropiados de protección, procesamiento y almacenamiento de su información, preservando la calidad y seguridad de acuerdo con los siguientes criterios:

- Disponibilidad: Asegurar que los clientes, contratistas, usuarios de los servicios, proveedores puedan acceder a la información cuando lo requieran.
- Confidencialidad: Asegurar que la información pueda ser accedida únicamente por los clientes, proveedores y usuarios de los servicios de la entidad debidamente autorizados.
- Integridad: Asegurar que la información almacenada y/o procesada por entidad no se alterada o modificada sin autorización
- Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.
- Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
- Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
- Eficacia: Asegurar que la información cumpla con lo planificado. [1, pp. 6, 7]

La seguridad de información es importante en un proceso administrativo y depende de los aspectos tecnológicos, por lo que se establece un compromiso institucional, mediante el desarrollo de un modelo de soporte para la gestión y la promoción de una cultura de seguridad, defendiendo los roles y responsabilidades por parte de su personal, clientes y usuarios, para la protección de los Activos de Información del Proceso de viáticos:

Se desarrollará en cuatro fases detalladas a nivel general:

1. Situación actual y descripción de proceso de viáticos. - Para conocer el estado actual de la entidad frente a la Seguridad de Información, Bases Legales y metodología de la Norma ISO/IEC 27001:2017, ventajas y beneficios por el empleo de la Norma, descripción de la estructura organizacional y del proceso de viáticos.
2. Alcance y Roles y Responsabilidades del Plan. – Alcance y Objetivos del Plan, definir y conocer las bases documentales, sobre las cuales se implementará el Plan de SGSI en la entidad, para conocer el cumplimiento actual de la Guía ISO/IEC 27002:2017, específicamente con los 114 controles definidos por lo que se define una tabla de ¨Nivel de cumplimiento¨, alineada al modelo de madurez de capacidades o CMM¨, políticas de seguridad, roles y responsabilidades del Comité y del Oficial de Seguridad.
3. Metodología de Riesgos. - Basados en la Guía para la Gestión de Riesgos de Seguridad de la Información ISO/IEC 27005:2008, se establecen criterios básicos para le gestión de riesgo, en el análisis de riesgo se identifican los activos de información con la valoración del impacto en cuanto a las dimensiones de la seguridad de la información y valoración de los niveles de probabilidad por las amenazas y vulnerabilidades que afectan a los activos ejecutando la estimación y evaluación de riesgos.

4. Tratamiento de Riesgos e impacto del proyecto actual versus la implementación del Plan -. En base a la evaluación de riesgos, se realiza la formulación de las acciones en base a los controles examinados, los recursos y las responsabilidades que permiten mitigar los riesgos para la seguridad de la información, aplicando la Matriz “Tratamiento de Riesgos” basados en la Guía para la Implementación de Controles de seguridad de la Información Norma ISO/IEC 27002:2017 que se aplican a la entidad y la justificación de su inclusión o exclusión al proceso de viáticos, comunicación y monitoreo de los riesgos, hoja de ruta para la Implementación del Plan y beneficios obtenidos.

CAPÍTULO 2

DESARROLLO DE LA SOLUCIÓN

2.1. BASE LEGAL Y METODOLOGIA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Toda entidad Pública especializada en ofrecer bienes y/o servicios sin fines de lucro, tiene como objetivo planificar, dirigir, coordinar y controlar las actividades técnicas y administrativas relacionado al cumplimiento del artículo 227 de la Constitución de la República que dispone: ¨La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación¨. [2, pp. 6,7]

La secretaria Nacional de la Administración Pública, en el Registro Oficial Nro. 088 del 25 de septiembre del 2013, publica, el Acuerdo Nro. 166 (derogado). Artículo 1.- Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

Artículo 2.- Las entidades de la Administración Pública implementarán en un plazo de dieciocho (18) meses el Esquema Gubernamental de Seguridad de la Información (EGSI) versión 1.0, que se adjunta a este acuerdo como Anexo 1, a excepción de las disposiciones o normas marcadas como prioritarias en dicho esquema, las cuales se implementarán en (6) meses desde la emisión del presente Acuerdo. La implementación del EGSI se realizará en cada institución de acuerdo

al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información. [3, p. 2]

La Asamblea Nacional, de conformidad con las atribuciones que le confiere la Constitución de la República del Ecuador y la Ley Orgánica de la Función Legislativa, discutió y aprobó el proyecto de la LEY ORGÁNICA DE TELECOMUNICACIONES, publicada en el Registro Oficial Nro. 439 del 18 de febrero del 2015, en la misma que según el TÍTULO XIV INSTITUCIONALIDAD PARA LA REGULACIÓN Y CONTROL, CAPÍTULO I Ministerio de Telecomunicaciones y de la Sociedad de la Información dispone:

Artículo 140.- ***Rectoría del sector.*** *El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información, es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información, de conformidad con lo dispuesto en la presente Ley, su Reglamento General y los planes de desarrollo que se establezcan a nivel nacional. Los planes y políticas que dicte dicho Ministerio deberán enmarcarse dentro de los objetivos del Plan Nacional de Desarrollo y serán de cumplimiento obligatorio tanto para el Sector Público como Privado.* [4, pp. 34,35]

Mediante Decreto Ejecutivo No. 5 de 24 de mayo 2017, se suprime la Secretaria Nacional de la Administración Pública y se transfiere al Ministerio de Telecomunicaciones y de la Sociedad de la Información entre otras la atribución: *¨b. Desarrollar y coordinar planes, programas o proyectos sobre gobierno electrónico que sean necesarios para su implementación¨.* [5, p. 2]

De acuerdo con el Código Orgánico Administrativo (COA), publicado en el Registro Oficial Nro. 31 del 07 de julio del 2017, sobre la Gestión Pública, en el Título II Actividades de las Administraciones Públicas, dispone:

Artículo 90.- ***Gobierno electrónico.*** *Las actividades a cargo de las administraciones pueden ser ejecutadas mediante el uso de nuevas tecnologías y medios electrónicos, en la medida en que se respeten los principios señalados en este Código, se precautelen la inalterabilidad e integridad de las actuaciones y se garanticen los derechos de las personas.*

Artículo 94.- ***Firma electrónica y certificados digitales.*** *La actividad de la administración será emitida mediante certificados digitales de firma electrónica. Las personas podrán utilizar certificados de firma electrónica en sus relaciones con las administraciones públicas.* [6, pp. 12, 13]

Que, mediante Acuerdo Ministerial Nro. 011-2018, del 08 de agosto del 2018, expide el Plan Nacional de Gobierno Electrónico, las acciones que serán ejecutadas en tres programas 2018-2021; Gobierno abierto, Gobierno Cercano y Gobierno Eficaz y Eficiente. En el capítulo 1. Fundamentos Generales, literal 5. Diagnostico; se

enfatiza que: *¨Dentro de las iniciativas relevantes que ha implementado el gobierno entorno a la ciberseguridad se encuentra la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI)…¨* [5, p. 3]

Actualmente en el Registro oficial Nro. 228 del 10 de enero del 2020 el Órgano Rector el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), expide el Acuerdo Nro. 025-2019 (vigente), en la cual detalla el procedimiento, modelo, responsables y recomienda utilizar para la Gestión de Seguridad de la Información, las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001:2017 ¨Guía de requisitos de implementación¨ [5, p. 9] NTE-INEN ISO/IEC 27005:2008 ¨Guía para la Gestión de riesgos de la información¨ [5, p. 16] y NTE-INEN ISO/IEC 27002:2017 ¨Guía para la implementación de controles¨, [5, p. 33] a fin construir el Esquema Gubernamental de Seguridad de la Información (EGSI) versión 2.0.

Para la aplicación de un Sistema de Gestión de Seguridad de la Información, en la Institución, es importante basarse en la Norma ISO/IEC 27001:2013 que está actualmente partiendo de la ISO/IEC 27001 es el estándar internacional que define como poner en práctica un SGSI evaluado independientemente y certificado, sienta las bases para el buen establecimiento del SGSI. Esto le permite asegurar más eficientemente toda la información confidencial de manera que reduzca la posibilidad de acceder a la misma de manera ilegal o sin autorización. [7, p. 63]

La norma ISO/IEC 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización.

Así también la ISO/IEC 27002:2013, proporciona las directrices para las normas de seguridad de la información organización y las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles, teniendo en cuenta los entornos de riesgo de seguridad de la información en la organización. [1, p. 49]

Los requerimientos establecidos en la ISO/IEC 27001:2017 propuestos son genéricos y están influenciados por las necesidades y objetivos de la Institución, los requisitos de seguridad, los procesos utilizados, el tamaño y estructura de la Institución. [5, p. 9]

La estructura de la ISO/IEC 27002:2017, contiene 14 capítulos (dominios), de donde emanan 35 categorías (objetivos de control) principales de seguridad y de estos un total de 114 controles disponibles. Una organización que se adecúe a este estándar tendrá en consideración cuáles de estos controles aplican y cuáles no. [5, p. 34]

Dentro de las ventajas competitivas al implementar un SGSI basado en la ISO/IEC 27001:2013 detallamos las siguientes:

- La seguridad de la información es parte integral de los procesos de negocio.
- Norma reconocida a nivel mundial.
- Incremento en la concientización y confianza de los empleados con respecto al tema de la seguridad de la información.
- Asesoramiento en los procesos con respecto a la seguridad de información.
- Ventaja competitiva a través de la Certificación.
- Cumplir la legislación vigente referente a la Seguridad de la información. [8, p. 16]

Entre los beneficios relevantes de un SGSI podemos citar los siguientes:

- Establece una metodología de Gestión de la Seguridad estructurada y clara.
- Reduce el riesgo de pérdida, robo o integridad de la información sensible.
- Los riesgos y los controles son continuamente revisados.
- Aumenta la confianza y las reglas claras para los miembros de la Institución.
- Se incrementa la motivación y la satisfacción del personal.
- La imagen de la Institución mejora. [5, pp. 13, 14]

Un sistema de SGSI debe mejorar continuamente su eficacia, es decir asegurar que la información cumpla con lo planificado, por ello es recomendable que sea desarrollado el Plan bajo la metodología de la ¨mejora continua¨ o ciclo de Deming, conocido como PDCA del inglés Plan-DO-Check-Act. Estos ciclos Planificar, Hacer, Verificar y Actuar, permitirán realizar mejoras continuas, estableciendo objetivos y controles de seguridad.

La relación que existe entre el modelo PDCA tanto su estructura general y funcionamiento en base al estándar ISO/IEC 27001:2013 son:

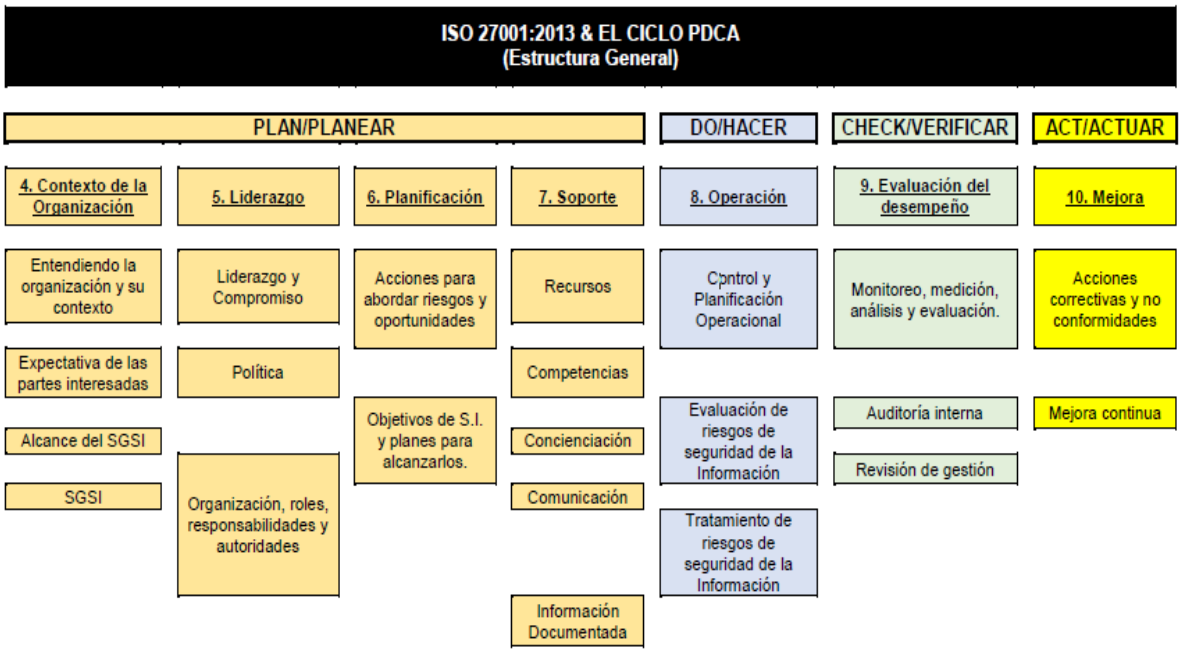


Figura 2.1 Estructura PDCA-ISO 27001:2013 Fuente: [5, p. 14]

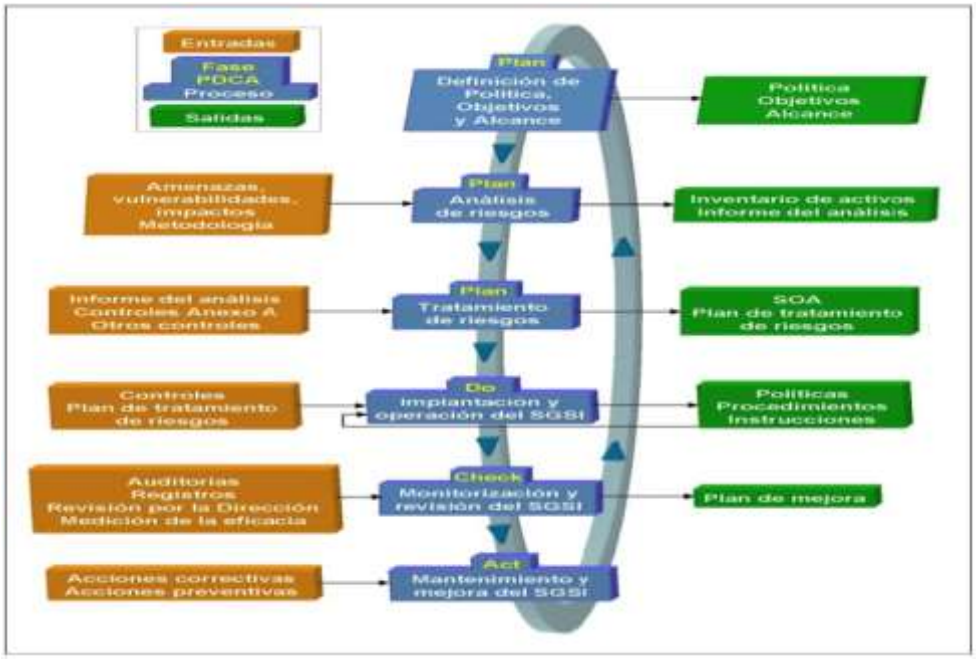


Figura 2. 2 Funcionamiento del proceso de SGSI bajo estándar ISO 27001:2013 [9]

2.1.1. ESTADO ACTUAL FRENTE A LA SEGURIDAD

"El gobierno electrónico es una innovación continua de los servicios, la participación de los ciudadanos y la forma de gobernar mediante la transformación de las relaciones externas e internas a través de la tecnología, el Internet y los nuevos medios de comunicación". (Gartner Group) [10]

Su objetivo es promover la participación ciudadana, democratización de los servicios públicos, simplificación de trámites y la gestión estatal eficiente por medio del aprovechamiento de los recursos que actualmente posee el Estado.

Las Tecnologías de Información y Comunicación (TIC) son el apoyo principal en las organizaciones para manejar los procesos e información en una sociedad cada día más competitiva, herramientas fundamentales para alcanzar la modernización del

Estado, no sólo desde la perspectiva de una gestión que genere ahorros e incremente la eficacia de su acción, sino para mejorar la calidad de los servicios públicos. [11, p. 4]

El empleo correcto de las TIC en el sector público ha permitido al ciudadano y a las entidades públicas, fortalecerse en los siguientes aspectos:

- Acceder de forma oportuna a la información y servicios del Estado.
- Mantener informado sobre la gestión de las entidades del Estado de manera que se pueda ejercer control efectivo sobre ellas.
- Mantener una comunicación interactiva por medio de peticiones, quejas y reclamos, a fin de interactuar muy de cerca con sus ciudadanos de carácter local como nacional.
- Intercambiar ideas con funcionarios públicos, líderes comunitarios y la comunidad en general, a fin de ahorrar papel, salario y tiempo. [11, p. 7]

Debido a la inseguridad de la información, las instituciones públicas se han visto obligadas a desarrollar esquemas que permitan orientar y controlar adecuadamente el uso de la información, a fin se implemente un Sistema de Gestión de Seguridad de Información, que protejan sus sistemas de información y mejore su seguridad.

Podríamos definir un Sistema de Gestión de Seguridad de la Información como herramienta de gestión que nos va a permitir conocer, gestionar y minimizar los

posibles riesgos que atentan contra la seguridad de información en la organización. [1, p. 3]

Los principios del Sistema de Gestión de Seguridad de la Información tienen como objetivo preservar la:

Confidencialidad: La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.

Integridad: La información debe permanecer correcta (integra de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.

Disponibilidad: La información debe estar siempre accesible para aquellos que estén autorizados. [5, pp. 13, 14]

Respecto a la seguridad de información del proceso de viáticos es importante destacar sobre; la información pública y su difusión, de acuerdo con la Ley de Transparencia y Acceso a la Información Pública, lo justifica en sus artículos:

Art. 5.- ***Información Pública. -*** *Se considera información pública, a todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.* [12, p. 3]

Art. 7.- ***Difusión de la Información Pública. -*** *Por la transparencia en la gestión administrativa que están obligadas a observar todas las instituciones del Estado que conforman el sector público en los términos del artículo 118 de la Constitución Política de la República y demás entes señalados en el artículo 1 de la presente Ley, difundirán a través de un portal de información o página web, así como de los medios necesarios a disposición del público, implementados en la misma institución, la siguiente información mínima actualizada, que para efectos de esta Ley, se la considera de naturaleza obligatoria:*

n) Los viáticos, informes de trabajo y justificativos de movilización nacional o internacional de las autoridades, dignatarios y funcionarios públicos; [12, p. 4]

Es así como, con el diseño del Plan de Sistema de Gestión de Seguridad de la Información, permitirá preservar la confidencialidad, integridad y disponibilidad de la información, al proceso de viáticos, mediante la aplicación de los requisitos para implementar y mantener mejoramiento continuo, análisis y evaluación de la gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos basados en las Normas ISO/IEC 27001:2017, ISO/IEC 27005:2008 e ISO/IEC 27002:2017.

Con la implementación y posterior certificación del SGSI, implica a toda la Institución, empezando por la Dirección, sin cuyo compromiso y aprobación, es imposible su puesta en marcha.

2.2. SITUACIÓN ACTUAL CONTEXTO

El presente proyecto busca diseñar un Plan para la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la Norma ISO/IEC 27001:2017, al proceso de viáticos del Instituto Oceanográfico y Antártico de la Armada, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información, así también la confianza de sus funcionarios y clientes.

Determinando las cuestiones internas y externas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de un SGSI:

- Las partes interesadas que son pertinentes al SGSI como son: Gobierno, Autoridades, funcionarios, clientes y proveedores.
- Los requisitos de estas partes interesadas pertinentes a la seguridad de la información incluyen requisitos: Legales y Reglamentarias (Contratos, Actas de compromiso, Propuestas, Políticas de la Organización, etc.) y las Obligaciones de Ley (Seguridad Social, Impuesto a la Renta, pago de honorarios, viáticos, compensaciones, seguridad laboral, etc.).

El Instituto Oceanográfico y Antártico de la Armada**,** es una Entidad Pública actualmente fusionada, entre el Instituto Oceanográfico de la Armada (INOCAR) y

el Instituto Antártico Ecuatoriano (INAE), según Decreto Ejecutivo 1038 del 08 de mayo del 2020, firmado por el presidente de la República. [13, p. 3]

¨Institución que cambio de nombre, pero su esencia permanece y se fortalece, así como el compromiso y el tesón con que todos trabajamos” [14]

En el marco de sus objetivos institucionales, continuará con su trabajo de brindar seguridad a la navegación, ejercer defensa y soberanía del territorio marítimo ecuatoriano y ejecutar expediciones coordinando actividades de investigación científica que promuevan la proyección Geopolítica y Oceanopolítica del Ecuador en la Antártica.

Productos del Instituto Oceanográfico y Antártico Ecuatoriano:

- Carta Náutica física y digital
- Tablas de marea e implementos náuticos

Servicios:

- Información especializada sobre seguridad marítima
- Boletines Meteorológicos

Clientes:

- Navieras
- Otras entidades públicas y privadas

Tamaño:

Formalmente la entidad cuenta con alrededor de 300 personas entre personal con nombramiento, personal contratado y militares.

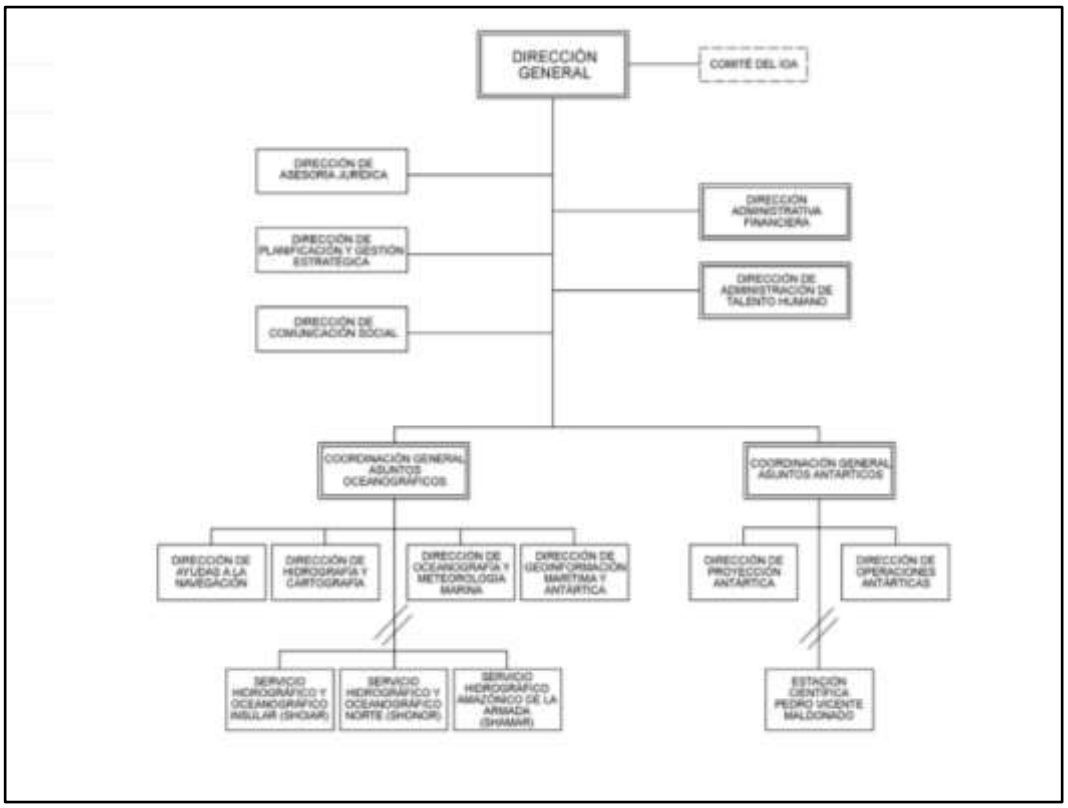


Figura 2. 3 Organigrama del Instituto Oceanográfico Antártico de la Armada Fuente: [14]

El Instituto ha tomado iniciativas relacionadas con la seguridad de la información de acuerdo con la normativa gubernamental referente al Esquema Gubernamental (EGSI) versión 01, desde el 4 mayo del 2015

- Existe un Esquema de Gestión de Seguridad de la Información de manera interna a nivel general, con un avance de ejecución del 51,72 %

- Las actividades de seguridad implantadas han sido iniciativa de la Dirección de Tecnología e Información del Instituto, por lo que la Dirección General las conoce de forma parcial.
- Existe un área específica que gestiona la seguridad interior del Instituto.
- Algunas de las actividades realizadas de manera informal como son: 1.- Definir algunas de las políticas de seguridad de la información de la entidad. 2.- Implementar software de seguridad como: (antivirus, firewall, antispam). 3.- Definición y gestión de una matriz de controles básica alineada a la Norma ISO/IEC 27002:2013.

2.3. DESCRIPCIÓN DEL PROCESO DE VIÁTICOS

La solución planteada, del diseño de un Plan para la implementación de un Sistema de Gestión de Seguridad de Información basado en la Norma ISO/IEC 27001:2017, al proceso de viáticos, como se mencionaron sus limitaciones y debido a que la información constituye uno de los activos de mayor valor e importancia, cualquiera que sea el medio en el que se encuentre y procese. Los Servidores y Trabajadores Públicos, por necesidad institucional deben desplazarse fuera de su domicilio y/o lugar habitual del trabajo, a cumplir tareas oficiales o desempeñar actividades inherentes a sus puestos, a continuación, se muestra el mapa del proceso y el proceso como tal:

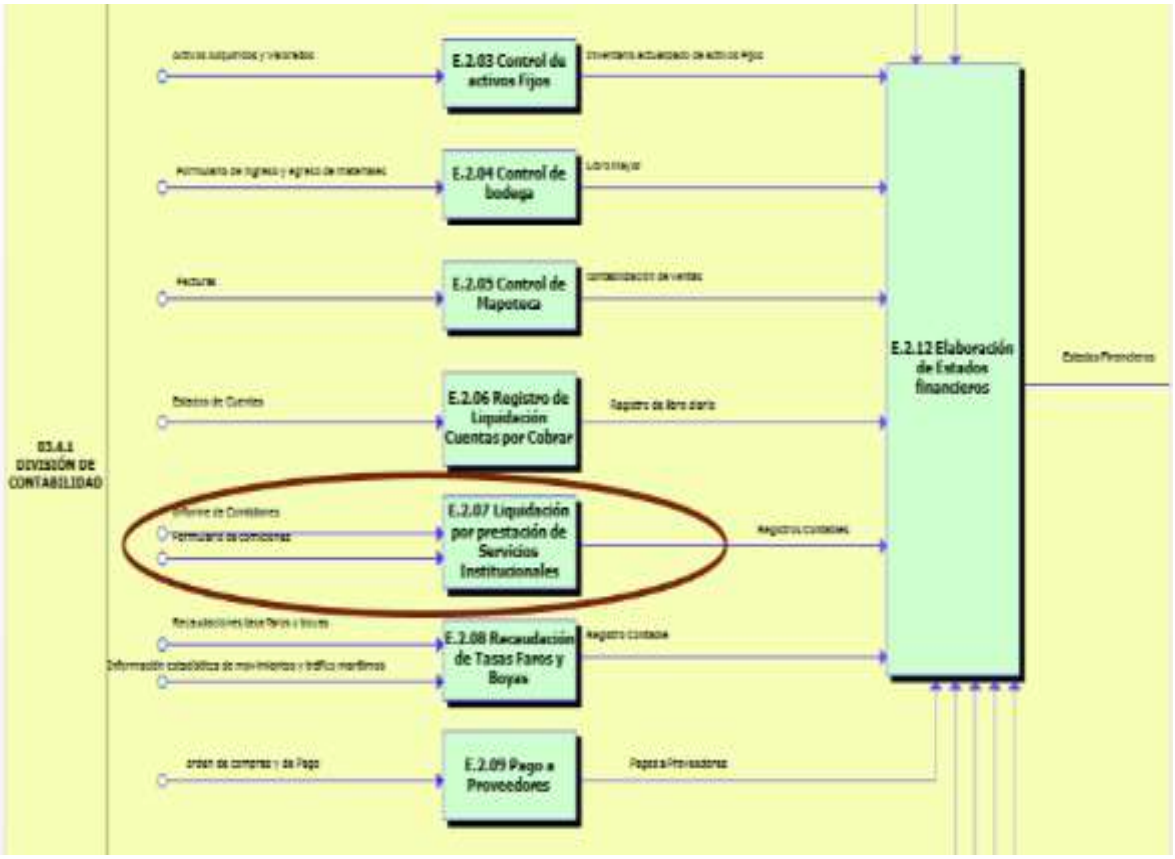


Figura 2.4 Mapa de Proceso Área Financiera Fuente: [14]

En la Figura 2.4 se muestra el mapa de proceso de la Gestión Contable, cuya función Básica es: *Interpretar, registrar, clasificar, medir y resumir en términos monetarios la actividad económica del Instituto y asegurar el correcto funcionamiento del sistema de contabilidad, según Normas de Control Interno, Normas Técnicas de Contabilidad Gubernamental y los Principios de Contabilidad generalmente aceptados*.

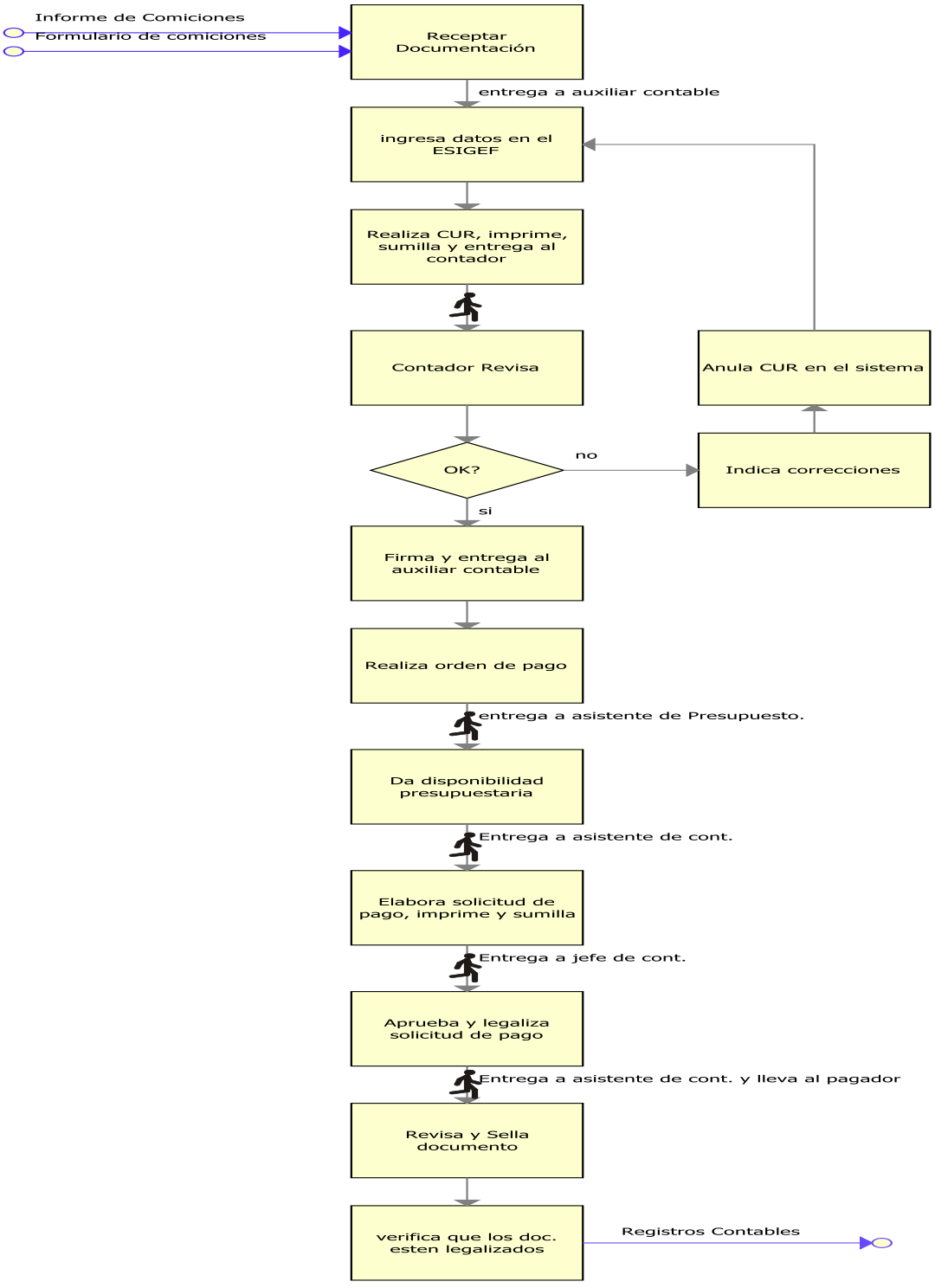


Figura 2. 5 Proceso de Viáticos Fuente: [14]

Como se muestra en la Figura 2. 5 Proceso de Viáticos, la función básica es: *Llevar la contabilización y el control de los pagos por concepto de prestación de servicios institucionales de los trabajadores y servidores públicos del Instituto*.

2.4. ALCANCE DEL PLAN

El alcance del Plan busca especificar los lineamientos que deben ser acatados por todo su personal de tal manera que pueda prever, corregir y actuar ante un evento que podría poner en riesgo la seguridad de la información, del “Proceso de Viáticos¨ con los siguientes subprocesos, procedimientos y los activos de información de la Institución.

Tabla 2. 1 Proceso, Subproceso y Procedimientos de Viáticos Fuente: elaboración propia.

Proceso	Subproceso	Procedimientos
C. Proceso de viáticos	C1. anticipo de viáticos	C1.P1. Oficio motivador
		C1.P2. Llenado de formularios
		C1.P3. Hoja de movimiento
		C1.P4. Certificación Financiera
	C2. liquidación de viáticos	C2.P1. Oficio de liquidación
		C2.P2. Llenado de formularios
		C2.P3. Informe de cumplimiento
		C2. P4. Cur de Compromiso
	C3. registro y control	C3.P1. Revisión de comprobantes de venta
		C3.P2. Elaboración de asiento contable

Proceso	Subproceso	Procedimientos
		C3.P3. Cur Dev pago al funcionario
		C3.P4. Cur Contable Rendición de fondos

2.5. OBJETIVOS DEL PLAN

La Institución debe definir los objetivos de seguridad encaminados a los objetivos institucionales, en busca de mejora no solo a nivel interno sino también para con sus clientes y entidades de Control.

- Identificar el estado actual de la organización frente a un sistema de gestión de seguridad de la información en relación con el proceso de viáticos.
- Definir los planes de acción a corto, mediano y largo plazo, que la Institución debe implementar para garantizar la correcta gestión de un sistema de seguridad de la información, cuyo fin es evitar la materialización de incidentes de seguridad y de los riesgos ya identificados.
- Establecer un marco de seguridad como estrategia, que defina los riegos de seguridad de la información, así como el tratamiento de estos, con el objetivo de proteger los activos de información más sensibles de la entidad alineada a una metodología y gestión de riesgos establecida.
- Formalizar lineamientos de mejores prácticas en temas de seguridad de información, basado en las Normas ISO/IEC 27001:2017 Guía de Requisitos de Implementación, ISO/IEC 27005 Guía de Gestión de Riesgos e ISO/IEC

27002:2017 Guía de Implantación de Controles, para el proceso de viáticos, con el fin de su implementación y posterior certificación.

- Definir la ruta para la implementación de las medidas de seguridad de la información en la Institución.

2.5.1. NIVEL DE CUMPLIMIENTO

Para conocer el estado actual de la entidad frente al desempeño de la Norma ISO/IEC 27002:2013, específicamente en los 114 controles definidos a fin cumplir los diferentes objetivos de control, definiendo una tabla de Nivel de Cumplimiento alineada al Modelo de Madurez de Capacidades (CMM).

Tabla 2. 2 Valoración de Criterios de Madurez CMM vs % actual de cumplimiento, Fuente: elaboración propia

No. Dominio	Dominio de la Norma	% actual de cumplimiento
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACION	80,00%
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	62,00%
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	31,11%
A.8	GESTIÓN DE ACTIVOS	67,78%
A.9	CONTROL DE ACCESO	66,46%
A.10	CRIPTOGRAFÍA	50,00%
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	78,33%
A.12	SEGURIDAD DE LAS OPERACIONES	61,61%
A.13	SEGURIDAD EN LAS COMUNICACIONES	71,67%
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	23,52%
A.15	RELACIONES CON PROVEEDORES	40,00%
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	11,43%
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	25,00%
A.18	CUMPLIMIENTO	55,17%

NIVEL DE CUMPLIMIENTO **51,72%**

2.6. SISTEMA DE GESTIÓN DOCUMENTAL

Para garantizar la seguridad y continuidad de los activos de información críticos que participan en el proceso de Viáticos, se realiza el análisis y tratamiento de riesgos, de tal manera se pueda prever, corregir y actuar ante un evento que podría poner en peligro la confidencialidad, integridad y disponibilidad de la información. Gracias a la implementación del Plan, basado en las Normas ISO/IEC 27001:2017 Guía de Requisitos de Implementación, ISO/IEC 27005 Guía de Gestión de Riesgos e ISO/IEC 27002:2017 Guía de Implantación de Controles, en la Institución se podrán alcanzar los objetivos de un SGSI los cuales vienen establecidos en la propia Norma.

A continuación, se muestran los documentos del Plan que serán explicados:

- Políticas de Seguridad
- Gestión de roles y responsabilidades
- Metodología y Guía para la Gestión de Riesgos
- Tratamiento de Riesgos
- Impacto del cumplimiento actual vs. Cumplimiento con la implementación.
- Hoja de ruta para implementación del Plan

2.7. POLÍTICAS DE SEGURIDAD

- Fortalecer la presencia de la Institución asegurando los recursos en tratamiento de la información que se entrega a la ciudadanía.

- Proteger ante riesgos inherentes de los activos de información, es de vital importancia para el éxito de la Institución.
- Cumplimiento de procedimientos para la gestión de activos de información en cuanto al uso aplicable a los mismos con que cuenta la Institución.
- La política de seguridad de la información cumpla con los requisitos de los entes que controlan a las Instituciones Públicas y demás Entidades de control.

2.8. GESTIÓN DE ROLES Y RESPONSABILIDADES

La seguridad de la información es un factor clave para determinar la habilidad de la Institución en proteger la información, por lo que se debe definir un comité de seguridad y el oficial de seguridad, encargados de coordinar, informar, asesorar, supervisar, verificar, reportar y recomendar la correcta gestión del Plan para un SGSI al proceso de viáticos, tiene como objetivo:

Garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la Institución. [5, p. 4]

Considerando la naturaleza del Instituto, que no tiene operaciones en otros países y que las Leyes y Normas que lo regulan y aplican son las adoptadas y establecidas para Ecuador, se plantea una Estructura Organizacional centralizada de acuerdo con el siguiente esquema.

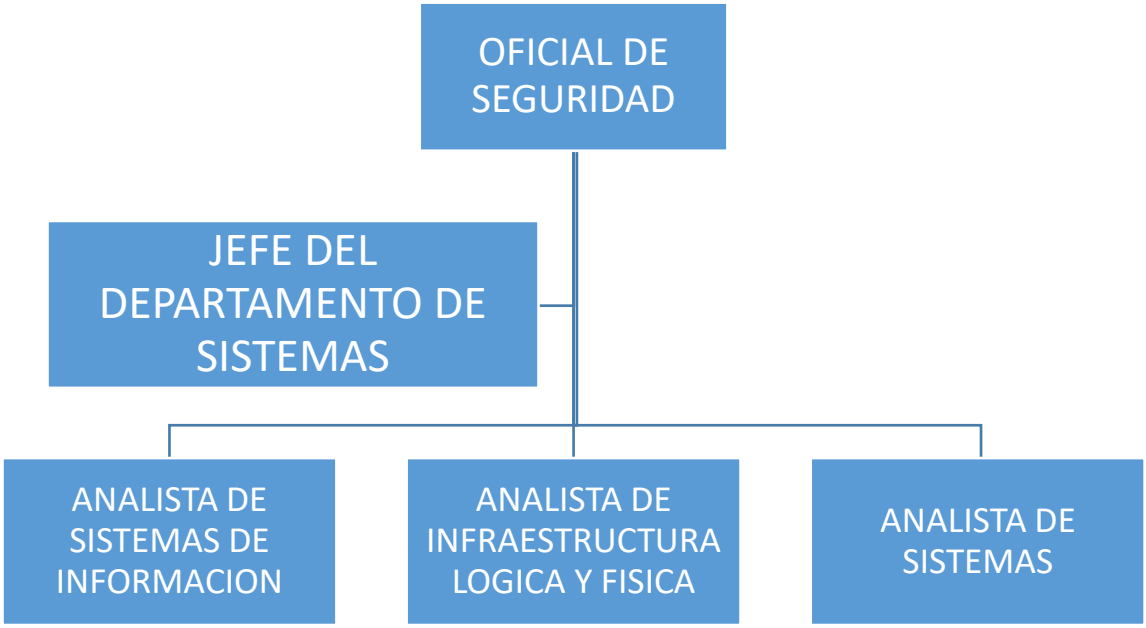


Figura 2. 6 Esquema del Comité de Seguridad Fuente: Elaboración propia

El comité de seguridad de la Información (CSI), tendrá las siguientes responsabilidades:

- Gestionar la aprobación de la Políticas y Normas Institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la institución.
- Realizar el seguimiento de los cambios significativos de los riesgos que afecten a los recursos de información frente a las amenazas más importantes.
- Coordinar la implementación de controles específicos de seguridad de la información al proceso de viáticos en base al Plan diseñado.

- El comité deberá convocarse bimestralmente o cuando las circunstancias lo ameriten, se deberá llevar registros y acta de las reuniones.
- Reportar a la máxima autoridad las alertas que impidan la implementación del Plan.
- Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Plan. [5, p. 12]

Así también designarán, al interior de la Institución a un funcionario como Oficial de Seguridad de la Información (OSI), mismo que debe tener conocimiento en Seguridad de la Información y Gestión de Proyectos, se recomienda que no pertenezca al área de Tecnologías de la Información o Sistemas, puesto que deberá mantener su independencia para observar las necesidades de seguridad entre la estrategia de la Institución y tecnología.

Cualidades como: Liderazgo, capacidad para lograr acuerdos, aceptación de todas las partes interesadas, poder de gestión; Son fundamentales para llevar con éxito la tarea de Oficial de Seguridad de la Información. [5, p. 10]

Dentro de sus principales responsabilidades se encuentran:

- Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.
- Generar propuestas para la elaboración de la documentación esencial del Plan basado en el EGSI.

- Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.
- Elaborar el Plan de concienciación en la Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI).
- Mantener la documentación de la Implementación del Plan debidamente organizada.
- Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.
- Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de seguridad, en caso de ausencia, al Comité de Seguridad de la Información. [5, p. 4]

2.9. METODOLOGÍA Y GUÍA PARA LA GESTIÓN DE RIESGO

Es importante para el Instituto, capacitarse y estar preparado en el desafío de proteger sus Activos de información, lo que conlleva a conocer y aplicar en detalle la terminología, estándares, la normatividad y las diferentes herramientas, para lograr el objetivo de seguridad. [7, p. 42]

Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y

confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. [15, pp. 8,9].

Para facilitar el proceso de valoración, análisis y tratamiento de riesgos es importante comprender algunos conceptos básicos:

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información, Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Evaluación de riesgo: Proceso global de identificación, análisis y estimación de riesgos.

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.

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

Impacto: Es la consecuencia de la materialización de una amenaza sobre un activo. El costo para la Institución de un incidente de la escala que sea, que puede o no ser

medido en términos estrictamente financieros (ejemplo: pérdida de reputación, implicaciones legales, entre otros).

Riesgo Inherente: Es el riesgo existente y propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Activo: Es todo aquello que tiene valor para la organización y que, por lo tanto, requiere de protección. [5, p. 17]

Activo de Información: Conocimiento o datos que tienen valor para la Institución. [12, p. 3]

Tratamiento de riesgo: Proceso de modificar el riesgo, mediante la implementación de controles.

El marco de referencia que nos permite la identificación de riesgos de seguridad de la información, en la cual se toma como base el ¨Proceso de Viáticos¨, cubierto por el Sistema de Gestión de Seguridad de la Información, para la identificación de amenazas o fuentes de riesgo, causas, vulnerabilidades y las posibles consecuencias con sus efectos o nivel de impacto para la Entidad; una vez identificados los riesgos, se evalúan y se presentan las opciones para el Tratamiento de Riesgos, en base a los estándares y mejores prácticas de la seguridad de información.

Actividades para la Gestión de Riesgo de la seguridad de Información:

- Establecimiento del contexto
- Valoración de Riesgo
- Análisis de Riesgo
- Evaluación de Riesgos
- Tratamiento de Riesgos
- Comunicación del Riesgo
- Monitoreo y Control

2.9.1. ESTABLECIMIENTO DE CONTEXTO

Implica establecer los criterios básicos, que son necesarios para la gestión del riesgo de la seguridad de información, así también, definir el alcance, de todos los activos relevantes que se tomen en consideración e identificar los límites para abordar aquellos riesgos considerados en el proceso de viáticos con el fin de garantizar y establecer una Institución adecuada que opere la gestión de riesgos de la seguridad de información.

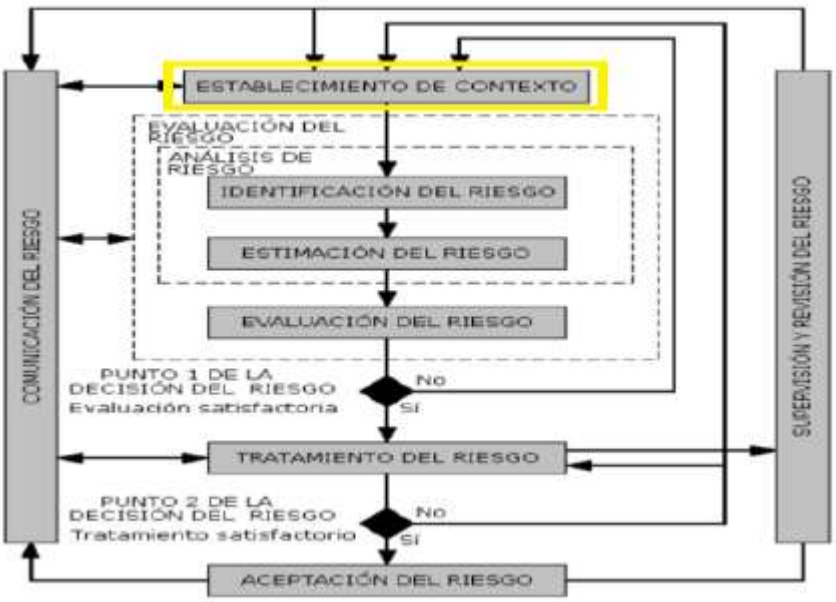


Figura 2. 7 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18]

Criterios de identificación del riesgo. - Es recomendable considerar los activos de información con el valor de impacto alto para el proceso de evaluación del riesgo.

Criterios de evaluación del riesgo. - Es recomendable desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo de la seguridad de la información de la Institución.

Criterios de impacto. – Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la organización, causados por un evento de seguridad de la información.

Criterios de la aceptación del riesgo. – Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la Institución y de las partes interesadas

2.9.2. VALORACIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

Los riesgos identificados para el proceso de viáticos se describen cuantitativa y/o cualitativamente, el cual se priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Institución.

Un riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. [5, p. 20]

En este proceso se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos.

La valoración del riesgo consta de las siguientes actividades:

- Análisis del riesgo
    - Identificación del riesgo
    - Estimación del riesgo
- Evaluación del riesgo

2.9.3. ANALISIS DEL RIESGO

En el desarrollo de identificación y estimación del riesgo, se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos identificados, que intervienen en el Proceso de Viáticos.

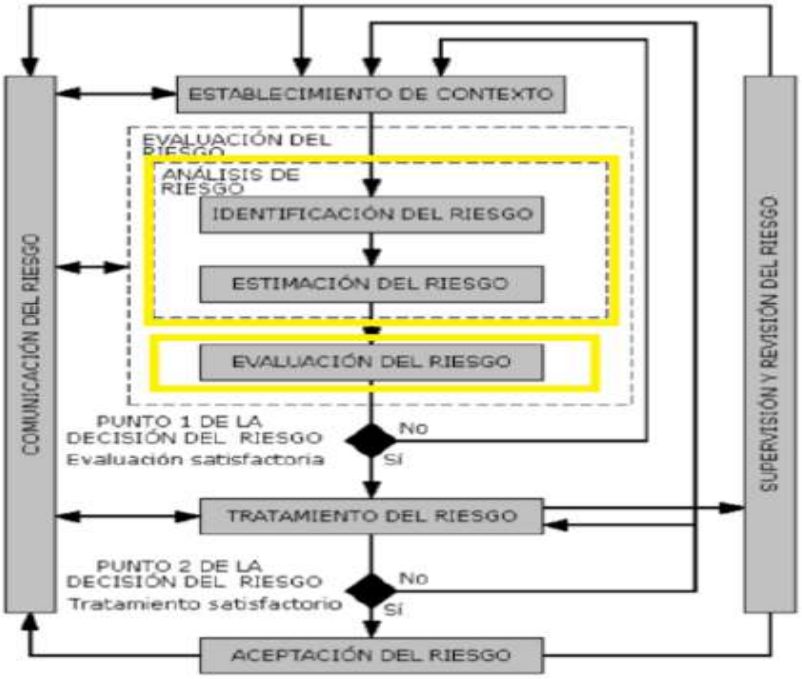


Figura 2. 8 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18]

2.9.3.1. IDENTIFICACIÓN DEL RIESGO.

Consiste en determinar que puede provocar pérdidas de recursos a la Institución, consta de las siguientes actividades:

2.9.3.1.1. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Un activo son todos los elementos de una entidad que requiere para el correcto desarrollo de sus procesos misionales y de soporte, los cuales son objeto de tratamiento en la Gestión de riesgos durante el diseño del Plan para la implementación de un SGSI, al Proceso de Viáticos, identificando 34 de acuerdo con el tipo de activo, propietario, custodio y ubicación del Activo de Información del Instituto.

Tipos de activos:

PRIMARIOS

- Información (Electrónica, Impresa)
- Actividades y Procesos del Negocio

SOPORTE

- Software (aplicaciones de herramientas, software)
- Hardware (servidores, Networking otros equipos)
- Servicios (computación, comunicaciones)
- Personal (habilidades, experiencia calificación)
- Ubicación
- Estructura de la Institución

Figura 2. 9 Activos de Información Fuente: [16]

Tabla 2. 3 Identificación de Activos de Información, Fuente: Elaboración propia

INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA					
MATRIZ IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO DE VIÁTICOS					
No.	**TIPO**	**NOMBRE DE ACTIVO**	**PROPIETARIO**	**CUSTODIO**	**UBICACIÓN**
A1	Personal	Personal Administrativo-Financiero	Institución	Jefe de Talento Humano	Edificio Administrativo /Financiero/Sistemas
A2	Hardware	Servidores	Institución	Analista de Infraestructura	Edificio Administrativo /Financiero/Sistemas
A3	Servicio	Correo electrónico Zimbra	Proveedor externo Open Source	Analista de Tecnologías de Información	Data Center
A4	Comunicaciones	Internet	Proveedor externo CEDIA	Analista de Tecnologías de Información	Data Center
A5	Software	Sistema de gestión documental QUIPUX	Proveedor externo Gobierno	Analista de Tecnologías de Información	Edificio Administrativo /Financiero/Sistemas
A6	Comunicaciones	Conectividad Red de área local	Institución	Analista de Telecomunicaciones	Edificio Administrativo /Financiero/Sistemas
A7	Hardware	Unidad de Sistema de Energía UPS	Institución	Analista de Telecomunicaciones	Edificio Administrativo /Financiero/Sistemas
A8	Hardware	Computadoras de escritorio	Institución	Analista y Asistentes Contables y Tesorero	Edificio Administrativo /Financiero/Sistemas
A9	Servicio	Impresoras	Proveedor Externo	Proveedor Externo	Edificio Administrativo /Financiero/Sistemas
A10	Hardware	Equipos de Seguridad física	Institución	Oficial de Seguridad	Edificio Administrativo /Financiero/Sistemas

INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA					
MATRIZ IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO DE VIÁTICOS					
No.	**TIPO**	**NOMBRE DE ACTIVO**	**PROPIETARIO**	**CUSTODIO**	**UBICACIÓN**
A11	Personal	Personal de sistemas	Institución	Jefe de Talento Humano	Edificio Administrativo /Financiero/Sistemas
A12	Comunicaciones	Sistema de telefonía voz sobre IP	Institución	Analista de Telecomunicaciones	Edificio Administrativo /Financiero/Sistemas
A13	Software	Sistema Institucional Sigefi	Institución	Analista de Tecnología	Edificio Administrativo /Financiero/Sistemas
A14	Software	Sistema del Estado Esigef	Proveedor externo Gobierno	Proveedor Externo	Data Center
A15	Información	Formulario Solicitud y liquidación de Comisión	Proveedor Externo	Analista Contable y Archivo	Edificio Administrativo /Financiero/Sistemas
A16	Servicio	Software Antivirus	Institución	Analista de Tecnología	Edificio Administrativo /Financiero/Sistemas
A17	Información	Comprobante de Pago CUR de pagos	Jefe de Tesorería	Oficinista archivo de Contable	Edificio Administrativo /Financiero/Sistemas
A18	Información	Asientos Contables	Analista y Asistente Contable	Oficinista de archivo contable	Edificio Administrativo /Financiero/Sistemas
A19	Información	Oficios, memorandos físicos y electrónicos	Institución	Secretaria Ejecutiva	Edificio Administrativo /Financiero/Sistemas
A20	Información	Manuales e Instructivos	Institución	Jefe de Contabilidad, Analistas, jefe de sistemas y Archivo	Edificio Administrativo /Financiero/Sistemas
A21	Información	Estados Financieros	Institución	Jefe de Contabilidad	Edificio Administrativo /Financiero/Sistemas
A22	Personal	Comisionados	Institución	Jefe de Talento Humano	Edificio Matriz y Edificio Administrativo /Financiero/Sistemas
A23	Servicio	Sistema de autenticación	Institución	Analista de Tecnología	Edificio Administrativo /Financiero/Sistemas
A24	Hardware	Router	Institución	Analista de Telecomunicaciones	Edificio Administrativo /Financiero/Sistemas
A25	Hardware	Switch concentrador	Institución	Analista de Telecomunicaciones	Edificio Administrativo /Financiero/Sistemas

INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA					
MATRIZ IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO DE VIÁTICOS					
No.	**TIPO**	**NOMBRE DE ACTIVO**	**PROPIETARIO**	**CUSTODIO**	**UBICACIÓN**
A26	Hardware	Escáner	Institución	Analista de Contabilidad	Edificio Administrativo /Financiero/Sistemas
A27	Información	Publicaciones de Comisiones	Institución	Analista de Tecnología	Edificio Administrativo /Financiero/Sistemas
A28	Estructura física	Oficinas de Sistemas, Administrativo/Financiero	Institución	Analista de Activos Fijos	Edificio Administrativo /Financiero/Sistemas
A29	Información	Código Fuente	Institución	Analista de Tecnología	Edificio Administrativo /Financiero/Sistemas
A30	Software	Sistemas Operativos	Jefe de Sistemas de Información	Analista Técnico	Edificio Administrativo /Financiero/Sistemas
A31	Hardware	Firewall	Institución	Analista de Telecomunicaciones	Edificio Administrativo /Financiero/Sistemas
A32	Información	Copias de Seguridad de los Sistemas de Información	Institución	Analista de Tecnología	Edificio Administrativo /Financiero/Sistemas
A33	Hardware	Dispositivo Electrónico Biométrico Lector (huella digital)	Proveedor externo Gobierno	Analista de Tesorería	Edificio Administrativo /Financiero/Sistemas
A34	Servicio	Intranet	Institución	Analista de Tecnología	Edificio Administrativo /Financiero/Sistemas

2.9.3.1.2. VALORACIÓN DE LOS ACTIVOS / PONDERACIÓN DE LA CRITICIDAD DE ACTIVOS

La valoración / ponderación de la criticidad de cada activo de información que participa en el proceso de viáticos, fue realizada en términos ¨alto, medio o bajo¨, donde se asigna un valor cuantitativo a cada valor cualitativo de acuerdo con la pérdida de confidencialidad, integridad y disponibilidad, de la información.

A continuación, se presentan las referencias para la valoración del impacto en los activos de información.

Tabla 2. 4 Valoración del impacto en términos Pérdida de la confidencialidad Fuente: [5, p. 22]

Confidencialidad	**Criterio**
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la Institución. Ej. Divulgación de información sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la Institución. Ej. Divulgación de información de uso interno.
Bajo (1)	La divulgación de la información no tiene ningún efecto para la Institución. Ej. Divulgación de información pública.

Tabla 2. 5 Valoración del impacto en términos Pérdida de la integridad Fuente: [5, p. 22]

Integridad	**Criterio**
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la Institución
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la Institución
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la Institución

Tabla 2. 6 Valoración del impacto en términos Pérdida de la disponibilidad Fuente: [5, p. 22]

Disponibilidad	**Criterio**

Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la Institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la Institución
Bajo (1)	La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la Institución

Con referencia a las tablas mencionadas la valoración del impacto del activo (VA), es el promedio de las tres dimensiones en que se basa la Seguridad de la información, a los 34 activos de información para el proceso de viáticos.

$$VA = \frac{C + I + D}{3}$$

Tabla 2. 7 Valoración de activos de información, Fuente: Elaboración propia

INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA
MATRIZ VALORACIÓN DE IMPACTO DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO VIATICOS

No.	NOMBRE DE ACTIVO	TIPO DE SOPORTE	UBICACIÓN	VALOR DE IMPACTO (PÉRDIDA) C: Confidencialidad I: Integridad D: Disponibilidad			
				C	I	D	VA
A1	Personal Administrativo-Financiero	Físico	Edificio Administrativo /Financiero/Sistemas	2	3	3	2,67
A2	Servidores	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A3	Correo electrónico Zimbra	Físico y Lógico	Data Center	2	3	2	2,33
A4	Internet	Físico y Lógico	Data Center	3	3	3	3,00
A5	Sistema de gestión documental QUIPUX	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00

No.	NOMBRE DE ACTIVO	TIPO DE SOPORTE	UBICACIÓN	VALOR DE IMPACTO (PÉRDIDA) C: Confidencialidad I: Integridad D: Disponibilidad			
				C	I	D	VA
A6	Conectividad Red de área local	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	2	2	2	2,00
A7	Unidad de Sistema de Energía UPS	Físico	Edificio Administrativo /Financiero/Sistemas	1	1	1	1,00
A8	Computadoras de escritorio	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A9	Impresoras	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	1	1	2	1,33
A10	Equipos de Seguridad física	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A11	Personal de sistemas	Físico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A12	Sistema de telefonía voz sobre IP	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A13	Sistema Institucional Sigefi	Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A14	Sistema del Estado Esigef	Lógico	Data Center	3	3	3	3,00
A15	Formulario Solicitud y liquidación de Comisión	Físico	Edificio Administrativo /Financiero/Sistemas	2	3	3	2,67
A16	Software Antivirus	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	2	2	2	2,00
A17	Comprobante de Pago CUR de pagos	Físico	Edificio Administrativo /Financiero/Sistemas	2	2	3	2,33
A18	Asientos Contables	Físico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A19	Oficios, memorandos físicos y electrónicos	Físico	Edificio Administrativo /Financiero/Sistemas	1	3	3	2,33
A20	Manuales e Instructivos	Físico	Edificio Administrativo /Financiero/Sistemas	2	3	2	2,33
A21	Estados Financieros	Físico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A22	Comisionados	Físico	Edificio Matriz y Edificio Administrativo /Financiero/Sistemas	1	3	3	2,33

No.	NOMBRE DE ACTIVO	TIPO DE SOPORTE	UBICACIÓN	VALOR DE IMPACTO (PÉRDIDA) C: Confidencialidad I: Integridad D: Disponibilidad			
				C	I	D	VA
A23	Sistema de autenticación	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A24	Router	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	1	1	1	1,00
A25	Switch concentrador	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A26	Escáner	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	1	1	1	1,00
A27	Publicaciones de Comisiones	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	2	3	3	2,67
A28	Oficinas de Sistemas, Administrativo/Financiero	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A29	Código Fuente	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A30	Sistemas Operativos	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A31	Firewall	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A32	Copias de Seguridad de los Sistemas de Información	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A33	Dispositivo Electrónico Biométrico Lector (huella digital)	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00
A34	Intranet	Físico y Lógico	Edificio Administrativo /Financiero/Sistemas	3	3	3	3,00

TOTAL	88,00

2.9.3.1.3. IDENTIFICACIÓN DE LAS AMENAZAS

Con relación a las entrevistas realizadas a cada funcionario que interviene en el proceso de viáticos, se pudo identificar cualitativamente la probabilidad de

ocurrencia de amenazas y el impacto de estas, por cada activo y tipo de activo, que causan daños a Activos tales como información, procesos y sistemas, por lo tanto, a la Institución.

Ciertas amenazas pueden afectar a más de un activo, dando un total de 65 identificadas para los 34 activos de información como se muestran: Tabla 2.8

Tabla 2. 8 Identificación de amenazas de los activos de información, Fuente: Elaboración propia

INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA
MATRIZ IDENTIFICACIÓN DE AMENAZAS DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO VIÁTICOS

No.	NOMBRE DE ACTIVO	AMENAZAS
A1	Personal Administrativo-Financiero	Personal nuevo
		Desconocimiento de los procesos
		Finalización de Contrato
A2	Servidores	Error de usuario
		Desastre natural, incendio
A3	Correo electrónico Zimbra	Correos con ficheros adjuntos maliciosos
		Fuga de Información
A4	Internet	Fallas en la conectividad
		Divulgación de contraseñas
A5	Sistema de gestión documental QUIPUX	Fallas en la conectividad de enlace de red
		Saturación de Documentación
A6	Conectividad Red de área local	Fallas en la conectividad de enlace de red
		Código malicioso.
A7	Unidad de Sistema de Energía UPS	Mal funcionamiento del equipo.
A8	Computadoras de escritorio	Hurtos o vandalismo.
		Reutilización de PC escritorio
		Uso de dispositivos externos
A9	Impresoras	Configuración del servicio errónea
		Mal funcionamiento del equipo sin servicio
A10	Equipos de Seguridad física	Uso indebido de dispositivos de seguridad
A11	Personal de sistemas	Personal nuevo
		Finalización de Contrato
A12	Sistema de telefonía voz sobre IP	Fallo en los servicios de comunicación

No.	NOMBRE DE ACTIVO	AMENAZAS
A13	Sistema Institucional Sigefi	Fallo del enlace fuera de la Institución
		Pérdida de datos de información
A14	Sistema del Estado Esigef	Actualización de opciones en el sistema
		Fallas en la conectividad
		Registro de ID usuario caducado o nuevo
A15	Formulario Solicitud y liquidación de Comisión	Fallos en la elaboración de los formularios
		Pérdida de soportes
		Falsificación de información
A16	Software Antivirus	Errores de software
		Código malicioso
A17	Comprobante de Pago CUR de pagos	Fallas en la conectividad
		Pérdida de soportes
A18	Asientos Contables	Desastre natural, incendio
		Uso indebido de los sistemas de información
		Destrucción de registros.
A19	Oficios, memorandos físicos y electrónicos	Pérdida de soportes
		Duplicidad de documentos
A20	Manuales e Instructivos	Desactualización de Manuales e Instructivos
		Desastre natural, incendio
		Pérdida, destrucción
A21	Estados Financieros	Pérdida, destrucción
		Cambio involuntario de datos en sistema de información.
A22	Comisionados	Falsificación de información
		Pandemia Covid 19
A23	Sistema de autenticación	Divulgación de contraseñas
A24	Router	Falla en los servicios de comunicación
A25	Switch concentrador	Pérdida de electricidad.
A26	Escáner	Equipo obsoleto
A27	Publicaciones de Comisiones	Revelación de información.
		Fuga de Información
		Información incompleta
A28	Oficinas de Sistemas, Administrativo/Financiero	Acceso físico no autorizado
		Desastre natural, incendio
A29	Código Fuente	Daño causado por un tercero
A30	Sistemas Operativos	Abuso de privilegios de acceso
A31	Firewall	Ataque de denegación de servicio
A32		Cambios no autorizados de registros

No.	NOMBRE DE ACTIVO	AMENAZAS
	Copias de Seguridad de los Sistemas de Información	Comprometer información confidencial
A33	Dispositivo Electrónico Biométrico Lector (huella digital)	Innovación Tecnológica
		Desastre natural, incendio
A34	Intranet	Pandemia Covid 19
		Acceso al servicio por personas no autorizadas

2.9.3.1.4. IDENTIFICACIÓN DE VULNERABILIDADES

Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para verificar los cambios. Cabe mencionar que un control implementado incorrectamente, que funcione mal o que se utiliza de modo incorrecto, podría por si solo construir una vulnerabilidad. [5, p. 24]

Con las 65 vulnerabilidades encontradas pueden ser explotadas, las 65 amenazas detalladas, que causan daños a los activos o a la Institución. La sola presencia de una vulnerabilidad no causa daño por sí misma, como se muestran: Tabla 2.9

Tabla 2. 9 Identificación de las vulnerabilidades de los activos de información; Fuente: Elaboración propia

INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA
MATRIZ IDENTIFICACION DE VULNERABILIDADES DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO VIATICOS

No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES
A1		Personal nuevo	Gestión inadecuada al cambio

No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES
	Personal Administrativo-Financiero	Desconocimiento de los procesos	No validación de los datos procesados
		Finalización de Contrato	Inadecuada segregación de funciones
A2	Servidores	Error de usuario	Distracción del usuario
		Desastre natural, incendio	Desprotección en equipos nuevos sin seguro
A3	Correo electrónico Zimbra	Correos con ficheros adjuntos maliciosos	Infectar el equipo con un tipo de malware que roba información
		Fuga de Información	Uso incontrolado de envío y recepción de información.
A4	Internet	Fallas en la conectividad	Denegación del servicio
		Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas.
A5	Sistema de gestión documental QUIPUX	Fallas en la conectividad de enlace de red	Inadecuada gestión de capacidad del sistema
		Saturación de Documentación	Gestión inadecuada de Documentación
A6	Conectividad Red de área local	Fallas en la conectividad de enlace de red	Red saturada
		Código malicioso.	Código que le otorga a un atacante privilegios de administrador
A7	Unidad de Sistema de Energía UPS	Mal funcionamiento del equipo.	Equipos sin protección ante fallas de energía
A8	Computadoras de escritorio	Hurtos o vandalismo.	Control inadecuado del acceso no autorizado
		Reutilización de PC escritorio	Medios de almacenamiento seguros
		Uso de dispositivos externos	Estaciones de trabajo sin servicio
A9	Impresoras	Configuración del servicio errónea	Equipos conectados a la red sin ser detectados
		Mal funcionamiento del equipo sin servicio	Mantenimiento inadecuado.
A10	Equipos de Seguridad física	Uso indebido de dispositivos de seguridad	Acceso de personal no autorizado
A11	Personal de sistemas	Personal nuevo	Gestión inadecuada al cambio.
		Finalización de Contrato	Inadecuada segregación de funciones
A12	Sistema de telefonía voz sobre IP	Fallo en los servicios de comunicación	Inadecuada gestión de capacidad del sistema

No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES
A13	Sistema Institucional Sigefi	Fallo del enlace fuera de la Institución	Denegación del servicio
		Pérdida de datos de información	Cambios de plataforma de operación
A14	Sistema del Estado Esigef	Actualización de opciones en el sistema	Interfaz de usuario complicada
		Fallas en la conectividad	Denegación del servicio
		Registro de ID usuario caducado o nuevo	Sin acceso al sistema
A15	Formulario Solicitud y liquidación de Comisión	Fallos en la elaboración de los formularios	Información errónea
		Pérdida de soportes	Falta de documentación interna.
		Falsificación de información	Falta de políticas para la comprobación de la información
A16	Software Antivirus	Errores de software	Descarga y uso del software de internet no controlado
		Código malicioso	Exposición de usuarios a problemas de seguridad
A17	Comprobante de Pago CUR de pagos	Fallas en la conectividad	Denegación del servicio
		Pérdida de soportes	Falta de documentación interna
A18	Asientos Contables	Desastre natural, incendio	Protección física no apropiada
		Uso indebido de los sistemas de información	Falta de formación y conciencia sobre registros contables
		Destrucción de registros.	Control inadecuado del acceso físico.
A19	Oficios, memorandos físicos y electrónicos	Pérdida de soportes	Falta de documentación interna.
		Duplicidad de documentos	Insuficiente supervisión y control de los documentos
A20	Manuales e Instructivos	Desactualización de Manuales e Instructivos	Desconocimiento de los manuales e instructivos con normativa vigente
		Desastre natural, incendio	Protección física no apropiada
		Pérdida, destrucción	Insuficiente supervisión de los Manuales e Instructivos
A21	Estados Financieros	Pérdida, destrucción	Protección física no apropiada
		Cambio involuntario de datos en sistema de información.	Gestión inadecuada Normas de Control
A22	Comisionados	Falsificación de información	Falta de políticas para la comprobación de la información
		Pandemia Covid 19	No Liquidación de Comisión

No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES
A23	Sistema de autenticación	Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas
A24	Router	Falla en los servicios de comunicación	Equipos mal estado o descontinuados
A25	Switch concentrador	Pérdida de electricidad.	Sensibilidad del equipo a los cambios de voltaje
A26	Escáner	Equipo obsoleto	Sin utilizar
A27	Publicaciones de Comisiones	Revelación de información.	Ausencia de política de manejo de información
		Fuga de Información	Uso inapropiado de la información
		Información incompleta	Ausencia de política de manejo de información
A28	Oficinas de Sistemas, Administrativo/Financiero	Acceso físico no autorizado	Falta de procedimientos para acceso a las Oficinas
		Desastre natural, incendio	Protección física no apropiada
A29	Código Fuente	Daño causado por un tercero	Control inadecuado del acceso al código
A30	Sistemas Operativos	Abuso de privilegios de acceso	No revisión de privilegios de acceso
A31	Firewall	Ataque de denegación de servicio	Sin protección de red interna y externa
A32	Copias de Seguridad de los Sistemas de Información	Cambios no autorizados de registros	Pérdida de Datos
		Comprometer información confidencial	Ataque malicioso de personal interno
A33	Dispositivo Electrónico Biométrico Lector (huella digital)	Innovación Tecnológica	Denegación del servicio
		Desastre natural, incendio	Protección física no apropiada
A34	Intranet	Pandemia Covid 19	Fallas de conectividad
		Acceso al servicio por personas no autorizadas	No validación de los ID autorizados

2.9.3.2. ESTIMACIÓN DE RIESGO

Consiste en asignar valores calificativos y numéricos al criterio cualitativo (alto, medio y bajo) de la probabilidad y las potenciales consecuencias de un riesgo,

considerando los niveles de amenazas y vulnerabilidades encontradas en los activos de información del proceso de viáticos.

En las siguientes tablas se detallan los criterios calificativos y valores numéricos a ser utilizados para la valoración de la probabilidad de amenaza que podrá explotar alguna vulnerabilidad existente.

2.9.3.2.1. CRITERIOS DE PROBABILIDAD DE OCURRENCIA DE AMENAZAS:

Tabla 2. 10 Valoración al criterio de probabilidad de ocurrencia amenaza Fuente: [5, p. 26]

Nivel de amenaza	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo	Ejemplo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Código malicioso
Medio (2)	La ocurrencia es muy probable (probabilidad - 50%)	Por errores descuidados	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Falla del Hardware

Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y < 50%)	En rara ocasión	El atacante no se beneficia del ataque	Desastres naturales

2.9.3.2.2. CRITERIO DE PROBABILIDAD DE OCURRENCIA DE VULNERABILIDADES:

Tabla 2. 11 Valoración al criterio de probabilidad de ocurrencia de vulnerabilidades Fuente: [5, p. 26]

Nivel de vulnerabilidad	**Criterio**	**Ejemplo**
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza	No se utilizan contraseñas para que los usuarios ingresen a los sistemas
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable	Existen normas para la utilización de contraseñas, pero no se implementa
Bajo (1)	La medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

Así también durante la estimación del riesgo, se identificaron los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, en la duplicación de los controles.

Ver **Anexo 1** Matriz Identificación de controles existentes para la Estimación de Riesgos de los Activos de Información del Proceso de Viáticos

2.9.4. EVALUACIÓN DEL RIESGO

Consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

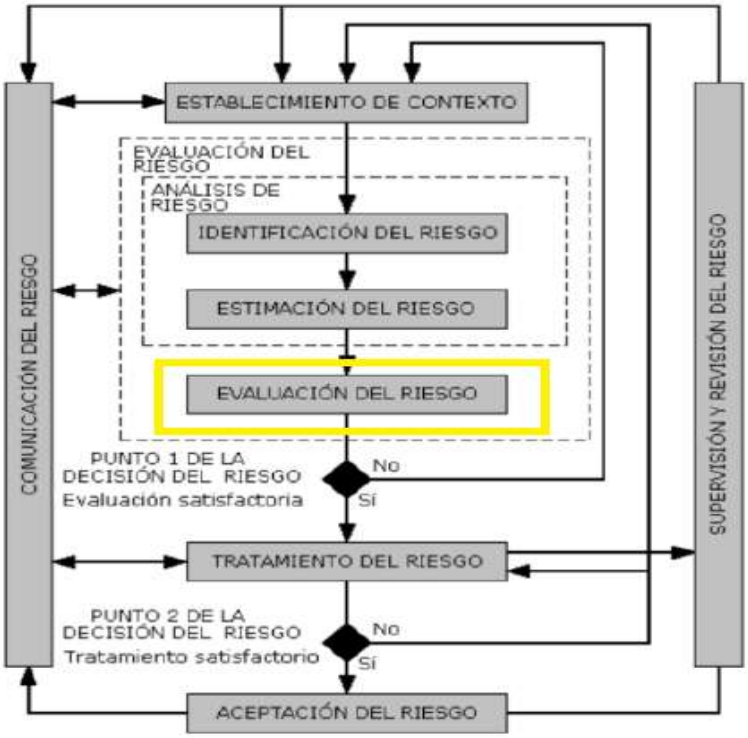


Figura 2. 10 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18]

Proceso de comparación del riesgo estimado contra un criterio de riesgo calculado dado para determinar la importancia del riesgo. el grado del riesgo es expresado

numéricamente basado en las mediadas del valor de los activos de información, el impacto de la amenaza y el alcance de la vulnerabilidad. [5, pp. 25, 26]

2.9.4.1. CRITERIO DE LA EVALUACIÓN DE RIESGOS:

El producto de la probabilidad de ocurrencia de una amenaza y vulnerabilidad y el valor del impacto del activo de información (CID) obtenemos de resultado el cálculo de para evaluación de riesgo.

$$\boldsymbol{Nivel\ de\ Riesgo} = VA(CID) * Nivel\ de\ amenza * Nivel\ de\ vulnerabilidad$$

Tabla 2. 12 Valoración al criterio de probabilidad de ocurrencia de vulnerabilidades Fuente: [5, p. 26]

Nivel de Riesgo	
1 - 3	**El riesgo es BAJO**
4 - 8	**El riesgo es MEDIO**
9 - 27	**El riesgo es ALTO**

Ver **Anexo 2** Matriz Evaluación de Riesgo de los Activos de Información del Proceso de Viáticos.

2.9.5. TRATAMIENTO DE RIESGO

El tratamiento de los riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo con la estrategia de la Institución.

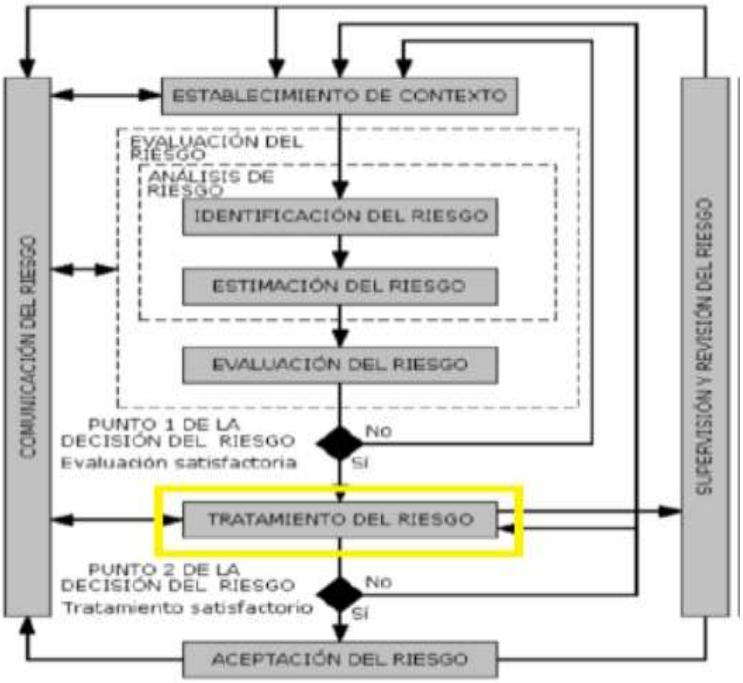


Figura 2. 11 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18]

Se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos se debe definir un plan para el tratamiento del riesgo. Existen cuatro opciones disponibles para el tratamiento del riesgo:

- Reducción del riesgo
- Retención/Aceptación del riesgo
- Evitación del riesgo
- Transferencia del riesgo

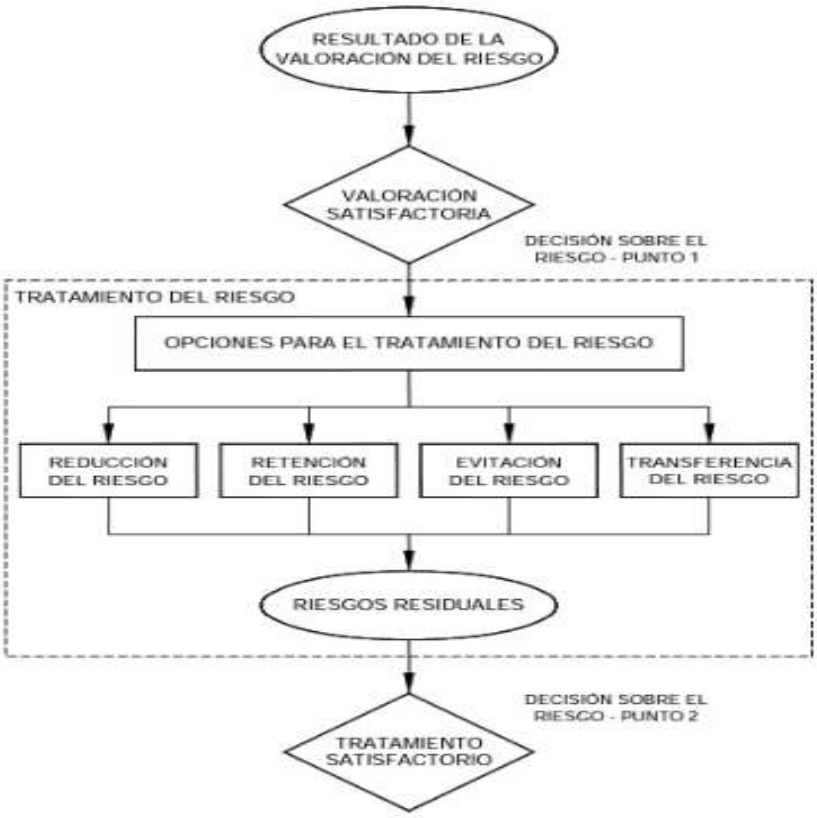


Figura 2. 12 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18]

La Figura 2. 12 ilustra la actividad del tratamiento del riesgo dentro de los procesos de gestión del riesgo de la seguridad de la información del proceso de viáticos.

2.9.6. REDUCCIÓN DEL RIESGO

Se debe reducir mediante la selección de controles, de tal manera que el riesgo residual se pueda reevaluar como aceptable.

Seleccionar controles adecuados y justificados que satisfagan los requisitos identificados en la valoración y tratamiento del riesgo. En la selección se debe tener en cuenta los criterios de aceptación del riesgo, los requisitos legales, reglamentarios y contractuales, así también considerar los costos y el tiempo para la implantación de controles o los aspectos técnicos, ambientales y culturales. [5, p. 26]

2.9.7. RETENCIÓN/ACEPTACIÓN DEL RIESGO

La decisión sobre la retención del riesgo sin acción posterior se debería tomar dependiendo de la evaluación del riesgo.

Aceptar los riesgos con conocimiento u objetividad, siempre y cuando satisfagan claramente la política y los criterios de la Institución para la aceptación de los riesgos.

2.9.8. EVITACIÓN DEL RIESGO

Cuando los riesgos identificados se consideran muy altos o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo. Por ejemplo, para los

riesgos causados por la naturaleza, puede ser una alternativa más eficaz en términos de costo, transferir físicamente las instalaciones de procesamiento a un lugar donde no exista el riesgo o esté bajo control.

2.9.9. TRANSFERENCIA DEL RIESGO

El riesgo se debe transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular dependiendo de la evaluación

2.9.9.1. MATRIZ DE TRATAMIENTO DE RIESGO

Ver el **Anexo 3** Matriz de tratamiento de riesgo de los activos de información del proceso viáticos, Fuente: Elaboración propia.

2.9.10. COMUNICACIÓN DE LOS RIESGOS DE LA SEGURIDAD DE INFORMACIÓN

Garantiza que los responsables de la implementación de la gestión del riesgo y aquellos con intereses establecidos comprendan las bases sobre las cuales toman las decisiones y porqué se requieren acciones particulares.

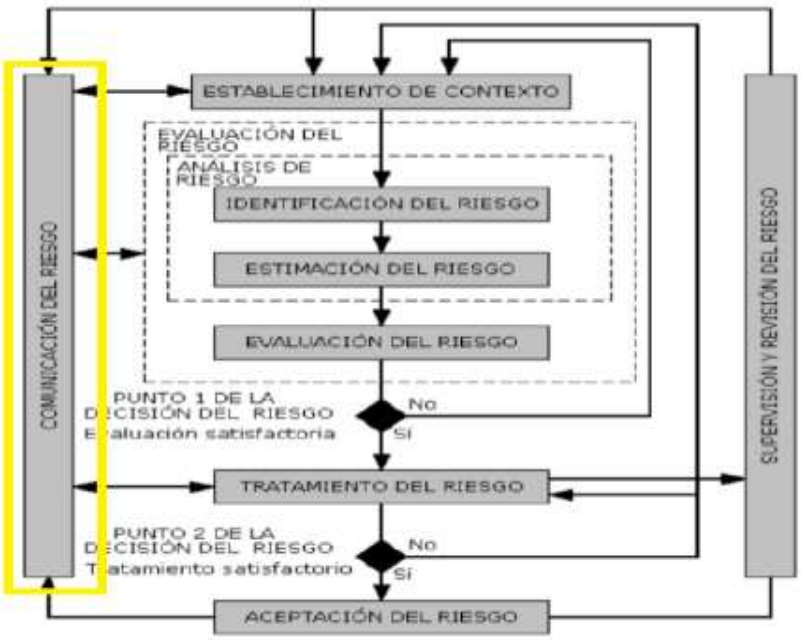


Figura 2. 13 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18]

La información acerca de los riesgos identificados se debe intercambiar y/o compartir entre quienes toman las decisiones y las partes involucradas dentro el proceso de viáticos como se muestra el proceso en la Figura 2. 13

La comunicación del riesgo se debe realizar con el fin de lograr lo siguiente:

- Proporcionar seguridad del resultado de la Gestión del riesgo al proceso de viáticos de la Institución´.
- Compartir los resultados de la valoración del riesgo y presentar el plan para el tratamiento del riesgo.
- Brindar soporte para la toma de decisiones.

- Obtener conocimientos nuevos sobre la seguridad de la información.
- Dar a quienes toman las decisiones y a las partes involucradas un sentido de responsabilidad acerca de los riegos del proceso de viáticos.
- Mejorar la toma de conciencia. [5, p. 31]

La coordinación entre las personas principales que toman las decisiones y las partes involucradas del proceso de viáticos se puede lograr a través del Comité de Seguridad de la Información (CSI) y él Oficial de Seguridad de la Información (OSI) en el cual pueda tener lugar al debate de los riesgos, su prioridad, el tratamiento y la aceptación adecuada. [5, p. 31]

2.9.11. MONITOREO Y REVISIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

Los factores de riesgo como son las amenazas, las vulnerabilidades, la probabilidad o las consecuencias pueden cambiar abruptamente sin ninguna indicación es debido a que los riesgos identificados en el proceso de viáticos no son estáticos. Por ende, es necesario el monitoreo constante para detectar estos cambios.

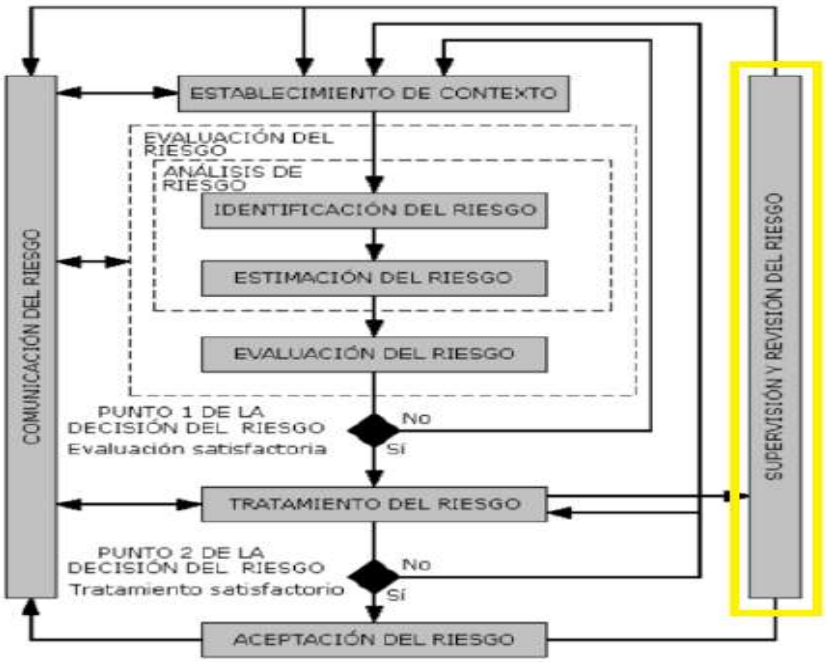


Figura 2. 14 Proceso de Gestión de Riesgo en la Seguridad de la Información, Fuente: [5, p. 18]

El proceso de gestión del riesgo en la seguridad de la información se debe monitorear, revisar y mejorar continuamente, según sea necesario y adecuado, como se muestra en la Figura 2. 14 [5, p. 32]

El Instituto debería garantizar el monitoreo continuo de los siguientes aspectos:

- Activos nuevos que se han incluido en el alcance de la gestión del riesgo.
- Modificaciones necesarias de los valores de los activos de información, por ejemplo, debido a Fusiones con otras entidades o cambios en los requisitos del negocio.

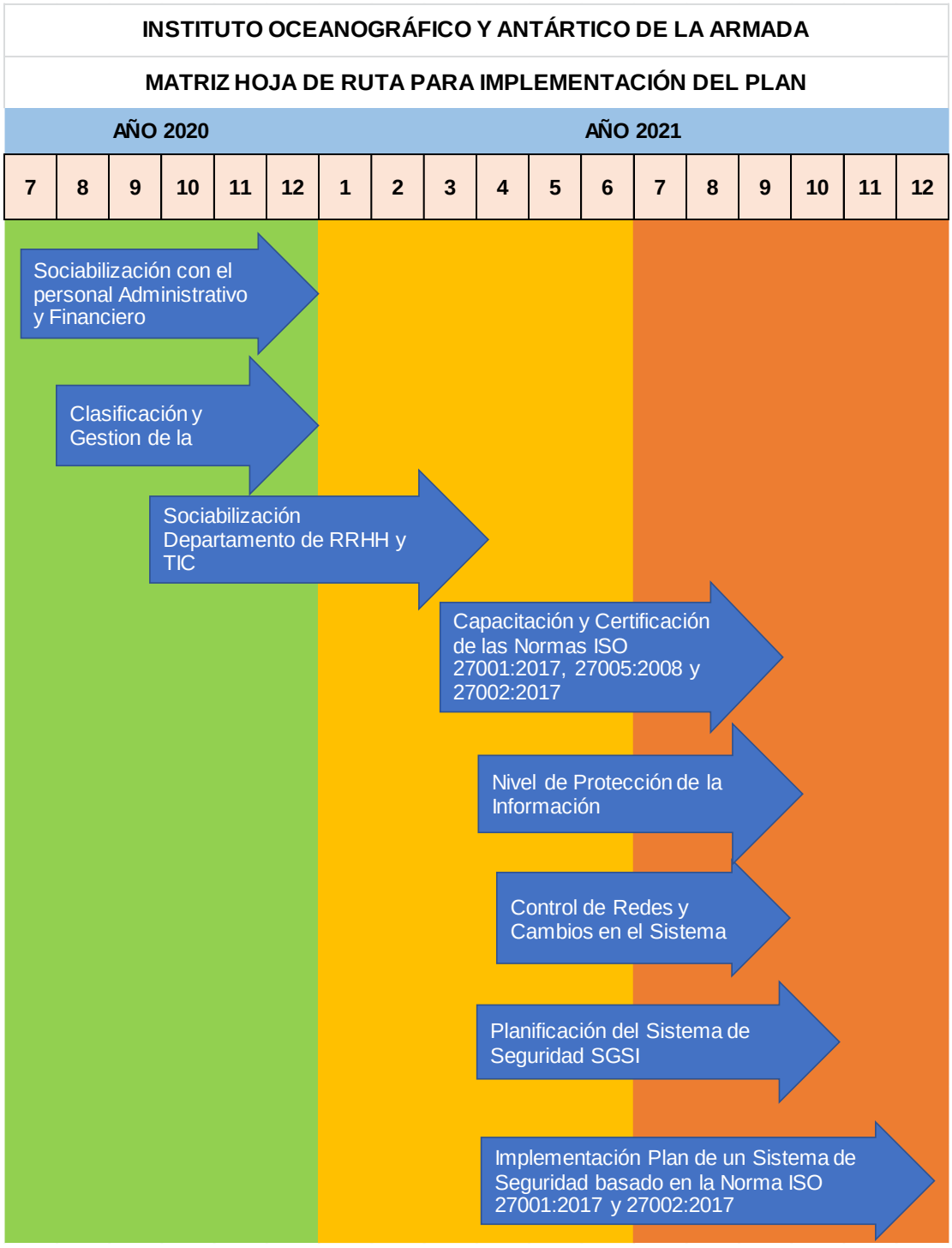
- Nuevas amenazas que podrían estar activas tanto fuera como dentro de la Institución y que no se han valorado.
- Probabilidad de que nuevas vulnerabilidades o el incremento en las vulnerabilidades existentes permitan que las amenazas las exploten.
- Vulnerabilidades identificadas para determinar aquellas que se exponen a nuevas amenazas o que vuelven a surgir.
- El incremento en el impacto o las consecuencias de las amenazas evaluadas, las vulnerabilidades y los riesgos en conjunto que dan como resultado un nivel inaceptable de riesgo.
- Incidentes de la seguridad de la información [5, p. 32]

CAPÍTULO 3

ANALISIS DE RESULTADOS

3.1. HOJA DE RUTA DE IMPLEMENTACIÓN DEL PLAN

Figura 3. 1 Hoja de Ruta de implementación del Plan, Fuente: Elaboración propia.



3.2. IMPACTO DEL CUMPLIMIENTO ACTUAL VS. CUMPLIMIENTO CON LA IMPLEMENTACIÓN DEL PLAN

Comparando el porcentaje actual de nivel de cumplimiento 51,72% versus lo esperado 62.96%, y de acuerdo con el Modelo de Madurez de Capacidades o CMM (Capability Maturity Model) está dentro del 60% es decir:

¨***Los procesos se definen, y se comunican a través de un entramiento formal. Es obligatorio el cumplimiento de los procesos y por tanto la posibilidad de detectar desviaciones es alta. Los procedimientos por si mismos no son sofisticados, pero se formalizan las practicas existentes***¨**.**

Logrando brindar a sus funcionarios y clientes niveles apropiados de protección, procesamiento y almacenamiento, preservando la calidad en la prestación de servicios institucionales y la seguridad de la Información.

Tabla 2. 13 Cumplimiento actual vs. Cumplimiento con la implementación del plan

INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA
NIVEL DE CUMPLIMIENTO DE LA NORMA ISO/IEC 27002:2017

Nro. Dominio	Dominios de la Norma	% actual de cumplimiento ISO/IEC 27002:2013	% cumplimiento esperado ISO/IEC 27002:2017
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACION	80,00%	80,00%
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	62,00%	80,75%
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	31,11%	50,56%
A.8	GESTIÓN DE ACTIVOS	67,78%	69,03%
A.9	CONTROL DE ACCESO	66,46%	81,67%
A.10	CRIPTOGRAFÍA	50,00%	50,00%
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	78,33%	94,44%
A.12	SEGURIDAD DE LAS OPERACIONES	61,61%	65,18%
A.13	SEGURIDAD EN LAS COMUNICACIONES	71,67%	82,92%
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	23,52%	41,11%
A.15	RELACIONES CON PROVEEDORES	40,00%	55,00%
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	11,43%	31,43%
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	25,00%	25,00%
A.18	CUMPLIMIENTO	55,17%	74,33%
	NIVEL DE CUMPLIMIENTO	**51,72%**	**62,96%**

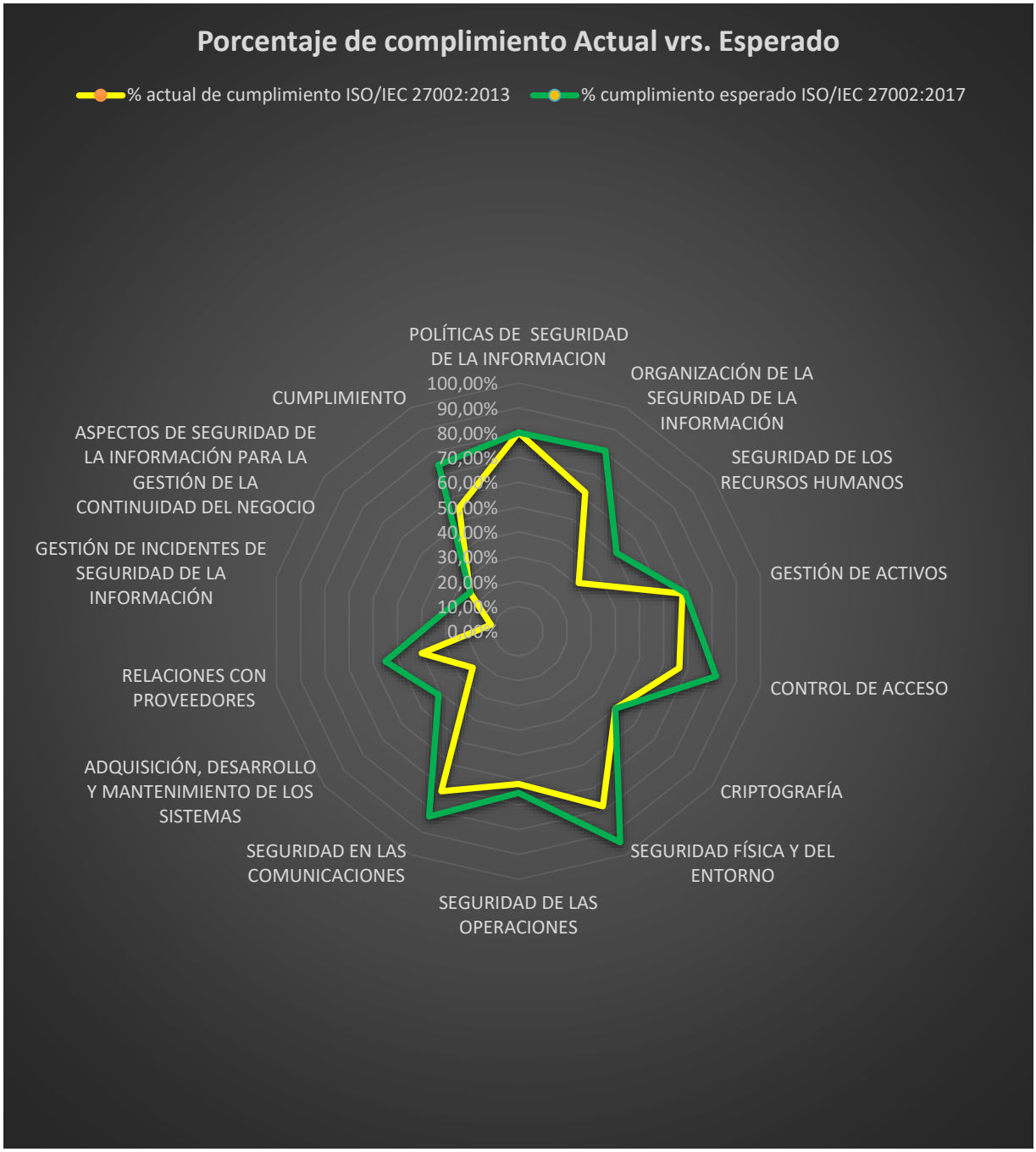


Figura 3. 2 Cumplimiento actual vs. Cumplimiento con la implementación del plan

3.3. BENEFICIOS POR LA IMPLEMENTACIÓN DEL PLAN

Una seguridad de la información eficaz reduce riesgos protegiendo a la Institución frente a las amenazas y vulnerabilidades y en consecuencia reduce el impacto que representa un costo en sus activos de información del proceso de viáticos.

- Reducción del riesgo de pérdida, robo o integridad de la información sensible por cambios o fusiones entre Instituciones públicas.
- Revisión continua de los riesgos y los controles de seguridad de la información implementados en las Institución
- Proyectos de adquisición alineados a la matriz de riesgos, que permitan la reducción de los costos en compra sistemática de productos y tecnologías de información
- Garantizar la continuidad del servicio tras un incidente de seguridad de la información de impacto alto, relacionado al acceso y transparencia en las condiciones de uso.
- Reformular los procesos y procedimientos en base a los lineamientos que exigen los objetivos institucionales basados en el cumplimiento de Políticas de Seguridad y Normas de Control de Interno con el fin de brindar a los ciudadanos un servicio con eficiencia y eficacia.

CONCLUSIONES

La estrecha relación que existe entre el Gobierno Electrónico y el valor agregado que se genera entre la integración de las Tecnologías de Información y Comunicación (TIC) en la prestación de servicios públicos, conjuntamente con la utilización óptima de los recursos independientemente del tiempo, distancia y complejidad organizacional es un factor fundamental para lograr una administración ágil, flexible, eficaz, eficiente y sobre todo transparente, lo que implica redefinir, agregar o eliminar procesos y procedimientos, definir políticas de calidad y seguridad de la información y normas de control interno.

Los sistemas de información y las TIC en general juegan un papel fundamental en la prestación de servicios del Instituto Oceanográfico y Antártico de la Armada, en la satisfacción del cliente y logro de objetivos Institucionales. Sin embargo, el uso de las TIC conlleva a riesgos que la mayoría de las veces son desconocidos por la Máxima Autoridad y no toma acción en mecanismos de protección como es la Implementación de modelos de seguridad de la información.

El diseño del plan permitió conocer los beneficios que genera un Sistema de Gestión de Seguridad de la Información en el Instituto al proceso de viáticos mediante la aplicación del estándar Internacional de Seguridad de la Información Norma ISO/IEC 27001:2017, que proporciona los requisitos para establecer, implementar y mantener mejoramiento continuo y desarrollo de las fases expuestas, estableciendo la documentación base que requiere la aplicación de la Norma.

Por otra parte, identificar los activos de información y determinar el nivel de riesgo potencial de cada uno de ellos, aplicando la metodología de Riesgos basados en la Guía para la Gestión de Riesgos de Seguridad de la Información ISO/IEC 27005:2008, identificando los activos más críticos y que requieren de mayor atención dado el alto impacto que tienen en la prestación de servicios institucionales y funcionamiento óptimo del proceso de viáticos.

Adicionalmente comparar el estado actual de los dominios, objetivos y controles de seguridad con el Nivel de cumplimiento de acuerdo a la Guía para la Implementación de Controles de Seguridad de Información ISO/IEC 27002:2017, lo que permitió a su vez elaborar las Políticas de Seguridad de la Información que deberán ser comunicadas a todos los funcionarios que intervienen en el proceso de Viáticos, por las dos figuras o roles que son los pilares fundamentales para el trabajo en seguridad de información: Comité de Seguridad de la información (CSI) y Oficial de Seguridad (OSI).

Culminando con la nueva evaluación de riesgos se efectuó el tratamiento de riesgos aplicando nuevos controles y mejorando los existentes en los niveles de aceptación de riesgos alto medio y bajo con la finalidad de reducir, evitar/transferir y aceptar los niveles de riesgo comparando el porcentaje actual de nivel de cumplimiento 51,72% versus lo esperado 62.96%, que de acuerdo al modelo de madurez CMM está dentro del 60% ¨Los procesos se definen, y se comunican a través de un entramiento formal. Es obligatorio el cumplimiento de los procesos y por tanto la posibilidad de

detectar desviaciones es alta. Los procedimientos por si mismos no son sofisticados, pero se formalizan las practicas existentes.

Con la implementación de plan se logrará brindar a sus funcionarios y clientes niveles apropiados de protección, procesamiento y almacenamiento, preservando la calidad en la prestación de servicios institucionales y la seguridad de la Información.

RECOMENDACIONES

La necesidad de evolución y mejores prácticas tecnológicas en la administración pública para ofrecer un servicio de calidad a los ciudadanos o sobre la interoperabilidad de los sistemas en la administración electrónica, con lleva a la simplificación de procedimientos administrativos y mejor control en la seguridad de la información, mediante la aplicación de un proceso de gestión de riesgos de la seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados, basados en la Norma ISO/IEC 27001:2017 , para el proceso de viáticos del Instituto.

Se describen las recomendaciones para la aplicación del Plan:

- Creación de una Oficina de Gestión de Proyectos
- Designación formal y fortalecimiento del Comité de Seguridad de Información y del Oficial de Seguridad de la Información basados en la parte documental del desarrollo del Plan.
- Monitoreo, revisión y mejoramiento del proceso de gestión del riesgo en la seguridad de la información según lo establecido en el Plan.
- Aprobación de la Máxima Autoridad el Plan propuesto.
- Planificación del presupuesto a fin aplicar un Sistema de Gestión de Seguridad de la Información (SGSI).
- Consultoría y posterior Certificación del SGSI.

BIBLIOGRAFÍAS

[1] INTECO, «Implantación de un SGSI en la empresa,» https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf. [Último acceso: 5 mayo 2020].

[2] Asamblea Constituyente, «CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR,» WIPO, https://www.wipo.int/edocs/lexdocs/laws/es/ec/ec030es.pdf. [Último acceso: 2 mayo 2020].

[3] Secretaría Nacional de la Administraciòn Pública, «Registro Oficial,» 25 septiembre 2013. https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/2532-segundo-suplemento-al-registro-oficial-no-88.html. [Último acceso: 5 mayo 2020].

[4] R. Correa Delgado, «Ministerio de Telecomunicaciones y sociedad de la Información,» 28 diciembre 2015. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/02/Reglamento-Ley-Organica-de-Telecomunicaciones.pdf. [Último acceso: 5 mayo 2020].

[5] Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL, «Registro Oficial Nro 228 ACUERDO MINISTERIAL 025-2019,» 1 enero 2020. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf. [Último acceso: 1 mayo 2020].

[6] CODIGO ORGANICO INTEGRAL PENAL, COIP, «Ministerio de Defensa,» 5 febrero 2018. https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf. [Último acceso: 2 mayo 2020].

[7] A. M. Ávila Quiceno, *DISEÑO DE UN PROTOTIPO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN,* Medellín, 2016, pp. 33, 34, 63.

[8] F. E. Sanchez Ardila, *PLAN DE IMPLEMENTACION DE LA ISO/IEC 27001:2013 EN LA FUNDACION UNIVERSITARIA SAN MATEO,* Bogotá, 2018.

[9] A. R. Mantilla Guerra, «Revista Espacios,» 15 enero 2018. http://www.revistaespacios.com/a18v39n18/18391805.html. [Último acceso: 14 mayo 2020].

[10] Comisión Económica para América Latina y el Caribe, «CEPAL,» https://www.cepal.org/ilpes/noticias/paginas/5/39255/gobierno_electronico_anaser.pdf. [Último acceso: 17 05 2020].

[11] W. D. Ávila, «Aplicación de las `TIC` en la administración pública colombiana en línea,» http://alfa-redi.org/sites/default/files/articles/files/avila.pdf. [Último acceso: 3 mayo 2020].

[12] Asamblea Nacional de la República del Ecuador, «Ministerio de Telecomunicaciones y sociedad de la información,» 18 febrero 2019. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf. [Último acceso: 5 mayo 2020].

[13] Presidente Lenín Moreno, *Decreto Ejecutivo 1038,* Quito, Pichincha, 2020.

[14] Instituto Oceanográfico y Antártico de la Armada, Guayaquil, 2020.

[15] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» MAGERIT – versión 3.0, octubre 2012. https://administracionelectronica.gob.es/pae_Home. [Último acceso: 2 06 2020].

[16] Ministerio de Telecmunicaciones y Sociedad de la Información, «ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN –EGSI –,» Quito, 2020.

[17] SGSI, «Beneficios que nos ofrece la norma ISO/IEC 27001:2013,» https://www.pmg-ssi.com/2015/09/beneficios-iso-iec-27001-2013/. [Último acceso: 26 Abril 2020].

[18] ESAN, «4 pasos para implementar un Sistema de Seguridad de Información,» 4 febrero 2019. https://www.esan.edu.pe/apuntes-empresariales/2019/02/4-pasos-para-implementar-un-sistema-de-seguridad-de-informacion/. [Último acceso: 26 abril 2020].

[19] G. Pedraza Rodríguez, «PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN UNA ENTIDAD DEL SECTOR PÚBLICO BASADO EN LA NTC ISO 27001:2013,» Octubre 2017. http://repository.uamerica.edu.co/bitstream/20.500.11839/7008/1/686091-2017-II-GC.pdf. [Último acceso: 26 abril 2020].

[20] CÓDIGO ORGÁNICO ADMINISTRATIVO, «Segundo Suplemento del Registro Oficial No.31 , 7 de Julio 2017,» 07 07 2017. https://www.emov.gob.ec/sites/default/files/transparencia_2018/a2.7.pdf. [Último acceso: 16 5 2020].

ANEXOS

Anexo 1 Matriz Identificación de controles existentes para Estimación de Riesgos de los Activos de Información del Proceso de Viáticos, Fuente: Elaboración propia

INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA
MATRIZ IDENTIFICACIÓN DE CONTROLES EXISTENTES EN ESTIMACIÓN DE RIESGO A LOS ACTIVOS DE INFORMACIÓN DEL PROCESO VIATICOS

EVALUACIÓN DE RIESGO									
ANALISIS DE RIESGO				IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES	actual	CÁLCULO DE EVALUACIÓN RIESGO
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad		% cumplimiento	
A1	Personal Administrativo-Financiero	Personal nuevo	Gestión inadecuada al cambio	2,67	1	3	A.7.2.1 RESPONSABILIDADES DE GESTIÓN	0	8,00
		Desconocimiento de los procesos	No validación de los datos procesados	2,67	3	2	A.7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DDE LA INFORMACIÓN	25	16,00
		Finalización de Contrato	Inadecuada segregación de funciones	2,67	2	2	A.7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	0	10,67
A2	Servidores	Error de usuario	Distracción del usuario	3,00	2	1	A.9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	50	6,00
		Desastre natural, incendio	Desprotección en equipos nuevos sin seguro	3,00	1	2	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	80	6,00
A3	Correo electrónico Zimbra	Correos con ficheros adjuntos maliciosos	Infectar el equipo con un tipo de malware que roba información	2,33	3	2	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	20	14,00

EVALUACIÓN DE RIESGO									
ANALISIS DE RIESGO				IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES	actual	CÁLCULO DE EVALUACIÓN RIESGO
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad		% cumplimiento	
		Fuga de Información	Uso incontrolado de envío y recepción de información.	2,33	2	2	A.12.4.2 PROTECCIÓN DE LA INFORMACIÓN	50	9,33
A4	Internet	Fallas en la conectividad	Denegación del servicio	3,00	2	2	A.6.2.2 TELETRABAJO	0	12,00
		Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas.	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	50	18,00
A5	Sistema de gestión documental QUIPUX	Fallas en la conectividad de enlace de red	Inadecuada gestión de capacidad del sistema	3,00	1	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	50	6,00
		Saturación de Documentación	Gestión inadecuada de Documentación	3,00	2	3	A.6.2.2 TELETRABAJO	0	18,00
A6	Conectividad Red de área local	Fallas en la conectividad de enlace de red	Red saturada	2,00	2	2	A.9.1.2 ACCESO A LAS REDES Y A LOS SERVICIOS DE RED	75	8,00
		Código malicioso.	Código que le otorga a un atacante privilegios de administrador	2,00	2	2	A.9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	50	8,00
A7	Unidad de Sistema de Energía UPS	Mal funcionamiento del equipo.	Equipos sin protección ante fallas de energía	1,00	1	2	A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	80	2,00
A8	Computadoras de escritorio	Hurtos o vandalismo.	Control inadecuado del acceso no autorizado	3,00	2	2	A.11.2.6 SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	0	12,00
		Reutilización de PC escritorio	Medios de almacenamiento seguros	3,00	2	2	A.11.2.7 DISPOSICIÓN SEGURA O	0	12,00

EVALUACIÓN DE RIESGO									
ANALISIS DE RIESGO				IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES	actual	CÁLCULO DE EVALUACIÓN RIESGO
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad		% cumplimiento	
							REUTILIZACIÓN DE EQUIPOS		
		Uso de dispositivos externos	Estaciones de trabajo sin servicio	3,00	1	2	A.11.2.8 EQUIPO DE USUARIO DESATENDIDO	0	6,00
A9	Impresoras	Configuración del servicio errónea	Equipos conectados a la red sin ser detectados	1,33	2	2	A.15.1.3 CADENA DE SUMINISTRO DE TÉCNOLOGIA DE LA INFORMACIÓN Y DE LAS COMUNICACIÓN	0	5,33
		Mal funcionamiento del equipo sin servicio	Mantenimiento inadecuado.	1,33	2	2	A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	80	5,33
A10	Equipos de Seguridad física	Uso indebido de dispositivos de seguridad	Acceso de personal no autorizado	3,00	2	2	A.9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	50	12,00
A11	Personal de sistemas	Personal nuevo	Gestión inadecuada al cambio.	3,00	1	2	A.7.2.1 RESPONSABILIDADES DE GESTIÓN	25	6,00
		Finalización de Contrato	Inadecuada segregación de funciones	3,00	2	2	A.7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	0	12,00
A12	Sistema de telefonía voz sobre IP	Fallo en los servicios de comunicación	Inadecuada gestión de capacidad del sistema	3,00	1	2	A.15.1.3 CADENA DE SUMINISTRO DE TÉCNOLOGIA DE LA INFORMACIÓN Y DE LAS COMUNICACIÓN	0	6,00

EVALUACIÓN DE RIESGO									
ANALISIS DE RIESGO				IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES	actual	CÁLCULO DE EVALUACIÓN RIESGO
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad		% cumplimiento	
A13	Sistema Institucional Sigefi	Fallo del enlace fuera de la Institución	Denegación del servicio	3,00	2	3	A.6.2.2 TELETRABAJO	0	18,00
		Pérdida de datos de información	Cambios de plataforma de operación	3,00	2	2	A.14.2.3 REVISIÓN TÉCNICA DE APLICACIONES DESPUÉS DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN	0	12,00
A14	Sistema del Estado Esigef	Actualización de opciones en el sistema	Interfaz de usuario complicada	3,00	3	2	A.14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	50	18,00
		Fallas en la conectividad	Denegación del servicio	3,00	2	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	50	12,00
		Registro de ID usuario caducado o nuevo	Sin acceso al sistema	3,00	2	2	A.9.4.2 PROCEDIMIENTO INGRESO SEGURO	75	12,00
A15	Formulario Solicitud y liquidación de Comisión	Fallos en la elaboración de los formularios	Información errónea	2,67	2	2	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	20	10,67
		Pérdida de soportes	Falta de documentación interna.	2,67	2	2	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	20	10,67
		Falsificación de información	Falta de políticas para la comprobación de la información	2,67	2	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	20	10,67

EVALUACIÓN DE RIESGO									
ANALISIS DE RIESGO				IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES	actual	CÁLCULO DE EVALUACIÓN RIESGO
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad		% cumplimiento	
A16	Software Antivirus	Errores de software	Descarga y uso del software de internet no controlado	2,00	2	2	A.18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	50	8,00
		Código malicioso	Exposición de usuarios a problemas de seguridad	2,00	3	3	A.12.4.1 REGISTRO DE EVENTOS	50	18,00
A17	Comprobante de Pago CUR de pagos	Fallas en la conectividad	Denegación del servicio	2,33	3	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	50	14,00
		Pérdida de soportes	Falta de documentación interna	2,33	2	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	20	9,33
A18	Asientos Contables	Desastre natural, incendio	Protección física no apropiada	3,00	1	3	A.18.1.3 PROTECCIÓN DE REGISTROS	50	9,00
		Uso indebido de los sistemas de información	Falta de formación y conciencia sobre registros contables	3,00	2	2	A.12.4.2 PROTECCIÓN DE LA INFORMACIÓN	50	12,00
		Destrucción de registros.	Control inadecuado del acceso físico.	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	50	18,00
A19	Oficios, memorandos fisicos y electrónicos	Pérdida de soportes	Falta de documentación interna.	2,33	3	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	20	14,00
		Duplicidad de documentos	Insuficiente supervisión y control de los documentos	2,33	3	2	A.12.4.1 REGISTRO DE EVENTOS	50	14,00

EVALUACIÓN DE RIESGO									
ANALISIS DE RIESGO				IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES	actual	CÁLCULO DE EVALUACIÓN RIESGO
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad		% cumplimiento	
A20	Manuales e Instructivos	Desactualización de Manuales e Instructivos	Desconocimiento de los manuales e instructivos con normativa vigente	2,33	3	3	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	20	21,00
		Desastre natural, incendio	Protección física no apropiada	2,33	3	2	A.18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	50	14,00
		Pérdida, destrucción	Insuficiente supervisión de los Manuales e Instructivos	2,33	3	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	20	14,00
A21	Estados Financieros	Pérdida, destrucción	Protección física no apropiada	3,00	3	2	A.12.3.1 RESPALDO DE INFORMACIÓN	50	18,00
		Cambio involuntario de datos en sistema de información.	Gestión inadecuada Normas de Control	3,00	3	2	A.18.1.3 PROTECCIÓN DE REGISTROS	50	18,00
A22	Comisionados	Falsificación de información	Falta de políticas para la comprobación de la información	2,33	3	2	A.18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	50	14,00
		Pandemia Covid 19	No Liquidación de Comisión	2,33	3	2	A.6.2.2 TELETRABAJO	0	14,00
A23	Sistema de autenticación	Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas	3,00	3	2	A.13.2.4 ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN	50	18,00

EVALUACIÓN DE RIESGO									
ANALISIS DE RIESGO				IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES	actual	CÁLCULO DE EVALUACIÓN RIESGO
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad		% cumplimiento	
A24	Router	Falla en los servicios de comunicación	Equipos mal estado o descontinuados	1,00	2	1	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	80	2,00
A25	Switch concentrador	Pérdida de electricidad.	Sensibilidad del equipo a los cambios de voltaje	3,00	3	1	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	80	9,00
A26	Escáner	Equipo obsoleto	Sin utilizar	1,00	2	2	A.8.1.4 DEVOLUCION DE ACTIVOS	85	4,00
A27	Publicaciones de Comisiones	Revelación de información.	Ausencia de política de manejo de información	2,67	3	1	A.13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN	50	8,00
		Fuga de Información	Uso inapropiado de la información	2,67	3	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	50	16,00
		Información incompleta	Ausencia de política de manejo de información	2,67	3	2	A.14.1.3 PROTECCIÓN DE LAS TRANSACCIONES DE SERVICIOS DE APLICACIONES	50	16,00
A28	Oficinas de Sistemas, Administrativo/Financiero	Acceso físico no autorizado	Falta de procedimientos para acceso a las Oficinas	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	50	18,00
		Desastre natural, incendio	Protección física no apropiada	3,00	1	2	A.18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	50	6,00
A29	Código Fuente	Daño causado por un tercero	Control inadecuado del acceso al código	3,00	3	1	A.14.2.2 PROCEDIMIENTO DE CONTROL DE	25	9,00

EVALUACIÓN DE RIESGO									
ANALISIS DE RIESGO				IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES	actual	CÁLCULO DE EVALUACIÓN RIESGO
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad		% cumplimiento	
							CAMBIOS EN SISTEMAS		
A30	Sistemas Operativos	Abuso de privilegios de acceso	No revisión de privilegios de acceso	3,00	2	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	50	12,00
A31	Firewall	Ataque de denegación de servicio	Sin protección de red interna y externa	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	50	18,00
A32	Copias de Seguridad de los Sistemas de Información	Cambios no autorizados de registros	Pérdida de Datos	3,00	2	2	A.12.3.1 RESPALDO DE INFORMACIÓN	50	12,00
		Comprometer información confidencial	Ataque malicioso de personal interno	3,00	3	2	A.12.4.2 PROTECCIÓN DE LA INFORMACIÓN	50	18,00
A33	Dispositivo Electrónico Biométrico Lector (huella digital)	Innovación Tecnológica	Denegación del servicio	3,00	2	1	A.8.1.3 USO ACEPTABLE DE LOS ACTIVOS	85	6,00
		Desastre natural, incendio	Protección física no apropiada	3,00	2	2	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	80	12,00
A34	Intranet	Pandemia Covid 19	Fallas de conectividad	3,00	2	2	A.6.2.2 TELETRABAJO	0	12,00

EVALUACIÓN DE RIESGO									
ANALISIS DE RIESGO				IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES	actual	CÁLCULO DE EVALUACIÓN RIESGO
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad		% cumplimiento	
		Acceso al servicio por personas no autorizadas	No validación de los ID autorizados	3,00	2	2	A.9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	50	12,00

Anexo 2 Matriz Evaluación de Riesgo de los Activos de Información del Proceso de Viáticos, Fuente: Elaboración propia

INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA
MATRIZ EVALUACIÓN DE RIESGO DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO VIATICOS

EVALUACIÓN DE RIESGO									
ANALISIS DEL RIESGO							CONTROLES IMPLEMENTADOS EXISTENTES	CÁLCULO DE EVALUACIÓN RIESGO	NIVEL DE RIESGO
				IMPACTO	PROBABILIDAD				
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad			
A1	Personal Administrativo-Financiero	Personal nuevo	Gestión inadecuada al cambio	2,67	1	3	A.7.2.1 RESPONSABILIDADES DE GESTIÓN	8,00	MEDIO
		Desconocimiento de los procesos	No validación de los datos procesados	2,67	3	2	A.7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DDE LA INFORMACIÓN	16,00	ALTO
		Finalización de Contrato	Inadecuada segregación de funciones	2,67	2	2	A.7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	10,67	ALTO
A2	Servidores	Error de usuario	Distracción del usuario	3,00	2	1	A.9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	6,00	MEDIO
		Desastre natural, incendio	Desprotección en equipos nuevos sin seguro	3,00	1	2	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	6,00	MEDIO
A3	Correo electrónico Zimbra	Correos con ficheros adjuntos maliciosos	Infectar el equipo con un tipo de malware que roba información	2,33	3	2	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	14,00	ALTO
		Fuga de Información	Uso incontrolado de envío y recepción de información.	2,33	2	2	A.12.4.2 PROTECCIÓN DE LA INFORMACIÓN	9,33	ALTO

EVALUACIÓN DE RIESGO									
ANALISIS DEL RIESGO							CONTROLES IMPLEMENTADOS EXISTENTES	CÁLCULO DE EVALUACIÓN RIESGO	NIVEL DE RIESGO
				IMPACTO	PROBABILIDAD				
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad			
A4	Internet	Fallas en la conectividad	Denegación del servicio	3,00	2	2	A.6.2.2 TELETRABAJO	12,00	ALTO
		Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas.	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	18,00	ALTO
A5	Sistema de gestión documental QUIPUX	Fallas en la conectividad de enlace de red	Inadecuada gestión de capacidad del sistema	3,00	1	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	6,00	MEDIO
		Saturación de Documentación	Gestión inadecuada de Documentación	3,00	2	3	A.6.2.2 TELETRABAJO	18,00	ALTO
A6	Conectividad Red de área local	Fallas en la conectividad de enlace de red	Red saturada	2,00	2	2	A.9.1.2 ACCESO A LAS REDES Y A LOS SERVICIOS DE RED	8,00	MEDIO
		Código malicioso.	Código que le otorga a un atacante privilegios de administrador	2,00	2	2	A.9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	8,00	MEDIO
A7	Unidad de Sistema de Energía UPS	Mal funcionamiento del equipo.	Equipos sin protección ante fallas de energía	1,00	1	2	A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	2,00	BAJO
A8	Computadoras de escritorio	Hurtos o vandalismo.	Control inadecuado del acceso no autorizado	3,00	2	2	A.11.2.6 SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	12,00	ALTO
		Reutilización de PC escritorio	Medios de almacenamiento seguros	3,00	2	2	A.11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	12,00	ALTO

EVALUACIÓN DE RIESGO									
ANALISIS DEL RIESGO							CONTROLES IMPLEMENTADOS EXISTENTES	CÁLCULO DE EVALUACIÓN RIESGO	NIVEL DE RIESGO
				IMPACTO	PROBABILIDAD				
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad			
		Uso de dispositivos externos	Estaciones de trabajo sin servicio	3,00	1	2	A.11.2.8 EQUIPO DE USUARIO DESATENDIDO	6,00	MEDIO
A9	Impresoras	Configuración del servicio errónea	Equipos conectados a la red sin ser detectados	1,33	2	2	A.15.1.3 CADENA DE SUMINISTRO DE TÉCNOLOGIA DE LA INFORMACIÓN Y DE LAS COMUNICACIÓN	5,33	MEDIO
		Mal funcionamiento del equipo sin servicio	Mantenimiento inadecuado.	1,33	2	2	A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	5,33	MEDIO
A10	Equipos de Seguridad física	Uso indebido de dispositivos de seguridad	Acceso de personal no autorizado	3,00	2	2	A.9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	12,00	ALTO
A11	Personal de sistemas	Personal nuevo	Gestión inadecuada al cambio.	3,00	1	2	A.7.2.1 RESPONSABILIDADES DE GESTIÓN	6,00	MEDIO
		Finalización de Contrato	Inadecuada segregación de funciones	3,00	2	2	A.7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	12,00	ALTO
A12	Sistema de telefonía voz sobre IP	Fallo en los servicios de comunicación	Inadecuada gestión de capacidad del sistema	3,00	1	2	A.15.1.3 CADENA DE SUMINISTRO DE TÉCNOLOGIA DE LA INFORMACIÓN Y DE LAS COMUNICACIÓN	6,00	MEDIO
A13	Sistema Institucional Sigefi	Fallo del enlace fuera de la Institución	Denegación del servicio	3,00	2	3	A.6.2.2 TELETRABAJO	18,00	ALTO

EVALUACIÓN DE RIESGO									
ANALISIS DEL RIESGO							CONTROLES IMPLEMENTADOS EXISTENTES	CÁLCULO DE EVALUACIÓN RIESGO	NIVEL DE RIESGO
				IMPACTO	PROBABILIDAD				
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad			
		Pérdida de datos de información	Cambios de plataforma de operación	3,00	2	2	A.14.2.3 REVISIÓN TÉCNICA DE APLICACIONES DESPUÉS DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN	12,00	ALTO
A14	Sistema del Estado Esigef	Actualización de opciones en el sistema	Interfaz de usuario complicada	3,00	3	2	A.14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	18,00	ALTO
		Fallas en la conectividad	Denegación del servicio	3,00	2	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	12,00	ALTO
		Registro de ID usuario caducado o nuevo	Sin acceso al sistema	3,00	2	2	A.9.4.2 PROCEDIMIENTO INGRESO SEGURO	12,00	ALTO
A15	Formulario Solicitud y liquidación de Comisión	Fallos en la elaboración de los formularios	Información errónea	2,67	2	2	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	10,67	ALTO
		Pérdida de soportes	Falta de documentación interna.	2,67	2	2	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	10,67	ALTO
		Falsificación de información	Falta de políticas para la comprobación de la información	2,67	2	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	10,67	ALTO
A16	Software Antivirus	Errores de software	Descarga y uso del software de internet no controlado	2,00	2	2	A.18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	8,00	MEDIO

EVALUACIÓN DE RIESGO									
ANALISIS DEL RIESGO							CONTROLES IMPLEMENTADOS EXISTENTES	CÁLCULO DE EVALUACIÓN RIESGO	NIVEL DE RIESGO
				IMPACTO	PROBABILIDAD				
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad			
		Código malicioso	Exposición de usuarios a problemas de seguridad	2,00	3	3	A.12.4.1 REGISTRO DE EVENTOS	18,00	ALTO
A17	Comprobante de Pago CUR de pagos	Fallas en la conectividad	Denegación del servicio	2,33	3	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	14,00	ALTO
		Pérdida de soportes	Falta de documentación interna	2,33	2	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	9,33	ALTO
A18	Asientos Contables	Desastre natural, incendio	Protección física no apropiada	3,00	1	3	A.18.1.3 PROTECCIÓN DE REGISTROS	9,00	ALTO
		Uso indebido de los sistemas de información	Falta de formación y conciencia sobre registros contables	3,00	2	2	A.12.4.2 PROTECCIÓN DE LA INFORMACIÓN	12,00	ALTO
		Destrucción de registros.	Control inadecuado del acceso físico.	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	18,00	ALTO
A19	Oficios, memorandos fisicos y electrónicos	Pérdida de soportes	Falta de documentación interna.	2,33	3	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	14,00	ALTO
		Duplicidad de documentos	Insuficiente supervisión y control de los documentos	2,33	3	2	A.12.4.1 REGISTRO DE EVENTOS	14,00	ALTO
A20	Manuales e Instructivos	Desactualización de Manuales e Instructivos	Desconocimiento de los manuales e instructivos con normativa vigente	2,33	3	3	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	21,00	ALTO

EVALUACIÓN DE RIESGO									
ANALISIS DEL RIESGO							CONTROLES IMPLEMENTADOS EXISTENTES	CÁLCULO DE EVALUACIÓN RIESGO	NIVEL DE RIESGO
				IMPACTO	PROBABILIDAD				
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad			
		Desastre natural, incendio	Protección física no apropiada	2,33	3	2	A.18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	14,00	ALTO
		Pérdida, destrucción	Insuficiente supervisión de los Manuales e Instructivos	2,33	3	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	14,00	ALTO
A21	Estados Financieros	Pérdida, destrucción	Protección física no apropiada	3,00	3	2	A.12.3.1 RESPALDO DE INFORMACIÓN	18,00	ALTO
		Cambio involuntario de datos en sistema de información.	Gestión inadecuada Normas de Control	3,00	3	2	A.18.1.3 PROTECCIÓN DE REGISTROS	18,00	ALTO
A22	Comisionados	Falsificación de información	Falta de políticas para la comprobación de la información	2,33	3	2	A.18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	14,00	ALTO
		Pandemia Covid 19	No Liquidación de Comisión	2,33	3	2	A.6.2.2 TELETRABAJO	14,00	ALTO
A23	Sistema de autenticación	Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas	3,00	3	2	A.13.2.4 ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN	18,00	ALTO
A24	Router	Falla en los servicios de comunicación	Equipos mal estado o descontinuados	1,00	2	1	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	2,00	BAJO
A25	Switch concentrador	Pérdida de electricidad.	Sensibilidad del equipo a los cambios de voltaje	3,00	3	1	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	9,00	ALTO
A26	Escáner	Equipo obsoleto	Sin utilizar	1,00	2	2	A.8.1.4 DEVOLUCION DE ACTIVOS	4,00	MEDIO

EVALUACIÓN DE RIESGO									
ANALISIS DEL RIESGO							CONTROLES IMPLEMENTADOS EXISTENTES	CÁLCULO DE EVALUACIÓN RIESGO	NIVEL DE RIESGO
				IMPACTO	PROBABILIDAD				
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad			
A27	Publicaciones de Comisiones	Revelación de información.	Ausencia de política de manejo de información	2,67	3	1	A.13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN	8,00	MEDIO
		Fuga de Información	Uso inapropiado de la información	2,67	3	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	16,00	ALTO
		Información incompleta	Ausencia de política de manejo de información	2,67	3	2	A.14.1.3 PROTECCIÓN DE LAS TRANSACCIONES DE SERVICIOS DE APLICACIONES	16,00	ALTO
A28	Oficinas de Sistemas, Administrativo/Financiero	Acceso físico no autorizado	Falta de procedimientos para acceso a las Oficinas	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	18,00	ALTO
		Desastre natural, incendio	Protección física no apropiada	3,00	1	2	A.18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	6,00	MEDIO
A29	Código Fuente	Daño causado por un tercero	Control inadecuado del acceso al código	3,00	3	1	A.14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	9,00	ALTO
A30	Sistemas Operativos	Abuso de privilegios de acceso	No revisión de privilegios de acceso	3,00	2	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	12,00	ALTO
A31	Firewall	Ataque de denegación de servicio	Sin protección de red interna y externa	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	18,00	ALTO

EVALUACIÓN DE RIESGO									
ANALISIS DEL RIESGO							CONTROLES IMPLEMENTADOS EXISTENTES	CÁLCULO DE EVALUACIÓN RIESGO	NIVEL DE RIESGO
				IMPACTO	PROBABILIDAD				
No.	NOMBRE DE ACTIVO	AMENAZAS	VULNERABILIDADES	CID	Nivel de Amenaza	Nivel de Vulnerabilidad			
A32	Copias de Seguridad de los Sistemas de Información	Cambios no autorizados de registros	Pérdida de Datos	3,00	2	2	A.12.3.1 RESPALDO DE INFORMACIÓN	12,00	ALTO
		Comprometer información confidencial	Ataque malisioso de personal interno	3,00	3	2	A.12.4.2 PROTECCIÓN DE LA INFORMACIÓN	18,00	ALTO
A33	Dispositivo Electrónico Biometrico Lector (huella digital)	Innovación Tecnológica	Denegación del servicio	3,00	2	1	A.8.1.3 USO ACEPTABLE DE LOS ACTIVOS	6,00	MEDIO
		Desastre natural, incendio	Protección física no apropiada	3,00	2	2	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	12,00	ALTO
A34	Intranet	Pandemia Covid 19	Fallas de conectividad	3,00	2	2	A.6.2.2 TELETRABAJO	12,00	ALTO
		Acceso al servicio por personas no autorizadas	No validación de los ID autorizados	3,00	2	2	A.9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	12,00	ALTO

Anexo 3 Matriz de tratamiento de riesgo de los activos de información del proceso viáticos, Fuente: Elaboración propia

INSTITUTO OCEANOGRÁFICO Y ANTÁRTICO DE LA ARMADA
MATRIZ DE TRATAMIENTO DE RIESGO DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO VIATICOS

EVALUACIÓN DE RIESGO										TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
A1	Personal Administrativo-Financiero	Personal nuevo	Gestión inadecuada al cambio	2,67	1	3	A.7.2.1 RESPONSABILIDADES DE GESTIÓN	8,00	MEDIO	REDUCIR/TRANSFERIR	Dar a conocer y hacer cumplir con las Políticas Seguridad en la Institución	A.7.2.1 RESPONSABILIDADES DE LA MÁXIMA AUTORIDAD O SU DELEGADO	1	1	2,67	BAJO	ACEPTABLE
		Desconocimiento de los procesos	No validación de los datos procesados	2,67	3	2	A.7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DDE LA INFORMACIÓN	16,00	ALTO	EVITAR/TRANSFERIR	Recibir periódicamente una vez al año Normas y procedimientos para la seguridad de la Información	A.7.2.2 CONCIENCIACIÓN, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN	1	1	2,67	BAJO	ACEPTABLE
		Finalización de Contrato	Inadecuada segregación de funciones	2,67	2	2	A.7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	10,67	ALTO	EVITAR/TRANSFERIR	Normativa interna y procedimientos aprobados para la seguridad de información	A.7.3.1 RESPONSABILIDADES ANTE LA FINALIZACIÓN O CAMBIO DE EMPLEO	1	1	2,67	BAJO	ACEPTABLE
A2	Servidores	Error de usuario	Distracción del usuario	3,00	2	1	A.9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	6,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar y aprobar política de responsabilidades de uso credenciales	A.9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	1	1	3,00	BAJO	ACEPTABLE
		Desastre natural, incendio	Desprotección en equipos nuevos sin seguro	3,00	1	2	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	6,00	MEDIO	REDUCIR/TRANSFERIR	Existe sistemas de protección de equipos en la mayoría instalados en el Instituto y Seguro	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE EQUIPOS	1	1	3,00	BAJO	ACEPTABLE
A3	Correo electrónico Zimbra	Correos con ficheros adjuntos maliciosos	Infectar el equipo con un tipo de malware que roba información	2,33	3	2	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	14,00	ALTO	EVITAR/TRANSFERIR	Establecer normas y responsabilidades formales que aseguren que los procedimientos internos se cumplan	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	1	1	2,33	BAJO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
		Fuga de Información	Uso incontrolado de envio y recepción de información.	2,33	2	2	A.12.4.2 PROTECCIÓN DE LA INFORMACIÓN	9,33	ALTO	EVITAR/TRANSFERIR	Formalizar procedimientos y políticas de seguridad información para proteger contra alteraciones y accesos no autorizados	A.12.4.2 PROTECCIÓN DE LOS REGISTROS DE INFORMACIÓN	1	1	2,33	BAJO	ACEPTABLE
A4	Internet	Fallas en la conectividad	Denegación del servicio	3,00	2	2	A.6.2.2 TELETRABAJO	12,00	ALTO	EVITAR/TRANSFERIR	Elaborar directrices, disposiciones y políticas de seguridad por esta modalidad	A.6.2.2 TELETRABAJO	2	1	6,00	MEDIO	ACEPTABLE
		Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas.	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	18,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas de derecho de acceso a sistemas y redes	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	1	1	3,00	BAJO	ACEPTABLE
A5	Sistema de gestión documental QUIPUX	Fallas en la conectividad de enlace de red	Inadecuada gestión de capacidad del sistema	3,00	1	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	6,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar y aprobar políticas de derecho de acceso a sistemas y redes	A.14.1.2 ASEGURAR LOS SERVICIOS DE APLICACIONES EN REDES PÚBLICAS	1	1	3,00	BAJO	ACEPTABLE
		Saturación de Documentación	Gestión inadecuada de Documentación	3,00	2	3	A.6.2.2 TELETRABAJO	18,00	ALTO	EVITAR/TRANSFERIR	Elaborar directrices, disposiciones y políticas de seguridad por esta modalidad	A.6.2.2 TELETRABAJO	2	1	6,00	MEDIO	ACEPTABLE
A6	Conectividad Red de área local	Fallas en la conectividad de enlace de red	Red saturada	2,00	2	2	A.9.1.2 ACCESO A LAS REDES Y A LOS SERVICIOS DE RED	8,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar procedimientos de autorización permitido al acceso de redes y servicios de red	A.9.1.2 ACCESO A REDES Y SERVICIOS DE RED	1	1	2,00	BAJO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
		Código malicioso.	Código que le otorga a un atacante privilegios de administrador	2,00	2	2	A.9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	8,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar procedimientos de autorización permitido al acceso de redes y servicios de red	A.9.2.4 GESTIÓN DE LA INFORMACIÓN CONFIDENCIAL DE AUTENTICACIÓN DE LOS USUARIOS	1	1	2,00	BAJO	ACEPTABLE
A7	Unidad de Sistema de Energía UPS	Mal funcionamiento del equipo.	Equipos sin protección ante fallas de energía	1,00	1	2	A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	2,00	BAJO	ACEPTAR	Formalizar procedimientos y autorización de recursos para mantenimiento de equipos	A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	1	1	1,00	BAJO	ACEPTABLE
A8	Computadoras de escritorio	Hurtos o vandalismo.	Control inadecuado del acceso no autorizado	3,00	2	2	A.11.2.6 SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	12,00	ALTO	EVITAR/TRANSFERIR	Formalizar procedimientos y políticas para salida de equipos del Instituto	A.11.2.6 SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	1	2	6,00	MEDIO	ACEPTABLE
		Reutilización de PC escritorio	Medios de almacenamiento seguros	3,00	2	2	A.11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	12,00	ALTO	EVITAR/TRANSFERIR	Formalizar procedimientos y políticas para reúso de equipos del Instituto	A.11.2.7 SEGURIDAD DE LA REUTILIZACIÓN O ELIMINACIÓN SEGURA DE DISPOSITIVOS DE ALMACENAMIENTO	1	1	3,00	BAJO	ACEPTABLE
		Uso de dispositivos externos	Estaciones de trabajo sin servicio	3,00	1	2	A.11.2.8 EQUIPO DE USUARIO DESATENDIDO	6,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar procedimientos y políticas para atención al usuario	A.11.2.8 EQUIPO INFORMÁTICO DE USUARIO DESATENDIDO	1	1	3,00	BAJO	ACEPTABLE
A9	Impresoras	Configuración del servicio errónea	Equipos conectados a la red sin ser detectados	1,33	2	2	A.15.1.3 CADENA DE SUMINISTRO DE TÉCNOLOGIA DE LA INFORMACIÓN Y DE LAS COMUNICACIÓN	5,33	MEDIO	REDUCIR/TRANSFERIR	Formalizar procedimientos y políticas para atención de bienes externos	A.15.1.3 CADENA DE SUMINISTRO DE TÉCNOLOGIA DE LA INFORMACIÓN Y DE LAS COMUNICACIONES	2	1	2,67	BAJO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
		Mal funcionamiento del equipo sin servicio	Mantenimiento inadecuado.	1,33	2	2	A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	5,33	MEDIO	REDUCIR/TRANSFERIR	Formalizar procedimientos y políticas para atención de bienes externos	A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	2	1	2,67	BAJO	ACEPTABLE
A10	Equipos de Seguridad física	Uso indebido de dispositivos de seguridad	Acceso de personal no autorizado	3,00	2	2	A.9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	12,00	ALTO	EVITAR/TRANSFERIR	Formalizar procedimientos de autorización permitido al acceso de redes y servicios de red	A.9.2.4 GESTIÓN DE LA INFORMACIÓN CONFIDENCIAL DE AUTENTICACIÓN DE LOS USUARIOS	1	1	3,00	BAJO	ACEPTABLE
A11	Personal de sistemas	Personal nuevo	Gestión inadecuada al cambio.	3,00	1	2	A.7.2.1 RESPONSABILIDADES DE GESTIÓN	6,00	MEDIO	REDUCIR/TRANSFERIR	Dar a conocer y cumplir con las Políticas Seguridad	A.7.2.1 RESPONSABILIDADES DE LA MÁXIMA AUTORIDAD O SU DELEGADO	1	1	3,00	BAJO	ACEPTABLE
		Finalización de Contrato	Inadecuada segregación de funciones	3,00	2	2	A.7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	12,00	ALTO	EVITAR/TRANSFERIR	Normativa interna y procedimientos aprobados para la seguridad de información	A.7.3.1 RESPONSABILIDADES ANTE LA FINALIZACIÓN O CAMBIO DE EMPLEO	1	1	3,00	BAJO	ACEPTABLE
A12	Sistema de telefonía voz sobre IP	Fallo en los servicios de comunicación	Inadecuada gestión de capacidad del sistema	3,00	1	2	A.15.1.3 CADENA DE SUMINISTRO DE TÉCNOLOGIA DE LA INFORMACIÓN Y DE LAS COMUNICACIÓN	6,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar y aprobar políticas de seguridad a los servicios de TIC de los proveedores	A.15.1.3 CADENA DE SUMINISTRO DE TÉCNOLOGIA DE LA INFORMACIÓN Y DE LAS COMUNICACIONES	1	1	3,00	BAJO	ACEPTABLE
A13	Sistema Institucional Sigefi	Fallo del enlace fuera de la Institución	Denegación del servicio	3,00	2	3	A.6.2.2 TELETRABAJO	18,00	ALTO	EVITAR/TRANSFERIR	Elaborar directrices, disposiciones y políticas de seguridad por esta modalidad	A.6.2.2 TELETRABAJO	2	1	6,00	MEDIO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
		Pérdida de datos de información	Cambios de plataforma de operación	3,00	2	2	A.14.2.3 REVISIÓN TÉCNICA DE APLICACIONES DESPUÉS DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN	12,00	ALTO	EVITAR/TRANSFERIR	Formalizar y mantener actualizados procedimientos de control e integridad de aplicación "Proceso de desarrollo seguro"	A.14.2.3 REVISIÓN TÉCNICA DE APLICACIONES TRAS EFECTUAR CAMBIOS EN EL SISTEMA OPERATIVO	1	1	3,00	BAJO	ACEPTABLE
A14	Sistema del Estado Esigef	Actualización de opciones en el sistema	Interfaz de usuario complicada	3,00	3	2	A.14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	18,00	ALTO	EVITAR/TRANSFERIR	Plan de capacitación sobre funcionamiento y utilización de nueva versión	A.14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	2	1	6,00	MEDIO	ACEPTABLE
		Fallas en la conectividad	Denegación del servicio	3,00	2	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	12,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas de seguridad a los servicios de TIC del Instituto	A.14.1.2 ASEGURAR LOS SERVICIOS DE APLICACIONES EN REDES PÚBLICAS	2	1	6,00	MEDIO	ACEPTABLE
		Registro de ID usuario caducado o nuevo	Sin acceso al sistema	3,00	2	2	A.9.4.2 PROCEDIMIENTO INGRESO SEGURO	12,00	ALTO	EVITAR/TRANSFERIR	Formalizar y socializar procedimiento solo pueden acceder al servicio usuarios autorizados	A.9.4.2 PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN	1	1	3,00	BAJO	ACEPTABLE
A15	Formulario Solicitud y liquidación de Comisión	Fallos en la elaboración de los formularios	Información errónea	2,67	2	2	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	10,67	ALTO	EVITAR/TRANSFERIR	Establecer normas y responsabilidades formales que aseguren que los procedimientos internos se cumplan	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	1	1	2,67	BAJO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
		Pérdida de soportes	Falta de documentación interna.	2,67	2	2	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	10,67	ALTO	EVITAR/TRANSFERIR	Establecer normas y responsabilidades formales que aseguren que los procedimientos internos se cumplan	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	1	1	2,67	BAJO	ACEPTABLE
		Falsificación de información	Falta de políticas para la comprobación de la información	2,67	2	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	10,67	ALTO	EVITAR/TRANSFERIR	Formalizar Políticas de seguridad de información determinando la integridad y disponibilidad de la información	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	1	1	2,67	BAJO	ACEPTABLE
A16	Software Antivirus	Errores de software	Descarga y uso del software de internet no controlado	2,00	2	2	A.18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	8,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar procedimientos y políticas de seguridad que garantice la revisión, protección y registro de eventos periódicamente	A.18.2.3 COMPROBACIÓN DEL CUMPLIMIENTO TÉCNICO	1	1	2,00	BAJO	ACEPTABLE
		Código malicioso	Exposición de usuarios a problemas de seguridad	2,00	3	3	A.12.4.1 REGISTRO DE EVENTOS	18,00	ALTO	EVITAR/TRANSFERIR	Formalizar procedimientos para revisión, protección y registro de eventos de actividades de usuarios	A.12.4.1 REGISTRO DE EVENTOS	1	1	2,00	BAJO	ACEPTABLE
A17	Comprobante de Pago CUR de pagos	Fallas en la conectividad	Denegación del servicio	2,33	3	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	14,00	ALTO	EVITAR/TRANSFERIR	Formalizar Políticas internas determinando la confidencialidad e integridad de las transacciones ejecutadas	A.14.1.2 ASEGURAR LOS SERVICIOS DE APLICACIONES EN REDES PÚBLICAS	1	1	2,33	BAJO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
		Pérdida de soportes	Falta de documentación interna	2,33	2	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	9,33	ALTO	EVITAR/TRANSFERIR	Formalizar Políticas de seguridad de información determinando la integridad y disponibilidad de la información	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	1	1	2,33	BAJO	ACEPTABLE
A18	Asientos Contables	Desastre natural, incendio	Protección física no apropiada	3,00	1	3	A.18.1.3 PROTECCIÓN DE REGISTROS	9,00	ALTO	EVITAR/TRANSFERIR	Cumplimiento de los controles implementados para la seguridad de la información	A.18.1.3 PROTECCIÓN DE LOS REGISTROS	1	2	6,00	MEDIO	ACEPTABLE
		Uso indebido de los sistemas de información	Falta de formación y conciencia sobre registros contables	3,00	2	2	A.12.4.2 PROTECCIÓN DE LA INFORMACIÓN	12,00	ALTO	EVITAR/TRANSFERIR	Formalizar procedimientos para proteger información contra daños naturales, alteraciones y accesos no autorizados	A.12.4.2 PROTECCIÓN DE LOS REGISTROS DE INFORMACIÓN	1	1	3,00	BAJO	ACEPTABLE
		Destrucción de registros.	Control inadecuado del acceso físico.	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	18,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas de derecho de acceso a documentos y sistemas	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	1	1	3,00	BAJO	ACEPTABLE
A19	Oficios, memorandos físicos y electrónicos	Pérdida de soportes	Falta de documentación interna.	2,33	3	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	14,00	ALTO	EVITAR/TRANSFERIR	Formalizar Políticas de seguridad de información determinando la integridad y disponibilidad de la información	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	1	1	2,33	BAJO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
		Duplicidad de documentos	Insuficiente supervisión y control de los documentos	2,33	3	2	A.12.4.1 REGISTRO DE EVENTOS	14,00	ALTO	EVITAR/TRANSFERIR	Formalizar procedimientos para revisión, protección y registro de eventos de actividades de usuarios	A.12.4.1 REGISTRO DE EVENTOS	1	1	2,33	BAJO	ACEPTABLE
A20	Manuales e Instructivos	Desactualización de Manuales e Instructivos	Desconocimiento de los manuales e instructivos con normativa vigente	2,33	3	3	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	21,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas para la protección de la información	A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	1	1	2,33	BAJO	ACEPTABLE
		Desastre natural, incendio	Protección física no apropiada	2,33	3	2	A.18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	14,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas para la protección de las instalaciones	A.18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	1	2	4,67	MEDIO	ACEPTABLE
		Pérdida, destrucción	Insuficiente supervisión de los Manuales e Instructivos	2,33	3	2	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	14,00	ALTO	EVITAR/TRANSFERIR	Formalizar Políticas de seguridad de información determinando la integridad y disponibilidad de la información	A.16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	1	1	2,33	BAJO	ACEPTABLE
A21	Estados Financieros	Pérdida, destrucción	Protección física no apropiada	3,00	3	2	A.12.3.1 RESPALDO DE INFORMACIÓN	18,00	ALTO	EVITAR/TRANSFERIR	Formalizar procedimientos para el respaldo, resguardo y contención de la información y ubicarse en un ambiente físico seguro	A.12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	1	1	3,00	BAJO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
		Cambio involuntario de datos en sistema de información.	Gestión inadecuada Normas de Control	3,00	3	2	A.18.1.3 PROTECCIÓN DE REGISTROS	18,00	ALTO	EVITAR/TRANSFERIR	Formalizar Políticas de seguridad de información determinando la integridad y disponibilidad de la información	A.18.1.3 PROTECCIÓN DE LOS REGISTROS	1	1	3,00	BAJO	ACEPTABLE
A22	Comisionados	Falsificación de información	Falta de políticas para la comprobación de la información	2,33	3	2	A.18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	14,00	ALTO	EVITAR/TRANSFERIR	Dar a conocer y hacer cumplir con las Políticas Seguridad en la Institución	A.18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	1	1	2,33	BAJO	ACEPTABLE
		Pandemia Covid 19	No Liquidación de Comisión	2,33	3	2	A.6.2.2 TELETRABAJO	14,00	ALTO	EVITAR/TRANSFERIR	Elaborar directrices, disposiciones y políticas de seguridad por esta modalidad	A.6.2.2 TELETRABAJO	1	2	4,67	MEDIO	ACEPTABLE
A23	Sistema de autenticación	Divulgación de contraseñas	Inadecuada gestión y protección de contraseñas	3,00	3	2	A.13.2.4 ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN	18,00	ALTO	EVITAR/TRANSFERIR	Formalizar Políticas de seguridad para su revisión y emisión regularmente ¨acuerdos de confidencialidad¨¨	A.13.2.4 ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN	1	1	3,00	BAJO	ACEPTABLE
A24	Router	Falla en los servicios de comunicación	Equipos mal estado o descontinuados	1,00	2	1	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	2,00	BAJO	ACEPTAR	Formalizar procedimientos de protección y mantenimiento de equipos	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE EQUIPOS	1	1	1,00	BAJO	ACEPTABLE
A25	Switch concentrador	Pérdida de electricidad.	Sensibilidad del equipo a los cambios de voltaje	3,00	3	1	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	9,00	ALTO	EVITAR/TRANSFERIR	Formalizar procedimientos de protección y mantenimiento de equipos	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE EQUIPOS	1	1	3,00	BAJO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
A26	Escáner	Equipo obsoleto	Sin utilizar	1,00	2	2	A.8.1.4 DEVOLUCION DE ACTIVOS	4,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar proceso para devolución y baja de Activos de Información	A.8.1.4 DEVOLUCION DE ACTIVOS	1	1	1,00	BAJO	ACEPTABLE
A27	Publicaciones de Comisiones	Revelación de información.	Ausencia de política de manejo de información	2,67	3	1	A.13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN	8,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar Políticas de seguridad para evitar transmisiones incompletas o alteración no autorizada.	A.13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN	1	1	2,67	BAJO	ACEPTABLE
		Fuga de Información	Uso inapropiado de la información	2,67	3	2	A.14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	16,00	ALTO	EVITAR/TRANSFERIR	Formalizar Políticas de seguridad de información determinando la integridad y disponibilidad de la información	A.14.1.2 ASEGURAR LOS SERVICIOS DE APLICACIONES EN REDES PÚBLICAS	1	1	2,67	BAJO	ACEPTABLE
		Información incompleta	Ausencia de política de manejo de información	2,67	3	2	A.14.1.3 PROTECCIÓN DE LAS TRANSACCIONES DE SERVICIOS DE APLICACIONES	16,00	ALTO	EVITAR/TRANSFERIR	Formalizar Políticas de seguridad para evitar transmisiones incompletas o alteración no autorizada.	A.14.1.3 CONTROLES EN TRANSACIONES EN LÍNEA	1	1	2,67	BAJO	ACEPTABLE
A28	Oficinas de Sistemas, Administrativo/ Financiero	Acceso físico no autorizado	Falta de procedimientos para acceso a las Oficinas	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	18,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas de derecho de acceso a las instalaciones	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	1	1	3,00	BAJO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
		Desastre natural, incendio	Protección física no apropiada	3,00	1	2	A.18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	6,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar y aprobar políticas para la protección de las instalaciones	A.18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	1	2	6,00	MEDIO	ACEPTABLE
A29	Código Fuente	Daño causado por un tercero	Control inadecuado del acceso al código	3,00	3	1	A.14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	9,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas de derecho de acceso a los sistemas	A.14.2.1 POLÍTICA DE DESARROLLO SEGURO	1	1	3,00	BAJO	ACEPTABLE
A30	Sistemas Operativos	Abuso de privilegios de acceso	No revisión de privilegios de acceso	3,00	2	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	12,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas de derecho de acceso a los sistemas	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	1	1	3,00	BAJO	ACEPTABLE
A31	Firewall	Ataque de denegación de servicio	Sin protección de red interna y externa	3,00	3	2	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	18,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas de derecho de acceso a los equipos	A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	1	1	3,00	BAJO	ACEPTABLE
A32	Copias de Seguridad de los Sistemas de Información	Cambios no autorizados de registros	Pérdida de Datos	3,00	2	2	A.12.3.1 RESPALDO DE INFORMACIÓN	12,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas de seguridad de toda la información contenida en sistema Financiero	A.12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	1	1	3,00	BAJO	ACEPTABLE
		Comprometer información confidencial	Ataque malicioso de personal interno	3,00	3	2	A.12.4.2 PROTECCIÓN DE LA INFORMACIÓN	18,00	ALTO	EVITAR/TRANSFERIR	Formalizar y aprobar políticas de seguridad de toda la información contenida en sistema Financiero	A.12.4.2 PROTECCIÓN DE LOS REGISTROS DE INFORMACIÓN	1	1	3,00	BAJO	ACEPTABLE

EVALUACIÓN DE RIESGO									TRATAMIENTO DE RIESGOS							
No.	NOMBRE DE ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO	PROBABILIDAD		CONTROLES IMPLEMENTADOS EXISTENTES ISO/IEC 27002:2013	CÁLCULO DE EVALUACION RIESGO	NIVEL DE RIESGO	MÉTODO DE TRATAMIENTO DEL RIESGO	TIPO DE CONTROL	CONTROLES A IMPLEMENTAR ISO/IEC 27002:2017	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	CALCULO DE EVALUACIÓN RIESGO CON EL CONTROL IMPLEMENTADO	NIVEL DE RIESGO CON EL CONTROL IMPLEMENTADO	RIESGO RESIDUAL
				CID	Nivel de Amenaza	Nivel de Vulnerabilidad											
A33	Dispositivo Electrónico Biométrico Lector (huella digital)	Innovación Tecnológica	Denegación del servicio	3,00	2	1	A.8.1.3 USO ACEPTABLE DE LOS ACTIVOS	6,00	MEDIO	REDUCIR/TRANSFERIR	Formalizar los lineamientos para utilización de los recursos tecnológicos innovados	A.8.1.3 USO ACEPTABLE DE LOS ACTIVOS	1	1	3,00	BAJO	ACEPTABLE
		Desastre natural, incendio	Protección física no apropiada	3,00	2	2	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	12,00	ALTO	EVITAR/TRANSFERIR	Existe sistemas de protección de equipos en la mayoría instalados en el Instituto	A.11.2.1 UBICACIÓN Y PROTECCIÓN DE EQUIPOS	1	2	6,00	MEDIO	ACEPTABLE
A34	Intranet	Pandemia Covid 19	Fallas de conectividad	3,00	2	2	A.6.2.2 TELETRABAJO	12,00	ALTO	EVITAR/TRANSFERIR	Elaborar directrices, disposiciones y políticas de seguridad por esta modalidad	A.6.2.2 TELETRABAJO	1	2	6,00	MEDIO	ACEPTABLE
		Acceso al servicio por personas no autorizadas	No validación de los ID autorizados	3,00	2	2	A.9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	12,00	ALTO	EVITAR/TRANSFERIR	Formalizar procedimientos de autorización permitido al acceso de redes y servicios de red	A.9.2.4 GESTIÓN DE LA INFORMACIÓN CONFIDENCIAL DE AUTENTICACIÓN DE LOS USUARIOS	1	1	3,00	BAJO	ACEPTABLE