OFICINA POSGRADOS

Tema:

MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA INSTITUCIÓN FINANCIERA COOPERATIVA

Proyecto de investigación previo a la obtención del título de Magister en Gerencia Informática

Línea de investigación:

Seguridad de la información

Autor:

Carlos Efraín Arellano Veloz

Director:

Mg. Darío Javier Robayo Jácome

Ambato – Ecuador

Enero 2023

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA INSTITUCIÓN FINANCIERA COOPERATIVA

Línea de investigación:

Seguridad de la información

Autor:

Carlos Efraín Arellano Veloz

Darío Javier Robayo Jácome, Ing. Mg. f._____

CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f._____

CALIFICADOR

Verónica Maribel Pailiacho Mena, Ing. Mg. f._____

CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD. f._____

COORDINADOR DE LA OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
DIRECCIÓN CENTRO DE POSGRADOS Sede Ambato
Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL PROCURADURÍA
Pontificia Universidad Católica del Ecuador
BIBLIOTECA

Ambato – Ecuador

Enero 2023

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **CARLOS EFRAÍN ARELLANO VELOZ**, con CC. **180402811-4**, autor del trabajo de graduación intitulado: **"MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN UNA INSTITUCIÓN FINANCIERA COOPERATIVA"**, previa a la obtención del título profesional de **MAGISTER EN GERENCIA INFORMÁTICA**, en la oficina de POSGRADOS:

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la universidad.

Ambato, enero 2023

CARLOS EFRAÍN ARELLANO VELOZ

CC. 180402811-4

DEDICATORIA

A mi madre, su amor es la manifestación de la creación que inspira mi transitar.

A mi padre, quien ilumina mis pasos desde la eternidad.

A Mateo y Paula, mi corazón les pertenece.

A Ana, Carla y José David, su afecto es un aliciente.

A Sebastián y Alexo, su amistad resiste el tiempo, la distancia y el silencio.

AGRADECIMIENTO

Al arquitecto universal.

A la institución financiera que consolidó mi carrera profesional.

Al gerente general de la institución financiera.

A Darío Robayo, tutor del presente proyecto de investigación y desarrollo.

RESUMEN

Cualquier institución financiera que no disponga de un modelo de gestión de seguridad de la información, corre el riesgo de ser sancionada por el incumplimiento de la Ley relacionada con la protección de datos personales, sufrir el deterioro de su reputación organizacional e incluso paralizar sus operaciones tras sufrir un ataque cibernético. Por otro lado, la Superintendencia de Economía Popular y Solidaria exige que las instituciones bajo su control y supervisión regulen los niveles mínimos para la administración de la seguridad de la información con el fin de proteger sus activos de información y preservar su confidencialidad, integridad y disponibilidad. Este proyecto permite que la institución financiera cumpla con las regulaciones exigidas. El documento incorpora términos relacionados con privacidad de datos de carácter personal; emplea el cubo de McCumber para comprender los estados de la información y como estos están relacionados con los principios de la seguridad de la información; y utiliza *CIS Controls* como un conjunto de buenas prácticas que permite realizar el análisis de vulnerabilidades de los activos de información y definir las políticas de seguridad de la información con enfoque en defensa cibernética. La investigación es de campo, de tipo cuantitativa no experimental. El trabajo permite la implementación de un modelo de gestión de seguridad de la información basado en la norma ISO 27001 como parte del componente “procesos” del sistema de gobierno de seguridad de la información fundamentada en el modelo de gobierno de Cobit 2019.

Palabras clave: ISO 27001, *CIS Controls*, McCumber, Cobit.

ABSTRACT

Any financial institution that does not have an information security management model could be sanctioned for non-compliance with the Law related to the protection of personal data, suffer the deterioration of its organizational reputation and even paralyze its operations after suffering a cyberattack. On the other hand, the Superintendence of Popular and Solidarity-based Economy demands institutions under its control and supervision to regulate the minimum levels for the administration of information security to protect their information assets, preserving their confidentiality, integrity and availability. This project enabled the financial institution to comply with the required regulations. The document incorporates terms related to personal data privacy; uses The McCumber Cube to understand the status of information and how they relate to the principles of information security; and uses CIS Controls as a set of good practices that allow the analysis of vulnerabilities of information assets and the definition of information security policies with a focus on cyber defense. The research is field-based, quantitative and non-experimental. The work allowed the implementation of an information security management model based on the ISO 27001 standard as part of the "processes" component of the information security governance system based on the Cobit 2019 governance model.

Keywords: ISO 27001, CIS Controls, The McCumber Cube, Cobit 2019.

ÍNDICE

PRELIMINARES
DECLARACIÓN DE AUTENCIDAD iii
DEDICATORIA iv
AGRADECIMIENTO v
RESUMEN vi
ABSTRACT vii
INTRODUCCIÓN ix
CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA 10
1.1. Información 10
1.2. Sistema de gestión de seguridad de la información 16
1.3. Revisión de trabajos de investigación que emplean la ISO 27001 24
CAPÍTULO II. DISEÑO METODOLÓGICO 29
2.1. Caracterización de la empresa o institución 29
2.2. Metodología de investigación 32
2.3. Propuesta de investigación 33
CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN 83
3.1. Antecedentes 83
3.2. Evaluación final 84
CONCLUSIONES 91
RECOMENDACIONES 92
BIBLIOGRAFÍA 93
ANEXOS 100

ÍNDICE DE TABLAS

Tabla 1. Número de noticias del delito 2
Tabla 2. Segmentación de entidades del SFPS, año 2022 30
Tabla 3. Cumplimiento total de las cláusulas del SGSI 35
Tabla 4. Controles del Anexo A que están o no están implementados 35
Tabla 5. Determinación del riesgo inherente y riesgo intrínseco 40
Tabla 6. Resumen del inventario de activos de información 44
Tabla 7. Cumplimiento total de las cláusulas del SGSI 87
Tabla 8. Controles del Anexo A que están o no están implementados 87

ÍNDICE DE CUADROS

Cuadro 1. Integrantes del sistema de protección de datos personales 13
Cuadro 2. Estructura de la norma ISO 27001:2013 18
Cuadro 3. Modelo de madurez genérico según Cobit 4.1 22
Cuadro 4. Comparativo de proyectos con el estándar ISO 27001 27
Cuadro 5. Mapa general de procesos 31
Cuadro 6. Interrogantes para documentar las entidades y tipos de información..... 38
Cuadro 7. Tipos de información de la entidad socio..... 39
Cuadro 8. Confidencialidad e integridad de la entidad socio..... 41
Cuadro 9. Ficha para el inventario de activos de información 44
Cuadro 10. Resumen de activos de información 45
Cuadro 11. Canales de atención 49
Cuadro 12. Relación 1, servicio, disponibilidad del servicio y canal..... 50
Cuadro 13. Relación 2, confidencialidad e integridad del servicio..... 51
Cuadro 14. Confidencialidad, integridad y disponibilidad de los servicios..... 52
Cuadro 15. Relación 3, canales y tipos de información..... 53
Cuadro 16. Confidencialidad, integridad y disponibilidad de los canales 53
Cuadro 17. Relación 4, disponibilidad de las aplicaciones con los canales 54
Cuadro 18. Relación 5, confidencialidad e integridad de las aplicaciones y canales 54
Cuadro 19. Confidencialidad, integridad y disponibilidad de las aplicaciones..... 55
Cuadro 20. Relación 6, disponibilidad de servidores con las aplicaciones..... 56
Cuadro 21. Relación 7, confidencialidad e integridad de servidores y aplicaciones.. 56
Cuadro 22. Confidencialidad, integridad y disponibilidad de los servidores 57
Cuadro 23. Relación 8, disponibilidad bases de datos con las aplicaciones 58
Cuadro 24. Relación 9, confidencialidad e integridad bases de datos y aplicaciones58
Cuadro 25. Confidencialidad, integridad y disponibilidad de las bases de datos 58
Cuadro 26. Análisis de vulnerabilidades del servidor de base de datos..... 60
Cuadro 27. Plan de acción para mitigación de vulnerabilidades 63
Cuadro 28. Plan de implementación de política de seguridad..... 78

ÍNDICE DE GRÁFICOS

Gráfico 1. Ejemplo de titular, responsable y encargado 14
Gráfico 2. Beneficios del SGSI 17
Gráfico 3. Principios de *CIS Controls* 20
Gráfico 4. Controles macro de la versión 7.1 *CIS Controls* 21
Gráfico 5. Rangos de calificación del modelo genérico de madurez de Cobit 4.1 23
Gráfico 6. Partes interesadas 37
Gráfico 7. Las tres dimensiones del Cubo de McCumber 46
Gráfico 8. Relación servicio, canales, aplicaciones, servidores y base de datos 48
Gráfico 9. Componentes del sistema de gobierno de seguridad de la información ... 67
Gráfico 10. Modelo de GSI 69
Gráfico 11. Estructura del sistema de gobierno de SI 70
Gráfico 12. Nivel inicial y final de madurez de SI (primera sección) 89
Gráfico 13. Nivel inicial y final de madurez del cumplimiento del Anexo A 90

INTRODUCCIÓN

La innovación en el ámbito de las tecnologías de la información y comunicación requiere que las organizaciones enfrenten riesgos relacionadas con la protección de su información. A la par de esta constante producción de tecnología, las amenazas representadas –especialmente- por la delincuencia cibernética, más otras omisiones cometidas por los responsables de la información, generan ausencias que van desde la paralización parcial de las operaciones –en el mejor de los casos- hasta el cierre definitivo de la organización.

Hablar de omisiones es enfatizar en los errores frecuentes en seguridad de la información, que parten desde el empleo de contraseñas poco seguras, hardware y software obsoletos, ausencia de respaldos de información hasta no incluir cláusulas de confidencialidad en los contratos establecidos con los proveedores.

A raíz de la pandemia del coronavirus, las organizaciones dedicadas a la prestación de servicios, con el propósito de mantener sus operaciones, aplicaron métodos de teletrabajo y el despliegue de importantes sistemas de información que permiten –hasta hoy- interactuar con sus clientes. Las instituciones del sistema financiero, tanto públicas como privadas, trasladaron su esencia, representada en la captación y colocación de recursos, a plataformas tecnológicas para que sus clientes accedan a servicios de ahorro y crédito que generalmente tienen una atención presencial.

La emergencia sanitaria replanteó los mecanismos de las principales actividades de las organizaciones, sin embargo, los riesgos por intromisiones no autorizadas a estas plataformas, el robo de información de carácter confidencial, entre otras, se duplicaron considerablemente.

Reportes de información como el ESET *Security Report* Latinoamérica 2022 considera que “los eventos (…) que marcaron al año 2021 en materia de ciberseguridad y cibercrimen en el ámbito corporativo fueron los grandes ataques y

caídas de bandas de *ransomware*, las vulnerabilidades de gran criticidad y presencia como *Log4Shell* y el aumento desmedido de ataques que utilizan la modalidad de afección a la cadena de suministros" (ESET, 2022, pág. 2). El mismo reporte señala que los países con la mayor cantidad de hallazgos son: 1) Perú (18%); 2) México (17%); 3) Colombia (12%); 4) Argentina (11%); y, 5) Ecuador (9%).

Es posible asegurar que desde el año 2019 los delitos informáticos crecieron exponencialmente en Ecuador, según cifras de la Fiscalía General del Estado (FGE). Es así como los principales delitos son: 1) estafa, 2) apropiación fraudulenta por medios electrónicos, 3) violación a la intimidad, 4) acceso no consentido a un sistema informático, telemático o de telecomunicaciones, 5) ataque a la integridad de sistemas informáticos, 6) comercialización ilícita de terminales móviles, 7) transferencia electrónica de activo patrimonial, 8) interceptación ilegal de datos y 9) revelación ilegal de base de datos.

La tabla 1 presenta el número de noticias del delito comprendidas entre el 01/01/2019 y 31/08/2022:

Tabla 1. Número de noticias del delito

Delito	2019	2020	2021	2022	Total
C.O.I.P. Art. 190.- Apropiación fraudulenta por medios electrónicos.	830	1469	2779	1320	6398
C.O.I.P. Art. 178.- Violación a la intimidad.	921	1056	883	773	3633
C.O.I.P. Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	133	181	196	151	661
C.O.I.P. Art. 232.- Ataque a la integridad de sistemas informáticos.	57	60	62	114	293
C.O.I.P. Art. 230.- Interceptación ilegal de datos.	52	42	43	40	177
C.O.I.P. Art. 229.- Revelación ilegal de base de datos.	18	19	20	41	98
Total	2011	2827	3983	2439	11260

Fuente: modificado a partir de Fiscalía General del Estado (2022)

En el año 2019, el allanamiento de una reconocida empresa de venta de datos personales evidenció una lucrativa actividad que consistía en la recopilación de importantes bases de datos que permitían conocer la situación socioeconómica de

millones de ecuatorianos. Estos repositorios incluyen datos relacionados con el comportamiento crediticio, datos de instituciones públicas como, por ejemplo, SRI, IESS, Registro Civil, entre otras. Las motivaciones de estas claras violaciones son: 1) la ausencia de un sistema de gestión de seguridad de la información, 2) una legislación vigente que no entiende la realidad de la seguridad en el ámbito de la tecnología; y, 3) omisiones cometidas por parte de los custodios de los activos de información.

En octubre de 2021, Banco Pichincha padeció el mayor ataque informático que reportó una institución financiera (IFI) en Ecuador. Este ataque inhabilitó parte de los principales servicios de la entidad, lo que imposibilitó a millones de clientes de la IFI acceder a los servicios requeridos. Aunque la institución financiera afirmó, a través de varios comunicados de prensa, que la afectación a sus servicios no inhabilitó la red de cajeros automáticos ni los pagos con tarjetas de débito/crédito, las quejas mediante las redes sociales evidenciaron que el banco emitió un falso mensaje.

Al inicio del incidente, Banco Pichincha negó en reiteradas ocasiones que el ataque sufrido estaba relacionado con un secuestro de información –*ransomware*-. Pero, el portal *BleepingComputer* desmintió al banco. Posteriormente, ante la Comisión de Desarrollo Económico de la Asamblea Nacional del Ecuador, la ex superintendenta de Bancos, Ruth Arregui, afirmó que el banco sufrió “un acto delictivo, imprevisto e irresistible, cometido por atacantes expertos y conocidos a nivel internacional” (Diario El Universo, 2021).

A pesar de que el banco aseguró que el ataque no afectó su funcionamiento financiero, se incumplió con la disponibilidad de los servicios. La institución financiera tardó varios días en recuperar la normalidad de sus operaciones. Como consecuencia, la IFI perdió clientes que migraron a otras instituciones financieras de características similares.

El 14 de julio de 2021, la Corporación Nacional de Telecomunicaciones (CNT) sufrió un ataque informático. Pocos días después, fue declarada la emergencia en la empresa pública. Todo apuntó a que la CNT sufría un ataque de *ransomware* que inhabilitó los servicios de facturación, activaciones y recargas electrónicas. Posteriormente, todos los empleados fueron obligados a apagar sus estaciones de trabajo. Aunque la CNT mantiene vigente un sistema de seguridad de la información, es posible destacar que esta intromisión a sus sistemas, ocurrió –especialmente- por las omisiones cometidas por humanos que representan el eslabón más débil de la seguridad de la información.

La Superintendencia de Economía Popular y Solidaria (SEPS), se anticipó a los incidentes cibernéticos en su ámbito de control, entonces, en agosto de 2021, emitió un oficio que incluía una serie de recomendaciones para promover en las entidades financieras mejores prácticas que permitan resguardar la información de los socios y clientes.

El oficio señala que “bajo la coyuntura actual, en la que la pandemia mundial del COVID-19 ha marcado un punto de inflexión, la dependencia de la infraestructura tecnológica, la transformación digital de las economías, las transacciones y el acceso a plataformas móviles de servicios financieros, han experimentado una aceleración. (…) De acuerdo con lo anterior, es prácticamente un hecho que los ataques cibernéticos, el cibercrimen y los incidentes de seguridad no van a disminuir; por el contrario, aumentarán de forma exponencial en los próximos años” (SEPS, 2021, pág. 1).

El oficio circular Nro. SEPS-SGD-IGT-2021-21112-OFC, incluye una serie de recomendaciones como:

1. Inventariar los activos de información.
2. Clasificar la información.
3. Analizar y evaluar los riesgos de las aplicaciones, servicios y activos.
4. Identificar los procesos críticos.

5. Respaldar y resguardar la información sensible.
6. Generar una cultura de seguridad de la información y ciberseguridad dentro de la entidad.
7. Elaborar y ejecutar planes de contingencia, con procesos y procedimientos a ejecutarse.

Toda organización -sin importar el fin que persigue-, genera, almacena y transmite información. Este proceso en sí es parte del ciclo de vida de la información. Por tanto, el objetivo de un modelo de gestión de seguridad de la información es consolidar un conjunto de controles que permitan a las organizaciones proteger su información en todos sus estados. Sin un procedimiento que reconozca cuál es la información que representa el activo intangible de la organización, resulta inapropiado pretender custodiar lo desconocido.

Al dictar esta serie de siete recomendaciones, es evidente que la SEPS lo hizo -al menos- apegado a una normativa de seguridad de la información que permite plantear un modelo que proteja los activos de información. Para el año 2022, la Superintendencia emitió una nueva resolución en la que exige a todas las instituciones financieras de la economía popular y solidaria regular sus niveles mínimos para la administración de la seguridad de la información, con el fin de resguardar y proteger sus activos de información; y, preservar su confidencialidad, disponibilidad e integridad.

A finales de 2021, en un primer diagnóstico realizado en la institución financiera cooperativa (IFC), se evidencia una serie de omisiones que ponen en riesgo la seguridad de la información. En este análisis -que es actualizado al inicio de este proyecto de desarrollo-, se determina un inexistente nivel de maduración de la seguridad de la información. Estas desatenciones, por ejemplo, van desde la ausencia en la definición de los responsables de la seguridad de la información hasta la inexistencia de políticas claras que impiden establecer una estructura

organizacional que persiga preservar la confidencialidad, integridad y disponibilidad de la información.

Entonces, por ejemplo, al no contar con al menos un responsable de la seguridad de la información, una de las consecuencias de estas omisiones es la ausencia de una metodología que permita realizar los procedimientos concernientes al inventario de los tipos de información; a más del análisis de vulnerabilidades de los activos de información. Por tanto, no es posible proteger la información de una organización si esta desconoce cuál es la información que genera, almacena y transmite.

El citado diagnóstico preliminar evidenció que la institución incumplió con el principio de la confidencialidad (la confidencialidad, la integridad y la disponibilidad son los tres pilares de la seguridad de la información). Por ejemplo, los empleados, al aprovechar la ausencia de controles en el “Core financiero”, acceden a la información de los socios de la cooperativa.

Estas intromisiones son posibles porque la institución no cuenta con un área de seguridad de la información que pertenezca al segundo nivel del modelo de gobierno de las tres líneas de defensa, difícilmente, las áreas operativas que están en el primer nivel incorporan mecanismos que permitan cumplir con los tres principios ya citados. Incluso, es imposible identificar si la IFC sufrió el robo de información por parte de sus empleados. Si esto ocurrió, ¿qué información fue sustraída?, ¿es sensible la información?, ¿la información fue entregada a otra institución financiera de características similares?

Por otra parte, la ausencia de una cultura de seguridad de la información no solo pone en riesgo los activos de información de la institución financiera cooperativa, también supone un impacto considerable en la operación de la organización. La concientización no es un evento que pretenda custodiar –exclusivamente- la confidencialidad de la información. Busca, por un lado, crear una cultura que reduzca las omisiones por parte de los empleados de la organización, por ejemplo, evitar el

ingreso de *malware*, impedir –en lo posible- los ataques informáticos, entre otras. Por otro lado, exige que el éxito de un modelo de seguridad de la información sea una corresponsabilidad entre socios, proveedores, directivos y empleados que constituyen las partes interesadas.

Con estos antecedentes es necesario formular la pregunta: ¿existe alguna normativa internacional que permita resguardar y proteger los activos de información de una institución financiera cooperativa y preservar su confidencialidad, disponibilidad e integridad? Sí, existen varias normativas internacionales que permiten establecer un modelo de gestión de seguridad de la información.

Para la implementación del modelo de gestión de seguridad de la información, se emplea la normativa internacional ISO 27001. La investigación es de campo, de tipo cuantitativa no experimental. El proyecto de desarrollo está realizado en la oficina matriz de la institución financiera cooperativa. La observación, la entrevista y la encuesta son las técnicas empleadas para cumplir con los fines específicos.

Para cumplir con un tema normativo exigido por la SEPS, es necesario alcanzar la consecución de los siguientes objetivos específicos:

1. Verificar el estado del arte de la normativa internacional ISO 27001 y su aplicación.
2. Diagnosticar el cumplimiento de la normativa internacional ISO 27001 en la institución financiera cooperativa.
3. Establecer un modelo de gestión de la seguridad de la información basado en la normativa internacional ISO 27001.
4. Implementar el modelo de gestión de la seguridad de la información en la institución financiera cooperativa.

La consecución de los cuatros objetivos específicos exige cumplir con las siguientes actividades:

1. Recolección bibliográfica del estado del arte.
2. Diagnóstico de la situación actual de la institución financiera cooperativa.
3. Clasificación de los tipos de información e información crítica.
4. Inventarios de activos de información críticos, identificados y clasificados.
5. Análisis de amenazas y vulnerabilidades de activos de información.
6. Implementación del marco de referencia.

El objetivo principal de este proyecto de desarrollo es:

1. Evaluar la implementación del Modelo de Gestión de la Seguridad de la Información basado en la norma ISO 27001 en una institución financiera cooperativa.

Más allá de las exigencias impuestas por el organismo de control, la implementación de un modelo de gestión de seguridad de la información permite a la organización establecer mecanismos para la atención oportuna de ataques cibernéticos, lo que permite resguardar la información que representa el activo esencial de la IFC.

Pero, al mismo tiempo, la implementación del modelo facilita a la cooperativa cumplir con otras regulaciones vigentes como la “Ley de Protección de Datos Personales”. Si la IFC cumple con las obligaciones emitidas por el organismo de control, cumple con otras regulaciones de mayor jerarquía e implementa prácticas reconocidas a nivel internacional, entonces es posible: 1) generar valor agregado a la operación, 2) afianzar la confianza de las partes interesadas y 3) constituir a la organización en un referente del sector de la economía popular y solidaria.

A diferencia de otros proyectos de desarrollo de características similares que cumplen objetivos afines, a través de esta investigación, se incorporan términos de un sistema de gobierno de seguridad de la información basado en *Cobit* 2019 y, la implementación de *CIS Control* Versión 7.1 para: 1) analizar las vulnerabilidades de los activos de información y 2) definir parte de las políticas de seguridad de la información.

Las normativas ISO están enfocadas a los requisitos que las organizaciones requieren cumplir, pero omiten la forma en cómo cumplir con el objetivo. Por tanto, *CIS Control* permite implementar varios de los controles que están descritos en el Anexo A de la normativa ISO 27001. Revisar: 1) el anexo 5 del proyecto de desarrollo describe cómo implementar varios de los controles contenidos en el Anexo A mediante *CIS Controls*; 2) sección “Componentes: principios, políticas y procedimientos; y, personas, habilidades y competencias” del capítulo II.

Finalmente, este proyecto pretende ser una guía general que facilite a otras organizaciones afines implementar el modelo de gestión de seguridad de la información.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Información

Un dato “es la expresión general que describe aquellas características de la entidad sobre la que opera” (Concepto, s.f.). A diferencia de la información que representa un “(…) conjunto de datos con un significado (…) que reduce la incertidumbre o (…) aumenta el conocimiento de algo” (Chiavenato, 2006, pág. 365).

Los estados de la información, según el cubo de *McCumber*, hacen referencia “específicamente a los diferentes estados en que la información puede residir en un sistema y toda la gama de las salvaguardas de seguridad disponibles que deben ser considerados en el diseño“ (Copro, s.f.). Los estados de la información son: 1) procesamiento, 2) almacenamiento y 3) trasmisión.

El procesamiento (1) es la generación/utilización de la información con el fin de cumplir un objetivo específico. El almacenamiento (2) es la forma en cómo la información está guardada. Los datos correctamente estructurados tienen como destino una base de datos relacional. A diferencia de los datos no estructurados que tienen como destino una infinidad de bases de datos no relacionales representadas en hojas electrónicas de cálculo, archivos planos y más. Finalmente, la trasmisión (3) que es la “transferencia de datos entre sistemas de información” (Copro, s.f.).

Los distintos estados de la información permiten entender la importancia que tiene la información en cada uno de estos. Al visibilizarlos, los procesos internos de las organizaciones están en capacidad de identificar si la información –generada, almacenada y transmitida- requiere de protección, es decir, conocer en qué estados es necesario protegerla.

En términos contables, un activo es un “conjunto de bienes y derechos de los que es titular un empresario o una empresa (…) y que deben reflejarse en el balance” (Real

Academia Española, s.f.). La información, al igual que un bien, es un activo más de la empresa.

Un activo de información es “(el) elemento de información que se recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre en forma impresa (…), trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes” (Superintendencia de Industria y Comercio de Colombia, pág. 2).

Seguridad de la información

La Real Academia Española (RAE) define a la palabra “seguridad” como la “cualidad de seguro” (Real Academia Española, s.f.). De igual manera, la RAE hace referencia al término “de seguridad” como un “mecanismo que asegura su mejor funcionamiento” (Real Academia Española, s.f.). La relación entre “de seguridad” e “información” es entendida como los mecanismos que otorgan a la información una cualidad de seguro.

El principal objetivo de la seguridad de la información es proteger el principal activo intangible de las organizaciones: su información. Esto, es alcanzado mediante el establecimiento de un conjunto de políticas, procedimientos y controles que permita garantizar los tres principios fundamentales de la SI que son: 1) confidencialidad, 2) integridad y 3) disponibilidad.

La 1) confidencialidad es la protección que impide la divulgación no autorizada de la información. La 2) integridad es la protección que impide la modificación o eliminación de la información sin autorización. Finalmente, la 3) disponibilidad es la garantía de que la información esté disponible si las personas autorizadas lo requieran.

Confidencialidad y privacidad

Los fundamentos de la seguridad de la información representan conceptos relativamente simples de entender, pero proteger la información es un gran desafío. Al hablar de confidencialidad, el mayor reto es garantizar la privacidad de la información.

Aunque la confidencialidad y privacidad están relacionadas, su aplicación es totalmente distinta. Para entender esta afirmación, es necesario conceptualizar la información como un todo, categorizarla e identificar qué información es de carácter personal, por ejemplo, direcciones de correo electrónico, números de teléfono, números de identificación, entre otros. El ejercicio planteado permite entender que la confidencialidad es la "estrategia de protección aplicable a toda la información sin importar la categoría (a la que esté) asignada" (Muñoz, 2018). A diferencia de la privacidad que establece un conjunto de estrategias que permiten proteger los datos personales contra la divulgación no autorizada.

El artículo 66, numeral 19 de la Constitución de la República de Ecuador, establece "el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".

En mayo de 2021, la Asamblea Nacional de Ecuador aprobó la Ley Orgánica de Protección de Datos Personales (LOPDP) que garantiza "el derecho a la protección de datos personales, que incluye el acceso y decisión sobre la información y datos de este carácter, así como su correspondiente protección" (Naranjo Martínez&Subía, 2021).

Sin importar que los activos de información sean un bien intangible de las organizaciones, la legislación nacional otorga la calidad de titular de la información al

dueño de la información personal. La LOPDP manifiesta que un dato personal es un "dato que identifica o hace identificable a una persona natural, directa o indirectamente" (Asamblea Nacional del Ecuador, 2021, pág. 7).

La confidencialidad, en el mismo cuerpo legal, es el "tratamiento de datos personales (que) debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos" (Asamblea Nacional del Ecuador, 2021, pág. 11).

Al nivel de la protección de datos personales, la LOPDP identifica cuatro actores clave: 1) titular, 2) responsable, 3) delegado de protección de datos) y el 4) encargado. El cuadro 1 describe las funciones que cumple cada uno de los actores claves identificados en la Ley.

Cuadro 1. Integrantes del sistema de protección de datos personales

Actor	Función
Titular	Persona natural cuyos datos son objeto de tratamiento.
Responsables	Persona natural o jurídica, pública o privada, autoridad, u otro organismo, que solo o juntamente con otros decide sobre la finalidad y el tratamiento de datos personales.
Delegado de protección de datos	Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto.
Encargado	Persona natural o jurídica, pública o privada, autoridad, u otro organismo que solo o juntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.

Fuente: tomado a partir de Asamblea Nacional del Ecuador (2021)

El gráfico 1 ejemplifica un caso que permite comprender la función que cumplen el titular, el responsable y el encargado.

Gráfico 1. Ejemplo de titular, responsable y encargado

Fuente: elaboración propia

El capítulo VI de la LOPDP describe las medidas de control que requieren cumplir las organizaciones para garantizar la confidencialidad, integridad y disponibilidad. El mencionado capítulo incluye: la protección de datos personales desde el diseño y por defecto; análisis de riesgo, amenazas y vulnerabilidades, evaluación de impacto del tratamiento de datos personales; notificación de vulnerabilidad de seguridad; acceso a datos personales para atención a emergencias e incidentes informáticos; y, la notificación de vulneración de seguridad al titular. El capítulo XI, describe las multas o sanciones por el incumplimiento o tratamiento inadecuado de los datos de carácter personal.

Las entidades públicas y privadas tienen dos años para iniciar los procesos internos de adaptación a la LOPDP, el plazo vence el próximo 22 de mayo de 2023. Para cumplir con las obligaciones establecidas en la Ley, es posible complementar la implementación de la ISO 27001 con la norma ISO 27701. La última normativa mencionada “es una extensión de la ISO 27001 en materia de privacidad de datos” (DNV, s.f.). Norma que “(…) adopta un enfoque integral de la gestión de la privacidad de la información y permite a las organizaciones cumplir los requisitos de protección de información personal” (DNV, s.f.).

Integridad

Un error frecuente es considerar que la seguridad de la información abarca la protección exclusiva de la información lógica. La seguridad es transversal, es decir, no comprende únicamente la seguridad perimetral, también, resguarda la información almacenada en repositorios digitales (base de datos relacionales y no relacionales), repositorios físicos de documentos, incluso, la protección del conocimiento.

Para mantener -en lo posible- la integridad de la información lógica, es necesario limitar “los permisos de los usuarios sobre la información y reducirlos a los sistemas que la soportan a los mínimos indispensables” (Banco Santander S.A., s.f.). Este concepto tiene relación con el principio del mínimo privilegio que restringe el acceso a un mínimo nivel para que los usuarios -sin tener afectación-, cumplan con sus obligaciones. Pero esta definición, también, extiende su aplicación a hardware y software que no requieren una interacción frecuente con los humanos para cumplir con las actividades que demanda la organización. Este principio permite reducir la superficie expuesta a ataques cibernéticos, detener la propagación de los programas malignos y mejorar la productividad de los usuarios internos.

El mínimo privilegio es una de las prácticas de seguridad de *Identity and Access Managment* (IAM) que incluye recomendaciones tales como: evitar la utilización del usuario *root*, cambiar periódicamente las contraseñas de acceso a hardware y software, generar políticas lógicas de contraseñas robustas, crear roles para asignar permisos específicos, emplear mecanismos de autenticación multi factor y generar alertas si el usuario *root* está en uso.

Disponibilidad

Otro error de conceptualización -muy frecuente- es considerar que la disponibilidad es el acceso exclusivo a la información. *Cobit* 4.1 indica que “la disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos

del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas" (IT Governance Institute, 2007, pág. 11).

Los procesos de las organizaciones están soportados por un importante despliegue de servicios que permiten generar, almacenar y transmitir información. Por tanto, es posible concebir a la disponibilidad como el "grado en que un sistema o equipo se encuentra en condiciones operables al ser llamado en un momento determinado" (Covarrubias, 2015).

1.2. Sistema de gestión de seguridad de la información

Un sistema de gestión de seguridad de la información (SGSI) es un conjunto de políticas y procedimientos que permiten a las organizaciones proteger sus activos intangibles, es decir, sus activos de información. "La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica (…). El establecimiento y la implementación del (…) (SGSI) están influenciados por las necesidades y objetivos (…), los requisitos de seguridad, los procesos utilizados (…) y el tamaño y estructura de la organización" (Servicio Ecuatoriano de Normalización (INEN), 2017, pág. iii).

Su principal objetivo es garantizar el cumplimiento de tres principios básicos que están representados por la confidencialidad, integridad y disponibilidad. La ausencia de un SGSI genera pérdidas financieras, sanciones económicas por el incumplimiento de leyes relacionadas con la protección de datos personales, deterioro de la reputación organizacional, incluso, la paralización parcial o total de las operaciones de la organización. El gráfico 2 describe algunos de los beneficios de mantener vigente un SGSI.

Gráfico 2. Beneficios del SGSI

Fuente: modificado a partir de ISOTools (s.f.)

¿Qué es la norma ISO 27001?

El estándar internacional ISO 27001 "(…) permite el aseguramiento (de) la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan" (International Dynamic Advisors, 2014).

La norma ISO 27001 está compuesta por la introducción, diez capítulos, un anexo y la bibliografía. El cuadro 2 describe brevemente las secciones del citado estándar.

Cuadro 2. Estructura de la norma ISO 27001:2013

Capítulo	Descripción
1. Objeto y campo de aplicación	Uso, finalidad y método de aplicación de la normativa.
2. Referencias normativas	Revisión de documentos indispensables para la aplicación del estándar.
3. Términos y definiciones	Terminología aplicable al estándar.
4. Contexto de la organización	Conocimiento de la organización y su contexto, la compresión de las necesidades y expectativas de las partes interesadas; y, la determinación del alcance del SGSI.
5. Liderazgo	Necesidad de que los empleados de la organización contribuyan a la implementación de la normativa.
6. Planificación	Importancia de la identificación de riesgos y oportunidades de mejora al momento de implementar el SGSI, así como el establecimiento de los objetivos de la seguridad de la información y la forma de cómo alcanzarlos.
7. Soporte	Para el buen funcionamiento del SGSI, la organización cuenta con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.
8. Operación	Para cumplir con los requisitos de seguridad de la información, es necesario planificar, implementar y controlar los procesos de la organización; hacer una valoración de los riesgos de la seguridad de la información y un tratamiento de ellos.
9. Evaluación del desempeño	Establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del SGSI, para asegurar que funciona según lo planificado.
10. Mejora	Obligaciones que tiene una organización si encuentra una “no conformidad” y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.

Fuente: tomado a partir de ISOTools (s.f.)

El Anexo A es parte del estándar 27001. Este representa un conjunto de controles de seguridad específicos que buscan mejorar la seguridad de la información. La implementación de la normativa requiere la aplicación de todos los controles, excepto los que no son aplicables a la organización porque su giro de negocio no lo requiere.

El citado anexo describe 114 controles clasificados de la siguiente manera: A.5 política de seguridad de la información, A.6 organización de seguridad de la información, A.7 seguridad en recursos humanos, A.8 gestión de activos, A.9 control de acceso, A.10 criptografía, A.11 seguridad física y del entorno, A.12 seguridad de las operaciones, A.13 seguridad en las comunicaciones, A.14 adquisición, desarrollo y mantenimiento del sistema, A.15 relaciones con proveedores, A.16 gestión de

incidentes de seguridad de la información, A.17 aspectos de seguridad de la información para la gestión de la continuidad del negocio y A.18 cumplimiento. El anexo 1 describe cada uno de los sub-controles del Anexo A.

Se entiende como control “a todo aquel sistema que tiene la posibilidad de responder a una señal o entrada al sistema y producir un efecto deseado” (Sánchez, s.f.). En otras palabras, es la implementación de políticas que permiten cumplir un objetivo específico.

En resumen, el estándar está conformado por: 14 dominios, 35 objetivos de control y 114 controles. Varios de los controles descritos en el Anexo A del estándar ISO 27001 logran implementarse a través de *CIS Controls*.

CIS Controls

Los Controles de Seguridad Críticos, conocidos como *CIS Controls*, son un conjunto de buenas prácticas desarrolladas por el *Center for Internet Security*. Esta guía contiene recomendaciones relacionadas con la ciberseguridad y a la ciberdefensa.

Los controles, se “nutren (…) de ataques reales y defensas efectivas (…) (que) reflejan el conocimiento combinado de expertos de cada parte del ecosistema (empresas, gobiernos, individuos); con cada rol (…) y dentro de muchos sectores (gobierno, poder, defensa, finanzas, transporte, academia, consultoría, seguridad, TI) que se han unido para crear, adoptar y respaldar los Controles” (Center for Internet Security (CIS), s.f., pág. 6).

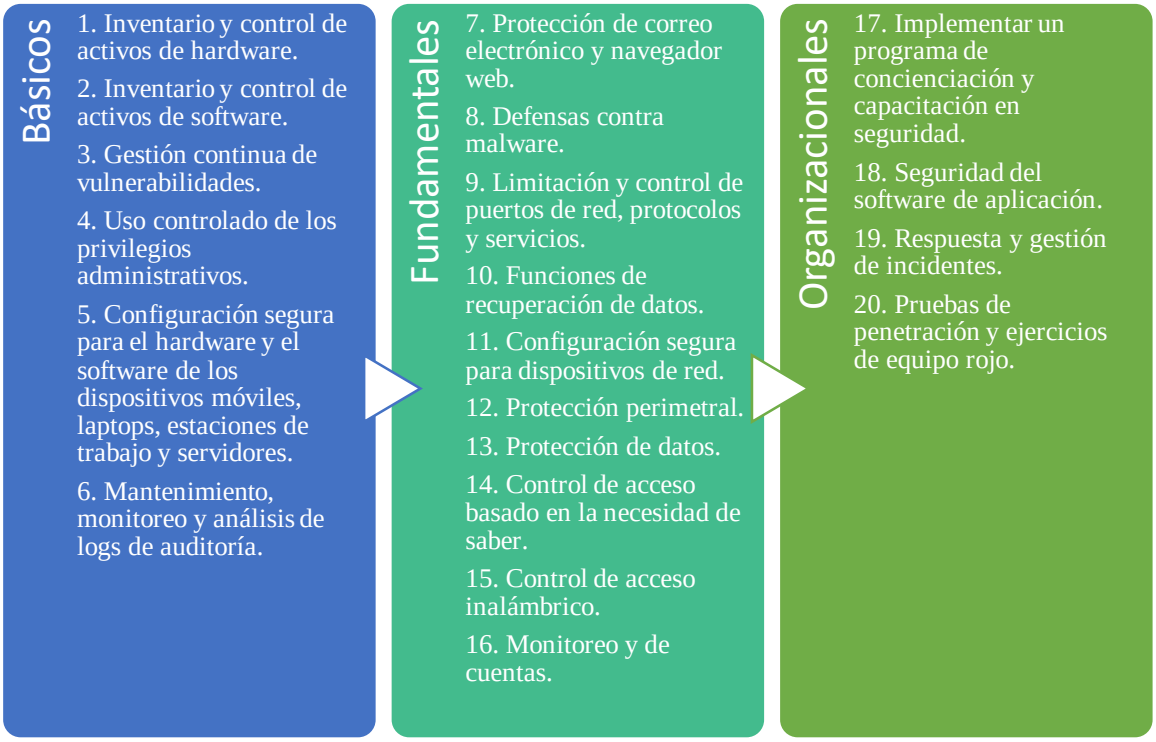
Los cinco principios de *CIS Controls* son: 1) "la ofensa informa a la defensa", 2) priorización, 3) mediciones y métricas, 4) diagnóstico y mitigación continuos y 5) automatización. El gráfico 3 describe brevemente cada uno de los cinco principios citados.

Gráfico 3. Principios de *CIS Controls*

Fuente: modificado a partir de ISEC Auditors (2019)

La versión 7.1 de *CIS Controls* comprende un conjunto de 20 controles macros divididos en tres categorías: 1) básicos, que corresponden a controles aplicables para cualquier organización; 2) fundamentales, que representan controles para el almacenamiento de información sensible; y, 3) organizacionales, que son controles para el almacenamiento de información muy sensible. Cada uno de estos controles, al igual que el Anexo A del estándar ISO 27001, está dividido en varios subcontroles. El gráfico 4 describe los subcontroles que conforman cada uno de los controles macros.

Gráfico 4. Controles macro de la versión 7.1 *CIS Controls*



Fuente: modificado a partir de *Center for Internet Security* (s.f.)

El anexo 2, describe los subcontroles que conforman cada uno de los controles macro.

Nivel de madurez de seguridad de la información

El (IT Governance Institute, 2007) reflexiona en la necesidad “de (que) toda empresa (...) (requiere) entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar” (pág. 17). Por otro lado, el término madurez, es definido como el “estado de una cosa que ha alcanzado su pleno desarrollo, o de una persona que ha alcanzado su mejor momento en algún aspecto”. Al relacionar la premisa planteada en *Cobit* 4.1 con el término madurez, es posible entender que toda organización requiere conocer el estado de maduración de sus propios sistemas al momento de evaluarlos con una serie de objetivos descritos en alguna normativa.

El estándar internacional *Cobit* 4.1 considera que “el modelo de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5)” (IT Governance Institute, 2007, pág. 17). El cuadro 3 describe el modelo de madurez genérico propuesto por *Cobit* 4.1.

Cuadro 3. Modelo de madurez genérico según Cobit 4.1

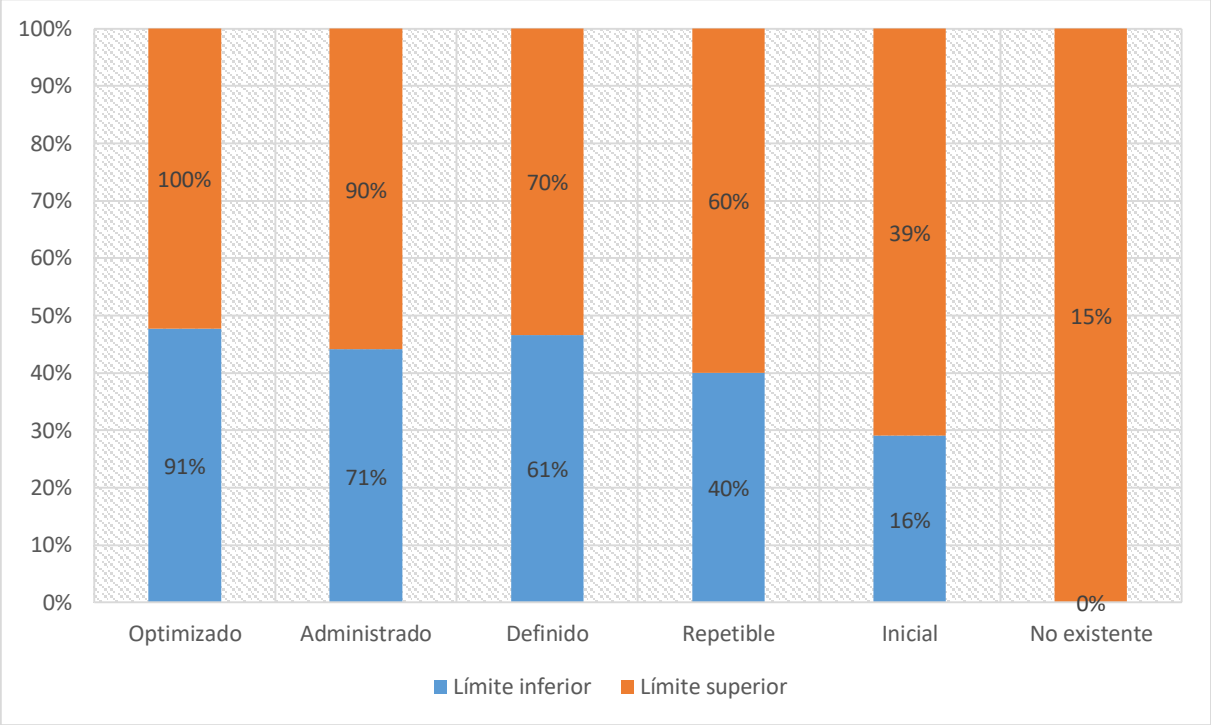
Nivel	Descripción
0 no existente	Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1 inicial	Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2 repetible	Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 definido	Los procedimientos están estandarizados y documentados, y están difundidos a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados, pero formalizan las prácticas existentes.
4 administrado	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas si los procesos no trabajan de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5 optimizado	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindar herramientas para mejorar la calidad y la efectividad, lo que permite que la empresa se adapte de manera rápida.

Fuente: tomado a partir de *IT Governance Institute* (2007)

A través del proyecto titulado “Identificación del estado de madurez y diseño de controles para la implementación de un sistema de gestión de seguridad de la información en el proceso TIC de Estrategias Empresariales de Colombia S.A.S.” de (Pérez Torres, 2018), propone utilizar el modelo genérico de madurez de *Cobit* 4.1 para establecer “los parámetros o rangos de calificación de cada objetivo de control

de la Norma NTC ISO 27001: 2013" (pág. 29). El gráfico 5 describe el modelo genérico de madurez de Cobit 4.1 que considera los rangos de calificación propuestos en el citado informe.

Gráfico 5. Rangos de calificación del modelo genérico de madurez de Cobit 4.1



Fuente: modificado a partir de Pérez Torres (2018)

La citada investigación realizó el análisis de brechas (análisis GAP) y empleó los rangos presentados en el gráfico 5. Para el presente proyecto de desarrollo, los rangos de calificación son utilizados para determinar el nivel de madurez de la institución financiera cooperativa. El análisis está limitado a evaluar el cumplimiento de las cláusulas y controles a través de tres únicas opciones: "cumple", "no cumple" y "no aplica". Para obtener el nivel de madurez de la seguridad de la información de la IFC, es empleada la siguiente formula:

Porcentaje de maduración = (total "cumple" / total de controles evaluados sin incluir los "no aplica") *100%

Por ejemplo, si luego de aplicar la fórmula descrita el porcentaje obtenido es 61,5%, esto significa que el nivel de madurez de la seguridad de la información de la IFC está en un nivel “definido”. Por tanto, se entiende que “los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento” (IT Governance Institute, 2007).

Para cumplir con el objetivo de evaluar la implementación del modelo de gestión de la seguridad de la información, se utiliza el mismo método de evaluación.

1.3. Otros trabajos de investigación que emplean la ISO 27001

Implementación de una metodología

Para gestión de riesgos de información basada en las normas ISO/IEC 27001 y 27002 en el Instituto Tecnológico Superior Sucre, el proyecto de investigación titulado “Implementación de una metodología para gestión de riesgos de información basada en las normas ISO/IEC 27001 y 27002 en el Instituto Tecnológico Superior Sucre”, desarrollado por Flavio Eduardo López Vasco en el año 2019, tiene como objetivo “implementar una metodología basada en las normas internacionales ISO/IEC 27001 y 27002 para la gestión de riesgos de información en el Instituto Tecnológico Superior ‘Sucre’ [ITSS] de la ciudad de Quito, para dar cumplimiento al acuerdo N.º 166 emitido por la Secretaría Nacional de la Administración Pública SNAP sobre el Esquema Gubernamental de Seguridad de la Información”.

Al nivel del estado del arte, el autor describe definiciones y conceptos relacionados con: seguridad, información, seguridad de la información, seguridad informática, sistema de gestión de seguridad de la información SGSI, ISO e IEC, normas ISO, normas técnicas ecuatorianas ISO /IEC 27000, normas técnicas ecuatorianas ISO /IEC 27000 y normas técnicas ecuatorianas ISO /IEC 27000.

El acápite relacionado con la metodología describe el diagnóstico inicial de seguridad de la información. Posteriormente, establece el diagnóstico de tres logros: definición

del marco de seguridad y privacidad de la información, plan de seguridad y privacidad de la información y procesos de monitoreo y mejoramiento continuo.

El proyecto de investigación permitió al Instituto Tecnológico Superior “Sucre” de la ciudad de Quito, contar con una “Metodología de Gestión de Riesgos de Seguridad de la Información que comprende procesos como Análisis y Evaluación de riesgos, así como, también, (la) Definición e Implementación del Plan de Tratamiento de Riesgos”.

La investigación concluye que el mayor riesgo para los activos de información del instituto de educación superior es “la exposición de contraseñas de acceso físico y lógico”. Al analizar los escenarios de riesgos descritos en la Tabla 40: Matriz de Cálculo de Vulnerabilidad Residual en la Unidad de Titulación ITSS, es posible concluir que la metodología de aplicación es inadecuada.

La ausencia de políticas relacionadas con la obligatoriedad del uso de contraseñas robustas es un problema generalizado, sin embargo, en el escenario planteado por el investigador, existen mayores riesgos a los que están expuestos los activos de información del centro de educación, tales como, “intercepción de datos de estudiantes por infección con software espía por deficiencias en software de protección: antimalware y antivirus” o “Hurto de dispositivos de almacenamiento, procesamiento e impresoras del área de secretaría sede Sur / Bienestar Estudiantil Sede Norte por falta de controles de acceso y al área en horarios de atención al público”.

Modelo de gestión

De seguridad de la información en entidades financieras cooperativas, el proyecto de investigación intitulado “Modelo de gestión de seguridad de la información en entidades financieras cooperativas”, desarrollado por Luis Alberto Mungabusi Sisa en

el año 2022, tiene como objetivo constituirse “en un proceso metodológico, (…) que (…) (permita) seguir una secuencia de pasos con las consideraciones necesarias para la implementación del (…) modelo de gestión”.

Al nivel del estado del arte, el autor aborda conceptos relacionados con la seguridad de la información y sus generalidades, sistema de gestión de seguridad de la información (SGSI), ciclo de mejora continua y gestión de riesgos.

La propuesta de la investigación describe tres fases: diagnóstico del SGSI, preparación del SGSI y planificación del SGSI. En el diagnóstico del SGSI, el investigador establece el nivel de cumplimiento de la norma ISO/IEC 27001:2013, mediante la verificación de los controles del estándar que emplea tres parámetros: no cumple, cumple parcialmente y cumple satisfactoriamente.

La investigación concluye que "el diagnóstico es el proceso más crítico a nivel de seguridad de la información en la organización, (...) (pero), también, existen procesos (…) críticos como (…) el otorgamiento de crédito que contribuyen significativamente al giro del negocio y (al) cumplimiento de los objetivos estratégicos de la Cooperativa de Ahorro y Crédito Ambato Ltda.". De igual manera, la investigación considera que la implementación del modelo propuesto permite “mejorar el aseguramiento de (…) datos valiosos tanto de la entidad financiera como de los clientes”.

Comparativo de proyectos de investigación afines a la ISO 27001

El cuadro 4 describe los elementos más importantes de dos investigaciones afines al estándar ISO 27001 y que guardan relación con el presente proyecto de desarrollo.

Cuadro 4. Comparativo de proyectos con el estándar ISO 27001

Proyecto	Investigador	Ámbito de aplicación	Implementación de controles del Anexo A
Implementación de una metodología para gestión de riesgos de información basada en las normas ISO/IEC 27001 y 27002 en el Instituto Tecnológico Superior Sucre.	Flavio Eduardo López Vasco	Institución de educación superior.	ISO 27002.
Modelo de gestión de seguridad de la información en entidades financieras cooperativas.	Luis Alberto Mungabusi Sisa	Institución financiera cooperativa.	ISO 27002.
Modelo de gestión de la seguridad de la información en una institución financiera cooperativa.	Carlos Efraín Arellano Veloz	Institución financiera cooperativa.	*CIS Controls*

Fuente: elaboración propia

El presente trabajo, a diferencia de otros proyectos afines con la implementación de la normativa internacional ISO 27001, tiene características que lo destacan, por ejemplo:

- Para el inventario de activos de información, los dos trabajos no indican la metodología empleada en el proceso. Durante la fase 2 (identificación y planes de acción) del diseño metodológico, se describe el método empleado para identificar los tipos de información y activos de información.
- Los trabajos citados emplean metodologías similares para valorar el riesgo de los activos de información. Durante la fase 2 (identificación y planes de acción) del diseño metodológico, se emplea *CIS Controls* para analizar las vulnerabilidades de un activo de información y establecer un plan de mitigación de vulnerabilidades.
- Para la implementación de los controles descritos en el Anexo A, los dos trabajos hacen referencia al estándar ISO 27002, sin embargo, en los documentos que sustentan sus actividades, no existen acápites que describan cómo emplearon el estándar. La presente investigación, durante la fase 3 (definición e implementación) del diseño metodológico indica como cumplir con la implementación de 53 controles descritos en el Anexo A del estándar ISO27001 mediante *CIS Controls*.

- Incluso, durante la fase 3 (definición e implementación) del diseño metodológico, se indica cómo la institución financiera cooperativa definió sus políticas de seguridad mediante el empleo *CIS Controls*.
- Los trabajos citados, están enfocados -especialmente- en cumplir con la primera sección de la norma ISO 27001. El presente trabajo, en la fase 3 (definición e implementación) del diseño metodológico, describe rápidamente como la institución establece un sistema de gobierno de seguridad de la información cuyo eje central es el plan de seguridad de la información.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la empresa o institución

Nota aclaratoria

Por confidencialidad y seguridad, el presente proyecto de desarrollo no está autorizado a emplear el nombre de la institución financiera cooperativa (IFC).

Reseña

A mediados de la década de los años 70, la institución financiera cooperativa arrancó sus actividades en la ciudad de Latacunga. Al principio la institución adoptó una conducta tradicional cooperativa que consiste en la captación de recursos a través del ahorro y la concesión de préstamos. Años más tarde ingresó al control de la Superintendencia de Bancos.

El manejo adecuado de los recursos de los depositantes permitió a la institución superar la crisis económica de finales de los años 90. A inicios del siglo XXI, con una nueva visión y misión, replanteó su tradicional conducta cooperativa mediante la adopción de una nueva estrategia comercial representada en la diversificación de servicios y productos financieros y en la apertura de oficinas operativas en distintas ciudades ecuatorianas.

En mayo de 2011, tras la promulgación de la Ley Orgánica de Economía Popular y Solidaria y del Sector Financiero Popular Solidario, la Superintendencia de Economía Popular y Solidaria (SEPS) asume el control y supervisión de la institución financiera que -por el saldo de sus activos- es parte del segmento 1. La tabla 2 describe la segmentación de las entidades del Sector Financiero Popular y Solidario.

Tabla 2. Segmentación de entidades del SFPS, año 2022

Segmento	Activos
1	Mayor a 80'000.000,00
2	Mayor a 20'000.000,00 hasta 80'000.000,00
3	Mayor a 5'000.000,00 hasta 20'000.000,00
4	Mayor a 1'000.000,00 hasta 5'000.000,00
5	Hasta 1'000.000,00

Fuente: modificado a partir de Superintendencia de Economía Popular y Solidaria (2022)

A finales de la primera década del presente siglo, la IFC implementa un sistema de gestión de la calidad (*Quality Management System*) basado en el estándar ISO 9001. El alcance de la certificación abarca la prestación de servicios de captaciones a la vista, captaciones a plazo fijo, préstamos, transferencias interbancarias, recaudación para terceros, tarjetas de débito y cajeros automáticos.

La institución cuenta con un mapa general de procesos que permite representar la visión global de la cooperativa y la relación que existe entre cada uno de los procesos que la conforman. Este mapa está compuesto por tres procesos mayores y trece procesos específicos. El cuadro 5 describe el mapa general de procesos.

Cuadro 5. Mapa general de procesos

Proceso mayor	Proceso general
Gobierno	Gerencia
	Administración integral de riesgos
Operativo	Atención en ventanillas
	Captaciones
	Crédito
	Servicios al cliente
Apoyo	Administrativo financiero
	Auditoría interna
	Marketing
	Prevención de lavado de activos
	Seguridad física
	Talento humano
	Tecnologías de la información y comunicación

Fuente: elaboración propia

Marco legal

El 3 de mayo de 2022, la Superintendencia de Economía Popular y Solidaria (SEPS) mediante resolución SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 expide la “Norma de control respecto a la seguridad de la información en las entidades del Sector Financiero Popular y Solidario bajo control de la Superintendencia de Economía Popular y Solidaria” que tiene como objeto "regular los niveles mínimos para la administración de seguridad de la información que las entidades, la CONAFIPS y las empresas, deben definir e implementar con el fin de resguardar y proteger sus activos de información, preservando su confidencialidad, disponibilidad e integridad" (Superintendencia de Economía Popular y Solidaria, 2022).

Según el Artículo 3 de la norma de control, la SEPS establece tres regímenes de aplicación: 1) régimen general: a las cooperativas de ahorro y crédito de los segmentos 1 y 2; a las asociaciones mutualistas de ahorro y crédito para la vivienda y a la CONAFIPS; 3) régimen especial: a las cooperativas de ahorro y crédito del segmento; y, 3) régimen simplificado: a las cooperativas de ahorro y crédito de los

segmentos 4 y 5. La institución financiera cooperativa, al pertenecer al segmento 1 (revisar tabla 2) es parte del régimen general.

2.2. Metodología de investigación

Tipo de investigación y enfoque de investigación

Para determinar el nivel de madurez de la seguridad de la información, se aplica la investigación de campo. Para el análisis de vulnerabilidades de los activos de información, se emplea la investigación cuantitativa no experimental basada en *CIS Controls*.

Finalmente, para la evaluación de la implementación del modelo de gestión de la seguridad de la información, se emplea la investigación explicativa que compara los resultados iniciales y finales del nivel de madurez de seguridad de la información.

Técnicas e instrumentos de recopilación de información

La recolección de información emplea las siguientes técnicas:

- Técnica documental, mediante la recolección bibliográfica del estado del arte que incluye la identificación y análisis de proyectos de características similares al presente trabajo que utilizan el estándar ISO 27001. Esta técnica permite definir metodologías para: 1) medir el nivel de madurez de la seguridad de la información; 2) clasificar los tipos de información e información crítica; 3) inventar los activos de información; y, 4) analizar las vulnerabilidades de los activos de información.
- Técnica de entrevista y observación, mediante conversatorios con los responsables de los procesos descritos en el cuadro 5, es posible determinar el nivel de cumplimiento del SGSI. Al mismo tiempo, la validación del cumplimiento incluye la observación de cómo los procesos de la institución son ejecutados.

2.3. Propuesta de investigación

Versión de la norma ISO 27001

El presente trabajo utiliza la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001. Tecnologías de la Información — Técnicas de Seguridad — Sistemas de Gestión de Seguridad de la Información – Requisitos (ISO/IEC 27001:2013+Cor.1:2014+ Cor.:2015, IDT).

El término “ISO 27001” hace referencia a la norma internacional “ISO/IEC 27001:2013”.

Propuesta de implementación

La implementación del “Modelo de Gestión de la Seguridad de la Información en una Institución Financiera Cooperativa”, considera las siguientes fases: 1) diagnóstico, 2) identificación y planes de acción, 3) definición e implementación y 4) evaluación.
El diagnóstico (1) determina el nivel inicial de madurez de la seguridad de la información. Esta fase abarca el análisis de brechas o análisis “GAP” del cumplimiento del SGSI y de los controles descritos en el Anexo A de la ISO 27001. El análisis incluye entrevistas con los responsables de los procesos descritos en el cuadro 5 y la revisión de la documentación que sustenta al sistema de gestión de la calidad (ISO 9001:2015).

La identificación y planes de acción (2) permite: clasificar los tipos de información, inventar los activos de información y analizar las vulnerabilidades de los activos de información.

La definición e implementación (3) define la política y objetivos de la seguridad de la información, el sistema de gobierno de seguridad de la información y sus componentes basado en el modelo de gobierno propuesto por *Cobit* 2019.

Finalmente, la evaluación (4) determina el nivel de madurez de la seguridad de la información posterior a la implementación del marco de referencia. Esta fase abarca un segundo análisis de brechas o análisis “GAP” del cumplimiento del SGSI y de los controles descritos en el Anexo A.

Fase 1: diagnóstico

Para determinar el nivel inicial de madurez de la seguridad de la información de la institución financiera cooperativa, se evalúa: 1) el cumplimiento de las cláusulas del sistema de gestión de seguridad de la información relacionada con la normativa ISO 27001 y, 2) el cumplimiento de los controles descritos en el Anexo A. El análisis GAP, está limitado a evaluar el cumplimiento de las cláusulas y controles a través de tres únicas opciones: “cumple”, “no cumple” y “no aplica”. El análisis GAP (entrevista) está destinado a los responsables de los procesos descritos en el cuadro 5.

La primera evaluación emplea un documento de 52 preguntas que permiten determinar el cumplimiento de las cláusulas del sistema de gestión de seguridad de la información (el anexo 3 describe cada una de las preguntas que conforman el cuestionario). La segunda evaluación emplea un documento que describe cuáles de los 114 controles están implementados por la institución (el anexo 4 describe qué controles están o no están implementados, o por la naturaleza de la institución no son aplicables).

La tabla 3, evalúa el cumplimiento total de las cláusulas del sistema de gestión de seguridad de la información. La tabla 4, evalúa qué controles descritos en el Anexo A están o no están implementados por la institución.

Tabla 3.Cumplimiento total de las cláusulas del SGSI

¿Cumple?	N.º Clausulas	Representación
Sí	5	9,62%
No	47	90,38%
TOTAL	**52**	**100,00%**

Fuente: elaboración propia

El nivel inicial de madurez de la seguridad de la información de la institución relacionado con el cumplimiento de las cláusulas de la norma ISO 27001 es del 9,62%. Según el modelo genérico de madurez de *Cobit* 4.1., descrito en la sección "1.2 Sistema de gestión de seguridad de la información" del Capítulo I, se determina que el nivel de madurez de la seguridad de la información es "inexistente", es decir, significa que la IFC carece de cualquier proceso reconocible relacionado con el sistema de gestión de la seguridad de la información.

Tabla 4. Controles del Anexo A que están o no están implementados

¿Cumple?	N.º Controles	Representación	Representación sin considerar "no aplica"
Sí	80	70,18%	74,77%
No	27	23,68%	25,23%
No aplica	7	6,14%	-
TOTAL	**114**	**100,00%**	**-**

Fuente: elaboración propia

El nivel inicial de madurez de la seguridad de la información de la institución relacionado con el cumplimiento de los controles descritos en el Anexo A del estándar ISO 27001 es del 74,77%. Según el modelo genérico de madurez de *Cobit* 4.1., se determina que el nivel de madurez de la seguridad de la información es "administrado", es decir, significa que la cooperativa monitorea y mide "el cumplimiento de los procedimientos y (para) tomar medidas (si) los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada" (IT Governance Institute, 2007).

Al determinar el nivel inicial de madurez de la seguridad de la información es posible concluir que la institución financiera cooperativa enfocó sus esfuerzos a la seguridad informática. Por tanto, es necesario que: 1) establezca un procedimiento para clasificar los tipos de información e información crítica; inventar los activos de información; y analizar las vulnerabilidades de los activos de información; y, 2) defina un sistema de gobierno de seguridad de la información.

Fase 2: identificación y planes de acción

Identificación y clasificación de tipos de información de acuerdo con el impacto al nivel de la confidencialidad e integridad

La norma de control respecto a la seguridad de la información (SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002), exige a las instituciones financieras del régimen general (segmento 1) ejecutar un procedimiento relacionado con el inventario y clasificación de información. El acápite requiere el cumplimiento de tres actividades: 1) identificación de tipos de información, 2) inventario de activos de información y 3) clasificación de activos de información.

La identificación de los tipos de información parte de la necesidad que tiene la institución financiera para “comprender todo el compendio de información con la que cuenta, de principio a fin, en lo que se conoce como ciclo de vida del dato”, (Severino & Carrillo, 2021). Para ejecutar el proceso, los citados autores plantean realizar siete interrogantes, sin embargo, para la ejecución del proyecto, se emplean cuatro:

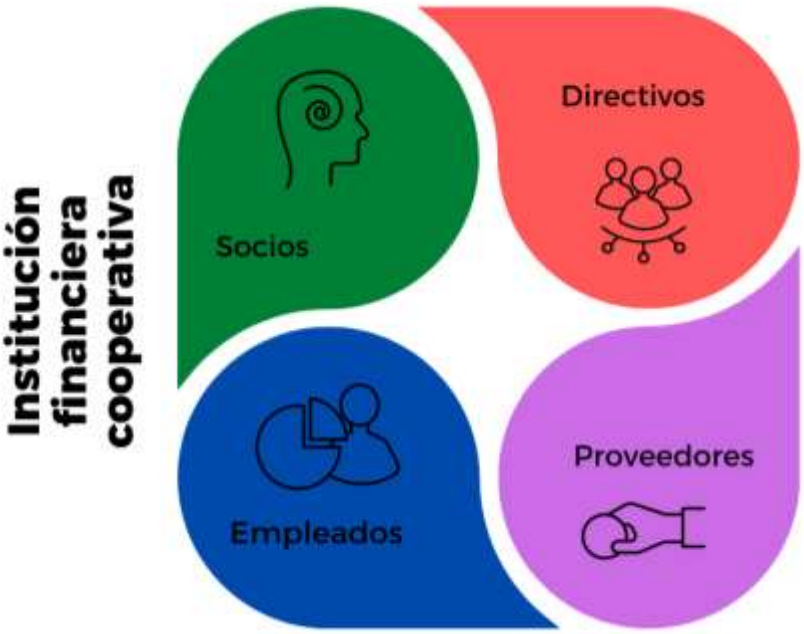
1. ¿Qué datos dispone la institución financiera?
2. ¿Dónde están almacenados los datos?
3. ¿Qué sistemas emplean esta información?
4. ¿Quién tiene acceso a la información?

Para identificar la información que dispone la institución, es necesario utilizar los conceptos de entidad y atributo asociados a una base de datos relacional. Una

entidad es un “objeto exclusivo único en el mundo real que se está controlando” (IBM, 2021). Un atributo es una “característica o rasgo de un tipo de entidad” (IBM, 2021), en otras palabras, es una “cualidad o característica propia de una persona o una cosa, especialmente algo que es parte esencial de su naturaleza”.

Para inventariar los tipos de información es necesario concebir a la institución financiera como el centro de información y determinar las partes interesadas que interactúan con ella (revisar gráfico 6), lo que permite definirlas como entidades. Incluso, la misma institución constituye una entidad de datos. Desde ese precepto, los tipos de información hacen referencia a las características/atributos que dispone una entidad.

Gráfico 6. Partes interesadas



Fuente: elaboración propia

La institución requiere replantearse y responder las interrogantes formuladas por (Severino & Carrillo, 2021). El cuadro 6 identifica las interrogantes necesarias para documentar las entidades y tipos de información.

Cuadro 6. Interrogantes para documentar las entidades y tipos de información

Identificador	Pregunta
VR1	¿Qué entidades dispone la institución?
VR2	¿Qué tipos de información registran las entidades?
VR3	¿Qué sistemas utilizan los tipos de información?
VR4	¿Quién es el responsable de las entidades?

Fuente: elaboración propia

La norma de control respecto a la seguridad de la información indica que la identificación de los tipos de información, inventario y clasificación de los activos de información estarán en “un documento evidenciable en el cual se identifique y cuantifique los tipos y activos de información considerando los criterios de disponibilidad, confidencialidad e integridad, así como su custodio, responsable y ubicación” (Superintendencia de Economía Popular y Solidaria, 2022).

Para cumplir con las disposiciones de las SEPS, se identifican las siguientes entidades (VR1 del cuadro 6) son: 1) socios, 2) directivos, 3) empleados, 4) proveedores e 5) institución financiera cooperativa. Al nivel de los responsables de las entidades (VR4 del cuadro 6), es necesario considerar la definición de la Ley Orgánica de Protección de Datos Personales que manifiesta que el encargado (responsable) es la “persona natural o jurídica, pública o privada, autoridad (…), u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales” (pág. 12). Los responsables de los procesos son los responsables de las entidades, de acuerdo con la definición planteada por la LOPDP.

La institución financiera identifica los tipos de información (VR2 del cuadro 6). Sin embargo, el ejercicio de levantamiento de los tipos de información corre el riesgo de descartar varios tipos que -por omisión de los responsables- no son incluidos. Es necesario que la institución –al menos una vez al año- actualice los tipos de información. El cuadro 7 hace referencia a los tipos de datos identificados en la

entidad socios. La información de la entidad socio es presentada a discreción del maestrante.

Cuadro 7. Tipos de información de la entidad socio

Entidad	Encargado	Tipo de información	Descripción del tipo de información
Socio	Jefe comercial	Datos generales	Datos de identificación como: número de cédula, apellidos y nombres, datos del cónyuge y familia.
		Información de contacto	Datos que permiten localizar al socio: ciudad de residencia, dirección domiciliaria, dirección de correo electrónico y números de teléfono.
		Posición financiera	Información relacionada con ingresos y egresos del socio, patrimonio, estados financieros. Documentación que sustente el patrimonio: certificaciones bancarias, fotocopias de pago de impuestos prediales, matriculación vehicular, entre otros.
		Vinculación con el sistema financiero y comercial (buró de crédito)	Saldo y evolución de las operaciones de crédito que mantiene el socio con otras entidades del sistema financiero y comercial.
		Datos transaccionales de préstamos	Número de préstamo, saldos, tabla de amortización, detalle de transacciones efectuadas, recargos por falta de pago, garantías prendarias/personales/hipotecarías, información relacionada con el seguro de desgravamen, estado de la situación legal del préstamo, entre otros.
		Datos transacciones de depósitos a la vista	Datos como: número de cuenta, saldos, detalle de transacciones efectuadas, entre otros.
		Datos transaccionales de depósitos a plazo fijo	Datos como: número del certificado de depósitos a plazo fijo, saldos, detalle de transacciones efectuadas, entre otros.
		Información de autenticación para servicios electrónicos.	Número de tarjeta de débito, CVV, PIN. Usuario y contraseña para el acceso al portal web transaccional.

Fuente: elaboración propia

La norma en la metodología de riesgos descrita en su Anexo 2, indica que “la clasificación de activos debe considerar al menos: aspectos del negocio, tipo de información y datos almacenados, importancia a la continuidad del servicio, consecuencias legales e impacto económico” (Superintendencia de Economía Popular y Solidaria, 2022). Para medir el riesgo inherente (revisar tabla 5) de la confidencialidad e integridad de los tipos de información, es necesario aplicar tres aristas de evaluación: 1) continuidad del servicio, 2) consecuencia legal e 3) impacto económico en la institución.

Tabla 5. Determinación del riesgo inherente y riesgo intrínseco

Nombre	Ponderación	Descripción
Crítico	5	Detener la operación de la institución, incluso, el cierre definitivo.
Alta	4	Genera retrasos importantes que afectan al cumplimiento de los objetivos institucionales.
Medio	3	La materialización del riesgo causa una pérdida momentánea.
Bajo	2	El impacto que causa la materialización del riesgo en los objetivos de la institución es mínimo.
Muy bajo	1	El impacto no representa un problema para la institución.

Fuente: modificado a partir de Superintendencia de Economía Popular y Solidaria (2022) y Jiménez (2021)

Para determinar el impacto en la confidencialidad e integridad mediante las tres aristas planteadas, según la valoración del riesgo intrínseco descrita en la tabla 5, la institución responderá: 1) ¿cuál es la afectación en la continuidad del servicio si el principio de confidencialidad/integridad del tipo de información identificado es quebrantado?, 2) ¿cuál es la afectación legal el principio de confidencialidad/integridad del tipo de información identificado es quebrantado?, 3) ¿cuál es el impacto económico si el principio de confidencialidad/integridad del tipo de información identificado es quebrantado? El impacto total en la confidencialidad e integridad del tipo de información está sujeto al mayor riesgo asignado a cualquier de las tres aristas de evaluación.

El cuadro 8, describe el impacto total de la confidencialidad e integridad de los tipos de información que conforman la entidad socio.

Cuadro 8. Confidencialidad e integridad de la entidad socio

Tipo de información	Confidencialidad			Impacto confidencialidad	Integridad			Impacto integridad	Impacto total
	Servicio	Afectación legal	Impacto económico		Servicio	Afectación legal	Impacto económico		
Datos generales	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo
Información de contacto	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Medio	Muy bajo	Muy bajo	Medio	Medio
Posición financiera	Muy bajo	Medio	Muy bajo	Medio	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Medio
Vinculación con el sistema financiero y comercial (buró de crédito)	Muy bajo	Medio	Medio	Medio	Medio	Muy bajo	Muy bajo	Medio	Medio
Datos transaccionales de préstamos	Muy bajo	Medio	Muy bajo	Medio	Crítico	Medio	Crítico	Crítico	Crítico
Datos transaccionales de depósitos a la vista	Muy bajo	Medio	Muy bajo	Medio	Crítico	Medio	Crítico	Crítico	Crítico
Datos transaccionales de depósitos a plazo fijo	Muy bajo	Medio	Muy bajo	Medio	Crítico	Medio	Crítico	Crítico	Crítico
Información de autenticación para servicios electrónicos.	Muy bajo	Medio	Muy bajo	Medio	Crítico	Medio	Crítico	Crítico	Crítico

Fuente: elaboración propia

Inventario de activos de información

Un activo de información es un "(recurso) que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos (…) (propuestos) por la alta dirección" (ISOTools Excellence, 2017). (Varela, s.f.), considera que los activos de información son, por ejemplo: el hardware y el software utilizado para el procesamiento, transporte o almacenamiento de información; los servicios utilizados para la transmisión, recepción y control de la información; y, las herramientas o utilidades para el desarrollo y soporte de los sistemas de información.

El inventario de activos de información permite identificar: 1) motores de bases de datos, 2) servidores, 3) equipos de telecomunicaciones, 3) centros de cómputo, 4) estaciones de trabajo, 5) aplicaciones, 6) servicios externos (*outsourcing*) e 7) instalaciones (oficinas). En cambio, un centro de cómputo "hace referencia a la unidad que se encarga del diseño y la implementación de sistemas dentro de una empresa" (Definición de, s.f.).

Se entiende como aplicación al "software que se utiliza para la gestión del proceso" (Instituto Nacional de Ciberserguridad de España, 2016). Lo que incluye aplicaciones desarrolladas interna y externamente. El término *outsourcing* es un término en inglés que se utiliza para representar el acto de 'tercerizar' servicios (…) para reducir la carga de trabajos hechos internamente y escalar el alcance y la productividad del negocio" (Lisboa, 2019).

Un servidor, en términos informáticos, es un "ordenador que pone recursos a disposición a través de una red" (Digital Guide IONOS, 2020). Las estaciones de trabajo son "equipos de alto rendimiento que se emplean en cualquier trabajo con necesidades específicas." (Aurum Informática, 2021)

Para dinamizar el concepto de disponibilidad, es necesario entender al servicio interno como tal. “Un servicio es un medio para entregar valor a los clientes, facilitando los resultados que (…) (ellos) quieren lograr y sin que éstos tengan que asumir los costes y riesgos asociados a la consecución de dichos resultados” (SERVICETONIC, 2021).

La relación de un activo de información y de un servicio (interno), permite expresar la dependencia del segundo con el primero, es decir, cómo los activos de información son los medios que permiten acceder a un servicio. Aunque la disponibilidad de la información hace referencia a la que información esté disponible en el momento requerido, la definición no contempla que son los servicios –internos- los que permiten acceder a la información si esta sea requerida. En consecuencia, la disponibilidad de los activos de información tiene una estrecha dependencia con la disponibilidad de los servicios. Por ejemplo, si un centro de procesamiento de datos sufre una paralización total, los servicios –internos- no estarán disponibles, de tal manera que el principio de disponibilidad es quebrantado.

Para inventariar los activos de información es necesario identificar cada registro mediante un código, describir la función que cumple en la institución, su ubicación física, la oficina (instalación) a la que pertenece, el custodio (responsable) y su impacto en la disponibilidad. El cuadro 9 hace referencia a la ficha que describe los activos de información.

Para determinar el impacto en la disponibilidad, la institución formula la siguiente pregunta: ¿cuál es el impacto en la operación si el activo de información identificado no está disponible? Dicha consideración no aplica para las bases de datos ni para los servidores, la determinación de su disponibilidad es calculado al aplicar el procedimiento descrito en sección “Relación tipos de información / activos de información” (revisar relación servidores y aplicaciones y relación base de datos y aplicaciones).

La valoración de la disponibilidad tiene relación con la valoración del riesgo intrínseco que consta en la tabla 5.

Cuadro 9. Ficha para el inventario de activos de información

Código	Tipo	Descripción	Ubicación física	Oficina	Responsable	Impacto en la disponibilidad
	Uno de: - Motor de base de datos - Servidor - Telecomunicaciones - Centro de cómputo - Estación de trabajo - Aplicación - Servicio externo (*outsourcing*) - Instalación (oficina)					

Fuente: elaboración propia

La tabla 6 presenta el resumen del número total de activos de información clasificados de acuerdo con el tipo (motor de base de datos, servidor, telecomunicaciones, centro de cómputo, estación de trabajo, aplicación, servicio externo (*outsourcing*) e instalación). El cuadro 10 presenta algunos de los activos de información identificados y la valoración de su disponibilidad.

Tabla 6. Resumen del inventario de activos de información

Activo de información	Número de activos identificados
Motores de base de datos	2
Servidores	55
Equipos de telecomunicaciones	45
Centros de cómputo	2
Estaciones de trabajo	185
Aplicaciones	40
Servicios externos (*outsourcing*)	15
Instalaciones	15
TOTAL	359

Fuente: elaboración propia

Cuadro 10. Resumen de activos de información

Código	Tipo	Descripción	Ubicación física	Oficina	Responsable	Impacto en la disponibilidad
DC-0001	Centro de cómputo	Principal centro de cómputo.	Subsuelo	Matriz	Jefe de tecnologías de la información y comunicación	Crítico
SR-0074	Motor de base de datos	Base de datos SQL Server.	Subsuelo	Matriz	Jefe de tecnologías de la información y comunicación	Crítico*
SR-0090	Servidor	Servidor transaccional.	Subsuelo	Matriz	Jefe de tecnologías de la información y comunicación	Alta**
ET-00256	Estación de trabajo	Estación de trabajo Dell 8GB RAM y 500 GB.	Segundo piso	Pichincha	Supervisor de cajas	Muy bajo
TE-00147	Telecomunicaciones	Switch Cisco 48 puertos.	Subsuelo	Matriz	Jefe de tecnologías de la información y comunicación	Crítico
OF-0001	Instalación	Edificio Matriz.	-	Matriz	Jefe administrativo financiero	Crítico

Fuente: elaboración propia

* La determinación de la disponibilidad del activo de información es establecida mediante el procedimiento descrito en la sección “Relación base de datos y aplicaciones”.

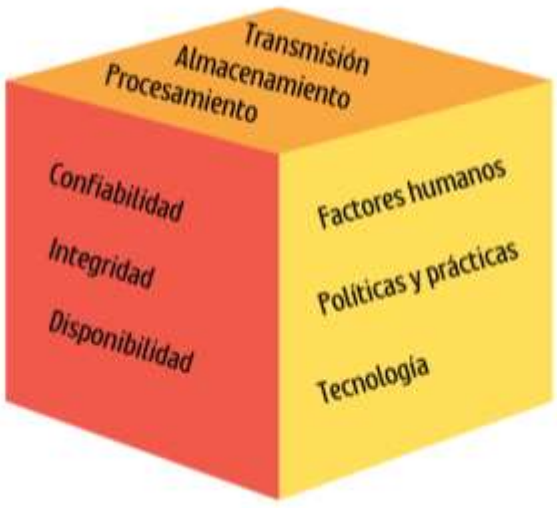
** La determinación de la disponibilidad del activo de información es establecida mediante el procedimiento descrito en la sección “Relación servidores y aplicaciones”.

Relación tipos de información / activos de información

El Cubo de *McCumber* es un marco de trabajo propuesto por Jhon McCumber enfocado a la ciberseguridad. “El cubo (…) es una aproximación estructurada que analiza todas las facetas de los requerimientos de la seguridad de la información, proveyendo al mismo tiempo un léxico común que puede emplearse para especificar requerimientos, tomar decisiones que mitiguen el riesgo, y desarrollar e implementar salvaguardas” (iPSEC, 2022).

La metodología de *McCumber* describe tres dimensiones (revisar gráfico 7): 1) los principios de seguridad, 2) estados de la información y 3) medidas de seguridad de la información. Los principios de seguridad (1) son: la confidencialidad, integridad y disponibilidad. Los estados de la información (2) hace referencia a la protección de estos en sus tres estados posibles: datos en tránsito (transmitir), datos almacenados (almacenar) y datos en proceso (generar). Finalmente, las medidas de ciberseguridad definen los mecanismos establecidos para protegerlos.

Gráfico 7. Las tres dimensiones del Cubo de McCumber



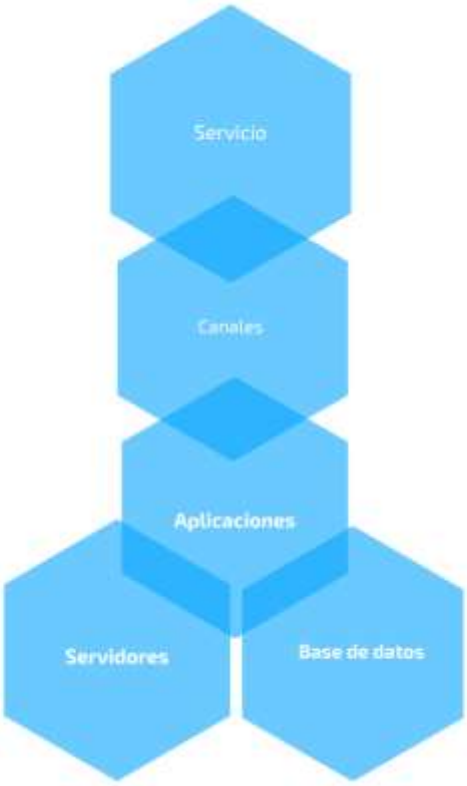
Fuente: modificado a partir de Huawei (2022)

La primera dimensión del cubo de *McCumber* describe los tres principios de la seguridad de la información. El impacto en la confidencialidad e integridad de la información fue definido mediante la identificación de los tipos de información. El impacto en la disponibilidad de los activos de información fue definido mediante su inventario.

Sin embargo, es necesario relacionar la primera dimensión con la segunda dimensión del marco de trabajo de *McCumber*. La metodología propuesta consiste en determinar cómo los tipos de información son generados, almacenados y transmitidos. Para cumplir con el requisito, es necesario comprender las relaciones de cinco componentes -identificados por la institución- que están relacionados con los estados de la información.

Los dos primeros componentes corresponden a los servicios y canales de atención. Los canales son los medios que permiten a los socios y clientes de la institución acceder a los servicios. “Los canales de atención (…) son (los) puntos de contacto que ofrece una empresa para comunicarse con sus consumidores” (Da Silva, 2021). Los otros componentes son las aplicaciones que soportan los servicios; y, los servidores y bases de datos que soportan a las aplicaciones (revisar gráfico 8).

Gráfico 8. Relación servicio, canales, aplicaciones, servidores y base de datos



Fuente: elaboración propia

De acuerdo con el cuadro 11, la institución financiera cooperativa disponible de cuatro canales de atención: 1) oficina, 2) internet, 3) cajero automático e 4) IVR. Los otros componentes son: las aplicaciones, los servidores y las bases de datos. La identificación de aplicaciones, servidores y base de datos es realizada durante el inventario de los activos de información.

Cuadro 11. Canales de atención

Canal	Observación
Oficina	
Internet	Incluye plataforma transaccional para computadores de escritorio y aplicaciones para dispositivos móviles
Cajero automático	-
IVR	-

Fuente: elaboración propia

Un servicio interno es el equivalente a un servicio financiero. “Los servicios financieros son un conjunto de servicios prestados por una entidad financiera, relacionados con el dinero de las personas y sus expectativas, con la finalidad de facilitar al usuario la intermediación financiera” (Cooperativa de ahorro y crédito Tulcán Ltda., s.f.). El cuadro 12 describe varios de los servicios provistos por la institución financiera cooperativa, el impacto en la disponibilidad (según valoración descrita en la tabla 5) y la relación con el canal que emplea la institución para ofertarlo.

Cuadro 12. Relación 1, servicio, disponibilidad del servicio y canal

Servicio	Disponibilidad	Oficina	Internet	Cajero automático	IVR
Apertura de cuenta	Bajo	X			
Apertura de depósitos a plazo	Bajo	X			
Cancelación o cierre de cuentas de ahorro	Bajo	X			
Cheque de emergencia	Bajo	X			
Cheque devuelto nacional	Bajo	X			
Consulta de saldo de cuenta de ahorro	Bajo	X	X	X	
Depósito en cuenta de ahorro	Bajo	X			
Emisión de tabla de amortización, primera impresión,	Bajo	X			
Renovación de plástico de tarjeta de débito con chip	Bajo	X			
Reposición de libreta y estado de cuenta por actualización	Bajo	X			
Retiro de dinero	Alta	X		X	
Transferencias dentro de la misma entidad	Bajo	X	X		
Transferencias interbancarias SCI recibidas	Bajo	X			
Transferencias interbancarias SPI enviadas	Bajo	X	X		
Transferencias nacionales otras entidades	Bajo	X	X		

Fuente: elaboración propia

Relación servicio y tipo de información

Una vez identificados los canales y los servicios y cómo estos están relacionados, es necesario relacionar el impacto de la confidencialidad e integridad de los servicios con los tipos de información. El ejercicio requiere que la institución determine cuál es el servicio que genera el tipo de información asociado a la entidad (VR3 del cuadro 6) y asignar el impacto total de la confidencialidad e integridad (revisar cuadro 8). Por ejemplo, si el impacto total de la confidencialidad e integridad del tipo de información es “alta”, el impacto de la confidencialidad e integridad del servicio es el mismo.

El cuadro 13 presenta la relación del impacto en la confidencialidad e integridad del servicio relacionados con los tipos de información.

Cuadro 13. Relación 2, confidencialidad e integridad del servicio

Servicio	Información de contacto	Posición financiera	Datos transaccionales de préstamos	Datos transacciones de depósitos a la vista	Datos transaccionales de depósitos a plazo fijo	Información de autenticación para servicios electrónicos
Apertura de cuenta	Medio					
Apertura de depósitos a plazo					Crítico	
Cancelación o cierre de cuentas de ahorro				Crítico		
Cheque de emergencia				Crítico		
Cheque devuelto nacional				Crítico		
Consulta de saldo de cuenta de ahorro				Crítico		
Depósito en cuenta de ahorro				Crítico		
Emisión de tabla de amortización, primera impresión,			Crítico			
Renovación de plástico de tarjeta de débito con chip				Crítico		
Reposición de libreta, cartola, estado de cuenta por actualización				Crítico		
Retiro de dinero				Crítico		
Transferencias dentro de la misma entidad				Crítico		
Transferencias interbancarias SCI recibidas				Crítico		
Transferencias interbancarias SPI enviadas				Crítico		
Transferencias nacionales otras entidades				Crítico		

Fuente: elaboración propia

Las relaciones propuestas en los cuadros 12 y 13, permiten identificar la confidencialidad, integridad y disponibilidad de los servicios (revisar cuadro 14).

Cuadro 14. Confidencialidad, integridad y disponibilidad de los servicios

Servicio	Confidencialidad e integridad	Disponibilidad
Apertura de cuenta	Medio	Bajo
Apertura de depósitos a plazo	Critico	Bajo
Cancelación o cierre de cuentas de ahorro	Critico	Bajo
Cheque de emergencia	Critico	Bajo
Cheque devuelto nacional	Critico	Bajo
Consulta de saldo de cuenta de ahorro	Critico	Bajo
Depósito en cuenta de ahorro	Critico	Bajo
Emisión de tabla de amortización, primera impresión,	Critico	Bajo
Renovación de plástico de tarjeta de débito con chip	Critico	Bajo
Reposición de libreta o estado de cuenta por actualización	Critico	Bajo
Retiro de dinero	Critico	Alta
Transferencias dentro de la misma entidad	Critico	Bajo
Transferencias interbancarias SCI recibidas	Critico	Bajo
Transferencias interbancarias SPI enviadas	Critico	Bajo
Transferencias nacionales otras entidades	Critico	Bajo

Fuente: elaboración propia

Relación canal y tipo de información

Para determinar el impacto de la confidencialidad e integridad del canal, la institución relaciona el canal que genera el tipo de información asociado a la entidad y asigna el impacto total de la confidencialidad e integridad (revisar cuadro 8). Por ejemplo, si el impacto total de la confidencialidad e integridad del tipo de información es “alta”, el impacto de la confidencialidad e integridad del canal es el mismo. El cuadro 15 presenta la relación del impacto en la confidencialidad e integridad de los canales relacionados con los tipos de información.

Cuadro 15. Relación 3, canales y tipos de información

Canal / Tipo de información	Información de contacto	Posición financiera	Datos transaccionales de préstamos	Datos transacciones de depósitos a la vista	Datos transaccionales de depósitos a plazo fijo	Información de autenticación para servicios electrónicos
Oficina	X	X	X	X	X	X
Internet			X	X	X	X
Cajero automático				X		X
IVR						

Fuente: elaboración propia

La disponibilidad del canal está relacionada con el mayor impacto en la disponibilidad del servicio asociado al canal, es decir, la disponibilidad del canal es el mayor nivel de riesgo del servicio asociado al canal. Las relaciones propuestas en los cuadros 12 y 15, permiten identificar la confidencialidad, integridad y disponibilidad de los canales (revisar cuadro 16).

Cuadro 16. Confidencialidad, integridad y disponibilidad de los canales

Canal	Confidencialidad e integridad	Disponibilidad
Oficina	Critico	Alta
Internet	Critico	Bajo
Cajero automático	Critico	Alta
IVR	Muy bajo	Muy bajo

Fuente: elaboración propia

Relación aplicaciones y canales

Para determinar el impacto de la confidencialidad, integridad y disponibilidad de las aplicaciones, la institución relaciona la aplicación y el canal. La confidencialidad e integridad están relacionados con la confidencialidad e integridad del canal (revisar cuadro 16). La disponibilidad de la aplicación está relacionada con la disponibilidad del canal (revisar cuadro 16). Por ejemplo: 1) si el impacto total de la disponibilidad del canal es “alta”, el impacto de la disponibilidad de la aplicación es el mismo (revisar cuadro 17) y 2) si el impacto de la confidencialidad e integridad del canal es “alta”, el impacto de la confidencialidad e integridad de la aplicación es el mismo (revisar cuadro 18).

Cuadro 17. Relación 4, disponibilidad de las aplicaciones con los canales

Aplicación \ Canal	Oficina	Internet	Cajero automático	IVR
Aplicación móvil transaccional		Bajo		
Autorizador transaccional de cajeros automáticos			Alta	
Core financiero	Alta			
Kaspersky Internet Security				
Microsoft Office				
PDF24				
Portal web transaccional		Bajo		
Winrar				

Fuente: elaboración propia

Cuadro 18. Relación 5, confidencialidad e integridad de las aplicaciones y canales

Aplicación \ Canal	Oficina	Internet	Cajero automático	IVR
Aplicación móvil transaccional		Critico		
Autorizador transaccional de cajeros automáticos			Critico	
Core financiero	Critico			
Kaspersky Internet Security				
Microsoft Office				
PDF24				
Portal web transaccional		Critico		
Winrar				

Fuente: elaboración propia

Las relaciones propuestas en los cuadros 17 y 18, permiten identificar la confidencialidad, integridad y disponibilidad de las aplicaciones (revisar cuadro 19).

Cuadro 19. Confidencialidad, integridad y disponibilidad de las aplicaciones

Aplicación \ Canal	Confidencialidad e integridad	Disponibilidad
Aplicación móvil transaccional	Critico	Bajo
Autorizador transaccional de cajeros automáticos	Critico	Alta
Core financiero	Critico	Alta
Kaspersky Internet Security	Muy bajo	Muy bajo
Microsoft Office	Muy bajo	Muy bajo
PDF24	Muy bajo	Muy bajo
Portal web transaccional	Critico	Bajo
Winrar	Muy bajo	Muy bajo

Fuente: elaboración propia

Relación servidores y aplicaciones

Para determinar el impacto de la confidencialidad, integridad y disponibilidad de los servidores, la institución relaciona el servidor con la aplicación. La confidencialidad e integridad están relacionados con la confidencialidad e integridad de la aplicación (revisar cuadro 19). La disponibilidad del servidor está relacionada con la disponibilidad de la aplicación (revisar cuadro 19). Por ejemplo: 1) si el impacto de la disponibilidad de la aplicación es “alta”, el impacto de la disponibilidad del servidor es el mismo (revisar cuadro 20) y 2) si el impacto total de la confidencialidad e integridad de la aplicación es “alta”, el impacto de la confidencialidad e integridad del servidor es el mismo (revisar cuadro 21).

Aplicaciones: (1) Aplicación móvil transaccional, (2) autorizador transaccional de cajeros automáticos, (3) Core financiero, (4) Kaspersky Internet Security, (5) Microsoft Office, (6) PDF24, (7) portal web transaccional, (8) Winrar.

Cuadro 20. Relación 6, disponibilidad de servidores con las aplicaciones

Aplicación \ Canal	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Servidor aplicación móvil transaccional	Bajo							
Servidor transaccional	Alta	Alta	Alta					
Servidor de correo electrónico								
Servidor de sistema antivirus				Muy bajo				
Servidor portal web transaccional							Bajo	
Servidor transaccional de cajeros automáticos		Alta						

Fuente: elaboración propia

Cuadro 21. Relación 7, confidencialidad e integridad de los servidores y aplicaciones

Aplicación \ Canal	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Servidor aplicación móvil transaccional	Critico							
Servidor transaccional	Critico	Critico	Critico					
Servidor de correo electrónico								
Servidor de sistema antivirus				Muy bajo				
Servidor portal web transaccional							Critico	
Servidor transaccional de cajeros automáticos		Critico						

Fuente: elaboración propia

Las relaciones propuestas en los cuadros 20 y 21, permiten identificar la confidencialidad, integridad y disponibilidad de los servidores (revisar cuadro 22).

Cuadro 22. Confidencialidad, integridad y disponibilidad de los servidores

Aplicación \ Canal	Confidencialidad e integridad	Disponibilidad
Servidor aplicación móvil transaccional	Crítico	Bajo
Servidor transaccional	Crítico	Alto
Servidor de correo electrónico	Muy bajo	Muy bajo
Servidor de sistema antivirus	Muy bajo	Muy bajo
Servidor portal web transaccional	Crítico	Bajo
Servidor transaccional de cajeros automáticos	Crítico	Alto

Fuente: elaboración propia

Relación base de datos y aplicaciones

Para determinar el impacto de la confidencialidad, integridad y disponibilidad de las bases de datos, la institución relaciona la base de datos con la aplicación. La confidencialidad e integridad están relacionados con la confidencialidad e integridad de la aplicación (revisar cuadro 22). La disponibilidad de la base de datos está relacionada con la disponibilidad de la aplicación (revisar cuadro 21).

Por ejemplo: 1) si el impacto de la disponibilidad de la aplicación es “alta”, el impacto de la disponibilidad de la base de datos es el mismo (revisar cuadro 23) y 2) si el impacto de la confidencialidad e integridad de la aplicación es “alta”, el impacto de la confidencialidad e integridad de la base de datos es el mismo (revisar cuadro 24).

Aplicaciones: (1) Aplicación móvil transaccional, (2) autorizador transaccional de cajeros automáticos, (3) Core financiero, (4) Kaspersky Internet Security, (5) Microsoft Office, (6) PDF24, (7) portal web transaccional, (8) Winrar.

Cuadro 23. Relación 8, disponibilidad bases de datos con las aplicaciones

Aplicación \ Canal	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Base de datos SQL Server	Bajo	Alta	Alta	Muy bajo	Muy bajo	Muy bajo	Bajo	Muy bajo

Fuente: elaboración propia

Cuadro 24. Relación 9, confidencialidad e integridad bases de datos y aplicaciones

Aplicación \ Canal	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Base de datos SQL Server	Critico	Critico	Critico	Muy bajo	Muy bajo	Muy bajo	Critico	Muy bajo

Fuente: elaboración propia

Las relaciones propuestas en los cuadros 23 y 24, permiten identificar la confidencialidad, integridad y disponibilidad de los servidores (revisar cuadro 25).

Cuadro 25. Confidencialidad, integridad y disponibilidad de las bases de datos

Aplicación \ Canal	Confidencialidad e integridad	Disponibilidad
Base de datos SQL Server	Crítico	Alta

Fuente: elaboración propia

Todas las relaciones establecidas (revisar cuadros 12, 13, 15, 17, 18, 20, 21, 23 y 24) permiten a la institución financiera cooperativa determinar cómo la información (tipos) es generada, almacenada y transmitida. Con la metodología propuesta, es posible atender dos de las tres dimensiones del Cubo de McCumber.

Análisis de amenazas y vulnerabilidades de los activos de información

Las relaciones entre servicios, canales, aplicaciones, servidores y base de datos permiten generar una visión amplia y completa de los estados de la información. Para garantizar la confidencialidad, integridad y disponibilidad de la información, la institución establece un proceso para identificar las vulnerabilidades de los activos de información y formula sus planes de acción. Para considerar la prioridad al momento de analizar los activos de información es necesario con revisar los cuadros 14, 16, 19, 22 y 25 y seleccionar los activos de información requeridos.

El proyecto de desarrollo describe cómo la institución realiza el análisis de amenazas y vulnerabilidades de un activo de información. El activo seleccionado corresponde a la base de datos Microsoft SQL Server identificado con el código SR-0074, porque su impacto en la disponibilidad es alto y el impacto en la confidencialidad e integridad es crítico.

Una amenaza es una “cosa o persona que constituye una posible causa de riesgo o perjuicio para alguien o algo”. Una vulnerabilidad es entendida como la “cualidad de lo que es vulnerable”. “En la amenaza existe intencionalidad de realizar una acción por parte de un tercero mediante determinadas acciones, mientras que en la vulnerabilidad no se puede aplicar ese planteamiento, (…) (porque) se considera algo intrínseco e inherente, en mayor o menor medida, a la capacidad del sujeto de resolver las deficiencias o carencias que pueda tener” (INCIBE, 2020).

Para el análisis de vulnerabilidades del activo de información seleccionado, se verifica la aplicabilidad de los controles de *CIS Controls*. La versatilidad de *CIS Controls* permite no solo cumplir con la implementación de una parte de los controles del Anexo A en toda la institución, también, facilita la identificación de vulnerabilidades de los activos de información de manera individualizada. En la fase “definición e implementación”, se indica qué controles *CIS* permiten implementar –de forma general- varios de los controles del Anexo A de la ISO 27001. El cuadro 26 describe qué controles de *CIS Controls* están implementados en la base de datos, cuales no y qué controles no son aplicables.

Cuadro 26. Análisis de vulnerabilidades del servidor de base de datos

N.º	Control crítico	Control esperado	Cumple
3.1	Control crítico #3: Gestión continua de vulnerabilidades	Ejecutar herramientas de escaneo automatizados de vulnerabilidades.	No
3.2		Realizar análisis de vulnerabilidades autenticados.	No
3.3		Proteger las cuentas dedicadas a auditorías.	No
3.4		Implementar herramientas de gestión automatizada de parches del sistema operativo.	No
3.5		Implementar herramientas de gestión automatizada de parches de software.	No
3.6		Comparar escaneos de vulnerabilidades consecutivos.	No
3.7		Utilizar un proceso de calificación de riesgo.	No
4.1	Control crítico #4: Uso controlado de los privilegios administrativos	Mantener un inventario de cuentas administrativas.	No
4.2		Cambiar contraseñas por defecto.	Sí
4.3		Asegurar el uso de cuentas administrativas dedicadas.	No
4.4		Usar contraseñas únicas.	Sí
4.5		Usar autenticación multifactor para todo acceso administrativo.	No aplica
4.6		Usar máquinas dedicadas para toda tarea administrativa.	No
4.7		Limitar el acceso a herramientas de scripts.	No
4.8		Registrar y alertar cambios de miembros en grupos administrativos.	No
4.9		Registrar y alertar los inicios de sesión fallidos a cuentas administrativas.	No
6.1	Control crítico #6: Mantenimiento, monitoreo y análisis de *logs* de auditoría	Utilizar tres fuentes de tiempo sincronizadas.	Sí
6.2		Activar registros de auditoría.	Sí
6.3		Habilitar registros detallados.	Sí
6.4		Asegurar almacenamiento adecuado para registros.	Sí
6.5		Gestión centralizada de registros.	Sí
6.6		Desplegar herramientas SIEM o de Análisis de registros.	No aplica
6.7		Revisar regularmente los registros.	Sí
6.8		Ajustar regularmente el SIEM.	No aplica
8.1	Control crítico #8: Defensa contra *malware*	Utilizar software antimalware de gestión centralizada.	Sí
8.2		Asegurar que el software antimalware y las firmas estén actualizadas.	Sí
8.3		Habilitar características anti-explotación de sistemas operativos / implementar tecnologías anti-explotación.	No
8.4		Configurar escaneo antimalware de dispositivos removibles.	No aplica
8.5		Configurar equipos para no autoejecutar contenido.	No
8.6		Centralizar los registros antimalware.	No
8.7		Habilitar registros de consultas DNS.	No
8.8		Habilitar registros de auditoría de línea de comandos.	No
9.1	Control crítico #9: Limitación y control de puertos de red, protocolos y servicios	Asociar puertos, servicios y protocolos activos al inventario de activos.	No
9.2		Asegurar que solo puertos, protocolos y servicios aprobados están en ejecución.	No
9.3		Realizar regularmente escaneos automatizados de puertos.	No
9.4		Aplicar firewalls basados en host o filtrado de puertos.	Sí

9.5		Implementar firewalls de aplicación.	Sí
10.1	Control crítico #10: Funciones de recuperación de datos	Asegurar los respaldos regulares automatizados.	Sí
10.2		Realizar respaldos de sistemas completos.	Sí
10.3		Probar los datos en los medios de respaldo.	Sí
10.4		Asegurar la protección de las copias de respaldo.	Sí
10.5		Asegurar que las copias de respaldo tengan al menos un destino discontinuo.	Sí
12.1	Control crítico #12: Protección perimetral	Mantener un inventario de los bordes de la red.	Sí
12.2		Escanear de conexiones no autorizadas en los bordes confiables de la red.	No
12.3		Denegar comunicaciones con direcciones IPs maliciosas conocidas.	Sí
12.4		Denegar comunicaciones sobre puertos no autorizados.	Sí
12.5		Configurar sistemas de monitoreo para registro paquetes de red.	No
12.6		Desplegar sensores IDS basados en red.	No
12.7		Desplegar IPS basado en red.	No
12.8		Desplegar colectores *NetFlow* en equipos de borde de la red Active la colección de *NetFlow* y registro de datos en todos los equipos de borde de la red.	Sí
12.9		Desplegar servidor proxy de filtrado de capa de aplicación.	Sí
12.10		Descifrar el tráfico de red en el proxy.	Sí
12.11		Requerir autenticación multi factor en todos los inicios de sesión remotos.	No aplica
12.12		Gestionar todos los dispositivos remotos que están conectados a la red interna.	No aplica
13.1	Control crítico #13: Protección de datos	Mantener un inventario de información sensible.	Sí
13.2		Remover datos o sistemas sensibles que no son accedidos regularmente por la organización.	No aplica
13.3		Monitorear y bloquear el tráfico de red no autorizado.	No
13.4		Permitir solamente el acceso a proveedores de servicios de nube o correo autorizados.	No aplica
13.5		Monitorear y detectar cualquier uso no autorizado de cifrado.	No aplica
13.6		Cifrar el disco duro de todos los dispositivos móviles.	No aplica
13.7		Gestionar dispositivos USB.	No
13.8		Gestionar las configuraciones de lectura/escritura de sistemas para medios removibles externos.	No
13.9		Cifrar los datos en dispositivos de almacenamiento USB.	No aplica
14.1	Control crítico #14: Control de acceso basado en la necesidad de saber	Segmentar la red basado en sensibilidad.	No aplica
14.2		Habilitar filtrado de firewall entre VLAN.	Sí
14.3		Deshabilitar comunicaciones entre estaciones de trabajo.	Sí
14.4		Cifrar toda la información sensible en tránsito.	Sí
14.5		Utilizar una herramienta de descubrimiento activo para identificar datos sensibles.	No
14.6		Proteger la información mediante lista de control de	Sí

		acceso.	
14.7		Aplicar control de acceso a datos mediante herramientas automatizadas.	Sí
14.8		Cifrar información sensible en reposo.	Sí
14.9		Imponer el registro detallado para acceso o cambios en datos sensibles.	Sí

Fuente: modificado a partir de Center for Internet Security (CIS) (s.f.)

De los 72 controles seleccionados para el activo de información, la institución cumple con 31 (43,06%), incumple con 29 (40,27%) y 12 (16,67%) controles no son aplicables. “En informática, una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad” (Banco Santander S.A., s.f.). Con estos antecedentes es posible concluir que el activo de información registra 29 vulnerabilidades que son mitigadas a través de un plan de acción.

Los planes de acción permiten alcanzar las metas y objetivos de la institución. Estos son parte del mejoramiento continuo que está asociado al sistema de gestión de la calidad. Incluso, la norma ISO 27001, en su acápite 10.2, habla del mejoramiento continuo. “El mejoramiento continuo es una técnica, enfoque y un pilar básico de cada compañía, que consiste principalmente en mejorar todos y cada uno de los procesos operativos, servicios y productos (…) (de la) empresa” (Salazar, 2021). Al nivel del SGSI, el análisis de vulnerabilidades de los activos de información es una actividad esencial, lo que significa que la institución requiere establecer políticas que describan la temporalidad de estas acciones.

Para el activo de información seleccionado, se establece como proyecto “Reducción de las vulnerabilidades identificadas en el servidor de base de datos institucional”. El plan de acción planteado formula siete objetivos con base en los siete controles críticos seleccionados para el activo, cada una de las actividades de los objetivos están asociados a los subcontroles.

Cuadro 27. Plan de acción para mitigación de vulnerabilidades

PLAN DE ACCIÓN PARA MITIGACIÓN DE VULNERABILIDADES					
Reducción de las vulnerabilidades identificadas en el servidor de base de datos institucional					
Número	PMV-001				
Elaborado por:	Oficial de seguridad de la información				
Aprobado por:	Comité de seguridad de la información				
Acción	**Responsable**	**Prioridad**	**Estado**	**Fecha inicial**	**Fecha final**
Objetivo 1: gestionar continuamente las vulnerabilidades					
Ejecutar herramientas de escaneo automatizados de vulnerabilidades.	Analista de tecnologías de la información y comunicación / oficial de seguridad de la información	Alta	Pendiente	17/10/2022	17/10/2022
Realizar análisis de vulnerabilidades autenticados.	Analista de tecnologías de la información y comunicación / oficial de seguridad de la información	Alta	Pendiente	18/10/2022	18/10/2022
Proteger las cuentas dedicadas a auditorías.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	19/10/2022	19/10/2022
Implementar herramientas de gestión automatizada de parches del sistema operativo.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	24/10/2022	28/10/2022
Implementar herramientas de gestión automatizada de parches de software.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	24/10/2022	28/10/2022
Objetivo 2: Establecer mecanismos de uso controlado de los privilegios administrativos del servidor de base de datos					
Mantener un inventario de cuentas administrativas.	Analista de tecnologías de la información y comunicación	Baja	Pendiente	31/10/2022	31/10/2022
Asegurar el uso de cuentas administrativas dedicadas.	Analista de tecnologías de la información y comunicación	Baja	Pendiente	1/11/2022	1/11/2022
Usar máquinas dedicadas para toda tarea administrativa.	Analista de tecnologías de la información y comunicación	Baja	Pendiente	2/11/2022	2/11/2022
Limitar el acceso a herramientas de scripts.	Analista de tecnologías de la información y comunicación	Baja	Pendiente	2/11/2022	2/11/2022
Registrar y alertar	Analista de	Baja	Pendiente	2/11/2022	2/11/2022

cambios de miembros en grupos administrativos.	tecnologías de la información y comunicación				
Registrar y alertar los inicios de sesión fallidos a cuentas administrativas.	Analista de tecnologías de la información y comunicación	Baja	Pendiente	2/11/2022	2/11/2022
Objetivo 3: Activar y supervisar mecanismos de defensa contra *malware*					
Habilitar características anti-explotación de sistemas operativos / implementar tecnologías anti-explotación.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	7/11/2022	8/11/2022
Configurar equipos para no auto ejecutar contenido.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	9/11/2022	9/11/2022
Centralizar los registros antimalware.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	9/11/2022	9/11/2022
Habilitar registros de consultas DNS.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	9/11/2022	9/11/2022
Habilitar registros de auditoría de línea de comandos.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	9/11/2022	9/11/2022
Objetivo 4: Limitar y controlar los puertos de red, protocolos y servicios del servidor de base de datos					
Asociar puertos, servicios y protocolos activos al inventario de activos.	Analista de tecnologías de la información y comunicación / oficial de seguridad de la información	Media	Pendiente	10/11/2022	10/11/2022
Asegurar que solo puertos, protocolos y servicios aprobados están en ejecución.	Analista de tecnologías de la información y comunicación / oficial de seguridad de la información	Media	Pendiente	10/11/2022	10/11/2022
Objetivo 5: Habilitar la protección perimetral					
Escanear de conexiones no autorizadas en los bordes confiables de la red.	Analista de tecnologías de la información y comunicación	Baja	Pendiente	14/11/2022	14/11/2022
Configurar sistemas de monitoreo para registro paquetes de	Analista de tecnologías de la información y	Baja	Pendiente	15/11/2022	15/11/2022

red.	comunicación				
Desplegar sensores IDS basados en red.	Analista de tecnologías de la información y comunicación	Baja	Pendiente	16/11/2022	16/11/2022
Desplegar IPS basado en red.	Analista de tecnologías de la información y comunicación	Baja	Pendiente	17/11/2022	17/11/2022
Objetivo 6: Habilitar la protección de datos					
Monitorear y bloquear el tráfico de red no autorizado.	Oficial de seguridad de la información	Baja	Pendiente	18/11/2022	Indefinido
Gestionar dispositivos USB.	Analista de tecnologías de la información y comunicación	Baja	Pendiente	21/11/2022	21/11/2022
Gestionar las configuraciones de lectura/escritura de sistemas para medios removibles externos.	Analista de tecnologías de la información y comunicación	Baja	Pendiente	22/11/2022	22/11/2022
Objetivo 7: Controlar el acceso basado en la necesidad de saber					
Utilizar una herramienta de descubrimiento activo para identificar datos sensibles.	Oficial de seguridad de la información	Media	Pendiente	28/11/2022	15/11/2022

Fuente: elaboración propia

Fase 3: definición e implementación

El alcance (cumplimiento del acápite 4.3 de la ISO 27001) del modelo de gestión de seguridad de la información abarca todos los procesos de la institución descritos en el mapa general de procesos (revisar cuadro 5). La cooperativa identifica como partes interesadas (cumplimiento del acápite 4.2 de la ISO 27001) a: socios, directivos, empleados y proveedores (revisar gráfico 6).

La institución establece como política general de seguridad de la información (cumplimiento del acápite 5.2 de la ISO 27001) la siguiente:

“Ser una institución financiera cooperativa que garantice la confidencialidad, integridad y disponibilidad de la información, que cumpla con la normativa nacional

vigente en materia de seguridad de la información, y promueva un comportamiento responsable entre directivos, socios, empleados y proveedores".

Los objetivos de seguridad de la información (cumplimiento del acápite 6.2 de la ISO 27001) están alineados a la política general. Estos son:

- "Garantizar la confidencialidad, integridad y disponibilidad de la información generada, almacenada y transmitida por la institución".
- "Cumplir con la normativa nacional vigente aplicable en materia de seguridad de la información".
- "Crear y promover una cultura de seguridad de la información en socios, directivos, empleados y proveedores".

Para desarrollar la última dimensión del Cubo de McCumber relacionado con "factores humanos, políticas y prácticas", la institución define un sistema de gobierno de seguridad de la información. "Una de las principales razones para crear un modelo (…) de gobierno es definir y documentar los procesos, procedimientos y mecanismos de presentación de reportes que constituirán el gobierno, junto con el entrenamiento, la TI y los otros recursos que se necesitarán" (Deloitte Development LLC, 2013, pág. 9).

(Díaz Evans, 2011) indica: "el gobierno de seguridad de la información es un subconjunto del gobierno corporativo de la organización que provee dirección estratégica, garantiza los objetivos establecidos, gestiona los riesgos de forma apropiada, usa los recursos organizacionales responsablemente y monitorea el éxito o falla del programa de seguridad de la organización" (pág. 10).

La institución establece el sistema de gobierno de seguridad de la información basado en el modelo de gobierno propuesto por Cobit 2019[i] (revisar gráfico 9). Los componentes del sistema tienen como eje central el programa de seguridad de la información que están conformados por "un conjunto de proyectos, iniciativas y actividades realizadas de manera coordinada para lograr una estrategia de

seguridad, es decir, llevar a la práctica un plan trazado que busca alcanzar los objetivos de protección de una organización" (Mendoza, 2017).

Gráfico 9. Componentes del sistema de gobierno de seguridad de la información

Fuente: modificado a partir de ISACA (2019)

Componente: procesos

Cobit® 2019 *Framework*: *Introduction & Methodology*, define a los procesos como "un conjunto organizado de prácticas y actividades (…) (que permiten) alcanzar determinados objetivos y producir un conjunto de resultados que apoyan la consecución de los objetivos generales relacionados con las TI" (ISACA, 2019, pág. 21).

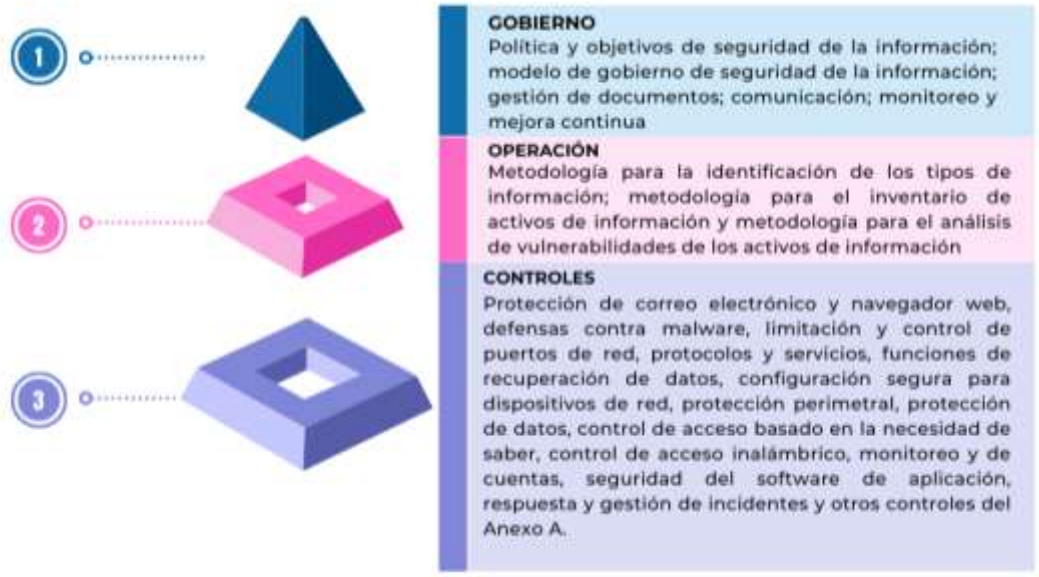
La institución establece en este componente al modelo de gestión de seguridad de la información basado en la norma ISO 27001. El modelo es un conjunto de prácticas y actividades que buscan garantizar la confidencialidad, integridad y disponibilidad de la información. Para el modelo del SGSI, la cooperativa plantea un esquema conformado por tres macro secciones: 1) gobierno, 2) operación y 3) controles.

La sección gobierno (1) asegura que los objetivos de la institución en materia de seguridad de la información sean alcanzados mediante la evaluación de las necesidades de las partes interesadas.

La sección operación (2) son las metodologías aplicadas para la identificación de los tipos de información, los inventarios de activos de información y análisis de vulnerabilidades de los activos de información (cumplimiento de los acápites 6.1.2 y 6.1.3 de la ISO 27001).

La sección controles (3) establece los mecanismos de seguridad que la institución define para proteger sus activos de información. Estos están relacionados con *CIS Controls* y el Anexo A. El gráfico 10 presenta el modelo de gestión de seguridad de la institución financiera.

Gráfico 10. Modelo de GSI



Fuente: elaboración propia

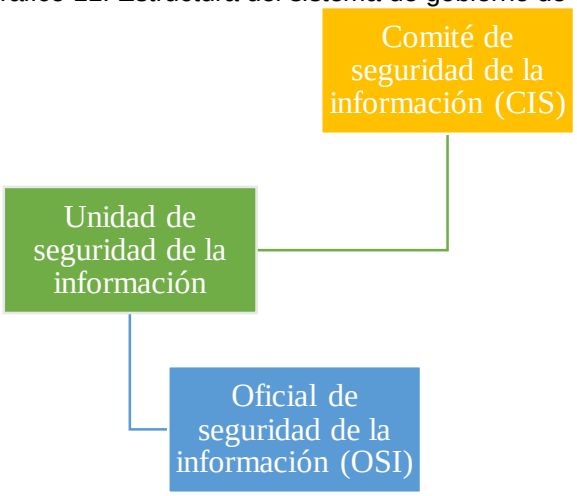
Componente: estructura organizacional

La estructura organizacional “es la forma en cómo se distribuyen las funciones y responsabilidades que debe cumplir cada miembro que forma parte de una empresa para alcanzar los objetivos propuestos” (Jaime, s.f.). El esquema planteado por la cooperativa está basado en la “Norma de control respecto a la seguridad de la información en las entidades del Sector Financiero Popular y Solidario bajo control de la Superintendencia de Economía Popular y Solidaria”.

La estructura (cumplimiento del acápite 5.3 de la ISO 27001), revisar gráfico 11, como parte del sistema de gobierno del SGSI (sección gobierno), tiene como máximo ente regulador al comité de seguridad de la información (CSI). Este comité de carácter técnico está conformado por: 1) el presidente del comité de administración integral de riesgos, quien presidie el comité de seguridad de la información y tiene voto dirimente; 2) el gerente general; 3) el oficial de seguridad de la información, quien actúa como secretario del comité; 4) el jefe de tecnologías de la información y

comunicación; y, 5) un delegado de auditoría interna. La unidad de seguridad de la información está liderada por el oficial de seguridad de la información.

Gráfico 11. Estructura del sistema de gobierno de SI



Fuente: elaboración propia

La norma de control respecto a la seguridad de la información indica que las funciones del comité de seguridad de la información están relacionadas con que este órgano de gobierno solicita al consejo de administración la aprobación de:

1) El plan estratégico de seguridad de la información.
2) Los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad.
3) Las políticas, procedimientos, roles y responsabilidades para la gestión de seguridad de la información y del SGSI.
4) El plan de concienciación y formación de su personal, en temas concernientes a seguridad de la información.
5) El plan de gestión de riesgos de seguridad de la información que está alineado al plan de administración de riesgos.

El oficial de seguridad de la información (OSI o CISO), “es un ejecutivo de alto nivel responsable de desarrollar e implementar un programa de seguridad de la información, que incluye procedimientos y políticas diseñadas para proteger las

comunicaciones, los sistemas y los activos de la empresa de amenazas internas y externas" (McLaughlin, 2021). La norma de control respecto a la seguridad de la información considera como responsabilidades del OSI las siguientes:

1) Desarrollar, gestionar y monitorear el plan estratégico de seguridad de la información y el SGSI.
2) Diseñar y proponer las políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información y del SGSI, al consejo de administración.
3) Solicitar la asignación de los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información, y velar que los mismos sean utilizados de forma eficiente y eficaz, alineados con los objetivos estratégicos institucionales.
4) Elaborar, implementar, mantener y actualizar las políticas, procesos, procedimientos, metodologías, planes y controles concernientes a la gestión de seguridad de la información, del SGSI, su mejora continua; y, una vez aprobados, difundirlos al personal que corresponde.
5) Desarrollar y ejecutar los planes de concienciación y formación a su personal, con temas concernientes a seguridad de la información.
6) Coordinar y supervisar, con los responsables de los procesos del negocio, la implementación efectiva de los controles de seguridad de la información, establecidos en el plan de gestión de riesgos.
7) Desarrollar, coordinar, ejecutar, evaluar, proponer y comunicar el plan de gestión de riesgos de seguridad de la información.
8) Coordinar las actividades para la gestión de seguridad de la información y del SGSI, que incluya su implementación y seguimiento.
9) Definir, ejecutar y mantener procedimientos para la gestión de incidentes de seguridad de la información.
10) Velar que los involucrados internos y/o externos cuenten con los conocimientos y capacitación necesaria para el cumplimiento de sus roles y responsabilidades para la ejecución de procedimientos de respuesta ante incidentes.

11) Ejecutar los procedimientos y lineamientos establecidos, de existir incidentes de seguridad de la información.
12) Informar, de acuerdo con la normativa pertinente, los incidentes de seguridad de la información catalogados como sensibles o críticos, a las instituciones públicas que correspondan.
13) Participar en la evaluación de las amenazas de seguridad de la información y proponer medidas de mitigación.
14) Asesorar en materia de seguridad de la información, a través de su participación en los proyectos que involucren el manejo de información sensible o critica de la misma, de sus socios, clientes y usuarios.
15) Recomendar medidas correctivas adicionales en temas relacionados con seguridad de la información,
16) Verificar que los servicios prestados por personas naturales o jurídicas cumplan con las políticas de seguridad de la información establecidas.
17) Generar la documentación que evidencie la gestión de la seguridad de la información y del SGSI.

Componentes: principios, políticas y procedimientos; y, personas, habilidades y competencias

Para cumplir con los requisitos exigidos por la SEPS, como parte de los controles del modelo del SGSI y del cumplimiento del Anexo A de la norma ISO 27001, la institución define el "*manual de políticas de seguridad de la información*" (principios, políticas y procedimientos) que constituye un conjunto de directrices para gestionar adecuadamente la seguridad de la información. El instrumento define los roles y responsabilidades en el ámbito de seguridad de la información (personas, habilidades y competencias).

En el contexto de la institución, el documento debe conocerse y cumplirse por toda la estructura organizacional. Una política es "serie de normas y directrices que permiten

garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan” (UNIR, s.f.).

La institución al empezar con la elaboración del manual planteó la siguiente interrogante: ¿cómo generar un conjunto de políticas (controles) de seguridad de la información que estén basadas en buenas prácticas internacionales y que protejan a la cooperativa?

Para implementar parte de los controles descritos en el Anexo A de la ISO 27001, la institución empleó *CIS Controls*. *AuditScripts Critical Security Control Master Mappings v7.0d*, es una herramienta de *AuditScripts* que permite gestionar parte del cumplimiento del Anexo A. El Anexo 5 presenta qué controles del Anexo A son aplicables mediante la metodología planteada por AuditScripts.

Para diseñar el "manual de políticas de seguridad de la información" la institución consideró los 20 macro controles (revisar gráfico 4) de *CIS Controls*. Los macros controles corresponden a:

1) Básicos:
    a) Inventario y control de activos de hardware.
    b) Inventario y control de activos de software.
    c) Gestión continua de vulnerabilidades.
    d) Uso controlado de los privilegios administrativos.
    e) Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores.
    f) Mantenimiento, monitoreo y análisis de *logs* de auditoría.
2) Fundamentales:
    g) Protección de correo electrónico y navegador web.
    h) Defensas contra *malware*.
    i) Limitación y control de puertos de red, protocolos y servicios.
    j) Funciones de recuperación de datos.
    k) Configuración segura para dispositivos de red.

l) Protección perimetral.
m) Protección de datos.
n) Control de acceso basado en la necesidad de saber.
o) Control de acceso inalámbrico.
p) Monitoreo y de cuentas.

3) Organizacionales
   q) Seguridad del software de aplicación.
   r) Respuesta y gestión de incidentes.
   s) Pruebas de penetración.

No obstante, la institución incorporó como políticas del manual, los controles del Anexo A que no son posible establecer mediante *CIS Controls*. Estos corresponden a:

1) A.7 Seguridad en recursos humanos: A.7.1.1 investigación de antecedentes, A.7.1.2 términos y condiciones del empleo, A.7.2.3 proceso disciplinario y A.7.3.1 responsabilidades ante la finalización o cambio de empleo.
2) A.8 Gestión de activos: A.8.1.2 propiedad de los activos, A.8.1.4 devolución de activos, A.8.2.1 clasificación de la información, A.8.2.2 etiquetado de la información y A.8.2.3 manejo de los activos. La clasificación de la información guarda relación con la metodología respectiva
3) A.11 seguridad física y del entorno: A.11.1.1 perímetro de seguridad física, A.11.1.2 controles físicos de entrada, A.11.1.3 seguridad de oficinas, despachos e instalaciones, A.11.1.4 protección contra las amenazas externas y ambientales, A.11.1.5 trabajo en áreas seguras, A.11.2.1 ubicación y protección de equipos, A.11.2.2 instalaciones de suministro, A.11.2.3 seguridad del cableado, A.11.2.4 mantenimiento de los equipos, A.11.2.5 eliminación de activos, A.11.2.6 seguridad de los equipos y activos fuera de las instalaciones, A.11.2.7 reutilización o eliminación segura de equipos, A.11.2.9 política de puesto de trabajo despejado y pantalla limpia.

4) A.12 Seguridad de las operaciones: A.12.1.1 documentación de procedimientos de operación, A.12.1.2 gestión de cambios y A.12.1.3 gestión de capacidades.
5) A.13 Seguridad en las comunicaciones: A.13.1.2 seguridad de los servicios de red y A.13.2.4 acuerdos de confidencialidad o no revelación.
6) A.14 Adquisición, desarrollo y mantenimiento del sistema: A.14.1.1 análisis de requisitos y especificaciones de seguridad de la información, A.14.1.3 protección de las transacciones de servicios de aplicaciones, A.14.2.2 procedimientos de control de cambios en sistemas, A.14.2.3 revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo, A.14.2.5 principios de ingeniería de sistemas seguros, A.14.2.9 pruebas de aceptación de sistemas y A.14.3.1 protección de los datos de prueba.
7) A.15 Relaciones con proveedores: A.15.1.1 política de seguridad de la información en las relaciones con los proveedores, A.15.1.2 requisitos de seguridad en contratos con terceros, A.15.1.3 cadena de suministro de tecnologías de la información y de las comunicaciones, A.15.2.1 monitoreo y revisión de los servicios de proveedores y A.15.2.2 gestión de cambios en los servicios de proveedores.
8) A.16 Gestión de incidentes de seguridad de la información: A.16.1.2 informe de los eventos de seguridad de la información y A.16.1.3 informe de debilidades de seguridad de la información.
9) A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio: A.17.1.1 planificación de la continuidad de la seguridad de la información, A.17.1.2 implementación de la continuidad de seguridad de la información, A.17.1.3 verificar, revisar y evaluar la continuidad de seguridad de la información, A.17.2 Redundancias y A.17.2.1 disponibilidad de las instalaciones de procesamiento de la información.
10) A.18 Cumplimiento: A.18.1.1 identificación de la legislación aplicable y de los requisitos contractuales, A.18.1.3 protección de los registros, A.18.1.4 protección y privacidad de la información de carácter personal, A.18.2

revisiones de seguridad de la información y A.18.2.2 cumplimiento de las políticas y normas de seguridad.

La estructura del “manual de políticas de seguridad de la información” está representada por: 1) objetivo, 2) alcance, 3) documentos de referencia, 4) vocabulario y 5) políticas. Cada política de seguridad está identificada con el tipo activo, la función de seguridad y qué principio o principios de la seguridad protege. Los tipos de activos son: datos, equipos, red y usuarios. Las funciones de seguridad son: identificar, responder, proteger y detectar. A continuación, son presentadas tres políticas del “manual de políticas de seguridad de la información”.

Política: mantener un inventario de información sensible

Mantener un inventario de información sensible		
Tipo de activo	**Función de seguridad**	**Principios**
Datos	Identificar	Confidencialidad Integridad

Son funciones del encargado de las entidades de información:

- Identificar, registrar y actualizar los tipos de información asociadas a las entidades correspondientes.
- Determinar el riesgo inherente de la confidencialidad e integridad de los tipos de información para lo cual, es necesario emplear las siguientes aristas de evaluación: impacto en la continuidad del servicio, impacto legal e impacto económico en la institución.
- Los tipos de información que registren el mayor impacto de la confidencialidad e integridad de los tipos de información son considerados como información sensible.

Política: etiquetado de información

Etiquetar la información		
Tipo de activo	**Función de seguridad**	**Principios**
Datos	Identificar	Confidencialidad Integridad

El encargado de las entidades de información, en coordinación con el oficial de seguridad de la información, etiquetan los activos de información bajo su custodio de acuerdo con el impacto total de la confidencialidad e integridad de la información según:

Impacto total de la confidencialidad e integridad del tipo de información	Etiqueta	Descripción
Crítico	Confidencial	La alta gerencia tiene acceso a la información.
Alto	Restringido	La alta gerencia tiene acceso a la información.
Medio	Interno	La alta gerencia y empleados tienen acceso a la información.
Bajo	Público	Cualquier persona tiene acceso a la información.
Muy bajo	Público	Cualquier persona tiene acceso a la información.

Política: prevención de fuga de información

Prevenir fuga de información		
Tipo de activo	**Función de seguridad**	**Principios**
Datos	Identificar	Confidencialidad Integridad

Son funciones del encargado de las entidades de información y del oficial de seguridad de la información:

- Solicitar al administrador de la base de datos cifrar los tipos de información sensibles.

- Inhabilitar el envío de correos electrónicos a cuentas que no pertenezcan a la cooperativa.
- Inhabilitar el ingreso al correo electrónico desde una red externa de comunicación.

Varias políticas de seguridad definidas por la institución requieren establecer un plan de acción que permita en un plazo determinado alcanzar su implementación. Estas acciones son parte del plan de seguridad de la información. Por ejemplo, para la política de prevención de fuga de información la cooperativa establece el siguiente plan de acción:

Cuadro 28. Plan de implementación de política de seguridad

PLAN DE IMPLEMENTACIÓN DE POLÍTICA DE SEGURIDAD					
Implementación de mecanismos de prevención de fuga de información					
Número	PIPS-001				
Elaborado por:	Oficial de seguridad de la información				
Aprobado por:	Comité de seguridad de la información				
Acción	**Responsable**	**Prioridad**	**Estado**	**Fecha inicial**	**Fecha final**
Objetivo 1: cifrar tipos de información sensibles					
Analizar herramientas compatibles con Microsoft SQL Server para el cifrado de información.	Jefe de tecnologías de la información y comunicación, oficial de seguridad de la información	Media	Pendiente	01/02/2023	28/02/2023
Solicitar adquisición de la herramienta de cifrado de información.	Jefe de tecnologías de la información y comunicación	Media	Pendiente	01/03/2023	31/03/2023
Implementar la herramienta de cifrado de información.	Administrador de base de datos	Alta	Pendiente	03/04/2023	28/04/2023
Cifrar tipos de información sensible.	Administrador de base de datos, oficial de seguridad de la información	Alta	Pendiente	02/05/2023	12/05/2023
Monitorizar comportamiento de aplicaciones.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	15/05/2023	26/05/2023
Informar al comité de seguridad de la información el cumplimiento del	Oficial de seguridad de la información	Baja	Pendiente	29/05/2023	02/06/2023

objetivo.					
Objetivo 2: proteger fugas de información mediante correo electrónico					
Identificar empleados que manejan tipos de información sensibles y que no pertenezcan a la alta gerencia.	Oficial de seguridad de la información	Alta	Pendiente	03/01/2023	13/01/2023
Inhabilitar el envío de correos electrónicos a cuentas que no pertenezcan a la cooperativa para los empleados previamente identificados.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	16/01/2023	20/01/2023
Inhabilitar el acceso al correo externo desde una red de externa de comunicación para los empleados previamente identificados.	Analista de tecnologías de la información y comunicación	Alta	Pendiente	16/01/2023	20/01/2023
Informar al comité de seguridad de la información el cumplimiento del objetivo.	Oficial de seguridad de la información	Baja	Pendiente	28/01/2023	03/02/2023

Fuente: elaboración propia

Componente: información

(ISACA, 2019), a través de *Cobit* 2019, considera que la información "es universal en cualquier organización e incluye toda la información producida y utilizada por la empresa. *Cobit,* se centra en la información necesaria para el funcionamiento eficaz del sistema de gobierno de la empresa" (pág. 21). Al nivel del sistema de gobierno de seguridad de la información, la cooperativa requiere de información oportuna para conocer el estado de sus procesos. Esto, se realiza mediante el establecimiento de métricas que representan un elemento esencial que permite a la institución tomar decisiones oportunas, enmarcadas en el mejoramiento continuo, con el fin de adaptar al sistema de gobierno al entorno cambiante.

La institución financiera cooperativa, a partir del marco de trabajo de *Cobit* 2019, establece un conjunto de métricas que permiten medir el desempeño de la organización en términos de seguridad de la información como, por ejemplo:

- Número de incidentes relacionados con el incumplimiento de la política de seguridad de la información.
- Porcentaje de las partes interesadas que entienden la política y objetivos de seguridad de la información.
- Porcentaje de políticas de seguridad descritas en el manual correspondiente que están implementadas y en ejecución.
- Porcentaje de planes de acciones de seguridad de la información ejecutados y cumplidos.
- Porcentaje de empleados capacitados en temas concernientes a seguridad de la información.
- Porcentaje de socios capacitados en temas concernientes a seguridad de la información.
- Porcentaje de proveedores capacitados en temas concernientes a seguridad de la información.
- Número de acuerdos de confidencialidad.
- Número de incidentes relacionados con el incumplimiento de las políticas de seguridad de la información.
- Número de incidentes de seguridad de la información.

El “manual de políticas de seguridad de la información” indica que es responsabilidad del oficial de seguridad de la información presentar una vez al año, al comité de seguridad de la información, un informe que detalle los resultados de las evaluaciones de las métricas relacionadas al componente ‘información’ del sistema de gobierno de seguridad de la información”.

Componente: cultura, ética y comportamiento

Para “Implementar un programa de concienciación y capacitación en seguridad” (macro control 17), la norma de control de seguridad de la información en su Artículo 9, indica que las organizaciones del régimen general contarán obligatoriamente con un “Plan de Concienciación y Formación de Seguridad de la Información”. El plan

propuesto por el comité de seguridad de la información está alineado al plan general de capacitación el que está aprobado por el consejo de administración. De esta manera, el componente “Cultura, ética y comportamiento” está cumplido.

Componente: servicios, infraestructura y aplicaciones

Este componente constituye la infraestructura, tecnología y aplicaciones que requiere la unidad de seguridad de la información para cumplir con sus fines.

El “manual de políticas de seguridad de la información” en varios de sus artículos describe la relación con el “manual de gestión de la infraestructura tecnológica”. El nuevo cuerpo normativo permite al proceso de tecnologías de la información y comunicación replantear sus roles y responsabilidades para mantener la disponibilidad de los activos de información.

La unidad de seguridad de la información asume varias de las responsabilidades que cumplía el proceso de TICS a la unidad. Por ejemplo, al nivel de servicios (externos) y aplicaciones, la unidad de seguridad de la información asume la responsabilidad de ejecutar el escaneo de vulnerabilidades de los activos de información y coordinar pruebas de penetración.

Para las pruebas de penetración (macro control 20), el Anexo 1 de la norma de control de seguridad de la información indica que la cooperativa debe al menos una vez al año: “a) Revisar la seguridad de sus activos mediante ejercicios prácticos y controlados, tales como *ethical hacking*, *pentesting*, entre otros, que simulen varios tipos de amenazas; y, b) Evaluar la infraestructura y aplicativos que soportan todos los servicios, en diferentes escenarios. Las pruebas y/o ejercicios serán ejecutadas por personas naturales o jurídicas externas que acrediten experiencia en este tipo de evaluaciones” (Superintendencia de Economía Popular y Solidaria, 2022).

La institución aprueba en el presupuesto para el año 2023 de la unidad de seguridad de la información los recursos económicos para adquirir o contratar servicios especializados de *ethical hacking*.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1. Antecedentes

La institución financiera cooperativa entiende las tres dimensiones del cubo de McCumber. Para relacionar la primera y segunda dimensión realizó: 1) el inventario de los tipos de información y activos de información; 2) la valoración del riesgo intrínseco que permite determinar el impacto en la confidencialidad, integridad y disponibilidad de los activos de información; y, 3) la relación entre servicios, canales, aplicaciones, servidores y base de datos. El ejercicio planteado facilita entender cómo los datos son generados (procesamiento), almacenados (almacenamiento) y transmitidos (transmisión), revisar gráfico 7.

La disponibilidad es parte de los tres principios fundamentales de la seguridad de la información. La RAE define el término “disponible” como “una cosa (…) que se puede disponer libremente de ella o que está lista para usarse o utilizarse” (Real Academia Española, s.f.). Bajo esta premisa, hablar de disponibilidad es hablar de la disponibilidad de los servicios (servicios financieros) y sus relaciones (revisar gráfico 8) al considerar que estos son los que permiten generar, almacenar y transmitir información.

¿Es posible evaluar un modelo de gestión de seguridad de la información al poco tiempo de implementarse? La institución entiende que el proceso de ejecución no significa que el modelo funciona adecuadamente. La cooperativa estima que la consolidación del modelo, como tal, durará al menos tres años, motivada por la experiencia al implementar la norma ISO 9001.

¿Qué ocurre en este período? Por ejemplo, la unidad de seguridad de la información -liderada por el oficial de seguridad de la información-, está en la obligación de verificar que los planes de acción y mitigación propuestos y aprobados por el comité de seguridad de la información cumplan sus objetivos. A más de verificar la

observancia de las políticas descritas en el “manual de políticas de seguridad de la información”. Esto no es suficiente porque a medida que el entorno tecnológico evoluciona, las amenazas cibernéticas crecen a la par, por tanto, los mecanismos que permiten proteger la información deben monitorearse y evaluarse constantemente.

También, por un lado, la institución ha considerado que la fuga de información es una amenaza. Para mitigarla ha creado mecanismos que desincentiven estas prácticas mediante el establecimiento de acuerdos de confidencialidad y no divulgación de la información entre los empleados.

Por otro lado, la mayor amenaza que enfrenta la institución son los ataques de “ransomware”. La IFC lo considera como la mayor amenaza por los antecedentes registrados en otras instituciones financieras nacionales -algunas de conocimiento público, otras no-. Con esta consideración, la propia cooperativa estableció un plan de prevención de ataques de “ransomware”, en los que están incluidas: prohibición de teletrabajo, actualización de software y hardware, análisis de vulnerabilidades, ejercicios de penetración y más.

3.2. Evaluación final

Introducción

Para “diagnosticar el cumplimiento de la normativa internacional ISO 27001 en la institución financiera cooperativa”, se determina el nivel inicial de madurez de la seguridad de la información mediante la aplicación del modelo de madurez genérico de *Cobit* 4.1. Esto, se logra mediante la verificación del cumplimiento de las cláusulas del sistema de gestión de seguridad de la información relacionada con la normativa ISO 27001 y de los controles descritos en el Anexo A. (revisar “Fase 1: diagnóstico” del capítulo II).

Para establecer e implementar un modelo de gestión de seguridad de la información (objetivos específicos 3 y 4), la institución financiera cooperativa definió un sistema de gobierno de seguridad de la información (revisar gráfico 10).

El sistema de gobierno está basado en el modelo de gobierno propuesto por *Cobit* 2019. Su eje central es el plan de seguridad de la información. El componente "procesos" es parte del gobierno que en sí es el modelo de gestión de seguridad de la información. El modelo articulado está representado por tres macro secciones: 1) gobierno, 2) operación y 3) controles (revisar sección "Fase 3: definición e implementación" del capítulo II).

Fase 4: evaluación (nivel final de madurez de la seguridad de la información)

A pesar de los antecedentes descritos en la sección "3.1 Antecedentes", es necesario evaluar la implementación del modelo de seguridad de la información. Para cumplir con el objetivo principal del proyecto de desarrollo, es necesario determinar el nivel final de madurez de la seguridad de la información.

No existe un modelo genérico que permita medir el nivel de madurez. Entonces, para cumplir con el fin, la evaluación de la implementación emplea el modelo genérico de madurez propuesto por *Cobit* 4.1; método descrito en el título "Nivel de madurez de seguridad de la información" del capítulo I, que fue empleado para medir el nivel de madurez inicial.

La evaluación emplea un análisis GAP que está limitado a evaluar el cumplimiento de las cláusulas y controles a través de tres únicas opciones: "cumple", "no cumple" y "no aplica". Para determinar el nivel final de madurez, es necesario evaluar: 1) el cumplimiento de las cláusulas del sistema de gestión de seguridad de la información relacionada con la normativa ISO 27001 y, 2) el cumplimiento de los controles descritos en el Anexo A.

La primera evaluación final -al igual que la evaluación inicial- emplea un documento de 52 preguntas que permite determinar el cumplimiento de las cláusulas del sistema de gestión de seguridad de la información (el anexo 6 describe cada una de las preguntas y respuestas que conforman el cuestionario). La segunda evaluación final emplea un documento que describe cuáles de los 114 controles están implementados por la institución (el anexo 7 describe qué controles están o no están implementados, o por la naturaleza de la institución no son aplicables).

El primer cuestionario, relacionado con la primera sección de la normativa ISO 27001, está destinado a los responsables de los procesos descritos en el cuadro 5. La segunda evaluación, relacionada con los controles del Anexo A, está destinado –mayoritariamente- para el jefe de tecnologías de la información y comunicación, jefe de talento humano, gerente general y auditor interno. La evaluación no está limitada únicamente a considerar lo descrito por los evaluados, todo lo contrario, es dinámico, es decir, el evaluador (investigador) supervisa instalaciones físicas, instalaciones de red e instalaciones eléctricas, estaciones de trabajo para verificar, por ejemplo, el cumplimiento de las políticas de escritorios y pantallas limpias, etc.

Para obtener el nivel final de madurez de la IFC, se emplea –nuevamente- la siguiente formula:

Porcentaje de maduración = (total “cumple” / total de controles evaluados sin incluir los “no aplica”) *100%

Finalmente, de acuerdo con lo descrito previamente, la tabla 7 evalúa el cumplimiento total de las cláusulas del sistema de gestión de seguridad de la información. La tabla 8 evalúa qué controles descritos en el Anexo A están o no están implementados por la institución.

Tabla 7. Cumplimiento total de las cláusulas del SGSI

¿Cumple?	N.º Clausulas	Representación
Sí	39	75,00%
No	13	25,00%
Total	**52**	**100,00%**

Fuente: elaboración propia

El nivel final de madurez de la seguridad de la información de la institución relacionado con el cumplimiento de las cláusulas de la norma ISO 27001 es del 75,00%. Según el modelo genérico de madurez de *Cobit* 4.1., descrito en la sección "1.2 Sistema de gestión de seguridad de la información" del capítulo I (revisar gráfico 5), se determina que el nivel de madurez de la seguridad de la información es "administrado", lo que significa que la cooperativa requiere "monitorear y medir el cumplimiento de los procedimientos y tomar medidas (si) los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas" (IT Governance Institute, 2007).

Tabla 8. Controles del Anexo A que están o no están implementados

¿Cumple?	N.º Controles	Representación	Representación sin considerar "no aplica"
Sí	105	92,11%	98,13%
No	2	1,75%	1,87%
No aplica	7	6,14%	-
Total	**114**	**100,00%**	**-**

Fuente: elaboración propia

El nivel final de madurez de la seguridad de la información de la institución relacionado con el cumplimiento de los controles descritos en el Anexo A del estándar ISO 27001 es del 92,11%. Según el modelo genérico de madurez de *Cobit* 4.1. (revisar gráfico 5), se determina que el nivel de madurez de la seguridad de la información es "optimizado", lo que significa que "los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas" (IT Governance Institute, 2007).

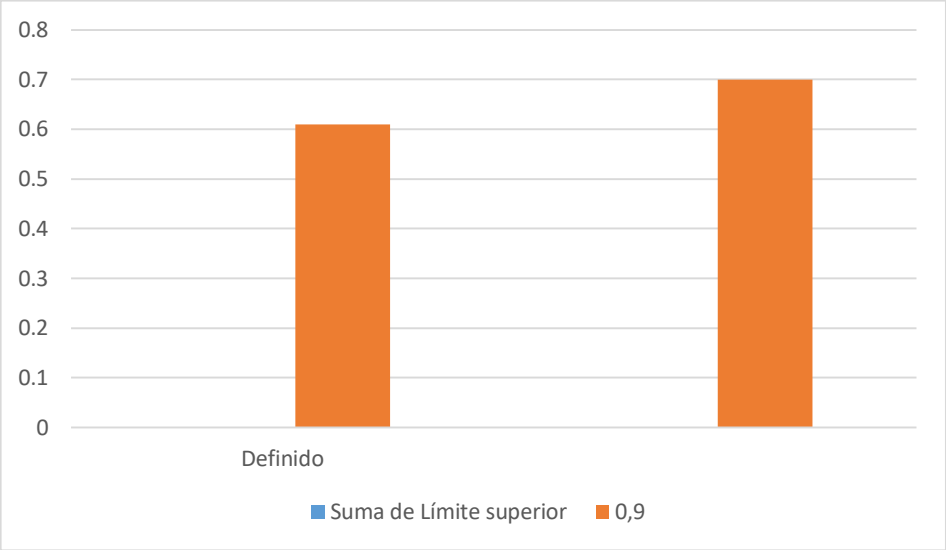
Comparación entre el nivel inicial y final de madurez de la seguridad de la información

El gráfico 12 evidencia que la implementación de la norma ISO 27001 mejora considerablemente el nivel de madurez de la seguridad de la información relacionado con el cumplimiento de las cláusulas de la norma (primera parte). En otras palabras, la institución pasa del 9,62% al 75,00% del cumplimiento de las cláusulas de la primera sección. Esto lo logró al implementar un sistema de gobierno de seguridad de la información, cuyo eje central es el plan de seguridad de la información.

Este hito, sin duda, guarda relación con los beneficios descritos en el gráfico 2, es decir, que la cooperativa reduce los riesgos de pérdidas financieras, gestiona la seguridad de la información mediante políticas claras y de planes de acción para cumplir con los objetivos trazados, evita la fuga de información y cumple con la normativa relacionada a la protección de datos personales.

Si la institución implementa el modelo de gestión, ¿por qué el nivel de madurez no alcanza el 100 %? La mayoría de los incumplimientos están relacionados con los acápites 9 (evaluación de desempeño) y 10 (auditoría interna), revisar anexo 6. La evaluación de desempeño y de auditoría interna deberán realizarse si el modelo esté implementado en la institución al menos un año. Sin embargo, la implementación de la norma requiere que la institución reformé otros manuales como, por ejemplo, el “manual de calidad” para incorporar un capítulo exclusivo de la evaluación del desempeño del SGSI, y el “manual de auditoría interna” para incorporar un capítulo exclusivo de la auditoría del SGSI.

Gráfico 12. Nivel inicial y final de madurez de SI (primera sección)

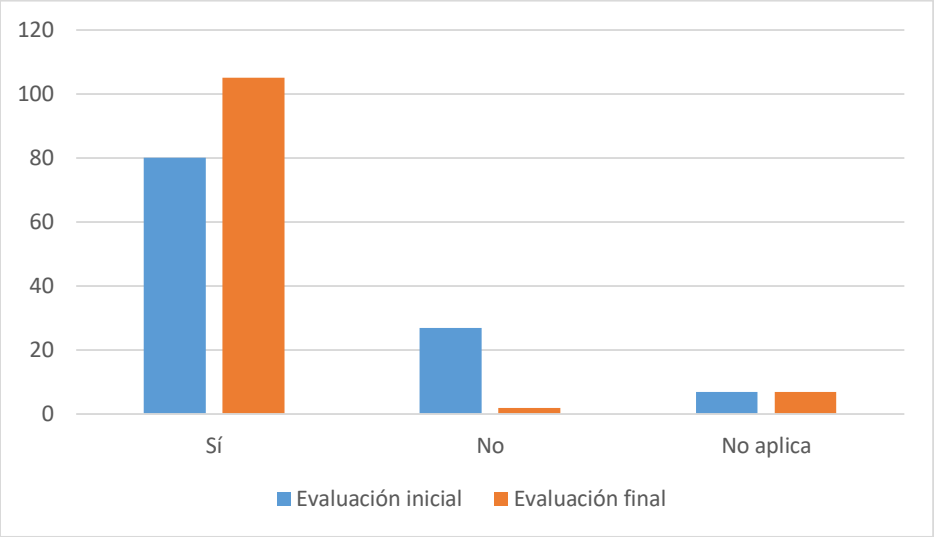


Fuente: elaboración propia

El gráfico 13 evidencia que la implementación de la norma ISO 27001 mejoró considerablemente el nivel de madurez de la seguridad de la información relacionado con el cumplimiento de los controles descritos en el Anexo A del estándar ISO 27001 (segunda parte). El control del Anexo A que la cooperativa no logra implementar es el A.15.2 (gestión de la provisión de servicios del proveedor), porque que es necesario reformar otros cuerpos normativos internos respecto a la relación con los proveedores. La reforma abarca cambios que van desde la calificación hasta la finalización de contratos con los proveedores.

El cumplimiento de los controles descritos en el Anexo A, permite a la cooperativa "comprender (…) que la seguridad de la información no se encuentra restringida (…) (a la unidad de seguridad de la información). " (Escuela Europea de Excelencia, 2019). El alcance de los controles abarca procesos tales como: tecnologías de la información y comunicación, auditoría interna, administrativo financiero, gerencia general, administración integral de riesgos, seguridad física y talento humano.

Gráfico 13. Nivel inicial y final de madurez relacionado al cumplimiento del Anexo A



Fuente: elaboración propia

CONCLUSIONES

- La verificación del estado del arte de la normativa internacional ISO 27001 permite aplicar un modelo de gestión de seguridad de la información, como parte del componente “procesos” del sistema de gobierno de seguridad de la información basado en el modelo de gobierno de Cobit 2019.

- El diagnóstico del cumplimiento de la normativa ISO 27001 identifica que la institución financiera cooperativa enfocó sus esfuerzos a la seguridad informática. El relacionar servicios, canales, aplicaciones, servidores y base de datos, permite a la institución entender cómo los principios de la seguridad de la información, representados por la confidencialidad, integridad y disponibilidad están relacionados con los estados de la información propuestos en el cubo de McCumber. Entender cómo la información es generada, almacenada y transmitida facilita diseñar y ejecutar planes de acción que resguarden la información en todos sus estados.

- El establecimiento del modelo de gestión de seguridad de la información es alcanzado mediante la utilización de *CIS Controls*, que es un conjunto de buenas prácticas destinadas a la defensa cibernética, además, de permitir a la institución financiera cooperativa analizar las vulnerabilidades de sus activos de información, establecer planes de acción para la mitigación de vulnerabilidades y formular el “manual de políticas de seguridad de la información”.

- La implementación del modelo de gestión de seguridad de la información está evidenciada en el “manual de políticas de seguridad de la información”, documento que constituye un conjunto de políticas de alto nivel que permite gestionar adecuadamente la seguridad de la información y complementarlos con los controles descritos en el Anexo A de la norma ISO 27001.

RECOMENDACIONES

- La actualización del inventario de los tipos de información y activos de información debe regirse a la metodología propuesta. La incorporación o baja de los activos de información requiere una estrecha comunicación con el proceso administrativo financiero porque es el responsable de inventariar los activos de la institución; y, el proceso de tecnologías de la información y comunicación porque es el responsable de custodiar varios activos de información como, por ejemplo: servidores, servicios, motores de base de datos, etc.

- Los planes de acción, como parte del programa de seguridad de la información, requieren monitorearse y evaluarse constantemente por la unidad de seguridad de la información. Los reportes de las evaluaciones deben conocerse y aprobarse por el comité de seguridad de la información.

- Si la institución financiera cooperativa consolida su modelo del GSI, es necesario que la IFC obtenga la certificación de la norma ISO 27001 y empiece con la implementación de la norma ISO 27701 (sistema de gestión de privacidad de la información), estándar complementario al 27001.

BIBLIOGRAFÍA

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales.* Quito.

AuditScripts. (s.f.). *The CIS Critical Security Controls*. Obtenido de The CIS Critical Security Controls: https://www.a ud its cripts. com/download/4229/?tmstv= 167 32 2 35 76

Aurum Informática. (08 de febrero de 2021). *Qué son las estaciones de trabajo y para qué sirven*. Obtenido de Qué son las estacione s de trabajo y para qué sirven: https://www.aurum-informatica.es/blo g/ que-s on-estaciones-de-trabajo-para-que-sirven

Banco Santander S.A. (s.f.). *¿Qué es la integridad de los datos?* Obtenido de https://www.ba n c o s a n t a n d e r . e s/gl osario/integrid ad-seguridad-online

Banco Santander S.A. (s.f.). *¿Qué es una vulnerabilidad informática?* Obtenido de https://www.bancosantander.es/glosario/vulnerabilidad-informatica

Center for Internet Security (CIS). (s.f.). *CIS Controls Spanish Translation*. Obtenido de https://www.cer t.gov.py/app licatio n/files/7415/3625/3 112/CIS_C ont rols_Vers ion_7_Spa nish_T ran s lation.pdf

Chiavenato, I. (2006). *Introducción a la Teoría General de la Administración.* México: McGraw-Hill Interamericana.

Concepto. (s.f.). *Enciclopedia Concepto*. Obtenido de https://concepto.de/dato/

Cooperativa de ahorro y crédito Tulcán Ltda. (s.f.). Obtenido de https ://ww w.co optulcan.fin.ec/productos-y-servicios-financieros/

Copro. (s.f.). *McCumber cubo*. Obtenido de McCumber cubo: https://copro.com.ar/McCu mber_cubo.html

Covarrubias, G. (16 de mayo de 2015). *¿Cómo definir la disponibilidad de un servicio?* Obtenido de http://w ww.gultij.org/wp-content/uploads/2015/05/Disponibilidad-de-Servicios-Presentacion-GULTij-Mayo-2015.pdf

Da Silva, D. (12 de marzo de 2021). *¿Qué son los canales de atención y qué tipos existen?* Obtenido de https://www.zendesk.com.mx/blog/canales-atencion-que-es/

Definición de. (s.f.). *Centro de cómputo*. Obtenido de https://definicion.de/centro-de-computo/

Deloitte Development LLC. (2013). *Desarrollo de un modelo*. Obtenido de h ttps://www2 .deloitte.com/cont ent/ d am/Del oitte/co/ Docu men ts/audit/BibliotecaTecnica/RecursosAuditoria/ComitedeAuditoria/Modelo%20gobierno.pdf

Diario El Universo. (2 de octubre de 2021). *Ciberataque a Banco Pichincha fue realizado por atacantes internacionales, se revela en Comisión de Desarrollo Económico*. Obtenido de https://www.eluniverso.c om/noti cias/economia/ciber ataque-a- banco-pichin cha-fue-r ealizado-por-atacantes- -se-revela-en-comision-de-desarrollo-e conomico-nota/

Díaz Evans, J. (junio de 2011). *Modelo de Seguridad de la Información*. Obtenido de https://acis.org.co/p ortal/sites/all/t hemes/argo/assets/img/Pagina/PresentacionJavierEvans.pdf

Digital Guide IONOS. (15 de septiembre de 2020). *¿Qué es un servidor?* Obtenido de ¿Qué es un servidor?: https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-un-concepto-dos-definiciones/

DNV. (s.f.). *ISO/IEC 27701 - Gestión de la privacidad de la información.* Obtenido de https://www.dnv.es/services/iso-iec-27701-gestion-de-la-privacidad-de-la-informacion-159186

Escuela Europea de Excelencia. (2 de mayo de 2019). *El Anexo A y los controles de seguridad en ISO 27001*. Obtenido de https://www.escuelaeurope aexcele ncia.com/2019/05 /el-anexo-a-y- los-controles-de-segurida d-en-iso-27001/

ESET. (2 de octubre de 2022). *We Live Security.* Obtenido de https://www.welivesecurity.com/ w p - c o n t e n t / u p l o a d s / 2022/07/ESE T- se cu rity -repo rt-LATAM-2022.pdf

Fiscalía General del Estado. (3 de octubre de 2022). [Ticket#2022092522000033] Información estadística.

IBM. (14 de abril de 2021). *Conceptos clave: entidad, atributo y tipo de entidad.* Obtenido de https://www.ibm.com/docs/es/imdm/11.6?topic=concepts-key-entity-attribute-entity-type

INCIBE. (22 de diciembre de 2020). *Amenaza vs vulnerabilidad: cómo diferenciarlos*. Obtenido de https://ww w.i nc ibe.e s/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-diferenciarlos

Instituto Nacional de Ciberserguridad de España. (29 de diciembre de 2016). *Inventario de activos y gestión de la seguridad en SCI.* Obtenido de https://www.inc ibe-cert .es/blog/i nventario- activos-y-ge stion-seguridad-

sci#:~: =Un %20inven tario %20 de % 2 0 a cti vos% 20s e, ser %20pr ote gido s%20de % 20 potenciales%20riesgos.

International Dynamic Advisors. (28 de noviembre de 2014). Obtenido de https://www.intedya.com/internacional/466/noticia-riesgos-y-seguridad-que-es-la-norma-iso-27001.html

iPSEC. (11 de marzo de 2022). *Conoce el Cubo de McCumber*. Obtenido de https://www.ipsec.mx/blog/conoce-el-cubo-de-mccumber/

ISACA. (2019). *Cobit® 2019 Framework: Introduction & Methodology.* Schaumburg.

ISOTools Excellence. (23 de febrero de 2017). *¿Cómo realizar un inventario de activos de información?* Obtenido de https:/ /www.pmg-ssi.com/2017/02/rea lizar-i nve ntario-activos-de-info rmacion/

IT Governance Institute. (2007). *COBIT 4.1.* Rolling Meadows.

Jaime, H. (s.f.). *Estructura organizacional: qué es, para qué sirve y cómo crearla*. Obtenido de https://www.holmeshr.com/blog/estructura-organizacional/

Lisboa, R. (18 de marzo de 2019). *Outsourcing: ¿qué es y por qué es importante en la era digital?* Obtenido de https://rockcontent.com/es/blog/que-es-outsourcing/

McLaughlin, E. (julio de 2021). *CISO o director de seguridad de la información*. Obtenido de https://www.computerweekly.com/es/definicion/CISO-o-director-de-seguridad-de-la-informacion

Mendoza, M. Á. (11 de enero de 2017). *Cómo desarrollar y aplicar un programa de seguridad de la información*. Obtenido de https://www.welivesecurity.com/la-es/2017/01/11/desarrollo-programa-de-seguridad-informacion/

Muñoz, I. (2 de agosto de 2018). *¿Cuál es la diferencia entre confidencialidad y privacidad?* Obtenido de https://blog.derecho-informatico.org/2018/08/02/cual-es-la-diferencia-entre-confidencialidad-y-privacidad/

Naranjo Martínez&Subía. (30 de mayo de 2021). *Entra en vigencia la Ley Orgánica de Protección de Datos Personales*. Obtenido de https://nmslaw.com.ec/ley-organica-proteccion-datos-personales/

Pérez Torres, L. A. (22 de febrero de 2018). *Identificación del estado de madurez y diseño de controles para la i mplementación de un sistema de gestión de seguridad de la información en el pro ceso TIC de Estrategias Empresariales de Colombia S.A.S.* Obtenido de https://repository.unad.edu.c o/b itstream/handle/ 105 9 6 / 1 7 3 99/38556608.pdf?sequence=1&isAllowed=y

Real Academia Española. (s.f.). *Diccionario panhispánico del español jurídico*. Obtenido de https://dpej.rae.es/lema/activo

Real Academia Española. (s.f.). *Real Academia Española*. Obtenido de https://dle.rae.es/disponibl e?m=form

Real Academia Española. (s.f.). *Real Academia Española.* Obtenido de https://dle.rae.es/seguridad

Salazar, N. (28 de febrero de 2021). *¿Qué es el mejoramiento continuo en una empresa y cómo aplicarlo de forma creativa? 6 beneficios*. Obtenido de https://asisteapp.co/blog/que-es-el-mejoramiento-continuo/

Sánchez, D. (s.f.). *Control Tecnologico*. Obtenido de Control Tecnologico: https://danielasnchz.wordpress.com/control-tecnologico/

SEPS. (23 de agosto de 2021). *Superintendencia de Economía Popular y Solidaria.* Obtenido de https://www.seps.gob.ec/wp-content/uploads/SEPS-SGD-IGT-2021-21112-OFC.pdf.pdf

SERVICETONIC. (2021 de agosto de 2021). *¿Qué es ITIL? Conceptos y principios*. Obtenido de https://www.servicetonic.com/es/itil/3-itil-conceptos-y-principios/#:~:text=Un%20Servicio%20es%20un%20medio,al%20negocio%20alcanzar%20sus%20metas.

Servicio Ecuatoriano de Normalización (INEN). (2017). *NTE INEN-ISO/IEC 27001.*

Severino, M., & Carrillo, J. C. (26 de enero de 2021). *Qué es un inventario de datos y por qué deberías saberlo.* Obtenido de Qué es un inventario de datos y por qué deberías saberlo: https://es.linkedin.com/pulse/qu%C3%A9-es-un-inventario-de-datos-y-por-deber%C3%ADas-saberlo-michelle

Superintendencia de Economía Popular y Solidaria (SEPS). (3 de mayo de 2022). *Norma de control respecto a la seguridad de la información en las entidades del Sector Financiero Popular y Solidario bajo control de la Superintendencia de Economía Popular y Solidaria.* Obtenido de https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

Superintendencia de Industria y Comercio de Colombia. (s.f.). *Metodología para la identificación, clasificación y valoración de activos de información.* Obtenido de https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Transparencia_ y_acceso_a_la_informacion_ publica/s c05-i03%20activos%20de% %20(1)%2 0(1).doc

UNIR. (s.f.). *¿Sabes qué son las políticas de seguridad informática? En UNIR analizamos de qué se trata y cuál es su importancia en el ámbito de la ciberseguridad.* Obtenido de ¿Sabes qué son las políticas de seguridad informática? En UNIR analizamo s de qué se trata y cuál es su importancia en el ámbito de la ciberseguridad.: https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

Varela, F. A. (s.f.). *¿Qué es la gestión de activos de información?* Obtenido de https://www.novasec.co/blog/67-gestion-de-activos-de-informacion

ANEXOS

Anexo 1, controles del Anexo A de la ISO 27001

Dominio	Objetivos de control	N.º	Control específico
A.5 Política de seguridad de la información	A.5.1 Dirección de gestión de seguridad de la información	A.5.1.1	Políticas para la seguridad de la información.
		A.5.1.2	Revisión de las políticas para la seguridad de la información.
A.6 Organización de seguridad de la información	A.6.1 Organización interna	A.6.1.1	Roles y responsabilidades de seguridad de la información.
		A.6.1.2	Separación de funciones.
		A.6.1.3	Contacto con las autoridades.
		A.6.1.4	Contacto con los grupos de interés especial.
		A.6.1.5	Gestión de proyectos de seguridad de la información.
	A.6.2 Dispositivos móviles y teletrabajo	A.6.2.1	Política de dispositivo móvil.
		A.6.2.2	Teletrabajo.
A.7 Seguridad en recursos humanos	A.7.1 Antes del empleo	A.7.1.1	Investigación de antecedentes.
		A.7.1.2	Términos y condiciones del empleo.
	A.7.2 Durante el empleo	A.7.2.1	Responsabilidades de la dirección.
		A.7.2.2	Concienciación, educación y formación en seguridad de la información.
		A.7.2.3	Proceso disciplinario.
	A.7.3 Finalización y cambio de empleo	A.7.3.1	Responsabilidades ante la finalización o cambio de empleo.
A.8 Gestión de activos	A.8.1 Responsabilidad de los activos	A.8.1.1	Inventario de activos.
		A.8.1.2	Propiedad de los activos.
		A.8.1.3	Uso aceptable de los activos.
		A.8.1.4	Devolución de activos.
	A.8.2 Clasificación de la información	A.8.2.1	Clasificación de la información.
		A.8.2.2	Etiquetado de la información.
		A.8.2.3	Manejo de los activos.
	A.8.3 Manejo de los medios	A.8.3.1	Gestión de medios extraíbles.
		A.8.3.2	Eliminación de los medios.
		A.8.3.3	Transferencia de medios físicos.
A.9 Control de acceso	A.9.1 Requisitos de negocio para el control de acceso	A.9.1.1	Política de control de acceso.
		A.9.1.2	Acceso a redes y servicios de red.
	A.9.2 Gestión de acceso de	A.9.2.1	Registro y retiro de usuario.
		A.9.2.2	Provisión de accesos a usuarios.

	los usuarios	A.9.2.3	Gestión de privilegios de derechos de acceso.
		A.9.2.4	Gestión de la información secreta de autenticación de los usuarios.
		A.9.2.5	Revisión de los derechos de acceso de usuario.
		A.9.2.6	Retirada y ajuste de los derechos de acceso.
	A.9.3 Responsabilidades del usuario	A.9.3.1	Uso de la información secreta de autenticación.
	A.9.4 Control de acceso a sistemas y aplicaciones	A.9.4.1	Restricción del acceso a la información.
		A.9.4.2	Procedimientos seguros de inicio de sesión.
		A.9.4.3	Sistema de gestión de contraseñas.
		A.9.4.4	Uso de programas utilitarios privilegiados.
		A.9.4.5	Control de acceso al código fuente del programa.
A.10 Criptografía	A.10.1 Controles criptográficos	A.10.1.1	Política de uso de los controles criptográficos.
		A.10.1.2	Gestión de llaves.
A.11 Seguridad física y del entorno	A.11.1 Áreas seguras	A.11.1.1	Perímetro de seguridad física.
		A.11.1.2	Controles físicos de entrada.
		A.11.1.3	Seguridad de oficinas, despachos e instalaciones.
		A.11.1.4	Protección contra las amenazas externas y ambientales.
		A.11.1.5	Trabajo en áreas seguras.
		A.11.1.6	Áreas de carga y entrega.
	A.11.2 Equipos	A.11.2.1	Ubicación y protección de equipos.
		A.11.2.2	Instalaciones de suministro.
		A.11.2.3	Seguridad del cableado.
		A.11.2.4	Mantenimiento de los equipos.
		A.11.2.5	Eliminación de activos.
		A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.
		A.11.2.7	Reutilización o eliminación segura de equipos.
		A.11.2.8	Equipo de usuario desatendido.
		A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia.
A.12 Seguridad de las operaciones	A.12.1 Procedimientos y responsabilidades operacionales	A.12.1.1	Documentación de procedimientos de operación.
		A.12.1.2	Gestión de cambios.
		A.12.1.3	Gestión de capacidades.
		A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción.
	A.12.2 Protección contra un *malware*	A.12.2.1	Controles contra un *malware*.
	A.12.3 Copia de seguridad	A.12.3.1	Copias de seguridad de la información.
	A.12.4 Registro	A.12.4.1	Registro de eventos.

	y monitoreo	A.12.4.2	Protección de la información de registro.
		A.12.4.3	Registro de administración y operación.
		A.12.4.4	Sincronización del reloj.
	A.12.5 Control de software operacional	A.12.5.1	Instalación del software en los sistemas operativos.
	A.12.6 Gestión de la vulnerabilidad técnica	A.12.6.1	Gestión de vulnerabilidades técnicas.
		A.12.6.2	Restricciones en la instalación del software.
	A.12.7 Consideraciones de auditoría de sistemas de información	A.12.7.1	Controles de auditoría en los sistemas de información.
A.13 Seguridad en las comunicaciones	A.13.1 Gestión de seguridad de la red	A.13.1.1	Controles de red.
		A.13.1.2	Seguridad de los servicios de red.
		A.13.1.3	Separación en las redes.
	A.13.2 Transferencia de información	A.13.2.1	Políticas y procedimientos de transferencia de información.
		A.13.2.2	Acuerdos de transferencia de información.
		A.13.2.3	Mensajería electrónica.
		A.13.2.4	Acuerdos de confidencialidad o no revelación.
A.14 Adquisición, desarrollo y mantenimiento del sistema	A.14.1 Requisitos de seguridad de los sistemas de información	A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información.
		A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas.
		A.14.1.3	Protección de las transacciones de servicios de aplicaciones.
	A.14.2 Seguridad en el desarrollo y en los procesos de soporte	A.14.2.1	Política de desarrollo seguro.
		A.14.2.2	Procedimientos de control de cambios en sistemas.
		A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
		A.14.2.4	Restricciones a los cambios en los paquetes de software.
		A.14.2.5	Principios de ingeniería de sistemas seguros.
		A.14.2.6	Ambiente de desarrollo seguro.
		A.14.2.7	Desarrollo externalizado.
		A.14.2.8	Pruebas de seguridad del sistema.
		A.14.2.9	Pruebas de aceptación de sistemas.
	A.14.3 Datos de prueba	A.14.3.1	Protección de los datos de prueba.
A.15 Relaciones con proveedores	A.15.1 Seguridad de la información en relación con los proveedores	A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores.
		A.15.1.2	Requisitos de seguridad en contratos con terceros.
		A.15.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones.

	A.15.2 Gestión de la provisión de servicios del proveedor	A.15.2.1	Monitoreo y revisión de los servicios de proveedores.
		A.15.2.2	Gestión de cambios en los servicios de proveedores.
A.16 Gestión de incidentes de seguridad de la información	A.16.1 Gestión de incidentes de seguridad de la información y mejoras	A.16.1.1	Responsabilidades y procedimientos.
		A.16.1.2	Informe de los eventos de seguridad de la información.
		A.16.1.3	Informe de debilidades de seguridad de la información.
		A.16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información.
		A.16.1.5	Respuesta a incidentes de seguridad de la información.
		A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.
		A.16.1.7	Recopilación de evidencias.
A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A.17.1 Continuidad de seguridad de la información	A.17.1.1	Planificación de la continuidad de la seguridad de la información.
		A.17.1.2	Implementación de la continuidad de seguridad de la información.
		A.17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información.
	A.17.2 Redundancias	A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información.
A.18 Cumplimiento	A.18.1 Cumplimiento de los requisitos legales y contractuales	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.
		A.18.1.2	Derechos de propiedad intelectual.
		A.18.1.3	Protección de los registros.
		A.18.1.4	Protección y privacidad de la información de carácter personal.
		A.18.1.5	Reglamentos de controles criptográficos.
	A.18.2 Revisiones de seguridad de la información	A.18.2.1	Revisión independiente de seguridad de la información.
		A.18.2.2	Cumplimiento de las políticas y normas de seguridad.
		A.18.2.3	Comprobación del cumplimiento técnico.

Fuente: modificado a partir de Servicio Ecuatoriano de Normalización (2017)

Anexo 2, controles contenidos en CIS Controls V. 7.1

Control crítico #1: Inventario y control de activos de hardware				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
1.1	Equipos	Identificar	Utilizar una herramienta de descubrimiento activo	Utilizar una herramienta de descubrimiento activo para identificar equipos conectados a la red de la organización y actualizar el inventario de activos hardware.
1.2	Equipos	Identificar	Utilizar una herramienta de descubrimiento pasivo de activos	Utilizar una herramienta de descubrimiento pasivo para identificar dispositivos conectados a la red de la organización y actualizar automáticamente el inventario de activos.
1.3	Equipos	Identificar	Utilizar DHCP *Logging* para actualizar el inventario de activos	Utilizar un sistema de *logging* de DHCP (*Dynamic Host Configuration Protocol*) en todos los servidores DHCP o herramientas de gestión de direcciones IPs para actualizar el inventario de activos hardware de la organización.
1.4	Equipos	Identificar	Mantener un inventario de activos detallado	Mantener un inventario veraz y actualizado de todos los activos tecnológicos capaces de almacenar y/o procesar información. El inventario debe incluir todos los activos de hardware, que estén o no conectados a la red de la organización.
1.5	Equipos	Identificar	Mantener la información del inventario de activos	Asegurar que el inventario de activos de hardware registre, como mínimo, las direcciones de red, nombre, propósito, responsable, departamento de cada activo, así como también si el activo de hardware ha sido aprobado o no para ser conectado a la red.
1.6	Equipos	Responder	Gestionar los activos no autorizados	Asegurar que los activos no autorizados se eliminen de la red, se pongan en cuarentena o el inventario se actualice oportunamente.
1.7	Equipos	Proteger	Implementar control de acceso a nivel de puerto	Implementar control de acceso a nivel de puertos según el estándar 802.1x para limitar y controlar qué equipo puede autenticarse en la red. El sistema de autenticación debe estar vinculado a los datos de inventario de activos de hardware para asegurar que sólo los equipos autorizados puedan conectar a la red.
1.8	Equipos	Proteger	Utilizar certificados clientes para autenticar	Utilizar certificados de cliente para autenticar el hardware que se conectan a la red de confianza de la organización.

			activos hardware	
CIS Control 2: Inventario y control de activos de software				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
2.1	Aplicaciones	Identificar	Mantener un inventario de software autorizado	Mantener una lista actualizada de todo el software autorizado que es requerido en la organización para todos los fines de negocio y todos los sistemas de negocio.
2.2	Aplicaciones	Identificar	Asegurar que el software tenga soporte del fabricante	Asegurar que en el inventario de software autorizado de la organización se incluya únicamente software (aplicaciones o sistemas operativos) que actualmente cuente con soporte del fabricante. El software que no cuenta con soporte debe ser marcado como no soportado en el sistema de inventario.
2.3	Aplicaciones	Identificar	Utilizar herramientas de inventario de software	Utilizar herramientas de inventario de software en toda la organización para automatizar la documentación de todo el software en los sistemas de negocio.
2.4	Aplicaciones	Identificar	Rastrear información del inventario de software	El sistema de inventario de software debe obtener el nombre, la versión, el autor y la fecha de instalación de todo el software, incluidos los sistemas operativos autorizados por la organización.
2.5	Aplicaciones	Identificar	Integrar los inventarios de activos de hardware y software	El sistema de inventario de software debe estar vinculado al inventario de activos de hardware para que todos los dispositivos y el software asociado sean rastreados desde una sola ubicación.
2.6	Aplicaciones	Responder	Gestionar el software no aprobado	Asegurar que el software no autorizado sea removido o que sea incluido en el inventario oportunamente.
2.7	Aplicaciones	Proteger	Utilizar lista blanca de aplicaciones	Utilizar tecnología de lista blanca de aplicaciones en todos los activos para asegurar que solo el software autorizado se pueda ejecutar, y prevenir la ejecución de todo el software que no esté autorizado en dichos activos.
2.8	Aplicaciones	Proteger	Implementar lista blanca de librerías	El sistema de lista blanca de aplicaciones de la organización debe garantizar que solo las librerías de software autorizadas (como * .dll, * .ocx, * .so, etc.) puedan cargarse en un proceso del sistema.
2.9	Aplicaciones	Proteger	Implementar lista blanca de scripts	El sistema de lista blanca de aplicaciones de la organización debe garantizar que solo los scripts autorizados y firmados digitalmente (como * .ps1, * .py, macros, etc.) puedan ejecutarse en un sistema.

2.10	Aplicaciones	Proteger	Separar física o lógicamente las aplicaciones de alto riesgo	Utilizar sistemas separados física o lógicamente para aislar y ejecutar aquel software que es requerido para fines de negocio, pero que conlleva un mayor riesgo para la organización.
Control crítico #3: Gestión continua de vulnerabilidades				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
3.1	Aplicaciones	Detectar	Ejecutar herramientas de escaneo automatizados de vulnerabilidades	Utilizar una herramienta actualizada de escaneo de vulnerabilidades compatible con SCAP para escanear automáticamente todos los sistemas en la red de forma semanal o más frecuente para identificar todas las vulnerabilidades potenciales en los sistemas de la organización.
3.2	Aplicaciones	Detectar	Realizar análisis de vulnerabilidades autenticados	Realizar escaneos de vulnerabilidades autenticados con agentes que se ejecutan localmente en cada sistema o con escáneres remotos que están configurados con derechos elevados en el sistema que se audita.
3.3	Aplicaciones	Proteger	Proteger las cuentas dedicadas a auditorías	Utilizar una cuenta de autentificación para el escaneo de vulnerabilidades, la cual no debe ser utilizada para otras tareas administrativas y que debe ser vinculada a máquinas específicas en direcciones IPs específicas.
3.4	Aplicaciones	Proteger	Implementar herramientas de gestión automatizada de parches del sistema operativo	Implementar herramientas de actualización de software automatizadas para garantizar que los sistemas operativos cuenten con las actualizaciones de seguridad más recientes provistas por el proveedor del software.
3.5	Aplicaciones	Proteger	Implementar herramientas de gestión automatizada de parches de software	Implementar herramientas de actualización de software automatizadas para garantizar que el software de terceros en todos los sistemas cuente con las actualizaciones de seguridad más recientes provistas por el proveedor del software.
3.6	Aplicaciones	Responder	Comparar escaneos de vulnerabilidades consecutivos	Comparar regularmente los resultados de escaneos de vulnerabilidades consecutivos para verificar que las vulnerabilidades se hayan remediado de manera oportuna.
3.7	Aplicaciones	Responder	Utilizar un proceso de calificación de riesgo	Utilizar un proceso de calificación de riesgo para priorizar la corrección de vulnerabilidades descubiertas.
Control crítico #4: Uso controlado de los privilegios administrativos				

N.º	Tipo de activo	Función de seguridad	Control	Descripción
4.1	Usuarios	Detectar	Mantener un inventario de cuentas administrativas	Usar herramientas automatizadas para inventariar todas las cuentas administrativas, incluidas las cuentas de dominio y locales, para garantizar que solo las personas autorizadas tengan privilegios elevados.
4.2	Usuarios	Proteger	Cambiar contraseñas por defecto	Antes de implementar cualquier activo nuevo, cambiar todas las contraseñas por defecto para que tengan valores consistentes con las cuentas de nivel administrativo.
4.3	Usuarios	Proteger	Asegurar el uso de cuentas administrativas dedicadas	Asegurar que todos los usuarios con acceso a la cuenta administrativa utilicen una cuenta dedicada o secundaria para actividades elevadas. Esta cuenta solo se debe usar para actividades administrativas y no para la navegación por Internet, correo electrónico o actividades similares.
4.4	Usuarios	Proteger	Usar contraseñas únicas	Cuando no está soportada la autenticación multifactor (como el administrador local, *root* o cuentas de servicio), las cuentas usarán contraseñas que son únicas de ese sistema.
4.5	Usuarios	Proteger	Usar autenticación multifactor para todo acceso administrativo	Utilizar autenticación de multifactor y canales encriptados para todos los accesos de cuentas administrativas.
4.6	Usuarios	Proteger	Usar máquinas dedicadas para toda tarea administrativa	Asegurar que los administradores utilicen una máquina dedicada para todas las tareas administrativas o tareas que requieren acceso administrativo. Esta máquina debe estar en un segmento de red diferente al principal de la organización y no se le permitirá el acceso a Internet. Esta máquina no se usará para leer correos electrónicos, manipular documentos o navegar en Internet.
4.7	Usuarios	Proteger	Limitar el acceso a herramientas de scripts	Limitar el acceso a las herramientas de scripting (como Microsoft PowerShell y Python) solo a usuarios administrativos o de desarrollo que necesiten acceder a esas funcionalidades.
4.8	Usuarios	Detectar	Registrar y alertar cambios de miembros en grupos administrativos	Configurar los sistemas para que generen una entrada de registro y una alerta cuando se agregue o elimine una cuenta a cualquier grupo que tenga asignados privilegios administrativos.

4.9	Usuarios	Detectar	Registrar y alertar los inicios de sesión fallidos a cuentas administrativas	Configurar los sistemas para generar una entrada de registro y una alerta de inicios de sesión fallidos en una cuenta administrativa.
Control crítico #5: Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
5.1	Aplicaciones	Proteger	Establecer configuraciones seguras	Mantener estándares de configuración de seguridad estándar documentados para todos los sistemas operativos y software autorizados.
5.2	Aplicaciones	Proteger	Mantener imágenes seguras	Mantener imágenes o plantillas seguras para todos los sistemas de la organización según los estándares de configuración aprobados por la organización. Cualquier implementación de sistema nuevo o sistema existente que se vea comprometido se debe volver a reconstruido con una de esas imágenes o plantillas.
5.3	Aplicaciones	Proteger	Almacenar las imágenes maestras de forma segura	Almacenar las imágenes maestras y las plantillas en servidores configurados de forma segura, validados con herramientas de monitoreo de integridad, para garantizar que solo sean posibles los cambios autorizados en las imágenes.
5.4	Aplicaciones	Proteger	Implementar herramientas de gestión de configuración de sistema	Implementar las herramientas de gestión de configuración de sistema que automáticamente fuercen y vuelvan a implementar los parámetros de configuración en los sistemas a intervalos regulares programados.
5.5	Aplicaciones	Detectar	Implementar sistemas de monitoreo automatizado de configuración	Utilizar un sistema de monitoreo de configuración compatible con el Protocolo de automatización de contenido de seguridad (SCAP) para verificar todos los elementos de configuración de seguridad, excepciones aprobadas por catálogo y que alerte cuando ocurran cambios no autorizados.
Control crítico #6: Mantenimiento, monitoreo y análisis de *logs* de auditoría				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
6.1	Red	Detectar	Utilizar tres fuentes de tiempo sincronizadas	Usar al menos tres fuentes de tiempo sincronizadas de las cuales todos los servidores y dispositivos de red recuperan información de tiempo regularmente para

				que las marcas de tiempo en los registros sean consistentes.
6.2	Red	Detectar	Activar registros de auditoría	Asegurar que los registros locales (*logs*) se han activado en todos los sistemas y equipos de red.
6.3	Red	Detectar	Habilitar registros detallados	Habilitar el registro del sistema para incluir información detallada, como origen de evento, fecha, usuario, marca de tiempo, direcciones de origen, direcciones de destino y otros elementos útiles.
6.4	Red	Detectar	Asegurar almacenamiento adecuado para registros	Asegurar que todos los sistemas que almacenan registros tengan el espacio de almacenamiento adecuado para los registros generados.
6.5	Red	Detectar	Gestión centralizada de registros	Asegurar que los registros apropiados se agreguen a un sistema central de gestión de registros para su análisis y revisión.
6.6	Red	Detectar	Desplegar herramientas SIEM o de Análisis de registros	Implementar un sistema de gestión de información de seguridad y eventos (*Security Information and Event Management* - SIEM) o una herramienta de análisis de registros para la correlación y el análisis de los registros.
6.7	Red	Detectar	Revisar regularmente los registros	Regularmente, revisar los registros para identificar anomalías o eventos anormales.
6.8	Red	Detectar	Ajustar regularmente el SIEM	Regularmente, ajustar el sistema SIEM para identificar mejor los eventos que requieren acción y disminuir el ruido.
Control crítico #7: Protección de correo electrónico y navegador web				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
7.1	Aplicaciones	Proteger	Asegurar el uso de navegadores y clientes de correo electrónico que cuenten con soporte	Asegurar que solo los navegadores web y los clientes de correo electrónico que cuenten con soporte completo puedan ejecutarse en la organización, idealmente solo con la última versión de los navegadores y clientes de correo electrónico proporcionados por el proveedor.
7.2	Aplicaciones	Proteger	Deshabilitar *plugins* innecesarios de navegadores o clientes de correo electrónico	Desinstalar o deshabilitar cualquier *plugin* o aplicación *add-on* para navegador o cliente de correo electrónico no autorizados.

7.3	Aplicaciones	Proteger	Limitar el uso de lenguajes de scripting en navegadores web y clientes de correo electrónico	Asegurar que solo los lenguajes de scripting autorizados puedan ejecutarse en los navegadores web y clientes de correo electrónico.
7.4	Red	Proteger	Mantener y aplicar filtros de URL basados en red	Aplicar los filtros de URL basados en red que limitan la capacidad de un sistema para conectarse a sitios web no aprobados por la organización. Este filtrado se aplicará para cada uno de los sistemas de la organización, ya sea que se encuentren físicamente en las instalaciones de una organización o no.
7.5	Red	Proteger	Suscribirse a servicios de categorización de URL	Suscribirse a servicios de categorización de URL para asegurar que estén actualizados con las definiciones de categoría de sitio web más recientes disponibles. Los sitios no categorizados deberían bloquearse de manera predeterminada.
7.6	Red	Detectar	Registrar todas las peticiones de URLs	Registrar todas las solicitudes de URL de cada uno de los sistemas de la organización, ya sea en el sitio o en un dispositivo móvil, para identificar actividades potencialmente maliciosas y ayudar a los responsables de gestionar incidentes a identificar sistemas potencialmente comprometidos.
7.7	Red	Proteger	Utilizar servicios de filtrado DNS	Utilizar servicios de filtrado de DNS para ayudar a bloquear el acceso a dominios maliciosos conocidos.
7.8	Red	Proteger	Implementar DMARC y habilitar verificación del lado del receptor	Para reducir la posibilidad de correos electrónicos falsificados o modificados de dominios válidos, implementar y verificar la política de Autenticación, Reporte y Conformidad de mensajes basada en dominio (*Domain-based Message Authentication, Reporting and Conformance* - DMARC), comenzando por implementar los estándares *Sender Policy Framework* (SPF) y *DomainKeys Identified Mail* (DKIM).
7.9	Red	Proteger	Bloquear tipos de archivos innecesarios	Bloquear todos los archivos adjuntos de correo electrónico que ingresen a la pasarela de correo electrónico de la organización si los tipos de archivos son innecesarios para los fines de negocio de la organización.
7.10	Red	Proteger	Utilizar técnicas de *sandbox* para todos los	Utilizar técnicas de *sandboxing* para analizar y bloquear los archivos adjuntos de correo electrónico que tengan un comportamiento malicioso.

			adjuntos de correo electrónico	
Control crítico #8: Defensa contra *malware*				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
8.1	Equipos	Proteger	Utilizar software antimalware de gestión centralizada	Utilizar software antimalware gestionado centralmente para monitorear y defender continuamente cada una de las estaciones de trabajo y servidores de la organización.
8.2	Equipos	Proteger	Asegurar que el software antimalware y las firmas estén actualizadas	Asegurar que el software antimalware de la organización actualice su motor de exploración y la base de datos de firmas periódicamente.
8.3	Equipos	Proteger	Habilitar características anti-explotación de sistemas operativos / implementar tecnologías anti-explotación	Habilitar las características anti-explotación como la Prevención de ejecución de datos (*Data Execution Prevention* - DEP) o *Address Space Layout Randomization* (ASLR) que están disponibles en los sistemas operativos o implemente los kits de herramientas adecuados que pueden configurarse para aplicar protección a un conjunto más amplio de aplicaciones y ejecutables.
8.4	Equipos	Detectar	Configurar escaneo anti-*malware* de dispositivos removibles	Configurar los dispositivos para que automáticamente realicen un análisis anti-*malware* de los medios extraíbles cuando se inserten o se conecten.
8.5	Equipos	Proteger	Configurar equipos para no autoejecutar contenido	Configurar los equipos para no ejecutar automáticamente el contenido de medios extraíbles.
8.6	Equipos	Detectar	Centralizar los registros anti-*malware*	Enviar todos los eventos de detección de *malware* a las herramientas de administración antimalware de la organización y a los servidores de registro de eventos para análisis y alertas.
8.7	Red	Detectar	Habilitar registros de consultas DNS	Habilitar los registros de las consultas al sistema de nombre de dominio (*Domain Name System* - DNS) para detectar búsquedas de nombres de host para dominios maliciosos conocidos.
8.8	Equipos	Detectar	Habilitar registros de auditoría de línea de comandos	Habilitar el registro de auditoría de línea de comandos para *shells* de comandos, como Microsoft *Powershell* y *Bash*.

Control crítico #9: Limitación y control de puertos de red, protocolos y servicios				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
9.1	Equipos	Identificar	Asociar puertos, servicios y protocolos activos al inventario de activos	Asociar puertos, servicios y protocolos activos a los activos de hardware en el inventario de activos.
9.2	Equipos	Proteger	Asegurar que solo puertos, protocolos y servicios aprobados se están ejecutando	Asegurar que en cada sistema se ejecuten solo los puertos de red, los protocolos y los servicios que se requieran con fines de negocio validados.
9.3	Equipos	Detectar	Realizar regularmente escaneos automatizados de puertos	Realizar escaneos automáticos de puertos de forma regular contra todos los sistemas y advierta si se detectan puertos no autorizados en un sistema.
9.4	Equipos	Proteger	Aplicar firewalls basados en host o filtrado de puertos	Aplicar firewalls basados en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.
9.5	Equipos	Proteger	Implementar firewalls de aplicación	Colocar firewalls de aplicaciones frente a servidores críticos para verificar y validar el tráfico que va al servidor. Cualquier tráfico no autorizado debe ser bloqueado y registrado.
Control crítico #10: Funciones de recuperación de datos				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
10.1	Datos	Proteger	Asegurar los respaldos regulares automatizados	Asegurar que se realicen regularmente copias de respaldo de todos los datos de sistemas de manera automatizadas.
10.2	Datos	Proteger	Realizar respaldos de sistemas completos	Asegurar que cada uno de los sistemas clave de la organización se esté respaldado como un sistema completo, a través de procesos tales como imágenes, para permitir la recuperación rápida de un sistema completo.

10.3	Datos	Proteger	Probar los datos en los medios de respaldo	Probar la integridad de los datos en los medios de copia de respaldo de forma periódica mediante la realización de un proceso de restauración de datos para garantizar que la copia de respaldo funcione correctamente.
10.4	Datos	Proteger	Asegurar la protección de las copias de respaldo	Asegurar que las copias de seguridad estén protegidas adecuadamente a través de la seguridad física o el cifrado cuando se almacenan, así como también cuando se mueven a través de la red. Esto incluye copias de seguridad remotas y servicios en la nube.
10.5	Datos	Proteger	Asegurar que las copias de respaldo tengan al menos un destino discontinuo	Asegurar que todas las copias de seguridad tienen al menos una copia fuera de línea, es decir, no accesible a través de una conexión de red.
Control crítico #11: Configuración segura para dispositivos de red				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
11.1	Red	Identificar	Mantener configuraciones de seguridad estandarizadas en equipos de red	Mantener las configuraciones de seguridad estandarizadas y documentadas para todos los equipos de red autorizados
11.2	Red	Identificar	Documentar las reglas de configuración de tráfico	Todas las reglas de configuración que permiten que el tráfico fluya a través de los dispositivos de la red deben estar documentadas en un sistema de gestión de la configuración.
11.3	Red	Detectar	Utilizar herramientas automatizadas para verificar configuraciones de equipos y detectar cambios	Comparar toda la configuración de equipos de red con las configuraciones de seguridad definidas y aprobadas para cada dispositivo de red en uso y alertar cuando se descubran desviaciones.
11.4	Red	Proteger	Instalar la última versión estable de cualquier actualización de seguridad en todos los equipos de red	Instalar la última versión estable de cualquier actualización de seguridad en todos los equipos de red.

11.5	Red	Proteger	Gestionar equipos de red utilizando autenticación multi-factor y sesiones cifradas	Gestionar los equipos de red utilizando autenticación multi-factor y sesiones cifradas.
11.6	Red	Proteger	Utilizar máquinas dedicadas para todas las tareas administrativas en la red	Asegurar que los administradores de la red utilicen una máquina dedicada para todas las tareas administrativas o tareas que requieren un acceso elevado. Esta máquina se segmentará de la red principal de la organización y no se le permitirá el acceso a Internet. Esta máquina no debe usarse para leer correos electrónicos, componer documentos o navegar en Internet.
11.7	Red	Proteger	Administrar la infraestructura de red mediante una red dedicada	Administrar la infraestructura de red a través de las conexiones de red que están separadas del uso de negocio de la red, mediante VLAN separadas o, preferiblemente, en una conectividad física completamente diferente para sesiones de administración para dispositivos de red.
Control crítico #12: Protección perimetral				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
12.1	Red	Identificar	Mantener un inventario de los bordes de la red	Mantener un inventario actualizado de todos los bordes de la red de la organización.
12.2	Red	Detectar	Escanear de conexiones no autorizadas en los bordes confiables de la red	Realizar regularmente escaneos desde el exterior del borde de cada red de confianza para detectar cualquier conexión no autorizada accesible a través del borde.
12.3	Red	Proteger	Denegar comunicaciones con direcciones IPs maliciosas conocidas	Denegar las comunicaciones con direcciones IP de Internet maliciosas conocidas o no utilizadas y limitar el acceso solo a los intervalos de direcciones IP confiables y necesarios en cada uno de los límites de la red de la organización.
12.4	Red	Proteger	Denegar comunicaciones sobre puertos no autorizados	Denegar la comunicación sobre los puertos TCP o UDP no autorizados o el tráfico de aplicaciones para garantizar que solo los protocolos autorizados puedan cruzar el límite de la red hacia o desde la red, en cada uno de los límites de la red de la organización.

12.5	Red	Detectar	Configurar sistemas de monitoreo para registro paquetes de red	Configurar los sistemas de monitoreo para registrar los paquetes de red que pasan a través del límite en cada uno de los bordes de la red de la organización.
12.6	Red	Detectar	Desplegar sensores IDS basados en red	Desplegar sensores de sistemas de detección de intrusos (IDS) basados en red para buscar mecanismos de ataque inusuales y detectar el compromiso de estos sistemas en cada uno de los bordes de la red de la organización.
12.7	Red	Proteger	Desplegar IPS basado en red	Desplegar sistemas de prevención de intrusos (IPS) basados en red para bloquear el tráfico de red malicioso en cada uno de los bordes de la red de la organización.
12.8	Red	Detectar	Desplegar colectores *NetFlow* en equipos de borde de la red Active la colección de *NetFlow* y registro de datos en todos los equipos de borde de la red.	Activar la colección de *NetFlow* y registro de datos en todos los equipos de borde de la red.
12.9	Red	Detectar	Desplegar servidor proxy de filtrado de capa de aplicación	Asegurar que todo el tráfico de red hacia o desde Internet pase a través de un proxy de capa de aplicación autenticado que esté configurado para filtrar conexiones no autorizadas.
12.10	Red	Detectar	Descifrar el tráfico de red en el proxy	Descifrar todo el tráfico de red cifrado en el proxy de borde antes de analizar el contenido. Sin embargo, la organización puede usar listas blancas de sitios permitidos a los que se puede acceder a través del proxy sin descifrar el tráfico.
12.11	Usuarios	Proteger	Requerir autenticación multi-factor en todos los inicios de sesión remotos	Requerir que todo acceso remoto a la red de la organización utilice cifrado de datos en tránsito y autenticación multi-factor.
12.12	Equipos	Proteger	Gestionar todos los dispositivos remotos que se conectan a la red interna	Analizar todos los dispositivos que inician sesión remotamente en la red de la organización antes de acceder a la red para asegurarse de que cada una de las políticas de seguridad de la organización se haya aplicado de la misma manera que los dispositivos de red local.

Control crítico #13: Protección de datos				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
13.1	Datos	Identificar	Mantener un inventario de información sensible	Mantener un inventario de toda la información sensible almacenada, procesada o transmitida por los sistemas de tecnología de la organización, incluidos los ubicados en la organización o en un proveedor de servicios remoto.
13.2	Datos	Proteger	Remover datos o sistemas sensibles que no son accedidos regularmente por la organización	Eliminar datos o sistemas sensibles a los que la organización no accede regularmente desde la red. Estos sistemas solo se utilizarán como sistemas autónomos (desconectados de la red) por parte de la unidad de negocio que necesite utilizar el sistema de vez en cuando o completamente virtualizados y apagados hasta que sea necesario.
13.3	Datos	Detectar	Monitorear y bloquear el tráfico de red no autorizado	Implementar una herramienta automatizada en el perímetro de la red que monitoree la transferencia no autorizada de información sensible y bloquee dichas transferencias mientras alerta a los profesionales de seguridad de la información.
13.4	Datos	Proteger	Permitir solamente el acceso a proveedores de servicios de nube o correo autorizados	Permitir solo el acceso a proveedores de servicio de almacenamiento en la nube o correo electrónico autorizados.
13.5	Datos	Detectar	Monitorear y detectar cualquier uso no autorizado de cifrado	Monitorear todo el tráfico que sale de la organización y detectar cualquier uso no autorizado de cifrado.
13.6	Datos	Proteger	Cifrar el disco duro de todos los dispositivos móviles	Utilizar software de cifrado de disco completo aprobado para cifrar el disco duro de todos los dispositivos móviles.
13.7	Datos	Proteger	Gestionar dispositivos USB	Si se requieren dispositivos de almacenamiento USB, se debe usar un software empresarial que permita configurar el uso de dispositivos específicos. Se debe mantener un inventario de dichos dispositivos.
13.8	Datos	Proteger	Gestionar las configuraciones de lectura/escritura de sistemas	Configurar los sistemas para que no escriban datos en medios extraíbles externos, si no existe una necesidad de negocio para admitir dichos dispositivos.

			para medios removibles externos	
13.9	Datos	Proteger	Cifrar los datos en dispositivos de almacenamiento USB	Si se requieren dispositivos de almacenamiento USB, todos los datos almacenados en dichos dispositivos se deben cifrar en reposo.
Control crítico #14: Control de acceso basado en la necesidad de saber				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
14.1	Red	Proteger	Segmentar la red basado en sensibilidad	Segmentar la red según la etiqueta o el nivel de clasificación de la información almacenada en los servidores; ubicar toda la información confidencial en redes de área local virtual (VLAN) separadas.
14.2	Red	Proteger	Habilitar filtrado de firewall entre VLANs	Habilitar el filtrado de firewall entre las VLAN para garantizar que solo los sistemas autorizados puedan comunicarse con otros sistemas necesarios para cumplir con sus responsabilidades específicas.
14.3	Red	Proteger	Deshabilitar comunicaciones entre estaciones de trabajo	Inhabilitar todas las comunicaciones de estación de trabajo a estación de trabajo para limitar la capacidad de un atacante de moverse lateralmente y poner en peligro los sistemas vecinos, a través de tecnologías como VLAN privadas o microsegmentación.
14.4	Datos	Proteger	Cifrar toda la información sensible en tránsito	Cifrar toda la información confidencial en tránsito.
14.5	Datos	Detectar	Utilizar una herramienta de descubrimiento activo para identificar datos sensibles	Utilizar una herramienta de descubrimiento activo para identificar toda la información sensible almacenada, procesada o transmitida por los sistemas de tecnología de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remoto, y actualizar el inventario de información sensible de la organización.
14.6	Datos	Proteger	Proteger la información mediante lista de control de acceso	Proteger toda la información almacenada en sistemas con listas de control de acceso específicas para sistema de archivos, uso compartido de redes, aplicaciones o bases de datos. Estos controles harán cumplir el principio de que solo las personas autorizadas deberían tener acceso a la información en función de su necesidad de acceder a la

				información como parte de sus responsabilidades.
14.7	Datos	Proteger	Aplicar control de acceso a datos mediante herramientas automatizadas	Utilizar una herramienta automatizada, como la prevención de pérdida de datos (*Data Loss Prevention* - DLP) basada en host, para hacer cumplir los controles de acceso a los datos, incluso cuando los datos se copian de un sistema.
14.8	Datos	Proteger	Cifrar información sensible en reposo	Cifrar toda la información sensible en reposo utilizando una herramienta que requiere un mecanismo de autenticación secundario no integrado en el sistema operativo, para poder acceder a la información.
14.9	Datos	Detectar	Imponer el registro detallado para acceso o cambios en datos sensibles	Imponer el registro de auditoría detallado para acceder o realizar cambios en datos sensibles (utilizando herramientas como Monitoreo de Integridad de Archivos o sistemas SIEM).
Control crítico #15: Control de acceso inalámbrico				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
15.1	Red	Identificar	Mantener un inventario de puntos de acceso inalámbrico autorizados	Mantener un inventario de los puntos de acceso inalámbrico autorizados conectados a la red cableada.
15.2	Red	Detectar	Detectar puntos de acceso inalámbricos conectados a la red cableada	Configurar las herramientas de exploración de vulnerabilidades de red para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red cableada.
15.3	Red	Detectar	Usar un sistema de detección de intrusión inalámbrica	Usar un sistema inalámbrico de detección de intrusos (WIDS) para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red.
15.4	Equipos	Proteger	Deshabilitar el acceso inalámbrico en dispositivos si no se requiere	Deshabilitar el acceso inalámbrico en dispositivos que no tienen un propósito de negocio para el acceso inalámbrico.

15.5	Equipos	Proteger	Limitar el acceso inalámbrico en dispositivos cliente	Configurar el acceso inalámbrico en máquinas cliente que tienen un propósito de negocio inalámbrico esencial, para permitir el acceso solo a redes inalámbricas autorizadas y para restringir el acceso a otras redes inalámbricas.
15.6	Equipos	Proteger	Inhabilitar las capacidades de red inalámbrica punto a punto en clientes inalámbricos	Inhabilitar las capacidades de redes inalámbricas punto a punto (*adhoc*) en clientes inalámbricos.
15.7	Red	Proteger	Usar estándar de cifrado avanzado (AES) para cifrar datos inalámbricos	Aprovechar el estándar de cifrado avanzado (*Advanced Encryption Standard* - AES) para cifrar datos inalámbricos en tránsito.
15.8	Red	Proteger	Usar protocolos de autenticación inalámbrica que requieran autenticación mutua multi-factor	Asegurar que las redes inalámbricas utilicen protocolos de autenticación como Protocolo de autenticación extensible / Seguridad de capa de transporte (*Extensible Authentication Protocol-Transport Layer Security* - EAP / TLS), que requiere autenticación mutua de múltiples factores.
15.9	Equipos	Proteger	Deshabilitar el acceso periférico inalámbrico de dispositivos Deshabilite el acceso periférico inalámbrico de dispositivos (como Bluetooth y NFC), a menos que dicho acceso sea necesario para fines de negocio.	Deshabilitar el acceso periférico inalámbrico de dispositivos (como Bluetooth y NFC), a menos que dicho acceso sea necesario para fines de negocio.
15.10	Red	Proteger	Crear una red inalámbrica separada para dispositivos personales y no confiables	Crear una red inalámbrica separada para dispositivos personales o que no sean de confianza. El acceso de la empresa desde esta red debe tratarse como no confiable y debe filtrarse y auditarse en consecuencia.
Control crítico #16: Monitoreo y control de cuentas				

N.º	Tipo de activo	Función de seguridad	Control	Descripción
16.1	Usuarios	Identificar	Mantener un inventario de sistemas de autenticación	Mantener un inventario de cada uno de los sistemas de autenticación de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remoto.
16.2	Usuarios	Proteger	Configurar un punto de autenticación centralizado	Configurar el acceso para todas las cuentas a través de la menor cantidad posible de puntos de autenticación centralizados, incluidos los sistemas de red, de seguridad y en la nube.
16.3	Usuarios	Proteger	Requerir Autenticación Multi-factor	Requerir autenticación de múltiples factores para todas las cuentas de usuario, en todos los sistemas, ya sea que se administren localmente en la organización o por un proveedor de terceros.
16.4	Usuarios	Proteger	Cifrar o “hashear” todas las credenciales de autenticación	Utilizar técnicas de cifrado o hash combinado con *salt* con todas las credenciales de autenticación cuando estas se almacenan.
16.5	Usuarios	Proteger	Cifrar la transmisión de nombres de usuario y credenciales de autenticación	Asegurar que todos los nombres de usuario y las credenciales de autenticación de la cuenta se transmitan a través de redes que utilizan canales cifrados.
16.6	Usuarios	Identificar	Mantener un inventario de cuentas	Mantener un inventario de todas las cuentas organizadas por sistema de autenticación.
16.7	Usuarios	Proteger	Establecer un proceso para revocar el acceso	Establecer y seguir un proceso automatizado para revocar el acceso a sistemas mediante la desactivación de cuentas inmediatamente después de la terminación o el cambio de responsabilidades de un empleado o contratista. Desactivar estas cuentas, en lugar de eliminar cuentas, permite preservar los registros de auditoría.
16.8	Usuarios	Responder	Deshabilitar cualquier cuenta no asociada	Deshabilitar cualquier cuenta que no pueda asociarse con un proceso de negocio o un propietario de la organización.
16.9	Usuarios	Responder	Desactivar cuentas inactivas	Deshabilitar automáticamente las cuentas inactivas después de un período de inactividad establecido.
16.10	Usuarios	Proteger	Asegurar que todas las	Asegurarse que todas las cuentas tengan una fecha de vencimiento monitoreada y

			cuentas tengan fecha de caducidad	forzada.
16.11	Usuarios	Proteger	Bloquear sesiones de estaciones de trabajo tras inactividad	Bloquear automáticamente las sesiones de la estación de trabajo después de un período estándar de inactividad.
16.12	Usuarios	Detectar	Monitorear los intentos de acceso a cuentas desactivadas	Monitorear los intentos de acceso a cuentas desactivadas a través de los registros de auditoría.
16.13	Usuarios	Detectar	Alertar sobre desviación de comportamiento de inicio de sesión de cuentas	Alertar cuando los usuarios se desvían del comportamiento normal de inicio de sesión, como la hora y/o el día, la ubicación de la estación de trabajo y la duración.
Control crítico #17: Implementar un programa de concienciación y capacitación en seguridad				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
17.1	N/A	N/A	Realizar un análisis de brecha de habilidades	Llevar a cabo un análisis de la brecha de habilidades para comprender las habilidades y los comportamientos a los que los miembros de la fuerza de trabajo no se están adhiriendo, usando esta información para construir una hoja de ruta base de educación.
17.2	N/A	N/A	Realizar capacitación para llenar la brecha de habilidades	Realizar capacitaciones para abordar el vacío de habilidades identificado para impactar positivamente en el comportamiento de seguridad de los miembros de la fuerza laboral.
17.3	N/A	N/A	Implementar un programa de concienciación de seguridad	Crear un programa de concienciación sobre la seguridad enfocada a todos los miembros de la organización para garantizar la seguridad de la organización. El programa de concienciación sobre seguridad de la organización debe comunicarse de forma continua y entendible.
17.4	N/A	N/A	Implementar un programa de concienciación de seguridad	Asegurar que el programa de concienciación sobre la seguridad de la organización se actualice con frecuencia (al menos anualmente) para abordar las nuevas tecnologías, amenazas, normas y requisitos empresariales.
17.5	N/A	N/A	Entrenar a la fuerza laboral en la autenticación	Capacitar a los miembros de la fuerza de trabajo sobre la importancia de habilitar y utilizar la autenticación segura.

			segura	
17.6	N/A	N/A	Capacitar a la fuerza laboral en la identificación de ataques de ingeniería social	Capacitar a los empleados sobre cómo identificar diferentes formas de ataques de ingeniería social, como *phishing*, fraudes telefónicos y llamadas de suplantación.
17.7	N/A	N/A	Capacitar a la fuerza laboral en manejo de datos sensibles	Capacitar a los empleados sobre cómo identificar y almacenar, transferir, archivar y destruir información confidencial de manera adecuada.
17.8	N/A	N/A	Capacitar a la fuerza laboral sobre las causas de la exposición involuntaria a los datos	Capacitar a los miembros de la fuerza de trabajo para que conozcan las causas de las exposiciones involuntarias de datos, cómo perder sus dispositivos móviles o enviar correos electrónicos a la persona equivocada debido al autocompletado en el correo electrónico.
17.9	N/A	N/A	Capacite a la fuerza laboral sobre cómo identificar y reportar incidentes	Capacitar a los empleados para que puedan identificar los indicadores más comunes de un incidente y poder informar tal incidente.
CIS Control 18: Seguridad del software de aplicación				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
18.1	N/A	N/A	Establecer prácticas seguras de codificación	Establecer prácticas seguras de codificación apropiadas para el lenguaje de programación y el entorno de desarrollo que se utiliza.
18.2	N/A	N/A	Asegurar que la verificación explícita de errores se realice para todo el software desarrollado internamente Para el software desarrollado internamente, asegúrese de que se realice y documente la verificación de errores	Para el software desarrollado internamente, asegurar que se realice y documente la verificación de errores explícita para todas las entradas, incluidos el tamaño, el tipo de datos y los rangos o formatos aceptables.

			explícita para todas las entradas, incluidos el tamaño, el tipo de datos y los rangos o formatos aceptables.	
18.3	N/A	N/A	Verificar que el software adquirido aún tiene soporte	Verificar que la versión de todo el software adquirido desde fuera de la organización aún cuente con soporte del desarrollador o esté debidamente asegurada en función de las recomendaciones de seguridad del desarrollador.
18.4	N/A	N/A	Usar sólo componentes de terceros actualizados y de confianza	Utilizar únicamente componentes de terceros actualizados y de confianza para el software desarrollado por la organización.
18.5	N/A	N/A	Usar únicamente algoritmos de cifrado revisados y estandarizados	Utilizar únicamente algoritmos de cifrado ampliamente revisados y estandarizados.
18.6	N/A	N/A	Asegurar que el personal de desarrollo de software esté capacitado en programación segura	Asegurar que todo el personal de desarrollo de software reciba capacitación para escribir código seguro para su entorno de desarrollo y responsabilidades específicas.
18.7	N/A	N/A	Aplicar herramientas de análisis de código estático y dinámico	Aplicar herramientas de análisis estático y dinámico para verificar que se cumplan las prácticas de codificación segura para el software desarrollado internamente.
18.8	N/A	N/A	Establecer un proceso para aceptar y tratar los reportes de vulnerabilidades del software	Establecer un proceso para aceptar y tratar los reportes de las vulnerabilidades del software, incluido proporcionar un mecanismo para que las entidades externas se comuniquen con el grupo de seguridad.
18.9	N/A	N/A	Sistemas separados de producción y no producción	Mantener entornos separados para sistemas de producción y no producción. Los desarrolladores no deberían tener acceso no supervisado a entornos de producción.

18.10	N/A	N/A	Implementar Firewall de aplicación Web (WAFs)	Proteger las aplicaciones web mediante la implementación de firewalls de aplicaciones web (WAF) que inspeccionen todo el tráfico. Para aplicaciones que no están basadas en web, se deben implementar firewalls de aplicaciones específicas si tales herramientas están disponibles para el tipo de aplicación dado. Si el tráfico está cifrado, el dispositivo debe colocarse detrás del cifrado o ser capaz de descifrar el tráfico antes del análisis. Si ninguna de las opciones es adecuada, se debe implementar un firewall de aplicaciones web basado en host.
18.11	N/A	N/A	Usar plantillas de configuración de *hardening* estándar para bases de datos	Para aplicaciones que dependen de una base de datos, usar plantillas de configuración de *hardening* estándar. Todos los sistemas que son parte de procesos de negocio críticos también deben ser probados.
Control crítico #19: Respuesta y gestión de incidentes				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
19.1	N/A	N/A	Documentar los procedimientos de respuesta de incidentes	Asegurar que haya planes escritos de respuesta a incidentes que definan las funciones del personal, así como las fases de manejo/gestión de incidentes.
19.2	N/A	N/A	Asignar cargos y responsabilidades para la respuesta a incidentes	Asignar los cargos y responsabilidades para el manejo de incidentes cibernéticos a personas específicas y asegurar el seguimiento y la documentación durante todo el incidente hasta la resolución.
19.3	N/A	N/A	Designar personal de gestión para apoyar el manejo de incidentes	Designar al personal de gestión, así como a sus suplentes, que apoyen el proceso de manejo de incidentes actuando en roles claves en la toma de decisiones.
19.4	N/A	N/A	Idear estándares para toda la organización para reporte de incidentes	Diseñar estándares para toda la organización con respecto a los tiempos requerido para que los administradores de sistemas y otros miembros de la fuerza laboral informen eventos anómalos al equipo de manejo de incidentes, los mecanismos para dichos informes y el tipo de información que debe incluirse en la notificación de incidente.

19.5	N/A	N/A	Mantener información de contacto para reportar incidentes de seguridad	Reunir y mantener información de contacto de terceros que se utilizará para informar un incidente de seguridad, como los organismos de aplicación de ley, organismos gubernamentales pertinentes, proveedores, socios de ISAC.
19.6	N/A	N/A	Publicar información relacionada con la notificación de anomalías e incidentes informáticos	Publicar información para todos los miembros de la fuerza laboral, con respecto a reportar anomalías e incidentes informáticos al equipo de manejo de incidentes. Dicha información debe incluirse en las actividades de concientización rutinarias de los empleados.
19.7	N/A	N/A	Llevar a cabo sesiones periódicas de escenarios de incidentes para el personal	Planificar y llevar a cabo ejercicios y escenarios rutinarios de respuesta a incidentes que involucren al personal implicado con el fin de prepararlos ante las amenazas del mundo real. Los ejercicios deben poner a prueba los canales de comunicación, la toma de decisiones y las capacidades técnicas de los incidentes utilizando las herramientas y los datos disponibles.
19.8	N/A	N/A	Crear un esquema de priorización y puntuación de incidentes	Crear un esquema de puntuación y priorización de incidentes basado en el impacto conocido o potencial para la organización. Utilizar una puntuación para definir la frecuencia de las actualizaciones de estado y los procedimientos de escalación.
Control crítico #20: Pruebas de penetración y ejercicios de equipo rojo				
N.º	**Tipo de activo**	**Función de seguridad**	**Control**	**Descripción**
20.1	N/A	N/A	Establecer un programa de prueba de penetración	Establecer un programa para pruebas de penetración que incluya un alcance completo de ataques combinados, como ataques inalámbricos, basados en cliente y aplicaciones web.
20.2	N/A	N/A	Llevar a cabo pruebas periódicas de penetración externa e interna	Realizar pruebas periódicas de penetración externa e interna para identificar vulnerabilidades y vectores de ataque que puedan utilizarse para explotar con éxito los sistemas de la organización.
20.3	N/A	N/A	Realizar Ejercicios Periódicos del Equipo Rojo	Realizar ejercicios periódicos del Equipo Rojo para evaluar la preparación de la organización para identificar y detener ataques o para responder de manera rápida y efectiva.

20.4	N/A	N/A	Incluir pruebas de presencia de información y artefactos no protegidos de sistema	Incluir pruebas para detectar la presencia de información y artefactos del sistema no protegidos que podrían ser útiles para los atacantes, incluyendo diagramas de red, archivos de configuración, informes de pruebas de penetración antiguos, correos electrónicos o documentos que contengan contraseñas u otra información crítica para el funcionamiento del sistema.
20.5	N/A	N/A	Crear banco de pruebas para elementos que normalmente no se prueban en producción	Crear un banco de pruebas que imite un entorno de producción para pruebas de penetración específicas y ataques del Equipo Rojo contra elementos que normalmente no se prueban en producción, como ataques contra control de supervisión y adquisición de datos y otros sistemas de control.
20.6	N/A	N/A	Usar herramientas de prueba de penetración y exploración de vulnerabilidades en conjunto	Utilizar herramientas de exploración de vulnerabilidades y pruebas de penetración en conjunto. Los resultados de las evaluaciones de escaneo de vulnerabilidad deben usarse como punto de partida para guiar y enfocar los esfuerzos de prueba de penetración.
20.7	N/A	N/A	Asegurar que los resultados de la prueba de penetración estén documentados usando estándares abiertos y legibles por máquina	Siempre que sea posible, asegurar que los resultados de los Equipos Rojos estén documentados utilizando estándares abiertos y legibles por máquina (por ejemplo, SCAP). Diseñar un método de puntuación para determinar los resultados de los ejercicios del Equipo Rojo para que los resultados puedan compararse a lo largo del tiempo.
20.8	N/A	N/A	Controlar y monitorear las cuentas asociadas con las pruebas de penetración	Las cuentas de usuario o de sistema utilizadas para realizar las pruebas de penetración deben monitorearse y controlarse para garantizar que solo se utilicen con fines legítimos y se eliminen o restablezcan a la función normal una vez finalizadas las pruebas.

Fuente: tomado a partir de Center for Internet Security (CIS) (s.f.)

Anexo 3, diagnóstico inicial de las cláusulas del sistema de gestión de seguridad de la información relacionada a la normativa ISO 27001

N.º	4 Contexto de la organización		
	4.1 Comprensión de la organización y su contexto	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
1	¿La institución determinó las cuestiones externas e internas que son relevantes para su propósito y que afecta a su capacidad para lograr el(los) resultado(s) deseado (s) de su sistema de gestión de seguridad de la información?	No	Gerencia
N.º	**4.2 Comprensión de las necesidades y expectativas de las partes interesadas**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
2	¿La institución determinó las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información?	No	Gerencia
3	¿La institución determinó los requisitos de estas partes interesadas pertinentes a la seguridad de la información?	No	Gerencia
N.º	**4.3 Determinar el alcance del sistema de gestión de seguridad de la información**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
4	¿La institución determinó los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance?	No	Gerencia
N.º	**4.4 Sistema de gestión de seguridad de la información**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
5	¿La institución estableció, implementó, mantiene y mejora continuamente el sistema de gestión de seguridad de la información, de acuerdo con los requisitos de la norma nacional?	No	Gerencia
N.º	**5 Liderazgo**		
	5.1 Liderazgo y compromiso	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
6	¿La alta gerencia asegura que la política de seguridad de la información y que los objetivos de seguridad de la información sean establecidos y compatibles con los objetivos estratégicos de la organización;	No	Gerencia
7	¿La alta gerencia asegura que la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización?	No	Gerencia

8	¿La alta gerencia asegura que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles?	No	Gerencia
9	¿La alta gerencia comunicó la importancia de la gestión de seguridad de la información de manera eficaz y de conformidad a los requisitos del sistema de gestión de seguridad de la información?	No	Gerencia
10	¿La alta gerencia asegura que el sistema de gestión de seguridad de la información alcance el(los) resultado(s) esperado(s)?	No	Gerencia
11	¿La alta gerencia dirige y apoya a las personas para contribuir a la eficacia del sistema de gestión de seguridad de la información?	No	Gerencia
12	¿La alta gerencia promueve la mejora continua?	No	Gerencia
13	¿La alta gerencia apoya a los otros roles de gestión pertinentes para demostrar su liderazgo aplicado a sus áreas de responsabilidad?	No	Gerencia
N.º	**5.2 Política**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
14	¿La alta gerencia estableció una política de seguridad de la información apropiada para el propósito de la organización?	No	Gerencia
15	¿La política de seguridad de la información está disponible como información documentada, fue comunicada dentro de la organización y está disponible para las partes interesadas?	No	Gerencia
N.º	**5.3 Roles organizacionales, responsabilidades y autoridades**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
16	¿La alta gerencia asegura que el sistema de gestión de seguridad de la información se ajuste a los requisitos del estándar adaptado a la realidad nacional?	No	Gerencia
17	¿La alta gerencia informó sobre el desempeño del sistema de gestión de seguridad de la información a los consejos de Administración y Vigilancia?	No	Gerencia
N.º	**6 Planificación**		
	6.1 Acciones para abordar los riesgos y oportunidades	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
	6.1.1 Generalidades		

18	¿La institución definió claramente las responsabilidades concernientes a la seguridad de la información?	No	Gerencia, administración integral de riesgos, atención en ventanillas, captaciones, crédito, servicios al cliente, administrativo financiero, auditoría interna, marketing, prevención de lavado de activos, seguridad física, talento humano y tecnologías de la información y comunicación
N.º	**6.1.2 Apreciación de riesgos de seguridad de la información**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
19	¿La institución definió y aplica un proceso de apreciación de riesgos de seguridad la información?	No	Administración integral de riesgos
N.º	**6.1.3 Tratamiento de riesgos de seguridad de la información**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
20	¿La institución definió y aplicó un proceso de tratamiento de riesgos de seguridad de la información?	No	Administración integral de riesgos
N.º	**6.2 Objetivos de seguridad de la información y la planificación para alcanzarlos**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
21	¿La institución estableció objetivos de seguridad de la información en las funciones y niveles pertinentes?	No	Gerencia
22	¿Los objetivos de seguridad de la información son coherentes con la política de seguridad de la información, son medibles (si es posible), tienen en cuenta los requisitos de seguridad de la información aplicables, y los resultados de la apreciación de riesgos y el tratamiento del riesgo; son comunicados; y son actualizados, ¿según sea apropiado?	No	Gerencia
N.º	**7 Soporte**		
	7.1 Recursos	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
23	¿La institución determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información?	Sí	Gerencia
N.º	**7.2 Competencia**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
24	¿La institución determina la competencia necesaria de la(s) persona(s) que realiza el trabajo bajo su control, que afecte a su desempeño de seguridad de la información?	No	Talento humano
25	¿La institución asegura que estas personas sean competentes con	No	Talento humano

	base en la educación, formación o experiencia adecuada?		
26	¿La institución cuándo sea aplicable, toma acciones para adquirir la competencia necesaria, y evaluar la eficacia de las acciones realizadas?	No	Talento humano
27	¿La institución conserva la información documentada apropiada, como evidencia de la competencia?	No	Talento humano
N.º	**7.3 Concienciación**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
28	¿Los trabajadores conocen la política de seguridad de la información?	No	Talento humano
29	¿Los trabajadores tienen en cuenta su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de una mejora del desempeño de seguridad de la información?	No	Talento humano
30	¿Los trabajadores están conscientes de las consecuencias de no cumplir con los requisitos del sistema de gestión de seguridad de la información?	No	Talento humano
N.º	**7.4 Comunicación**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
31	¿La institución determinó la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de seguridad de la información?	No	Talento humano
N.º	**7.5 Información documentada** **7.5.1 Generalidades**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
32	¿El sistema de gestión de seguridad de la información de la institución incluye la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de seguridad de la información?	Sí	Gerencia
N.º	**7.5.2 Creación y actualización**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
33	Cuando se crea y actualiza la información documentada, ¿la institución asegura la identificación y descripción; el formato y los medios de soporte; y la revisión y aprobación de idoneidad y adecuación?	Sí	Gerencia
N.º	**7.5.3 Control de la información documentada**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**

34	La información documentada requerida por el sistema de gestión de seguridad de la información asegura que: - Esté disponible y preparada para su uso, dónde y cuándo se necesite; y - Esté protegida adecuadamente.	Sí	Gerencia
N.º	**8 Operación**		
	8.1 Planificación y control operacional	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
35	¿La institución planificó, implementó y controló los procesos necesarios para cumplir con los requisitos de seguridad de la información?	No	Gerencia
N.º	**8.2 Apreciación de riesgos de seguridad de la información**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
36	¿La institución lleva a cabo las apreciaciones de riesgos de seguridad de la información a intervalos planificados o cuando se proponen o se producen cambios significativos?	No	Administración integral de riesgos
37	¿La institución conserva información documentada de los resultados de seguridad de la información y apreciaciones de riesgo?	No	Administración integral de riesgos
N.º	**8.3 Tratamiento del riesgo de seguridad de la información**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
38	¿La institución implementó el plan del tratamiento del riesgo de seguridad de la información?	No	Administración integral de riesgos
39	¿La institución conserva información documentada de los resultados del tratamiento del riesgo de seguridad de la información?	No	Administración integral de riesgos
N.º	**9 Evaluación del desempeño**		
	9.1 Monitoreo, medición, análisis y evaluación	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
40	¿La institución evaluó el desempeño de seguridad de la información y la eficacia del sistema de gestión de seguridad de la información?	No	Gerencia
41	¿La institución determinó qué es necesario monitorear y qué es necesario medir, incluyendo procesos y controles de seguridad de la información?	No	Gerencia
42	¿La institución determinó los métodos de monitoreo, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos?	No	Gerencia

43	¿La institución determinó cuándo se deben llevar a cabo el monitoreo y medición?	No	Gerencia
44	¿La institución determinó quién debe monitorear y medir?	No	Gerencia
45	¿La institución determinó cuándo se deben analizar y evaluar los resultados de monitoreo y medición?	No	Gerencia
46	¿La institución determinó quién debe analizar y evaluar los resultados?	No	Gerencia
N.º	**9.2 Auditoría interna**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
47	¿La institución realiza auditorías internas a intervalos planificados para proporcionar información acerca de si el sistema de gestión de seguridad de la información cumple con los requisitos propios de la institución para su sistema de gestión de seguridad de la información?	No	Auditoría interna
N.º	**9.3 Revisión por la dirección**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
48	¿La alta gerencia revisa el sistema de gestión de seguridad de la información de la organización a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia continuas?	No	Auditoría interna
N.º	**10 Mejora**		
	10.1 No conformidad y acciones correctivas	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
49	Cuando se produce una no conformidad, ¿la institución reacciona a la no conformidad para tomar medidas para controlar y corregirlos y hacer frente a las consecuencias?	No	Gerencia
50	¿La institución evalúa la necesidad de acciones para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte?	No	Gerencia
51	¿La institución conserva información documentada como evidencia de la naturaleza de las no conformidades y cualquier acción posterior llevada a cabo y los resultados de cualquier acción correctiva?	No	Gerencia
N.º	**10.2 Mejora continua**	**¿Cumple?**	**Proceso(s) específico(s) evaluado(s)**
52	¿La institución mejora de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información?	Sí	Gerencia

Fuente: modificado a partir de Servicio Ecuatoriano de Normalización (2017)

Anexo 4, diagnóstico inicial de los controles descritos en el Anexo A de la normativa ISO 27001

	A.5 Política de seguridad de la información			
	A.5.1 Dirección de gestión de seguridad de la información			
N.º	Objetivo: Proporcionar dirección y soporte a la gestión de seguridad de la información, de acuerdo con los requisitos del negocio, las leyes y reglamentos pertinentes.			¿Cumple?
1	A.5.1.1	Políticas para la seguridad de la información	Control Un conjunto de políticas de seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	No
2	A.5.1.2	Revisión de las políticas para la seguridad de la información	Control Las políticas de seguridad de la información deben ser revisadas a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	Sí
	A.6 Organización de seguridad de la información			
	A.6.1 Organización interna			
N.º	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.			¿Cumple?
3	A.6.1.1	Roles y responsabilidades de seguridad de la información	Control Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.	No
4	A.6.1.2	Separación de funciones	Control Las funciones en conflicto y áreas de responsabilidad deben estar separadas para reducir las oportunidades de modificación no autorizada o no intencional o el mal uso de los activos de la organización.	No
5	A.6.1.3	Contacto con las autoridades	Control Deben mantenerse los contactos apropiados con las autoridades pertinentes.	No
6	A.6.1.4	Contacto con los grupos de interés especial	Control Deben mantenerse los contactos apropiados con los grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.	No
7	A.6.1.5	Gestión de proyectos de seguridad de la información	Control La seguridad de la información debe ser tratada dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	No
	A.6.2 Dispositivos móviles y teletrabajo			
N.º	Objetivo: Asegurar la seguridad en el teletrabajo y en el uso de dispositivos móviles.			¿Cumple?

8	A.6.2.1	Política de dispositivo móvil	Control Una política de soporte y medidas de seguridad debe ser adoptada para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Sí
9	A.6.2.2	Teletrabajo	Control Una política y medida de soporte de seguridad debe ser implementada para proteger la información a la que se accede, procesa o almacena en los sitios de teletrabajo.	No aplica
	A.7 Seguridad en recursos humanos			
	A.7.1 Antes del empleo			
N.º	Objetivo: Asegurar que los empleados y contratistas comprendan sus responsabilidades y sean aptos para las funciones que están siendo contratados.			¿Cumple?
10	A.7.1.1	Investigación de antecedentes	Control La comprobación de antecedentes de todos los candidatos para el empleo debe ser realizada de acuerdo con las leyes, reglamentos pertinentes y la ética, y debe ser proporcional a los requisitos del negocio, la clasificación de la información que será accedida y el riesgo percibido.	Sí
11	A.7.1.2	Términos y condiciones del empleo	Control Los acuerdos contractuales con los empleados contratistas deben establecer sus responsabilidades y las de la organización en seguridad de la información.	Sí
	A.7.2 Durante el empleo			
N.º	**Objetivo: Asegurar que los empleados y contratistas estén conscientes y cumplan con sus responsabilidades de seguridad de la información.**			**¿Cumple?**
12	A.7.2.1	Responsabilidades de la dirección	Control La dirección debe exigir a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	No
13	A.7.2.2	Concienciación, educación y formación en seguridad de la información	Control Todos los empleados de la organización y, cuando corresponda, los contratistas deben recibir una adecuada educación, concienciación y formación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	No

14	A.7.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad de la información.	Sí
	A.7.3 Finalización y cambio de empleo			
N.º	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.			¿Cumple?
15	A.7.3.1	Responsabilidades ante la finalización o cambio de empleo	Control Las responsabilidades y obligaciones en seguridad de la información que siguen vigentes después del cambio o terminación del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.	Sí
	A.8 Gestión de activos			
	A.8.1 Responsabilidad de los activos			
N.º	Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuada.			¿Cumple?
16	A.8.1.1	Inventario de activos	Control La información, otros activos asociados con la información y las instalaciones para el procesamiento de la información, deben ser identificados y un inventario de los activos debe ser elaborado y mantenido.	No
17	A.8.1.2	Propiedad de los activos	Control Todos los activos que figuran en el inventario deben tener un propietario.	No
18	A.8.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información, los activos asociados con la información y las instalaciones de procesamiento de información.	Sí
19	A.8.1.4	Devolución de activos	Control Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	Sí
	A.8.2 Clasificación de la información			
N.º	Objetivo: Asegurar que la información reciba un nivel apropiado de protección de acuerdo con su importancia para la organización.			¿Cumple?
20	A.8.2.1	Clasificación de la información	Control La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.	Sí

21	A.8.2.2	Etiquetado de la información	Control Debe desarrollarse e implementarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	No
22	A.8.2.3	Manejo de los activos	Control Los procedimientos para el manejo de los activos deben ser desarrollados e implementados de acuerdo con el esquema de clasificación de la información adoptado por la organización.	Sí
	A.8.3 Manejo de los medios			
N.º	Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en los medios.			¿Cumple?
23	A.8.3.1	Gestión de medios extraíbles	Control Se deben implementar procedimientos para la gestión de los medios extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	No aplica
24	A.8.3.2	Eliminación de los medios	Control Los medios deben eliminarse de forma segura cuando ya no sea necesario, mediante procedimientos formales.	No aplica
25	A.8.3.3	Transferencia de medios físicos	Control Durante el transporte fuera de los límites físicos de la organización, los medios que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	No aplica
	A.9 Control de acceso			
	A.9.1 Requisitos de negocio para el control de acceso			
N.º	Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.			¿Cumple?
26	A.9.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	Sí
27	A.9.1.2	Acceso a redes y servicios de red	Control Únicamente se debe proporcionar a los usuarios el acceso a redes y a servicios en red para cuyo uso hayan sido específicamente autorizados.	Sí
	A.9.2 Gestión de acceso de los usuarios			
N.º	Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.			¿Cumple?
28	A.9.2.1	Registro y retiro de usuario	Control Debe implementarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	Sí

29	A.9.2.2	Provisión de accesos a usuarios	Control Debe implementarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	Sí
30	A.9.2.3	Gestión de privilegios de derechos de acceso	Control La asignación y el uso de privilegios de acceso deben estar restringida y controlada.	Sí
31	A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	Control La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	Sí
32	A.9.2.5	Revisión de los derechos de acceso de usuario	Control Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	No
33	A.9.2.6	Retirada y ajuste de los derechos de acceso	Control Los derechos de acceso de todos los empleados y terceras partes, a la información y a las instalaciones de procesamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	Sí
	A.9.3 Responsabilidades del usuario			
N.º	Objetivo: Hacer que los usuarios sean responsables de salvaguardar su información de autenticación.			¿Cumple?
34	A.9.3.1	Uso de la información secreta de autenticación	Control Se debe requerir que a los usuarios sigan las prácticas de la organización en el uso de la información secreta de autenticación.	Sí
	A.9.4 Control de acceso a sistemas y aplicaciones			
N.º	Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.			¿Cumple?
35	A.9.4.1	Restricción del acceso a la información	Control El acceso a la información y a las funciones de las aplicaciones del sistema debe ser restringido, de acuerdo con la política de control de acceso.	Sí
36	A.9.4.2	Procedimientos seguros de inicio de sesión	Control Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones debe ser controlado por medio de un procedimiento seguro de inicio de sesión.	Sí
37	A.9.4.3	Sistema de gestión de contraseñas	Control Los sistemas para la gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Sí

38	A.9.4.4	Uso de programas utilitarios privilegiados	Control El uso de programas utilitarios que puedan ser capaces de invalidar los controles del sistema y aplicaciones deben ser restringidos y fuertemente controlados.	Sí
39	A.9.4.5	Control de acceso al código fuente del programa	Control Se debe restringir el acceso al código fuente de los programas.	Sí
	A.10 Criptografía			
	A.10.1 Controles criptográficos			
N.º	Objetivo: Asegurar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.			¿Cumple?
40	A.10.1.1	Política de uso de los controles criptográficos	Control Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	Sí
41	A.10.1.2	Gestión de llaves	Control Se debe desarrollar e implementar una política para el uso, la protección y la duración de las llaves criptográficas a lo largo de todo su ciclo de vida.	Sí
	A.11 Seguridad física y del entorno			
	A.11.1 Áreas seguras			
N.º	Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a las instalaciones de procesamiento de la información.			¿Cumple?
42	A.11.1.1	Perímetro de seguridad física	Control Los perímetros de seguridad deben ser definidos y usados para proteger las áreas que contienen información crítica y sensible, así como las instalaciones de procesamiento de la información.	Sí
43	A.11.1.2	Controles físicos de entrada	Control Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	Sí
44	A.11.1.3	Seguridad de oficinas, despachos e instalaciones	Control La seguridad física para las oficinas, despachos e instalaciones debe ser diseñada y aplicada.	Sí
45	A.11.1.4	Protección contra las amenazas externas y ambientales	Control La protección física contra desastres naturales, ataques maliciosos o accidentes debe ser diseñada y aplicada.	Sí
46	A.11.1.5	Trabajo en áreas seguras	Control Los procedimientos para trabajar en las áreas seguras deben ser diseñados y aplicados.	Sí

47	A.11.1.6	Áreas de carga y entrega	Control Deben controlarse los puntos de acceso tales como las áreas de carga y entrega, y otros puntos donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de las instalaciones de procesamiento de la información para evitar accesos no autorizados.	No aplica
	A.11.2 Equipos			
N.º	Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.			¿Cumple?
48	A.11.2.1	Ubicación y protección de equipos	Control Los equipos deben situarse y protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados.	Sí
49	A.11.2.2	Instalaciones de suministro	Control Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	Sí
50	A.11.2.3	Seguridad del cableado	Control El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debe estar protegido contra interceptaciones, interferencias o daños.	Sí
51	A.11.2.4	Mantenimiento de los equipos	Control Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	Sí
52	A.11.2.5	Eliminación de activos	Control Sin autorización previa los equipos, la información o el software no deben sacarse de las instalaciones.	Sí
53	A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Control Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	Sí
54	A.11.2.7	Reutilización o eliminación segura de equipos	Control Todos los medios de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos o reutilizarlos.	Sí
55	A.11.2.8	Equipo de usuario desatendido	Control Los usuarios deben asegurarse de que el equipo desatendido tenga la protección adecuada.	Sí

56	A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Control Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento extraíbles junto con una política de pantalla limpia para las instalaciones de procesamiento de la información.	No
	A.12 Seguridad de las operaciones			
	A.12.1 Procedimientos y responsabilidades operacionales			
N.º	Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.			¿Cumple?
57	A.12.1.1	Documentación de procedimientos de operación	Control Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.	Sí
58	A.12.1.2	Gestión de cambios	Control Los cambios en la organización, los procesos de negocio, las instalaciones de procesamiento de la información y los sistemas que afectan a la seguridad de información deben ser controlados.	Sí
59	A.12.1.3	Gestión de capacidades	Control Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para asegurar el desempeño requerido del sistema.	Sí
60	A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción	Control Deben separarse los ambientes de desarrollo, pruebas y producción, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	Sí
	A.12.2 Protección contra un *malware*			
N.º	Objetivo: Asegurar que las instalaciones de procesamiento de la información y la información están protegidas contra un *malware*.			¿Cumple?
61	A.12.2.1	Controles contra un *malware*	Control Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra un *malware*, así como procedimientos adecuados de concienciación al usuario.	Sí
	A.12.3 Copia de seguridad			
N.º	Objetivo: Evitar la pérdida de datos.			¿Cumple?
62	A.12.3.1	Copias de seguridad de la información	Control Se deben realizar copias de seguridad de la información, del software y del sistema, estas deben verificarse periódicamente de acuerdo con la política de copias de seguridad acordada.	Sí
	A.12.4 Registro y monitoreo			
N.º	Objetivo: Registrar eventos y generar evidencias.			¿Cumple?

63	A.12.4.1	Registro de eventos	Control Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	Sí
64	A.12.4.2	Protección de la información de registro	Control El registro de instalaciones y el registro de la información deben ser protegidos contra manipulación y acceso no autorizado.	Sí
65	A.12.4.3	Registro de administración y operación	Control Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	Sí
66	A.12.4.4	Sincronización del reloj	Control Los relojes de todos los sistemas de procesamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.	Sí
	A.12.5 Control de software operacional			
N.º	Objetivo: Asegurar la integridad de los sistemas operativos.			¿Cumple?
67	A.12.5.1	Instalación del software en los sistemas operativos	Control Los procedimientos deben ser implementados para controlar la instalación de software en los sistemas operativos.	Sí
	A.12.6 Gestión de la vulnerabilidad técnica			
N.º	Objetivo: Prevenir la explotación de vulnerabilidades técnicas.			¿Cumple?
68	A.12.6.1	Gestión de vulnerabilidades técnicas	Control Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	Sí
69	A.12.6.2	Restricciones en la instalación del software	Control Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	Sí
	A.12.7 Consideraciones de auditoría de sistemas de información			
N.º	Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos			¿Cumple?
70	A.12.7.1	Controles de auditoría en los sistemas de información	Control Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	Sí
	A.13 Seguridad en las comunicaciones			
	A.13.1 Gestión de seguridad de la red			

N.º	Objetivo: Asegurar la protección de la información en redes y sus instalaciones de soporte en el procesamiento de información.			¿Cumple?
71	A.13.1.1	Controles de red	Control Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	Sí
72	A.13.1.2	Seguridad de los servicios de red	Control Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	Sí
73	A.13.1.3	Separación en las redes	Control Los grupos de servicios de información, usuarios y sistemas de información deben estar separados en las redes.	Sí
	A.13.2 Transferencia de información			
N.º	Objetivo: Mantener la seguridad de la información transferida de una organización y con cualquier entidad externa.			¿Cumple?
74	A.13.2.1	Políticas y procedimientos de transferencia de información	Control Deben establecerse políticas, procedimientos y controles formales que protejan la transferencia de información mediante el uso de todo tipo de recursos de comunicación.	No
75	A.13.2.2	Acuerdos de transferencia de información	Control Deben establecerse acuerdos para la transferencia segura de información del negocio y software entre la organización y terceros.	Sí
76	A.13.2.3	Mensajería electrónica	Control La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	Sí
77	A.13.2.4	Acuerdos de confidencialidad o no revelación	Control Deben ser identificados, revisados y documentados regularmente los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información.	Sí
	A.14 Adquisición, desarrollo y mantenimiento del sistema			
	A.14.1 Requisitos de seguridad de los sistemas de información			
N.º	Objetivo: Asegurar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.			¿Cumple?
78	A.14.1.1	Análisis de requisitos y especificaciones de seguridad	Control Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de	Sí

		de la información	información o mejoras a los sistemas de información existentes.	
79	A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Control La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizados.	Sí
80	A.14.1.3	Protección de las transacciones de servicios de aplicaciones	Control La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensajes no autorizados.	Sí
	A.14.2 Seguridad en el desarrollo y en los procesos de soporte			
N.º	Objetivo: Asegurar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.			¿Cumple?
81	A.14.2.1	Política de desarrollo seguro	Control Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	Sí
82	A.14.2.2	Procedimientos de control de cambios en sistemas	Control El desarrollo de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.	Sí
83	A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Control Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para asegurar que no existen efectos adversos en las operaciones o la seguridad de la organización.	Sí
84	A.14.2.4	Restricciones a los cambios en los paquetes de software	Control Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	Sí
85	A.14.2.5	Principios de ingeniería de sistemas seguros	Control Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.	Sí
86	A.14.2.6	Ambiente de desarrollo seguro	Control Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que	Sí

			cubren todo el ciclo de vida de desarrollo del sistema.	
87	A.14.2.7	Desarrollo externalizado	Control El desarrollo de software externalizado debe ser supervisado y controlado por la organización.	No aplica
88	A.14.2.8	Pruebas de seguridad del sistema	Control Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	Sí
89	A.14.2.9	Pruebas de aceptación de sistemas	Control Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	Sí
	A.14.3 Datos de prueba			
N.º	Objetivo: Asegurar la protección de los datos utilizados para la prueba			¿Cumple?
90	A.14.3.1	Protección de los datos de prueba	Control Los datos de prueba deben seleccionarse cuidadosamente, protegidos y controlados.	Sí
	A.15 Relaciones con proveedores			
	A.15.1 Seguridad de la información en relación con los proveedores			
N.º	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			¿Cumple?
91	A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Control Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.	No
92	A.15.1.2	Requisitos de seguridad en contratos con terceros	Control Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura TI, para la información de la organización.	No
93	A.15.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones	Control Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.	No
	A.15.2 Gestión de la provisión de servicios del proveedor			
N.º	Objetivo: Mantener un nivel acordado de seguridad de la información y la prestación de servicios en línea con los acuerdos con proveedores.			¿Cumple?

94	A.15.2.1	Monitoreo y revisión de los servicios de proveedores	Control Las organizaciones deben monitorear, revisar y auditar regularmente la provisión de servicios del proveedor.	No
95	A.15.2.2	Gestión de cambios en los servicios de proveedores	Control Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existente, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados, así como la reapreciación de los riesgos.	No
	A.16 Gestión de incidentes de seguridad de la información			
	A.16.1 Gestión de incidentes de seguridad de la información y mejoras			
N.º	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.			¿Cumple?
96	A.16.1.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	Sí
97	A.16.1.2	Informe de los eventos de seguridad de la información	Control Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	Sí
98	A.16.1.3	Informe de debilidades de seguridad de la información	Control Todos los empleados y contratistas que utilizan los sistemas y servicios de información de la organización deben ser obligados a anotar e informar cualquier debilidad de seguridad de la información que observen o sospechen que exista, en los sistemas o servicios.	Sí
99	A.16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información	Control Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	Sí
100	A.16.1.5	Respuesta a incidentes de seguridad de la información	Control Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	Sí
101	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Control El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los futuros incidentes.	Sí

102	A.16.1.7	Recopilación de evidencias	Control La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia.	Sí
	A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio			
	A.17.1 Continuidad de seguridad de la información			
N.º	Objetivo: La continuidad de seguridad de la información debe formar parte de los sistemas de gestión de continuidad de negocio de la organización.			¿Cumple?
103	A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	No
104	A.17.1.2	Implementación de la continuidad de seguridad de la información	Control La organización debe establecer, documentar, implementar y mantener procesos, procedimientos controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	No
105	A.17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información	Control Verificar, revisar y evaluar la de seguridad de la información establecidos e implementados en intervalos regulares, para asegurarse de que son válidos y eficaces durante situaciones adversas.	No
	A.17.2 Redundancias			
N.º	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de la información			¿Cumple?
106	A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Control Las instalaciones de procesamiento de la información se deben implementar con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	Sí
	A.18 Cumplimiento			
	A.18.1 Cumplimiento de los requisitos legales y contractuales			
N.º	Objetivo: Evitar incumplimientos de las obligaciones legales, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.			¿Cumple?
107	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control Todos los requisitos pertinentes, tanto legales como reglamentarios, contractuales, y el enfoque de la organización para cumplir con estos requisitos, deben definirse de forma explícita, documentarse y mantenerse	Sí

			actualizados para cada sistema de información de la organización.	
108	A.18.1.2	Derechos de propiedad intelectual	Control Deben implementarse procedimientos adecuados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	No aplica
109	A.18.1.3	Protección de los registros	Control Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, reglamentarios, contractuales y de negocio.	No
110	A.18.1.4	Protección y privacidad de la información de carácter personal	Control Debe asegurarse la protección y la privacidad de los datos, según se requiera en la legislación y en el reglamento donde sea aplicable.	No
111	A.18.1.5	Reglamentos de controles criptográficos	Control Los controles criptográficos deben ser utilizados de acuerdo con toda la información pertinente a acuerdos, leyes y reglamentos.	Sí
	A.18.2 Revisiones de seguridad de la información			
N.º	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos de la organización.			¿Cumple?
112	A.18.2.1	Revisión independiente de seguridad de la información	Control El enfoque de la organización para la gestión de seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos.	No
113	A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Control Los directivos deben revisar periódicamente el cumplimiento del procesamiento de la información y procedimientos dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.	No
114	A.18.2.3	Comprobación del cumplimiento técnico	Control Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la	No

			información de la organización.	

Fuente: modificado a partir de Servicio Ecuatoriano de Normalización (2017)

Anexo 5. Cómo implementar varios de los controles descritos en el Anexo A mediante CIS Controls

N.º	Descripción	Control esperado	*CIS Controls*
A.6.1.3	Contacto con las autoridades	Deben mantenerse los contactos apropiados con las autoridades pertinentes.	19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8
A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8
A.7.2.2	Concienciación, educación y formación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas deben recibir una adecuada educación, concienciación y formación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9
A.8.1.1	Inventario de activos	La información, otros activos asociados con la información y las instalaciones para el procesamiento de la información, deben ser identificados y un inventario de los activos debe ser elaborado y mantenido.	1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1,7, 1.8
A.8.1.3	Gestión de medios extraíbles	Se deben implementar procedimientos para la gestión de los medios extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8, 13.9, 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8, 14.9
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8, 14.9, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.9.1.2	Acceso a redes y servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a redes y a servicios en red para cuyo uso hayan sido específicamente autorizados.	1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 9.1, 9.2, 9.3, 9.4, 9.5, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12

A.9.2.1	Registro y retiro de usuario	Debe implementarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.9.2.2	Provisión de accesos a usuarios	Debe implementarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.9.2.3	Gestión de privilegios de derechos de acceso	La asignación y el uso de privilegios de acceso deben estar restringida y controlada.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.9.2.6	Retirada y ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a las instalaciones de procesamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.9.3.1	Uso de la información secreta de autenticación	Se debe requerir que a los usuarios sigan las prácticas de la organización en el uso de la información secreta de autenticación.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.9.4.1	Restricción del acceso a la información	El acceso a la información y a las funciones de las aplicaciones del sistema debe ser restringido, de acuerdo con la política de control de acceso.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.9.4.2	Procedimientos seguros de inicio de sesión	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones debe ser controlado por medio de un procedimiento seguro de inicio de sesión.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13

A.9.4.3	Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.9.4.4	Uso de programas utilitarios privilegiados	El uso de programas utilitarios que puedan ser capaces de invalidar los controles del sistema y aplicaciones deben ser restringidos y fuertemente controlados.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9
A.9.4.5	Control de acceso al código fuente del programa	Se debe restringir el acceso al código fuente de los programas.	18.1, 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8, 18.9, 18.10, 18.11
A.10.1.1	Política de uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	10.1, 10.2, 10.3, 10.4, 10.5, 13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8, 13.9, 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8, 14.9, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7, 15.8, 15.9, 15.10
A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política para el uso, la protección y la duración de las llaves criptográficas a lo largo de todo su ciclo de vida.	13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8, 13.9
A.11.2.8	Equipo de usuario desatendido	Los usuarios deben asegurarse de que el equipo desatendido tenga la protección adecuada.	16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13
A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción	Deben separarse los ambientes de desarrollo, pruebas y producción, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	18.1, 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8, 18.9, 18.10, 18.11
A.12.2.1	Controles contra un *malware*	Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra un *malware*, así como procedimientos adecuados de concienciación al usuario.	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8
A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema, estas deben verificarse periódicamente de acuerdo con la política de copias de seguridad acordada.	10.1, 10.2, 10.3, 10.4, 10.5

A.12.4.1	Registro de eventos	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7, 15.8, 15.9, 15.10
A.12.4.2	Protección de la información de registro	El registro de instalaciones y el registro de la información deben ser protegidos contra manipulación y acceso no autorizado.	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8
A.12.4.3	Registro de administración y operación	Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8
A.12.4.4	Sincronización del reloj	Los relojes de todos los sistemas de procesamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8
A.12.5.1	Instalación del software en los sistemas operativos	Los procedimientos deben ser implementados para controlar la instalación de software en los sistemas operativos.	2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10
A.12.6.1	Gestión de vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7
A.12.6.2	Restricciones en la instalación del software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10
A.12.7.1	Controles de auditoría en los sistemas de información	Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7, 15.8, 15.9, 15.10

A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar separados en las redes.	11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12
A.13.2.1	Políticas y procedimientos de transferencia de información	Deben establecerse políticas, procedimientos y controles formales que protejan la transferencia de información mediante el uso de todo tipo de recursos de comunicación.	9.1, 9.2, 9.3, 9.4, 9.5
A.13.2.2	Acuerdos de transferencia de información	Deben establecerse acuerdos para la transferencia segura de información del negocio y software entre la organización y terceros.	9.1, 9.2, 9.3, 9.4, 9.5
A.13.2.3	Mensajería electrónica	La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8, 13.9
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizados.	9.1, 9.2, 9.3, 9.4, 9.5
A.14.2.1	Política de desarrollo seguro	Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	18.1, 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8, 18.9, 18.10, 18.11
A.14.2.4	Restricciones a los cambios en los paquetes de software	Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	5.1, 5.2, 5.3, 5.4, 5.5, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10
A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que	18.1, 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8, 18.9, 18.10, 18.11

		cubren todo el ciclo de vida de desarrollo del sistema.	
A.14.2.7	Desarrollo externalizado	El desarrollo de software externalizado debe ser supervisado y controlado por la organización.	18.1, 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8, 18.9, 18.10, 18.11
A.14.2.8	Pruebas de seguridad del sistema	Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 5.1, 5.2, 5.3, 5.4, 5.5, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 18.1, 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8, 18.9, 18.10, 18.11, 20.1, 20.2, 20.3, 20.4, 20.5, 20.6, 20.7, 20.8
A.16.1.2	Informe de los eventos de seguridad de la información	Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8
A.16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8
A.16.1.5	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los futuros incidentes.	19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8
A.16.1.7	Recopilación de evidencias	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia.	19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8
A.18.1.5	Reglamentos de controles criptográficos	Los controles criptográficos deben ser utilizados de acuerdo con toda la información pertinente a acuerdos, leyes y reglamentos.	13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8, 13.9
A.18.2.1	Revisión independiente de seguridad de la información	El enfoque de la organización para la gestión de seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y	20.1, 20.2, 20.3, 20.4, 20.5, 20.6, 20.7, 20.8

		procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos.	
A.18.2.3	Comprobación del cumplimiento técnico	Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	5.1, 5.2, 5.3, 5.4, 5.5, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 20.1, 20.2, 20.3, 20.4, 20.5, 20.6, 20.7, 20.8

Fuente: modificado a partir de AuditScripts (s.f.)

Anexo 6, diagnóstico final de las cláusulas del sistema de gestión de seguridad de la información relacionada a la normativa ISO 27001

N.º	4 Contexto de la organización		
	4.1 Comprensión de la organización y su contexto	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
1	¿La institución determinó las cuestiones externas e internas que son relevantes para su propósito y que afecta a su capacidad para lograr el(los) resultado(s) deseado (s) de su sistema de gestión de seguridad de la información?	Sí	Gerencia
N.º	**4.2 Comprensión de las necesidades y expectativas de las partes interesadas**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
2	¿La institución determinó las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información?	Sí	Gerencia
3	¿La institución determinó los requisitos de estas partes interesadas pertinentes a la seguridad de la información?	Sí	Gerencia
N.º	**4.3 Determinar el alcance del sistema de gestión de seguridad de la información**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
4	¿La institución determinó los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance?	Sí	Gerencia
N.º	**4.4 Sistema de gestión de seguridad de la información**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
5	¿La institución estableció, implementó, mantiene y mejora continuamente el sistema de gestión de seguridad de la información, de acuerdo con los requisitos de la norma nacional?	Sí	Gerencia
N.º	**5 Liderazgo**		
	5.1 Liderazgo y compromiso	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
6	¿La alta gerencia asegura que la política de seguridad de la información y que los objetivos de seguridad de la información sean establecidos y compatibles con los objetivos estratégicos de la organización;	Sí	Gerencia
7	¿La alta gerencia asegura que la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización?	Sí	Gerencia
8	¿La alta gerencia asegura que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles?	Sí	Gerencia
9	¿La alta gerencia comunicó la importancia de la gestión de seguridad de la información de manera eficaz y de conformidad a los requisitos del sistema de gestión de seguridad de la información?	Sí	Gerencia

10	¿La alta gerencia asegura que el sistema de gestión de seguridad de la información alcance el(los) resultado(s) esperado(s)?	Sí	Gerencia
11	¿La alta gerencia dirige y apoya a las personas para contribuir a la eficacia del sistema de gestión de seguridad de la información?	Sí	Gerencia
12	¿La alta gerencia promueve la mejora continua?	Sí	Gerencia
13	¿La alta gerencia apoya a los otros roles de gestión pertinentes para demostrar su liderazgo aplicado a sus áreas de responsabilidad?	Sí	Gerencia
N.º	**5.2 Política**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
14	¿La alta gerencia estableció una política de seguridad de la información apropiada para el propósito de la organización?	Sí	Gerencia
15	¿La política de seguridad de la información está disponible como información documentada, fue comunicada dentro de la organización y está disponible para las partes interesadas?	Sí	Gerencia
N.º	**5.3 Roles organizacionales, responsabilidades y autoridades**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
16	¿La alta gerencia asegura que el sistema de gestión de seguridad de la información se ajuste a los requisitos del estándar adaptado a la realidad nacional?	Sí	Gerencia
17	¿La alta gerencia informó sobre el desempeño del sistema de gestión de seguridad de la información a los consejos de Administración y Vigilancia?	Sí	Gerencia
N.º	**6 Planificación**		
	6.1 Acciones para abordar los riesgos y oportunidades	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
	6.1.1 Generalidades		
18	¿La institución definió claramente las responsabilidades concernientes a la seguridad de la información?	Sí	Gerencia, administración integral de riesgos, atención en ventanillas, captaciones, crédito, servicios al cliente, administrativo financiero, auditoría interna, marketing, prevención de lavado de activos, seguridad física, talento humano y tecnologías de la información y comunicación
N.º	**6.1.2 Apreciación de riesgos de seguridad de la información**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
19	¿La institución definió y aplica un proceso de apreciación de riesgos de seguridad la información?	Sí	Administración integral de riesgos

	6.1.3 Tratamiento de riesgos de seguridad de la información	Cumple	Proceso(s) específico(s) evaluado(s)
20	¿La institución definió y aplicó un proceso de tratamiento de riesgos de seguridad de la información?	Sí	Administración integral de riesgos
	6.2 Objetivos de seguridad de la información y la planificación para alcanzarlos	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
21	¿La institución estableció objetivos de seguridad de la información en las funciones y niveles pertinentes?	Sí	Gerencia
22	¿Los objetivos de seguridad de la información son coherentes con la política de seguridad de la información, son medibles (si es posible), tienen en cuenta los requisitos de seguridad de la información aplicables, y los resultados de la apreciación de riesgos y el tratamiento del riesgo; son comunicados; y son actualizados, según sea apropiado?	Sí	Gerencia
N.º	**7 Soporte**		
	7.1 Recursos	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
23	¿La institución determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información?	Sí	Gerencia
N.º	**7.2 Competencia**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
24	¿La institución determina la competencia necesaria de la(s) persona(s) que realiza el trabajo bajo su control, que afecte a su desempeño de seguridad de la información?	Sí	Talento humano
25	¿La institución asegura que estas personas sean competentes con base en la educación, formación o experiencia adecuada?	Sí	Talento humano
26	¿La institución, cuando sea aplicable, toma acciones para adquirir la competencia necesaria, y evaluar la eficacia de las acciones realizadas?	Sí	Talento humano
27	¿La institución conserva la información documentada apropiada, como evidencia de la competencia?	Sí	Talento humano
N.º	**7.3 Concienciación**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
28	¿Los trabajadores conocen la política de seguridad de la información?	Sí	Talento humano
29	¿Los trabajadores tienen en cuenta su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de una mejora del desempeño de seguridad de la información?	Sí	Talento humano
30	¿Los trabajadores están conscientes de las consecuencias de no cumplir con los requisitos del sistema de gestión de seguridad de la información?	Sí	Talento humano

N.º	7.4 Comunicación	Cumple	Proceso(s) específico(s) evaluado(s)
31	¿La institución determinó la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de seguridad de la información?	Sí	Talento humano
N.º	7.5 Información documentada 7.5.1 Generalidades	Cumple	Proceso(s) específico(s) evaluado(s)
32	¿El sistema de gestión de seguridad de la información de la institución incluye la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de seguridad de la información?	Sí	Gerencia
N.º	7.5.2 Creación y actualización	Cumple	Proceso(s) específico(s) evaluado(s)
33	Cuando se crea y actualiza la información documentada, ¿la institución asegura la identificación y descripción; el formato y los medios de soporte; y la revisión y aprobación de idoneidad y adecuación?	Sí	Gerencia
N.º	7.5.3 Control de la información documentada	Cumple	Proceso(s) específico(s) evaluado(s)
34	La información documentada requerida por el sistema de gestión de seguridad de la información asegura que: - Esté disponible y preparada para su uso, dónde y cuándo se necesite; y - Esté protegida adecuadamente.	Sí	Gerencia
N.º	8 Operación 8.1 Planificación y control operacional	Cumple	Proceso(s) específico(s) evaluado(s)
35	¿La institución planificó, implementó y controló los procesos necesarios para cumplir con los requisitos de seguridad de la información?	No	Gerencia
N.º	8.2 Apreciación de riesgos de seguridad de la información	Cumple	Proceso(s) específico(s) evaluado(s)
36	¿La institución lleva a cabo las apreciaciones de riesgos de seguridad de la información a intervalos planificados o cuando se proponen o se producen cambios significativos?	Sí	Administración integral de riesgos
37	¿La institución conserva información documentada de los resultados de seguridad de la información y apreciaciones de riesgo?	Sí	Administración integral de riesgos
N.º	8.3 Tratamiento del riesgo de seguridad de la información	Cumple	Proceso(s) específico(s) evaluado(s)
38	¿La institución implementó el plan del tratamiento del riesgo de seguridad de la información?	Sí	Administración integral de riesgos

39	¿La institución conserva información documentada de los resultados del tratamiento del riesgo de seguridad de la información?	Sí	Administración integral de riesgos
N.º	**9 Evaluación del desempeño**		
	9.1 Monitoreo, medición, análisis y evaluación	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
40	¿La institución evaluó el desempeño de seguridad de la información y la eficacia del sistema de gestión de seguridad de la información?	No	Gerencia
41	¿La institución determinó qué es necesario monitorear y qué es necesario medir, incluyendo procesos y controles de seguridad de la información?	No	Gerencia
42	¿La institución determinó los métodos de monitoreo, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos?	No	Gerencia
43	¿La institución determinó cuándo se deben llevar a cabo el monitoreo y medición?	No	Gerencia
44	¿La institución determinó quién debe monitorear y medir?	No	Gerencia
45	¿La institución determinó cuándo se deben analizar y evaluar los resultados de monitoreo y medición?	No	Gerencia
46	¿La institución determinó quién debe analizar y evaluar los resultados?	No	Gerencia
N.º	**9.2 Auditoría interna**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
47	¿La institución realiza auditorías internas a intervalos planificados para proporcionar información acerca de si el sistema de gestión de seguridad de la información cumple con los requisitos propios de la institución para su sistema de gestión de seguridad de la información?	No	Auditoría interna
N.º	**9.3 Revisión por la dirección**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
48	¿La alta gerencia revisa el sistema de gestión de seguridad de la información de la organización a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia continuas?	No	Auditoría interna
N.º	**10 Mejora**		
	10.1 No conformidad y acciones correctivas	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
49	Cuando se produce una no conformidad, ¿la institución reacciona a la no conformidad para tomar medidas para controlar y corregirlos y hacer frente a las consecuencias?	No	Gerencia
50	¿La institución evalúa la necesidad de acciones para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte?	No	Gerencia

51	¿La institución conserva información documentada como evidencia de la naturaleza de las no conformidades y cualquier acción posterior llevada a cabo y los resultados de cualquier acción correctiva?	No	Gerencia
N.º	**10.2 Mejora continua**	**Cumple**	**Proceso(s) específico(s) evaluado(s)**
52	¿La institución mejora de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información?	Sí	Gerencia

Fuente: modificado a partir de Servicio Ecuatoriano de Normalización (2017)

Anexo 7, diagnóstico final de los controles descritos en el Anexo A de la normativa ISO 27001

	A.5 Política de seguridad de la información			
	A.5.1 Dirección de gestión de seguridad de la información			
N.º	Objetivo: Proporcionar dirección y soporte a la gestión de seguridad de la información, de acuerdo con los requisitos del negocio, las leyes y reglamentos pertinentes.			¿Cumple?
1	A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas de seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	Sí
2	A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas de seguridad de la información deben ser revisadas a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	Sí
	A.6 Organización de seguridad de la información			
	A.6.1 Organización interna			
N.º	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.			¿Cumple?
3	A.6.1.1	Roles y responsabilidades de seguridad de la información	Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.	Sí
4	A.6.1.2	Separación de funciones	Las funciones en conflicto y áreas de responsabilidad deben estar separadas para reducir las oportunidades de modificación no autorizada o no intencional o el mal uso de los activos de la organización.	Sí
5	A.6.1.3	Contacto con las autoridades	Deben mantenerse los contactos apropiados con las autoridades pertinentes.	Sí
6	A.6.1.4	Contacto con los grupos de interés especial	Deben mantenerse los contactos apropiados con los grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.	Sí
7	A.6.1.5	Gestión de proyectos de seguridad de la información	La seguridad de la información debe ser tratada dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	Sí
	A.6.2 Dispositivos móviles y teletrabajo			
N.º	Objetivo: Asegurar la seguridad en el teletrabajo y en el uso de dispositivos móviles.			¿Cumple?
8	A.6.2.1	Política de dispositivo móvil	Una política de soporte y medidas de seguridad debe ser adoptada para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Sí

9	A.6.2.2	Teletrabajo	Una política y medida de soporte de seguridad debe ser implementada para proteger la información a la que se accede, procesa o almacena en los sitios de teletrabajo.	No aplica
	A.7 Seguridad en recursos humanos			
	A.7.1 Antes del empleo			
N.º	Objetivo: Asegurar que los empleados y contratistas comprendan sus responsabilidades y sean aptos para las funciones que están siendo contratados.			¿Cumple?
10	A.7.1.1	Investigación de antecedentes	La comprobación de antecedentes de todos los candidatos para el empleo debe ser realizada de acuerdo con las leyes, reglamentos pertinentes y la ética, y debe ser proporcional a los requisitos del negocio, la clasificación de la información que será accedida y el riesgo percibido.	Sí
11	A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con los empleados contratistas deben establecer sus responsabilidades y las de la organización en seguridad de la información.	Sí
	A.7.2 Durante el empleo			
N.º	Objetivo: Asegurar que los empleados y contratistas estén conscientes y cumplan con sus responsabilidades de seguridad de la información.			¿Cumple?
12	A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	Sí
13	A.7.2.2	Concienciación, educación y formación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas deben recibir una adecuada educación, concienciación y formación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	Sí
14	A.7.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad de la información.	Sí
	A.7.3 Finalización y cambio de empleo			
N.º	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.			¿Cumple?

15	A.7.3.1	Responsabilidades ante la finalización o cambio de empleo	Las responsabilidades y obligaciones en seguridad de la información que siguen vigentes después del cambio o terminación del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.	Sí
	A.8 Gestión de activos			
	A.8.1 Responsabilidad de los activos			
N.º	Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuada.			¿Cumple?
16	A.8.1.1	Inventario de activos	La información, otros activos asociados con la información y las instalaciones para el procesamiento de la información, deben ser identificados y un inventario de los activos debe ser elaborado y mantenido.	Sí
17	A.8.1.2	Propiedad de los activos	Todos los activos que figuran en el inventario deben tener un propietario.	Sí
18	A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información, los activos asociados con la información y las instalaciones de procesamiento de información.	Sí
19	A.8.1.4	Devolución de activos	Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	Sí
	A.8.2 Clasificación de la información			
N.º	Objetivo: Asegurar que la información reciba un nivel apropiado de protección de acuerdo con su importancia para la organización.			¿Cumple?
20	A.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.	Sí
21	A.8.2.2	Etiquetado de la información	Debe desarrollarse e implementarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	Sí
22	A.8.2.3	Manejo de los activos	Los procedimientos para el manejo de los activos deben ser desarrollados e implementados de acuerdo con el esquema de clasificación de la información adoptado por la organización.	Sí
	A.8.3 Manejo de los medios			
N.º	Objetivo: Evitar la revelación, modificación, eliminación o destrucción no			¿Cumple?

	autorizadas de la información almacenada en los medios.			
23	A.8.3.1	Gestión de medios extraíbles	Se deben implementar procedimientos para la gestión de los medios extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	No aplica
24	A.8.3.2	Eliminación de los medios	Los medios deben eliminarse de forma segura cuando ya no sea necesario, mediante procedimientos formales.	No aplica
25	A.8.3.3	Transferencia de medios físicos	Durante el transporte fuera de los límites físicos de la organización, los medios que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	No aplica
	A.9 Control de acceso			
	A.9.1 Requisitos de negocio para el control de acceso			
N.º	Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.			¿Cumple?
26	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	Sí
27	A.9.1.2	Acceso a redes y servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a redes y a servicios en red para cuyo uso hayan sido específicamente autorizados.	Sí
	A.9.2 Gestión de acceso de los usuarios			
N.º	Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.			¿Cumple?
28	A.9.2.1	Registro y retiro de usuario	Debe implementarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	Sí
29	A.9.2.2	Provisión de accesos a usuarios	Debe implementarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	Sí
30	A.9.2.3	Gestión de privilegios de derechos de acceso	La asignación y el uso de privilegios de acceso deben estar restringida y controlada.	Sí
31	A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	Sí
32	A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	Sí

33	A.9.2.6	Retirada y ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a las instalaciones de procesamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	Sí
	A.9.3 Responsabilidades del usuario			
N.º	Objetivo: Hacer que los usuarios sean responsables de salvaguardar su información de autenticación.			¿Cumple?
34	A.9.3.1	Uso de la información secreta de autenticación	Se debe requerir que a los usuarios sigan las prácticas de la organización en el uso de la información secreta de autenticación.	Sí
	A.9.4 Control de acceso a sistemas y aplicaciones			
N.º	Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.			¿Cumple?
35	A.9.4.1	Restricción del acceso a la información	El acceso a la información y a las funciones de las aplicaciones del sistema debe ser restringido, de acuerdo con la política de control de acceso.	Sí
36	A.9.4.2	Procedimientos seguros de inicio de sesión	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones debe ser controlado por medio de un procedimiento seguro de inicio de sesión.	Sí
37	A.9.4.3	Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Sí
38	A.9.4.4	Uso de programas utilitarios privilegiados	El uso de programas utilitarios que puedan ser capaces de invalidar los controles del sistema y aplicaciones deben ser restringidos y fuertemente controlados.	Sí
39	A.9.4.5	Control de acceso al código fuente del programa	Se debe restringir el acceso al código fuente de los programas.	Sí
	A.10 Criptografía			
	A.10.1 Controles criptográficos			
N.º	Objetivo: Asegurar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.			¿Cumple?
40	A.10.1.1	Política de uso de los controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	Sí
41	A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política para el uso, la protección y la duración de las llaves criptográficas a lo largo de todo su ciclo de vida.	Sí

	A.11 Seguridad física y del entorno			
	A.11.1 Áreas seguras			
N.º	Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a las instalaciones de procesamiento de la información.			¿Cumple?
42	A.11.1.1	Perímetro de seguridad física	Los perímetros de seguridad deben ser definidos y usados para proteger las áreas que contienen información crítica y sensible, así como las instalaciones de procesamiento de la información.	Sí
43	A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	Sí
44	A.11.1.3	Seguridad de oficinas, despachos e instalaciones	La seguridad física para las oficinas, despachos e instalaciones debe ser diseñada y aplicada.	Sí
45	A.11.1.4	Protección contra las amenazas externas y ambientales	La protección física contra desastres naturales, ataques maliciosos o accidentes debe ser diseñada y aplicada.	Sí
46	A.11.1.5	Trabajo en áreas seguras	Los procedimientos para trabajar en las áreas seguras deben ser diseñados y aplicados.	Sí
47	A.11.1.6	Áreas de carga y entrega	Deben controlarse los puntos de acceso tales como las áreas de carga y entrega, y otros puntos donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de las instalaciones de procesamiento de la información para evitar accesos no autorizados.	No aplica
	A.11.2 Equipos			
N.º	Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.			¿Cumple?
48	A.11.2.1	Ubicación y protección de equipos	Los equipos deben situarse y protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados.	Sí
49	A.11.2.2	Instalaciones de suministro	Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	Sí
50	A.11.2.3	Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debe estar protegido contra interceptaciones, interferencias o daños.	Sí

51	A.11.2.4	Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	Sí
52	A.11.2.5	Eliminación de activos	Sin autorización previa los equipos, la información o el software no deben sacarse de las instalaciones.	Sí
53	A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	Sí
54	A.11.2.7	Reutilización o eliminación segura de equipos	Todos los medios de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos o reutilizarlos.	Sí
55	A.11.2.8	Equipo de usuario desatendido	Los usuarios deben asegurarse de que el equipo desatendido tenga la protección adecuada.	Sí
56	A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento extraíbles junto con una política de pantalla limpia para las instalaciones de procesamiento de la información.	Sí
	A.12 Seguridad de las operaciones			
	A.12.1 Procedimientos y responsabilidades operacionales			
N.º	Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.			**¿Cumple?**
57	A.12.1.1	Documentación de procedimientos de operación	Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.	Sí
58	A.12.1.2	Gestión de cambios	Los cambios en la organización, los procesos de negocio, las instalaciones de procesamiento de la información y los sistemas que afectan a la seguridad de información deben ser controlados.	Sí
59	A.12.1.3	Gestión de capacidades	Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para asegurar el desempeño requerido del sistema.	Sí
60	A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción	Deben separarse los ambientes de desarrollo, pruebas y producción, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	Sí

	A.12.2 Protección contra un *malware*			
N.º	Objetivo: Asegurar que las instalaciones de procesamiento de la información y la información están protegidas contra un *malware*.			¿Cumple?
61	A.12.2.1	Controles contra un *malware*	Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra un *malware*, así como procedimientos adecuados de concienciación al usuario.	Sí
	A.12.3 Copia de seguridad			
N.º	Objetivo: Evitar la pérdida de datos.			¿Cumple?
62	A.12.3.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información, del software y del sistema, estas deben verificarse periódicamente de acuerdo con la política de copias de seguridad acordada.	Sí
	A.12.4 Registro y monitoreo			
N.º	Objetivo: Registrar eventos y generar evidencias.			¿Cumple?
63	A.12.4.1	Registro de eventos	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	Sí
64	A.12.4.2	Protección de la información de registro	El registro de instalaciones y el registro de la información deben ser protegidos contra manipulación y acceso no autorizado.	Sí
65	A.12.4.3	Registro de administración y operación	Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	Sí
66	A.12.4.4	Sincronización del reloj	Los relojes de todos los sistemas de procesamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.	Sí
	A.12.5 Control de software operacional			
N.º	Objetivo: Asegurar la integridad de los sistemas operativos.			¿Cumple?
67	A.12.5.1	Instalación del software en los sistemas operativos	Los procedimientos deben ser implementados para controlar la instalación de software en los sistemas operativos.	Sí
	A.12.6 Gestión de la vulnerabilidad técnica			
N.º	Objetivo: Prevenir la explotación de vulnerabilidades técnicas.			¿Cumple?
68	A.12.6.1	Gestión de vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para	Sí

			afrontar el riesgo asociado.	
69	A.12.6.2	Restricciones en la instalación del software	Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	Sí
	A.12.7 Consideraciones de auditoría de sistemas de información			
N.º	Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos			¿Cumple?
70	A.12.7.1	Controles de auditoría en los sistemas de información	Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	Sí
	A.13 Seguridad en las comunicaciones			
	A.13.1 Gestión de seguridad de la red			
N.º	Objetivo: Asegurar la protección de la información en redes y sus instalaciones de soporte en el procesamiento de información.			¿Cumple?
71	A.13.1.1	Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	Sí
72	A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	Sí
73	A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar separados en las redes.	Sí
	A.13.2 Transferencia de información			
N.º	Objetivo: Mantener la seguridad de la información transferida de una organización y con cualquier entidad externa.			¿Cumple?
74	A.13.2.1	Políticas y procedimientos de transferencia de información	Deben establecerse políticas, procedimientos y controles formales que protejan la transferencia de información mediante el uso de todo tipo de recursos de comunicación.	Sí
75	A.13.2.2	Acuerdos de transferencia de información	Deben establecerse acuerdos para la transferencia segura de información del negocio y software entre la organización y terceros.	Sí
76	A.13.2.3	Mensajería electrónica	La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	Sí

77	A.13.2.4	Acuerdos de confidencialidad o no revelación	Deben ser identificados, revisados y documentados regularmente los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información.	Sí
	A.14 Adquisición, desarrollo y mantenimiento del sistema			
	A.14.1 Requisitos de seguridad de los sistemas de información			
N.º	Objetivo: Asegurar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.			¿Cumple?
78	A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	Sí
79	A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizados.	Sí
80	A.14.1.3	Protección de las transacciones de servicios de aplicaciones	La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensajes no autorizados.	Sí
	A.14.2 Seguridad en el desarrollo y en los procesos de soporte			
N.º	Objetivo: Asegurar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.			¿Cumple?
81	A.14.2.1	Política de desarrollo seguro	Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	Sí
82	A.14.2.2	Procedimientos de control de cambios en sistemas	El desarrollo de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.	Sí
83	A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para asegurar que no existen efectos adversos en las operaciones o la seguridad de la organización.	Sí

84	A.14.2.4	Restricciones a los cambios en los paquetes de software	Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	Sí
85	A.14.2.5	Principios de ingeniería de sistemas seguros	Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.	Sí
86	A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	Sí
87	A.14.2.7	Desarrollo externalizado	El desarrollo de software externalizado debe ser supervisado y controlado por la organización.	No aplica
88	A.14.2.8	Pruebas de seguridad del sistema	Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	Sí
89	A.14.2.9	Pruebas de aceptación de sistemas	Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	Sí
	A.14.3 Datos de prueba			
N.º	Objetivo: Asegurar la protección de los datos utilizados para la prueba			¿Cumple?
90	A.14.3.1	Protección de los datos de prueba	Los datos de prueba deben seleccionarse cuidadosamente, protegidos y controlados.	Sí
	A.15 Relaciones con proveedores			
	A.15.1 Seguridad de la información en relación con los proveedores			
N.º	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			¿Cumple?
91	A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.	Sí
92	A.15.1.2	Requisitos de seguridad en contratos con terceros	Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura TI, para la información de la organización.	Sí

93	A.15.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones	Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.	Sí
	A.15.2 Gestión de la provisión de servicios del proveedor			
N.º	Objetivo: Mantener un nivel acordado de seguridad de la información y la prestación de servicios en línea con los acuerdos con proveedores.			¿Cumple?
94	A.15.2.1	Monitoreo y revisión de los servicios de proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la provisión de servicios del proveedor.	No
95	A.15.2.2	Gestión de cambios en los servicios de proveedores	Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existente, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados, así como la reapreciación de los riesgos.	No
	A.16 Gestión de incidentes de seguridad de la información			
	A.16.1 Gestión de incidentes de seguridad de la información y mejoras			
N.º	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.			¿Cumple?
96	A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	Sí
97	A.16.1.2	Informe de los eventos de seguridad de la información	Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	Sí
98	A.16.1.3	Informe de debilidades de seguridad de la información	Todos los empleados y contratistas que utilizan los sistemas y servicios de información de la organización deben ser obligados a anotar e informar cualquier debilidad de seguridad de la información que observen o sospechen que exista, en los sistemas o servicios.	Sí
99	A.16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	Sí
100	A.16.1.5	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	Sí

101	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los futuros incidentes.	Sí
102	A.16.1.7	Recopilación de evidencias	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia.	Sí
	A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio			
	A.17.1 Continuidad de seguridad de la información			
N.º	Objetivo: La continuidad de seguridad de la información debe formar parte de los sistemas de gestión de continuidad de negocio de la organización.			¿Cumple?
103	A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Sí
104	A.17.1.2	Implementación de la continuidad de seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	Sí
105	A.17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información	Verificar, revisar y evaluar la de seguridad de la información establecidos e implementados en intervalos regulares, para asegurarse de que son válidos y eficaces durante situaciones adversas.	Sí
	A.17.2 Redundancias			
N.º	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de la información			¿Cumple?
106	A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Las instalaciones de procesamiento de la información se deben implementar con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	Sí
	A.18 Cumplimiento			
	A.18.1 Cumplimiento de los requisitos legales y contractuales			
N.º	Objetivo: Evitar incumplimientos de las obligaciones legales, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.			¿Cumple?
107	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos pertinentes, tanto legales como reglamentarios, contractuales, y el enfoque de la organización para cumplir con estos requisitos, deben definirse de forma	Sí

			explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.	
108	A.18.1.2	Derechos de propiedad intelectual	Deben implementarse procedimientos adecuados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	No aplica
109	A.18.1.3	Protección de los registros	Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, reglamentarios, contractuales y de negocio.	Sí
110	A.18.1.4	Protección y privacidad de la información de carácter personal	Debe asegurarse la protección y la privacidad de los datos, según se requiera en la legislación y en el reglamento donde sea aplicable.	Sí
111	A.18.1.5	Reglamentos de controles criptográficos	Los controles criptográficos deben ser utilizados de acuerdo con toda la información pertinente a acuerdos, leyes y reglamentos.	Sí
	A.18.2 Revisiones de seguridad de la información			
N.º	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos de la organización.			¿Cumple?
112	A.18.2.1	Revisión independiente de seguridad de la información	El enfoque de la organización para la gestión de seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos.	Sí
113	A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Los directivos deben revisar periódicamente el cumplimiento del procesamiento de la información y procedimientos dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.	Sí
114	A.18.2.3	Comprobación del cumplimiento técnico	Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	Sí

Fuente: modificado a partir de Servicio Ecuatoriano de Normalización (2017)

[i] Cobit® 2019 *Framework: Introduction & Methodology*