UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE CUENCA

CARRERA DE INGENIERÍA DE SISTEMAS

ELABORACIÓN DE UNA GUÍA DE IMPLEMENTACIÓN DE UN SGSI PARA LA CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA - CEDIA

Trabajo de titulación previo a la obtención del título de Ingeniera de Sistemas

AUTOR: MARÍA AUXILIADORA ORELLANA TOLEDO

TUTOR: ING. RODOLFO XAVIER BOJORQUE CHASI, Ph.D.

Cuenca - Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, María Auxiliadora Orellana Toledo con documento de identificación N° 0103404943 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Cuenca, 09 de marzo del 2022.

Atentamente,

_____

María Auxiliadora Orellana Toledo

0103404943

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, María Auxiliadora Orellana Toledo con documento de identificación Nº 0103404943, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Proyecto técnico: "Elaboración de una guía de implementación de un SGSI para la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia - CEDIA", el cual ha sido desarrollado para optar por el título de: Ingeniera de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Cuenca, 09 de marzo del 2022.

Atentamente,

_____

María Auxiliadora Orellana Toledo

0103404943

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Rodolfo Xavier Bojorque Chasi con documento de identificación N° 0103771648, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ELABORACIÓN DE UNA GUÍA DE IMPLEMENTACIÓN DE UN SGSI PARA LA CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA - CEDIA, realizado por María Auxiliadora Orellana Toledo con documento de identificación N° 0103404943, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Cuenca, 09 de marzo del 2022.

Atentamente,

Ing. Rodolfo Xavier Bojorque Chasi, Ph.D.
0103771648

DEDICATORIA

Dedico este trabajo de titulación a Dios por ser mi fuente de vida, a mi esposo Josué Ordóñez por el apoyo y amor incondicional, a mi mayor inspiración mi hija Zamar Isabella, a mis padres por todo el tiempo invertido para enseñarme a valorar cada esfuerzo, a mis hermanos Boris, Adriana por ser mis ejemplos de lucha y a mi pequeña princesa Alejandra que es mi ángel en el cielo, a mis amados sobrinos por ser uno de los motores para seguir mejorando, a mis abuelos paternos y maternos que no se encuentran en este mundo pero que fueron un impulso constante para que sus nietos seamos seres de bien, a mi tío Alberto quién todos los días se preocupa de nuestro bienestar y siempre comparte nuestros logros.

María Auxiliadora Orellana Toledo.

AGRADECIMIENTO

Agradezco a Dios por siempre estar en mi vida y salud.

A mi esposo Josué Ordóñez por apoyarme cada segundo y creer en mí.

A mi hija Zamar Isabella por comprender los sacrificios que hicimos en estos tiempos.

A mis padres y en especial a mi mamá por haberse sacrificado para que sus hijos cumplan sus sueños.

A mis hermanos Boris, Adriana y mi ángel Alejandra por estar cada día en mi vida.

A mis sobrinos quienes me enseñaron a que el amor no solo es madre a hijo sino de tía a sobrino.

Al Ing. Rodolfo Bojorque, PhD. por haberme apoyado desde el inicio y estar pendiente de la culminación de este proyecto, eternamente agradecida.

Al Ing. Juan Pablo Carvallo V., PhD. Director Ejecutivo de la CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA - CEDIA por haberme dado la oportunidad de pertenecer a tan distinguida Corporación y apoyarme en el tema de tesis.

A mi querida jefa Patricia Flores y sin dudarlo puedo decir que es la mejor, por ser un gran apoyo y ser una persona sumamente amorosa, gracias por cada día motivarme a ser mejor.

A mi querido Team Legal, Geovys, Francisco, Mabel y sin olvidar al amigo Dany, gracias por todo el ánimo que me brindaron para que este proyecto termine con éxito, forman parte de mi vida.

Al Ing. Luis Vargas Jefe de Planificación y Gestión Estratégica en CEDIA por su apoyo desde el primer momento, gracias por compartir su conocimiento e incentivarme a finalizar la tesis.

Finalmente, y sin ser menos importante, al área técnica de CEDIA en especial al Ing. Carlos Guzmán, Ing. Flavio Rodríguez, Ing. Ernesto Pérez, Ing. Enrique López, Ing. Claudio Chacón, Ing. Jorge Torres por impartir su conocimiento para poder plasmar en este documento.

GRACIAS A TODOS por confiar en mí.

ÍNDICE

ÍNDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

CEDIA es una organización sin fines de lucro que ejecuta procesos comunes como cualquier otra empresa, sin embargo, tiene sus propios métodos y procesos en cada departamento. Por esta razón desea obtener y cumplir con la Certificación ISO/IEC 27001 para brindar y servir de mejor manera a cada colaborador, miembro activo y/o nuevo de la organización.

Un Sistema de Gestión de Seguridad de la Información es el primer paso para la certificación, puesto que proporciona las mejores prácticas de seguridad de información y permite a la organización desarrollar, implementar y medir la práctica eficaz de gestión de la seguridad en todas sus áreas unificadas en sus operaciones (comúnmente el día a día de la organización) con el fin de alinearse al cumplimiento de los objetivos de la misma y para minimizar los riesgos existentes.

ABSTRACT

CEDIA is a non-profit organization that runs common processes like any other company, however, it has its own methods and processes in each department. For this reason, it wishes to obtain and comply with the ISO/IEC 27001 Certification to better provide and serve each collaborator, active member and/or new member of the organization.

An Information Security Management System is the first step for certification, since it provides the best information security practices and allows the organization to develop, implement and measure the effective practice of security management in all its areas. unified in its operations (commonly the day-to-day of the organization) in order to align with the fulfillment of its objectives and to minimize existing risks.

1. INTRODUCCIÓN Y PROBLEMA DE ESTUDIO

1.1. INTRODUCCIÓN

La CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA - CEDIA, realiza la articulación entre investigadores, docentes y estudiantes de las diferentes instituciones miembros a través de proyectos, concursos y otras iniciativas de desarrollo científico promueve con sus tecnologías, aliados, miembros y recursos la exploración y resultados de proyectos innovadores que vinculan a instituciones ecuatorianas en el desarrollo científico para el crecimiento constante entre las instituciones académicas.

CEDIA es una organización que tiene procesos comunes que se ejecutan como cualquier otra empresa, sin embargo, tiene sus propios métodos y procesos en sus departamentos. Por esta razón desea obtener y cumplir con la Certificación ISO 27001 para brindar y servir de mejor manera a cada colaborador, miembro activo y/o nuevo de la organización.

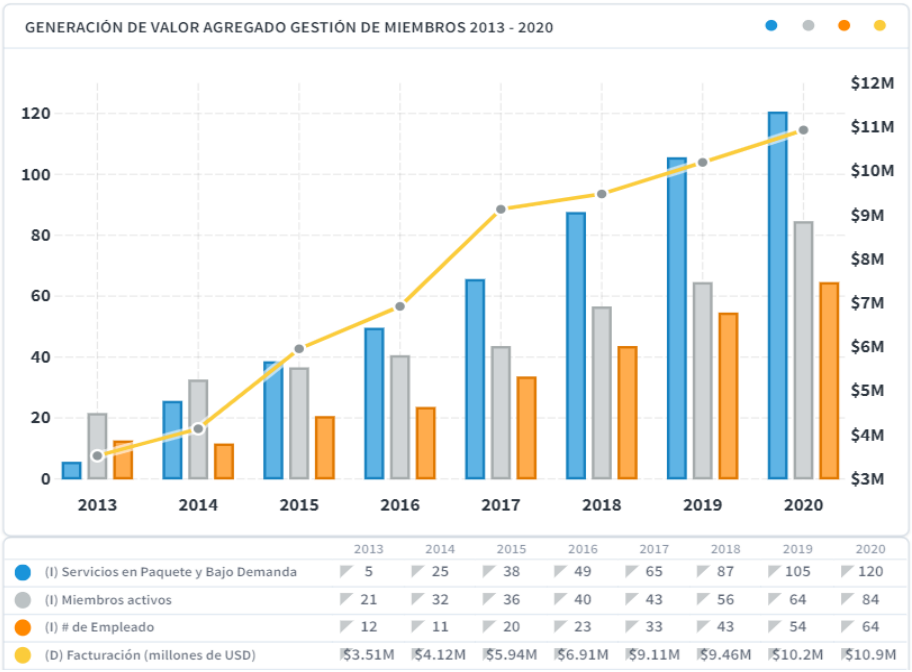
Y un Sistema de Gestión de Seguridad de la Información (SGSI) es el primer paso para la certificación, puesto que proporciona las mejores prácticas de seguridad de información y permite a la organización desarrollar, implementar y medir la práctica eficaz de gestión de la seguridad en todas sus áreas unificadas en sus operaciones (comúnmente el día a día de la organización) con el fin de alinearse al cumplimiento de los objetivos de la misma y para minimizar los riesgos existentes.

1.2. PROBLEMA

CEDIA es una organización privada sin fines de lucro que tiene por misión fomentar, promover y coordinar el desarrollo de la investigación científica, la academia, la innovación, transferencia tecnológica, emprendimiento, internacionalización y ofrecer servicios relacionados a estas áreas y otras afines, conformada por miembros plenos y adherentes, en los cuales se encuentran Universidades e Institutos a nivel nacional. (CEDIA, 2020)

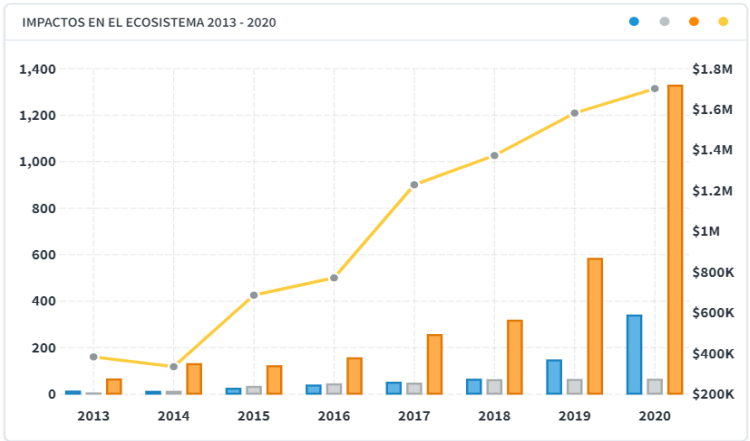
Con el transcurso de los años CEDIA ha evolucionado significativamente permitiendo generar, albergar y promover tecnologías, conexiones y recursos para la investigación, educación y colaboración por medio de sus tecnologías ofertadas como redes avanzadas, alojamiento, educación continua y academia, proyectos de innovación, investigación, etc., es así que en la

Figura 1. Valor Agregado 2013 – 2020 se puede apreciar el crecimiento tanto en los Servicios en Paquete (Red Avanzada) y Servicios Bajo Demanda, al mismo tiempo el número de miembros activos y número de empleados ha incrementado notablemente y por ende la facturación de CEDIA de igual manera, ocurre algo similar en la Figura 2. Impactos generados en el ecosistema por tal crecimiento, se puede visualizar a continuación:



	2013	2014	2015	2016	2017	2018	2019	2020
(I) Servicios en Paquete y Bajo Demanda	5	25	38	49	65	87	105	120
(I) Miembros activos	21	32	36	40	43	56	64	84
(I) # de Empleado	12	11	20	23	33	43	54	64
(D) Facturación (millones de USD)	$3.51M	$4.12M	$5.94M	$6.91M	$9.11M	$9.46M	$10.2M	$10.9M

Figura 1 Valor agregado 2013 -2020



	2013	2014	2015	2016	2017	2018	2019	2020
(I) Capacitaciones ejecutadas	9	8	21	35	47	60	143	336
(I) Publicaciones realizadas	1	8	29	40	43	58	59	60
(I) Investigadores y Técnicos beneficiados	61	127	118	152	252	314	580	1,325
(D) Fondos asignados para investigación	$381K	$333K	$684K	$769K	$1.23M	$1.37M	$1.58M	$1.7M

Figura 2 Impactos generados en el ecosistema

De la misma manera ha evolucionado la seguridad de la información por las necesidades reales de cada negocio y de las partes interesadas, esto ha llevado a que las organizaciones tomen conciencia sobre el adecuado control interno y las iniciativas relacionadas a cada organización.

A continuación, se puede evidenciar que en la Figura 3 ha evolucionado el crecimiento en las empresas certificadas en ISO 27001 a nivel mundial.

Figura 3 Crecimiento de los modelos de gestión ISO *(Prisma Consultoría SAS, 2017)*

De la misma manera en la Figura 4, se puede observar los primeros países en América con certificación ISO 27001.

Figura 4 10 primeros países con certificación ISO 27001 en América. *(Prisma Consultoría SAS, 2017)*

En la Figura 5 se observa los sectores con las mayores certificaciones a nivel mundial.

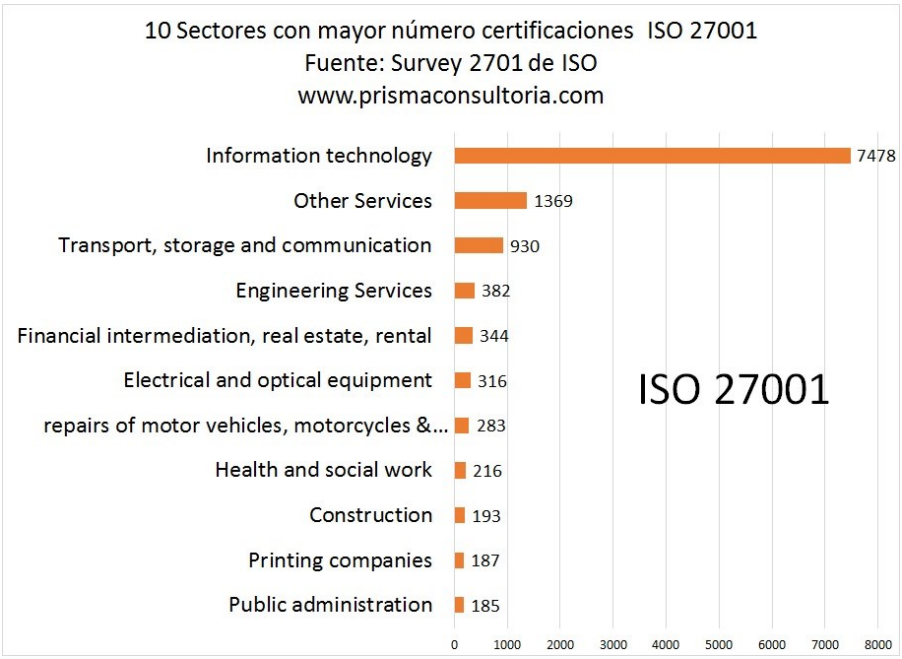


Figura 5 10 sectores con mayor certificaciones ISO 27001 en el mundo. *(Prisma Consultoría SAS, 2017)*

CEDIA como toda organización tiene vulnerabilidades y por falta de aplicación de controles es posible que su información esté expuesta, por esta razón, CEDIA ha visto la necesidad como organización de garantizar la seguridad, confidencialidad, integridad, disponibilidad y una gestión administrada de los datos y que la información resulte estandarizada y certificada, es así que desea incorporar y obtener la certificación ISO 27001 en la organización y como punto de partida y primera solución es la elaboración de una guía de implementación de un SGSI para CEDIA.

El proyecto técnico de titulación se realiza en la CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA - CEDIA ubicada en la ciudad de Cuenca, parroquia Sucre, en las calles Gonzalo Cordero 2-122 y José Fajardo. A lado del Parque de las Candelas.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Elaborar una guía de implementación de un SGSI para la CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA - CEDIA enfocado en la norma ISO/IEC 27002:2013.

1.3.2. OBJETIVOS ESPECÍFICOS

- OE1. Estudiar y conocer los conceptos, fundamentos requeridos por un Sistema de Gestión de Seguridad de la Información y los objetivos y controles de seguridad.
- OE2. Analizar las diferentes metodologías existentes de riesgos para seleccionar y ejecutar un análisis de riesgos para CEDIA.
- OE3. Elaborar la declaración de aplicabilidad según el análisis de brechas para CEDIA en base al anexo A (Normativo) Objetivos de control y controles de referencia de la norma ISO/IEC 27002:2013.

2. CONCEPTOS, FUNDAMENTOS REQUERIDOS POR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LOS OBJETIVOS Y CONTROLES DE SEGURIDAD

2.1. ANTECEDENTES

La Norma ISO/IEC 27001 tiene sus inicios en el año 1990 como Apoyo del Departamento de Comercio e Industria del Reino Unido para su desarrollo como código de las mejores prácticas.

En el año de 1995 se adoptó como British Standard (BS), que en español significa Estándar Británico y se llama BS 7799-1 que se trataba de un código de buenas *prácticas para apoyar a las empresas británicas a gestionar la seguridad de la información.* (ISO27000.es, 2005)

En 1999 se publicó la segunda edición BS 7799-2 donde se adiciona el e-commence, m-computer y el contrato con terceros, a diferencia de la primera edición, ésta norma definía los requisitos a cumplir para certificar del Sistema de Gestión de Seguridad de la Información.

En diciembre de 2000, la Organización Internacional de Normas Técnicas, adopta y publica la primera parte de la norma BS 7799 bajo el nombre de ISO 17799.

El 5 de septiembre del 2002 se publicó la versión de la BS 7799-2:2002 que permitía acreditar a las empresas por una entidad certificadora en varios países, entre ellos, Reino Unido. En este mismo año se adoptó el modelo PDCA (Planificar – Hacer – Verificar – Actuar).

En el año 2005 se publicó como estándar ISO 27001 y la ISO 17799 se modifica a ISO 27001:2005 siendo su publicación formal, misma que contiene especificaciones del SGSI, los controles de la ISO 17799 en el anexo de la norma demostrando la conexión entre la ISO 9001 e ISO 14001. (Prof. Edward J. Humphreys, 2013)

En el año 2007 la ISO 17799 pasa a ser ISO 27002:2005, misma que hace referencia a recomendaciones de mejores prácticas en el sistema de gestión de la seguridad de la información donde involucra a todos los interesados y responsables en iniciar, implantar o mantener dichos sistemas. En el mismo año se publica la versión ISO 27001:2007, dos años más tarde se publica un nuevo documento que corresponde a las modificaciones que es llamado ISO 27001:2007/1M:2009.

En el año 2008 se publica la norma ISO 27002:2008 describe los objetivos de control y controles recomendables para la seguridad de la información y se publica la norma ISO

27011:2008 que se refiere a las directrices para la gestión de la seguridad de la información para las organizaciones de telecomunicaciones basadas en la norma ISO 27002.

En el año 2009 se publica la norma ISO 27000:2009 que hace referencia a la Información general y Vocabulario de los Sistemas de Gestión de Seguridad de la Información, en este mismo año también se publica la norma ISO 27004:2009 que se basa en la Medición de la Gestión de seguridad de la información, de igual manera se publica la norma ISO 27033-1:2009 se basa en la Seguridad de la red – Parte 1: Introducción y conceptos.

En el año 2010 se publica la norma ISO 27003:2010 para la guía de aplicación del sistema de gestión de seguridad de la información, en el mismo año se publica la norma ISO 27033-3:2010 se basa en la Seguridad de la red – Parte 3: Escenarios de referencia de redes – Las amenazas, técnicas de diseño y temas de control.

En el año 2011 se publicó la norma ISO 27005:2011 para la gestión de riesgos de seguridad de la información, también se publicó la norma ISO 27006:2011 donde hace referencia a los requisitos para los organismos de auditoría y certificación de sistemas de gestión de seguridad de la información. En este mismo año se publicó la norma ISO 27007:2011 para Directrices para la auditoría de sistemas de gestión de seguridad de la información y la norma ISO 27008:2011 basada en la Seguridad de red – Parte 3: Escenarios de referencia de redes – Las amenazas, técnicas de diseño y temas de control.

En el año 2012 se publican otras normas de la familia 27000 esta segunda edición cancela y reemplaza la primera edición del año 2009 y se revisa las normas ISO 27001 e ISO 27002.

En el año 2013 la norma ISO 27001 e ISO 27002 se revisan y publican su nueva versión (segunda edición) en concordancia con otros, misma que trae modificaciones en la estructura, evaluación y tratamiento de riesgos reemplazando a la primera edición del 2005. (ISOTools Excellence, 2013)

2.2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El significado de Sistema de Gestión de Seguridad de la Información es muy similar para varios autores porque todos se basan de la Norma ISO 27001:

2.2.1. NORMA ESPAÑOLA UNE-EN ISO/IEC 27001

"La adopción de un sistema de gestión de la seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de la seguridad de la información por una organización está condicionado por sus necesidades y objetivos, sus requisitos de seguridad, los procesos organizativos utilizados y su tamaño y estructura. Lo previsible es que todos estos factores condicionantes cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos.

Es importante que el sistema de gestión de la seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles. Es de esperar que la implementación del sistema de gestión de la seguridad de la información se ajuste a las necesidades de la organización." (Normalización, 2017)

2.2.2. ISO27000.ES

"Un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales.

Un SGSI desde la visión del estándar internacional ISO/IEC 27001 es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio (p.ej. en empresas públicas, organizaciones sin ánimo de lucro, ...).

El alcance de un SGSI puede incluir, en función de dónde se identifiquen y ubiquen los activos de información esenciales, total co sólo un parte de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones en un grupo de organizaciones.

El término seguridad de la información generalmente se basa en que la información se considera un activo que tiene un valor que requiere protección adecuada, por ejemplo, contra la pérdida de disponibilidad, confidencialidad e integridad.

Cada organización puede extender e integrar en un SGSI las tres características básicas iniciales de definición de la seguridad a otras adicionales como suelen ser la autenticidad, trazabilidad, no repudio, auditabilidad,... según se considere oportuno para cumplir con los requerimientos internos y/o externos aplicables en cada actividad." (López Neira & Ruiz Spohr, 2005)

2.2.3. ISOTOOLS EXCELLENCE

"El SGSI es la abreviatura usada para referirse al Sistema de Gestión de la Seguridad de la Información e ISMS son las siglas equivalentes en ingles a Information Security Management System." (Excellence, 2015)

Se entiende por información todo el conjunto de datos que se constituyen en una organización y otorgan valor añadido para ésta, de manera independiente de la forma en la que se guarde o transmita, el origen que tenga o la fecha de elaboración.

El Sistema de Gestión de Seguridad de la Información, según ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización.

Según el conocimiento que se tiene del ciclo de vida de la información relevante se puede adoptar la utilización de un proceso sistemático, documentado y conocido por toda la empresa, desde un enfoque de riesgos empresarial. El proceso es el que constituye un SGSI." (Excellence, 2015)

Se concluye que el concepto de SGSI es global para todas las empresas, es decir, que un SGSI es un sistema que se enfoca en establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para cumplir con los objetivos del negocio.

El término SGSI es utilizado principalmente por la ISO/IEC 27001, sin embargo, existen otras normas que también la utilizan.

La ISO/IEC 27001, es un estándar internacional que fue aprobado en octubre de 2005 por la International Organization for Standardization (en español: Organización Internacional de Normalización) y por la International Electrotechnical Commission (en español: Comisión Electrotécnica Internacional), mismas que constituyen el sistema especializado para la normalización a nivel mundial. Se basa en los requisitos para establecer, implementar, mantener y dar mejora a un Sistema de SGSI por medio del "Ciclo de Deming": PDCA o PHVA – acrónimo de Plan (Planificar), Do (Hacer), Check (Verificar), Act (Actuar), con la proyección a la mejora continua.

Es así, que el concepto clave de un SGSI es el diseño, implementación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe continuar siendo eficiente a lo largo del tiempo, adaptándose a los cambios internos de la organización, así como los externos del entorno.

La norma indica que la organización debería evaluar el desempeño y la eficacia del sistema de gestión de seguridad de la información (cláusula 9.1 de la norma ISO/IEC 27001). Esta cláusula es un componente prioritario de un sistema de gestión puesto que sin la evaluación de la eficacia de los procesos y controles que se lleven a cabo, es imposible validar que la organización haya logrado o logre sus objetivos.

2.3. ENFOQUE A PROCESOS

La norma ISO 27001 se ha desarrollado de acuerdo al enfoque orientado a procesos y siguiendo el ciclo o modelo PDCA para regularizar todos los procesos del Sistema de Gestión de Seguridad de la Información.

Se define como "proceso" a*: Un conjunto de actividades que utiliza recursos y se gestiona de modo que permite la transformación de unos elementos de "entrada" en unos elementos de "salida"*. (Colegio Oficial de Ingenieros de Telecomunicación, 2012)

En efecto, el enfoque a procesos consiste en identificar un conjunto de procesos en la organización, sus interacciones y su gestión.

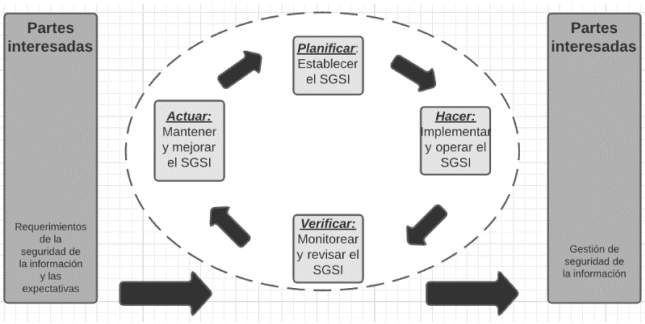


Figura 6 Modelo PHVA aplicado a los procesos del SGSI. (PECB Group Inc, 2005)

En la Figura 6 se puede apreciar la adaptación del modelo o ciclo de Deming para el SGSI.

El modelo o ciclo de Deming es una estrategia de mejora continua de la calidad que está compuesto en 4 fases cíclicas que se detallan a continuación cada una de ellas: (Colegio Oficial de Ingenieros de Telecomunicación, 2012)

- **Planificar** (Plan): Fase de diseño del SGSI para evaluar los riesgos de seguridad de la información y seleccionar controles respectivos y adecuados. Establecer el sistema de gestión, es decir, la política, los objetivos, los procesos y procedimientos relacionados con la gestión de riesgos y mejora de la seguridad de la información para proporcionar resultados esperados con las políticas mundiales y los objetivos de la organización. El PLANIFICAR se puede encontrar en las cláusulas 4, 5 y 6 de la Norma ISO 27001, que se refiere al Contexto de la organización, Liderazgo y Planificación.
- **Hacer (Do):** Fase de implementación y operación de los controles. Implementar y operar el sistema de gestión, es decir, la política, controles, procesos y procedimientos, si es posible en una pequeña escala. El HACER se encuentra en las cláusulas 7 y 8 de la Norma ISO 27001, se refiere al Soporte y Operación.
- **Verificar** (Check): Fase de revisión y evaluación del desempeño (eficiencia y eficacia) del SGSI. Monitorear y revisar el sistema de gestión, es decir, se debe evaluar si se procede a medir las actuaciones del proceso frente a la política, los objetivos y la experiencia práctica y se informa los resultados a la gerencia para su revisión. El VERIFICAR se puede encontrar en la cláusula 9 de la Norma ISO 27001, se refiere a la Evaluación del desempeño.
- **Actuar** (Act): Fase de cambios necesarios que lleven al SGSI a su máximo rendimiento. Mantener y mejorar el sistema de gestión, es decir, adopta las

acciones correctivas y preventivas, en base a los resultados de la auditoría interna y revisión por parte de la Dirección, u otra información relevante para lograr la mejora continua del SGSI. El ACTUAR se encuentran en la cláusula 10 de la Norma ISO 27001, se refiere a la Mejora.

La aplicación del enfoque a procesos variará de una organización a otra en función de su tamaño, actividades y complejidad, teniendo en común que se debe implementar y gestionar numerosos procesos inter relacionados e interactivos y sabiendo que un elemento de salida de un proceso podría significar un elemento de entrada del siguiente proceso.

Como conclusión, se puede decir que la gestión ordenada, la identificación de los procesos e interacción dentro de la organización se denomina como enfoque basado en procesos.

2.4. FUNDAMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

Para garantizar que el Sistema de Gestión de Seguridad de la Información gestione de manera correcta se debe y tiene que identificar el ciclo de vida basado en fundamentos o principios que se detallan a continuación:

- **Confidencialidad**: La información no se puede ofrecer o revelar a ningún individuo, entidad o proceso no autorizado.
- **Integridad**: La información y los métodos de proceso deben y tienen que mantenerse de forma completa y exacta de la que se introdujo en el sistema, solo el personal autorizado puede modificar el contenido y la cantidad.
- **Disponibilidad**: La información y los sistemas de tratamiento deben y tienen que ser accesible para cualquier persona, entidad o proceso autorizado en cualquier momento que lo requieran.

Figura 7¿Qué es un Sistema de Gestión de la Seguridad de la Información (SGSI)? (LISOT, 2018)

En la figura 7 se muestra que la seguridad de la información consiste en salvaguardar la confidencialidad, integridad y disponibilidad mediante la aplicación de un proceso de gestión de riesgos otorgando a las partes interesadas confianza en la organización.

2.5. OBJETIVOS Y CONTROLES DE SEGURIDAD

Los objetivos de control y controles de seguridad se enumeran y definen en el anexo A Tabla A.1 que se encuentra en la Norma ISO/IEC 27002:2013. Este anexo es un documento normativo que sirve de guía para implementar los controles de seguridad específicos de ISO 27001, es decir, para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para toda organización que así lo desee.

Todos estos controles están dirigidos para la mejora en la seguridad de la información de la organización en caso de implementar la norma, la aplicación de los controles es obligatoria a excepción de los casos que no se puede aplicar.

Al tener conocimiento de estos controles, se puede comprender que la seguridad de la información no solo se refiere a lo que comúnmente se conoce como "ciberseguridad". El enfoque va más allá de eso, puesto que un SGSI abarca tanto ese tipo de información como la que se encuentra en formato físico y de diferentes áreas de la organización como lo es: Recursos Humanos, Departamento financiero, tecnología, ventas, legal, etc., para ello se describe una pequeña definición y diferencia entre ciberseguridad y seguridad de la información.

2.5.1. CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

La definición de ciberseguridad desde ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información) es la "*Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados*". (ESIC BUSINESS & MARKETING SCHOOL, 2020)

La Norma ISO/IEC 27001 define el Activo de la Información como *"conocimientos o datos que tienen valor para una organización"*, y Sistemas de Información *como "los que comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros*

componentes que permiten el manejo de la misma". (ESIC BUSINESS & MARKETING SCHOOL, 2020)

Por consiguiente, la ciberseguridad tiene como propósito la protección de la información digital de los sistemas interconectados y está comprendida dentro de la seguridad de la información.

De acuerdo con la Real Academia Española (RAE), la seguridad se define como "*libre o exento de todo peligro, daño o riesgo*". (Welivesecurity by ESET - ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia, 2015)

Pero en toda área informática se trata de una condición ideal, pues es bien conocido que en la realidad no se puede tener la certeza ni la garantía de que se pueden evitar todos los peligros.

La "seguridad" tiene como propósito reducir riesgos hasta un nivel aceptable para los interesados y de igual forma se entiende que son aquellas actividades que se encargan de proteger de algún tipo de peligro.

Y cuando se habla de la información, ésta, puede encontrarse y ser almacenada de diferentes maneras, sea en formato digital (a través de archivos en medios electrónicos u ópticos), en forma física (ya sea escrita o impresa en papel), así como de manera no representada, como pueden ser las ideas o el conocimiento de las personas.

La información, sin importar su forma o estado, de acuerdo con su importancia y criticidad, debe tener medidas de protección adecuadas, y es aquí donde trabaja la seguridad de la información.

De acuerdo a lo antes mencionado, se puede definir a la seguridad informática o ciberseguridad como la protección de hardware, redes, software, infraestructura tecnológica o servicios y a la seguridad de la información incluye actividades de seguridad relacionadas con la información que manejan las personas, seguridad física, cumplimiento o concientización.

2.6. ANÁLISIS DE LA FAMILIA ISO/IEC 27000

La familia ISO 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que aportan un marco de gestión de la seguridad de la información para cualquier tipo de organización. A continuación, listamos los más relevantes a criterio del autor:

2.6.1. ISO/IEC 27000 INTRODUCCIÓN Y VOCABULARIO

Fue publicada el 1 de mayo de 2009, su segunda edición el 01 de diciembre de 2012, una tercera edición el 14 de enero de 2014 y una cuarta en el mes de febrero de 2016. Este estándar de seguridad establece una visión general de las normas que forman parte de la serie 27000, donde indica las definiciones, el alcance de actuación y el propósito de la publicación para cada una de las normas, así como el vocabulario que se aplica en el análisis de un SGSI.

2.6.2. ISO/IEC 27001 REQUISITOS

Es la norma más importante y principal de la familia ISO/IEC 27000 porque contiene los requisitos para la implantación del SGSI (Cláusula 4 a 10) en las organizaciones y la única norma que se puede obtener la certificación. Su inicio fue la British Standard BS 7799-2:2002. En el Anexo A se enumera los objetivos de control y controles que lleva a cabo la ISO 27002:2005 basándose en la gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005 y revisada en septiembre de 2013.

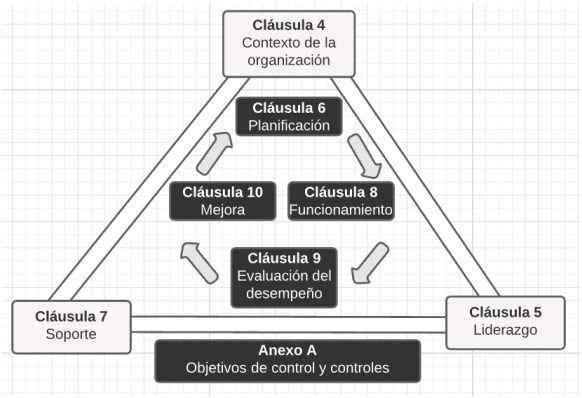


Figura 8 Estructura de la norma ISO 27001 (PECB Group Inc, 2005)

La figura 8 muestra la estructura de la norma ISO 27001, esto significa que cualquier tipo de organización que desee certificarse en esta norma debe cumplir con cada uno de los términos definidos en las cláusulas 4 a 10, definir en la declaración de aplicabilidad, los controles aplicables y justificar la inaplicabilidad de los controles del Anexo A.

2.6.3. ISO/IEC 27002 (ANTIGUA ISO 17799:2005) CÓDIGO DE BUENAS PRÁCTICAS PARA SISTEMAS DE GESTIÓN DE SEGURIDAD

Es una guía de buenas prácticas que establece los objetivos de control y controles para la gestión de seguridad de la información y fue publicada en julio de 2005 como ISO 17799:2005 y se publicó con el nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007. La última versión es la ISO/IEC 27002:2013, de septiembre de 2013.

Esta norma contiene los objetivos de control que se mencionan a continuación:

- *A.5 Políticas de seguridad de la información*
- *A.6 Organización de la Seguridad de la Información*
- *A.7 Seguridad relativa a los 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 de las comunicaciones*
- *A.14 Adquisición, desarrollo y Mantenimiento de los sistemas de información*
- *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 de Negocio*
- *A.18 Cumplimiento* (ISO/IEC 27002:2013, 2013)

Es importante recordar que la efectividad de la gestión de la seguridad de la información depende mucho de la aplicación de estos estándares a la realidad de la organización para ayudar a incrementar su eficiencia. No es certificable.

2.6.4. ISO/IEC 27010 DIRECTRICES DE SEGURIDAD PARA LAS COMUNICACIONES ENTRE ORGANIZACIONES

Se orienta a la gestión de la seguridad de la información en comunicaciones entre el mismo sector, entre sectores y con los gobiernos. Se aplica a todas las formas de intercambio y difusión de información. Fue publicada en octubre de 2012 y revisada en noviembre de 2015.

2.6.5. ISO/IEC 27011 DIRECTRICES DE SEGURIDAD PARA ORGANIZACIONES DE TELECOMUNICACIONES

Esta norma hace referencia a una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones de telecomunicaciones que se basan en la ISO/IEC 27002. Fue publicada en diciembre de 2008 y revisada en diciembre de 2016, se encuentra también como norma ITU-T X.1051.

2.6.6. ISO/IEC 27012 DIRECTRICES PARA LA INTEGRACIÓN DE ISO 27001 E ISO 20000-1

Es una guía que hace referencia a un conjunto de requisitos (complementarios a ISO/IEC 27001) y directrices (complementarias a ISO/IEC 27002) de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración.

2.6.7. ISO/IEC 27015 DIRECTRICES PARA SERVICIOS FINANCIEROS

Guía de sistema de gestión de seguridad de la información que se orienta a las organizaciones del sector financiero y de seguros. Fue publicada en noviembre de 2012.

2.6.8. ISO/IEC 27799 GUÍA PARA IMPLEMENTAR ISO/IEC 27002 EN LA INDUSTRIA DE LA SALUD

Es una guía que orienta y apoya la interpretación y aplicación en la industria de la salud de ISO/IEC 27002, en la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, lo desarrolla el comité técnico TC 215.

A continuación, se detalla la norma y su contenido como resumen de la familia ISO 27000: (ISO27000.es, 2005)

- 27000 Introducción y vocabulario

- 27001 Norma principal. Requisitos del SGSI. Certificable
- 27002 Guía de buenas prácticas: (11) dominios, (39) objetivos de control y (133) controles en la versión 2005 mientras que en la versión 2013 son 114 controles.
- 27003 Proporciona aspectos críticos para el diseño e implementación del SGSI. Es el soporte de la norma ISO/IEC 27001. Se publicó el 1 de febrero de 2010.
- 27004 Es una guía para el desarrollo y uso de métricas y técnicas de medida de la eficacia de un SGSI y de los controles y objetivos de controles. Se publicó el 7 de diciembre de 2009, no tiene traducción al español.
- 27005 Es una guía para la gestión de riesgo y tiene más relación con la actual British Standard BS 7799 parte 3. Fue publicada en junio de 2008 y revisada en junio de 2011.
- 27006 Es una norma para la acreditación de organizaciones de auditoría y certificación, estableciendo requisitos específicos para la certificación de SGSI y es utilizada en conjunto con la 17021-1, que es la norma genérica de acreditación. Fue publicada en 2007 y revisada en diciembre de 2011 y septiembre de 2015.
- 27007 Es la guía de auditoría de un SGSI y se publicó en noviembre de 2011.
- 27008 Es una guía de auditoría de los controles seleccionados, no es una norma certificable. Fue publicada en octubre de 2011.
- 27013 Es una guía de implementación integrada de la ISO/IEC 27001 que hace referencia a la gestión de seguridad de la información y de la norma ISO/IEC 20000-1 que hace referencia a la gestión de servicios de TI. Se publicó el 15 de octubre de 2012 y se actualizó el 24 de noviembre de 2015.
- 27014 Es una guía de gobierno corporativo de la seguridad de la información, la ciberseguridad y privacidad. Se publicó el 23 de abril de 2013 y se actualizó su segunda edición en diciembre 2020.
- 27016 Es una norma que se centra en un análisis financiero y económico de los equipos y los procedimientos de la seguridad de la información, se publicó en febrero de 2014.
- 27017 Es la guía de seguridad para la computación en la nube. Fue publicada en diciembre de 2015.
- 27018 Es una guía para controlar la protección de datos para servicios de computación en la nube. Fue publicada en julio de 2014.
- 27019 Es una guía para el proceso de sistemas de control específicos en el sector de la industria de la energía.

- 27031 Guía de continuidad de negocio en tecnologías de la información y comunicaciones. No es certificable. Fue publicada en marzo de 2011.
- 27032 Guía relativa a la seguridad informática. Fue publicada en julio de 2012.
- 27033 Es la guía de seguridad de la administración, operación y uso de las redes en 7 partes y se publicó en el año 2010.
- 27034 Es la guía de seguridad en aplicaciones informáticas y se publicó en el 2011.
- 27035 Es la guía de gestión de incidentes y técnicas de seguridad de la información, que hace referencia en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades. Fue publicada en agosto de 2011.
- 27036 Guía de seguridad de externalización de servicios (proveedores). Fue publicada en el año 2013.
- 27037 Es una guía de identificación, recopilación y preservación de evidencias digitales.

3. ANÁLISIS DE RIESGOS

3.1. METODOLOGÍAS PARA EL ANÁLISIS DEL RIESGO

Para conocer de las metodologías para el análisis del riesgo, lo primero que se debería conocer es el significado de "riesgo" y según la Real Academia Española es la *Contingencia o proximidad de un daño*, y el significado según la Norma IEC/ISO 27001 es el *efecto de la incertidumbre*, es decir, es el no cumplimiento de algún objetivo de la organización.

Día a día estamos en riesgo, indistintamente de la actividad que se realiza, se puede atravesar riesgos inesperados, el simple hecho de bajar gradas implica el riesgo de pisar mal y/o caerse, o comprar comida en un nuevo restaurante el riesgo puede ser que la comida no esté bien preparada. Es evidente que a nivel personal no se puede hacer un análisis de riesgos de cada acción o decisión que se tome y mucho menos de documentarlo.

En el ámbito organizacional, las acciones se deben tomar de un modo objetivo, y ser capaz de medir el riesgo puede ser la diferencia entre el éxito o el fracaso. En este sentido, las áreas de Tecnología de Información de las organizaciones son uno de los departamentos pioneros en acometer análisis de riesgos, impulsado por ser uno de los requisitos de normas como la ISO/IEC 27001 o como proyecto de organización propia.

El análisis de riesgos es la herramienta a través de la cual se puede obtener un enfoque claro y priorizado de los riesgos a los que se enfrenta una organización, teniendo como objetivo identificar los principales, sean estos: desastres naturales, fallos en infraestructura o riesgos introducidos por el mismo personal.

En este sentido se pretende identificar los riesgos más significativos que puede afectar a la operatividad de la organización y priorizar medidas a implantar para minimizar la probabilidad de materialización de dichos riesgos o el impacto en caso de materializarse.

En una organización el activo más importante es la información, por lo que es necesario introducir las diferentes metodologías diseñadas para el análisis y gestión de riesgos, mismas que se detallan a continuación:

3.1.1. CRAMM

CRAMM es una metodología diseñada para el uso en análisis y gestión de riesgos que fue desarrollada por la Agencia Central de Comunicación y Telecomunicación del Gobierno Británico, por sus siglas en inglés, CCTA Rick Analysis and Management Method, su versión inicial data de 1987 y la vigentes es la versión 5.2.

CRAMM dispone de un amplio reconocimiento y tiene un alto valor en administración pública británica, sin embargo, también puede ser usado en organizaciones e instituciones de gran tamaño, está orientada a proteger la confidencialidad, integridad y disponibilidad de la organización y de sus activos.

Las evaluaciones se consideran cuantitativas, aunque también pueden ser cuantitativas y cualitativas, por esta razón se considera mixta.

La metodología de CRAMM incluye 3 etapas:

- Primera: Definición global de los objetivos de seguridad entre los cuales esta: la definición del alcance, la identificación y evaluación de los activos físicos y software implicados, la determinación del valor de los datos en cuanto a impacto en la organización y la identificación.
- Segunda: El análisis de riesgos, que identifica las amenazas que afecta al sistema o a la organización, las vulnerabilidades que explotan dichas amenazas y el cálculo de los riesgos de materialización de las mismas.
- Tercera: Identifican y seleccionan las medidas de seguridad aplicadas en la organización obteniendo los riesgos residuales, CRAMM proporciona una librería con unas 3000 medidas de seguridad. (Huerta, 2012)

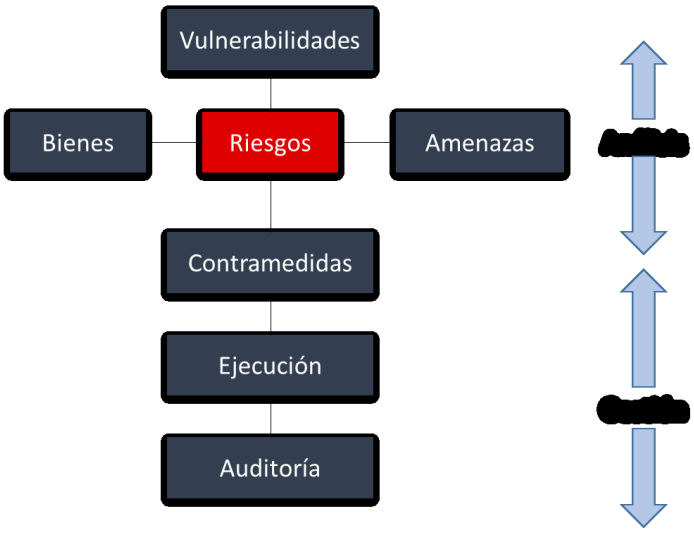


Figura 9 Evaluación de CRAMM (Huerta, 2012)

En la figura 9 se establece como es la evaluación de la metodología CRAMM durante las tres etapas.

Adicional, CRAMM ayuda a demostrar la eficiencia del costo invertido en la administración de riesgos, la seguridad y la planificación de emergencias. Contiene una amplia biblioteca única de contramedidas de seguridad. La aplicación de la metodología CRAMM permite a las organizaciones prepararse para su certificación de acuerdo con ISO 27001 y con otras normas ISO (ISO 9001 e ISO 14001). (Pineda, 2021)

El procedimiento de CRAMM es el siguiente:

- *Utiliza reuniones, entrevistas y cuestionarios para la recolección de datos.*
- *Identifica y clasifica los activos de TI en tres categorías; datos, software y activos físicos.*
- *Requiere que se consideren el impacto de la pérdida de confidencialidad, integridad y disponibilidad del activo.*
- *Mide la vulnerabilidad por niveles: muy alto, alto, medio, bajo o muy bajo.*
- *Mide el riesgo por niveles: alta, media o baja.* (Ideas y proyectos promocionales, 2019)

3.1.2. MAGERIT

MAGERIT es el acrónimo de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones, creada por el Consejo Superior de Administración

Electrónica del Gobierno de España actualmente llamada Comisión de Estrategia TIC, el uso de MAGERIT es de carácter público para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, La primera versión se creó en el año de 1997, actualmente se encuentra en la versión 3, donde cubre la fase AGR que significa Análisis y Gestión de Riesgos.

MAGERIT interactúa en todas las fases de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico. (Pineda, 2021)

Entre sus objetivos están:

Directos:

- *Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.*
- *Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).*
- *Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control*

Indirectos:

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

MAGERIT implementa el proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados de uso de tecnologías de la información. (Dirección General de Modernización Administrativa, 2012)

La metodología de MAGERIT tiene los siguientes pasos:

1. *Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio o coste supondría su degradación.*
2. *Determinar a qué amenazas están expuestos aquellos activos.*
3. *Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.*
4. *Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.*
5. *Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.*

MAGERIT consiste en 3 libros en versiones inglés, español e italiano:

- *Libro I: Método*
- *Libro II: Catálogo de Elementos*
- *Libro III: Guía de Técnicas* (Ideas y proyectos promocionales, 2019)

3.1.3. NIST SP 800-30

NIST por sus siglas en inglés National Institute of Standards and Technology de EEUU (Instituto Nacional de Estándares y Tecnología) ha publicado documentos relacionados con el análisis de riesgos en las cuales se encuentra la Special Publication (SP) 800-30 que es una guía de gestión de riesgos de los Sistemas de Tecnología de la Información y deben cumplir todos los productos y servicios que dependan de alguna tecnología.

La Ley de Gestión de la Seguridad de la Información Federal (FISMA) requiere a las agencias federales cumplir con un conjunto de estándares de seguridad. Estos estándares son provistos por NIST y son conocidos como Estándares Federales de Procesamiento de Información (FIPS).

FIPS es una serie de publicaciones especiales de la serie SP 800 sobre la seguridad de la información. Esta serie incluye una metodología para el análisis y gestión de riesgos de la seguridad de la información, alineada y complementaria con el resto de documentos de la serie. (Ideas y proyectos promocionales, 2019)

La metodología NIST SP 800-30 está compuesta por 9 pasos básicos para el análisis de riesgo, de acuerdo a la siguiente figura:

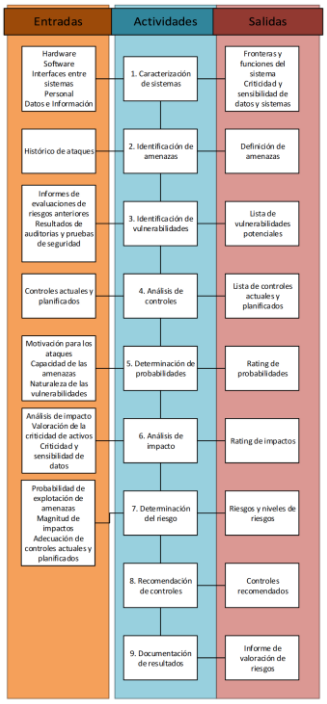


Figura 10 Metodología NIST SP 800-30 (Ideas y proyectos promocionales, 2019)

Según NIST (2012), señala que la NIST SP 800-30 está orientada especialmente a los profesionales vinculados con la gestión de riesgos en las organizaciones como: jefes de los organismos, directores generales, jefe de operaciones, ejecutivo de riesgo; los individuos encargados de la vigilancia de la seguridad de la información, su gestión y responsabilidades operativas (por ejemplo, los directores de información, oficiales de alto rango, los administradores y propietarios de sistemas de información, los proveedores de control comunes etc). (PINZÓN, 2017)

3.1.4. ISO/IEC 27001

El análisis de riesgos es muy importante al momento de definir un proyecto y las iniciativas con las que se desea mejorar la seguridad de la información en una organización.

El análisis de riesgo proporciona elementos de entrada para la evaluación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados. (PECB Group Inc, 2005)

La norma ISO/IEC 27001 proporciona altos niveles de seguridad para datos confidenciales y específica los requisitos para establecer, implementar, documentar, revisar, mantener y evaluar

el SGSI de la organización, fomenta a que los usuarios que son todos los colaboradores tengan en cuenta:

- *Comprender los requisitos de la seguridad de la información de la organización.*
- *Deben participar en la evaluación y tratamiento de riesgos.*

En el capítulo 6 (Planificación) de la Norma ISO/IEC 27001 se puede profundizar sobre las acciones para tratar los riesgos y oportunidades de la organización.

La evaluación y tratamiento de riesgos se aplican a todo el alcance del SGSI; es decir, a todos los activos que se utilizan dentro de la organización o que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

La gestión de riesgos asegura que el SGSI pueda conseguir los resultados previstos.

El propósito de la ISO/IEC 27001 es protegerse ante riesgos, por ello se tiende a pensar que es primordial la implementación de la ISO/IEC 31000 para obtener la certificación en la ISO/IEC 27001, lo cual no es realmente necesario, sin embargo, si se debe comprender que existe una vinculación entre estas dos normas, puesto que la norma ISO/IEC 31000 se encarga de ofrecer principios y directrices para la gestión de cualquier tipo de riesgo, realiza la evaluación de dichos riesgos identificando y analizando los mismos, mientras que, la ISO/IEC 27001 cuenta con fases para la metodología de evaluación y tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización.

En la cláusula 4.1 de la norma ISO/IEC 27001 determina que se debe establecer el contexto interno y externo de la organización, tal como se describe en la cláusula 5.4 de la ISO/IEC 31000:2018, en los puntos 5.4.1 y 5.4.2 se analizan y comprenden los contextos interno y externo a la hora de diseñar el marco de referencia para administrar o gestionar los riesgos y oportunidades en ISO/IEC 27001.

De igual manera como lo indica la nota de la cláusula 6.1.3 de la norma ISO/IEC 27001 que la evaluación y el proceso de tratamiento de riesgos se alinea con los principios y lineamientos de la norma ISO/IEC 31000.

Esto quiere decir, que una puede ser muy útil en la implementación de la otra, puesto que comparten lineamientos sobre la gestión de riesgos comunes y porque a nivel estratégico tienen evidentes semejanzas. (Escuela Europea de Excelencia, 2019)

3.1.4.1. EVALUACIÓN DE RIESGOS

La evaluación y tratamiento de riesgos se aplican a todo el alcance del SGSI; es decir, a todos los activos que se utilizan dentro de la organización o los que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

El proceso de evaluación de riesgos, la identificación de amenazas y vulnerabilidades es coordinado y realizado por el propietario de cada activo, así como la evaluación de consecuencias y probabilidad será realizada por el mismo propietario. (27001Academy, 2015)

3.1.4.1.1. IDENTIFICACIÓN DE ACTIVOS

Se debe identificar todos los activos que guardan relación con el área, proceso o sistema objeto del estudio en la organización, es decir, los activos son todos los que pueden afectar la confidencialidad, integridad y disponibilidad de la información en la organización.

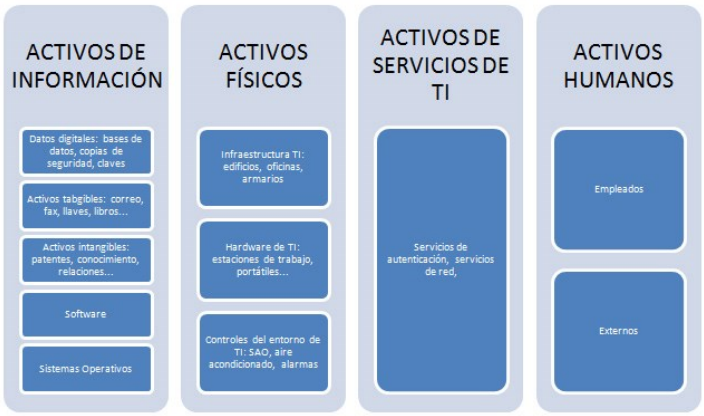


Figura 11 ISO 27001. El inventario de activos en la implementación de la norma (ISOTools Excellence, 2013)

La figura 11 muestra los activos que existen en una organización:

- Documentos impresos o en formato electrónico
- Software: aplicaciones y bases de datos
- Personas / Empleados y/o Externos
- Equipos de TI: servidores, computadoras, impresoras, etc.
- Infraestructura: oficinas, alarmas, armarios, etc.
- Servicios o procesos externos

Donde, la información es uno de los activos más primordiales en una organización.

Al identificar los activos también es necesario identificar a sus propietarios, es decir, la persona o unidad organizativa responsable de cada activo, la recomendación de la norma ISO/IEC 27001 es que el propietario de cada activo sea el mismo responsable del riesgo.

3.1.4.1.2. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Todos los activos de la organización están expuestos a amenazas, mismas que se deben identificar manteniendo un enfoque práctico y aplicado, y estas son explotadas por vulnerabilidades.

Lo recomendable suele ser identificar amenazas/vulnerabilidades por tipo de activo, lo cual ahorrará tiempo, ya que todos los activos que estén bajo el paraguas de una misma categoría podrán compartir amenazas/vulnerabilidades. No obstante, se debe hacer un análisis por cada activo y comprobar si las amenazas/vulnerabilidades que le corresponden por su categoría son adecuadas. (ISOTools Excellence)

Una situación de vulnerabilidad en la organización favorece que las amenazas se materialicen. (ISOTools Excellence)

Se debe también analizar y documentar las medidas de seguridad implementadas en la organización.

3.1.4.1.3. EVALUAR O CALCULAR EL NIVEL DE RIESGO

Al llegar a este punto, se entiende que ya se dispone de la siguiente información:

- Activos.
- Amenazas a las que está expuesta cada activo.
- Vulnerabilidades asociadas a cada activo.

Y significa que es posible evaluar el riesgo. *Para cada activo-amenaza, se estimará la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede llevar a cabo utilizando tanto criterios cuantitativos como cualitativos.* (ISOTool Excellence, 2019)

El proceso de apreciación de riesgos en la Norma ISO 27001 capítulo 6 cláusula 6.1.2 indica que se establezca y mantenga criterios sobres los riesgos que incluya criterios de aceptación

de los riesgos y los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información. (Normalización, 2017)

Estos criterios para apreciar los riesgos deben venir desde el Direccionamiento Estratégico y de los requisitos de las partes interesadas.

La negación de los objetivos estratégicos y el incumplimiento de los requisitos de las partes interesadas son los primeros riesgos de la organización, sin embargo, se deben identificar otros riesgos a más de los mencionados.

Los riesgos se clasifican o aprecian por los criterios de aceptación de los mismos y tienen afectos relacionados a la probabilidad y consecuencia (Impacto), los cuales se pueden medir en valores porcentuales o como lo defina y establezca la organización.

La probabilidad se refiere a que una amenaza se materialice e impacto es el resultado de la materialización de una amenaza.

En algunos casos se considerará la valoración del activo basada en la confidencialidad, integridad y disponibilidad.

Una vez que se han identificado los riesgos, es necesario evaluar las consecuencias para cada combinación de amenazas y vulnerabilidades de un activo específico, en caso que ello se pueda producir: (27001Academy, 2015)

Baja consecuencia	*0*	*La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.*
Consecuencia moderada	*1*	*La pérdida de confidencialidad, disponibilidad o integridad causa gastos y tiene consecuencias bajas o moderadas sobre obligaciones legales o contractuales o sobre el prestigio de la organización.*

Alta consecuencia	*2*	*La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias importantes y/o inmediatas sobre las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización.*

Tabla 1 Medición para la evaluación de las consecuencias, ISO 27001 (27001Academy, 2015)

Luego de la evaluación de consecuencias es necesario evaluar la probabilidad de que se materialice ese riesgo; es decir, la probabilidad de que una amenaza se aproveche de la vulnerabilidad del activo en cuestión. (27001Academy, 2015)

Baja probabilidad	*0*	*Los controles de seguridad existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección. En el futuro no se esperan incidentes nuevos.*
Probabilidad moderada	*1*	*Los controles de seguridad existentes son moderados y en general han suministrado un adecuado nivel de protección. Es posible la ocurrencia de nuevos incidentes, pero no muy probable.*
Alta probabilidad	*2*	*Los controles de seguridad existentes son bajos o ineficaces. Existe una gran probabilidad de que haya incidentes así en el futuro.*

Tabla 2 Medición para la evaluación de las probabilidades, ISO 27001 (27001Academy, 2015)

Ingresando los valores de consecuencia y probabilidad en el Cuadro de evaluación de riesgos, el nivel de riesgo se calcula automáticamente sumando los dos valores. Los controles de seguridad existentes tienen que ser ingresados en la última columna del Cuadro de evaluación de riesgos. (27001Academy, 2015)

Los criterios para la aceptación de riesgos según las tablas 1 y 2 se refieren al resultado de la probabilidad e impacto que produce en la organización, l*os valores 0, 1 y 2 son riesgos aceptables, mientras que los valores 3 y 4 son riesgos no aceptables. Los riesgos no aceptables deben ser tratados.* (27001Academy, 2015)

El riesgo aceptable es el nivel de riesgo que establece la organización como permitido, es decir, si el nivel de riesgo aceptable por ejemplo es 1, únicamente supondrá un peligro para la organización aquellos riesgos que estén por encima de 2.

Por tanto, si el nivel de riesgo está por encima del aceptable, se tiene que hacer un tratamiento del mismo con el objetivo de reducirlo (a un nivel aceptable). (ISOTools Excellence)

3.1.4.1.4. TRATAMIENTO DE RIESGOS

Los controles de seguridad son fundamentales, puesto que con ellos los riesgos no sobrepasarían el nivel aceptable y no existiría peligro para la organización y para aquellos riesgos que si superen el nivel aceptable y se deberá aplicar los controles implementando dichos controles de manera ordenada, estructurada y planificada para ello se debe establecer un plan de tratamiento.

El plan para tratar los riesgos debe contener una serie de información básica:

- **Responsable del control:** Persona que se encarga de la correcta implantación del control.
- **Recursos:** Personas, personal técnico, equipo de trabajo que forman parte de la implantación del control
- **Acciones necesarias para la implantación del control**
- **Prioridad:** Es necesario establecer prioridades, puesto que los niveles de riesgos y el valor de cada activo son diferentes y por esta razón cada control debe tener su prioridad.

Posterior a implantar todos los controles de seguridad se debe calcular el riesgo residual.

El riesgo residual es el riesgo que sigue apareciendo después de implantar los controles de seguridad.

Cuando implantamos los controles reducimos el riesgo, pero este no dejará de existir, siempre quedará un nivel, aunque sea mínimo.

¿Qué ocurre si el nivel de riesgo, reducido por la implantación de los controles de seguridad, sigue estando por encima del nivel de riesgo aceptable? (ISOTools Excellence)

Para los riesgos no aceptables se debe seleccionar una o más de las siguientes opciones de tratamiento de riesgos:

1. Elección de un control o varios controles de seguridad del Anexo A de la norma ISO/IEC 27001 u otros controles de seguridad.
2. Transferir el riesgo a terceros, puede ser a una compañía de seguros o a una compañía externa.
3. Evitar el riesgo, siempre que se justifique, esta opción se permite solamente si la selección de otras opciones de tratamiento del riesgo costaría más que el potencial impacto en el caso de que se materializara dicho riesgo.
4. Aceptar el riesgo. (27001Academy, 2015)

Los propietarios de riesgos deben revisar los riesgos vigentes y deben actualizar la evaluación de riesgos y el tratamiento de riesgos de acuerdo con los nuevos riesgos identificados.

La revisión se debería realizar al menos una vez por año, o con mayor frecuencia en caso de cambios organizacionales significativos, cambios importantes en tecnología, en los objetivos de negocios, en el entorno empresarial, etc.

4. EVALUACIÓN Y ANÁLISIS DE RIESGO PARA CEDIA

4.1. SELECCIONAR LA METODOLOGÍA PARA LA EVALUACIÓN Y ANÁLISIS DE RIESGO PARA CEDIA

Uno de los objetivos del presente documento es seleccionar la metodología más adecuada para evaluar y analizar los riesgos de la información en CEDIA, definir el nivel de riesgo aceptable y residual. Al existir varias metodologías para evaluar el riesgo asociado a los activos de la organización y establecer las medidas para reducirlo, se realizó un análisis y comparación entre las metodologías mencionadas en el capítulo anterior y la elección más adecuada es la metodología de evaluación de riesgos de la Norma ISO/IEC 27001 porque se alinea a la estrategia y propósito organizacional y proporciona resultados comparables y reproducibles.

4.2. EJECUCIÓN DEL ANÁLISIS DE RIESGO PARA CEDIA (ESPECIFICO)

CEDIA es una organización privada sin fines de lucro dedicada a fomentar, promover y coordinar el desarrollo de la investigación científica, la academia, la innovación, transferencia tecnológica, emprendimiento, internacionalización y a ofrecer servicios relacionados a sus diferentes áreas y otras afines, a los miembros y a quienes se autorice; de manera comercial o gratuita con actores del sector público, privado, nacional o internacional.

CEDIA al ser una organización puede sufrir riesgos o ataques en su sistema de información debido a personas o recursos internos o externos, para ello se define la metodología para evaluar y tratar los riesgos de la información en CEDIA y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001.

Como se indicó anteriormente, la evaluación y tratamiento de riesgos se aplican a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los activos de la organización o que tienen un impacto sobre la seguridad de la información en el ámbito del SGSI, sin embargo, para este estudio solo se realizará la evaluación y tratamiento de riesgos a nivel del activo Infraestructura de los Servidores de la Nube.

Los usuarios de esta metodología son todos los colaboradores de CEDIA quienes participan en la evaluación y tratamiento de riesgos.

4.2.1. EVALUACIÓN DE RIESGOS EN SERVIDORES DE LA NUBE DE CEDIA

La evaluación de riesgos es coordinada por el Oficial de Seguridad de la Información y los Especialistas en Servidores del área Técnica de CEDIA, la identificación de amenazas y vulnerabilidades la realizan los propietarios de los activos, y la evaluación de la consecuencia (impacto) y probabilidad es realizada por el Comité de Seguridad de la Información junto con el propietario del activo.

No	Nombre del activo	Propietario del activo	Amenaza	Vulnerabilidad	Propietario del riesgo	Consecuencia	Probabilidad	Riesgo	Controles existentes
1	Infraestructura de Servidores	Especialistas en Servidores	Acceso no controlados a la infraestructura física	Ubicación donde se encuentra la infraestructura no cumpla con normas de seguridad de ingreso de personal	Especialistas en Servidores	0	0	0	A11.1.3
2	Infraestructura de Servidores	Especialistas en Servidores	Accesos no controlados a portales de administración	No cuenten con las seguridades debidas al ingreso de portales de administración	Especialistas en Servidores	2	1	3	
3	Infraestructura de Servidores	Especialistas en Servidores	Fallas en la infraestructura física	No contar con equipamiento en alta disponibilidad	Especialistas en Servidores	1	1	2	A11.1.1 A11.1.2 A11.2.1 A11.2.4 A11.2.6

No	Nombre del activo	Propietario del activo	Amenaza	Vulnerabilidad	Propietario del riesgo	Consecuencia	Probabilidad	Riesgo	Controles existentes
4	Infraestructura de Servidores	Especialistas en Servidores	Ingreso de software mal intencionado	No cuente con políticas de parcheado de seguridad	Especialistas en Servidores	1	1	2	A12.2.1
5	Infraestructura de Servidores	Especialistas en Servidores	Amenazas de tipo secuestro o ransomware	Sistemas de respaldo deficiente o no protegidos adecuadamente	Especialistas en Servidores	1	1	2	A12.3.1
6	Infraestructura de Servidores	Especialistas en Servidores	Autenticación simple con un factor (password)	El atacante pueda ingresar a las cuentas de usuarios privilegiados en permisos y realizar ataques a infraestructura critica	Especialistas en Servidores	2	1	3	
7	Infraestructura de Servidores	Especialistas en Servidores	La falta de visibilidad de logs, alertas, equipam	Los equipos pueden estar alertados y estando bajo ataque, se desconoce el tipo de	Especialistas en Servidores	1	1	2	A12.4.1 A16.1.2 A16.1.4 A16.1.5

No	Nombre del activo	Propietario del activo	Amenaza	Vulnerabilidad	Propietario del riesgo	Consecuencia	Probabilidad	Riesgo	Controles existentes
			iento con problemas de hardware.	servicio al cual está atacando y podría provocar problemas graves					
8	Infraestructura de Servidores	Especialistas en Servidores	Incidentes provocados por humanos	Falta de política de uso del equipamiento da acceso a terceros para realizar un bypass a infraestructura critica afectando la integridad de la empresa	Especialistas en Servidores	2	2	**4**	

Tabla 3 Evaluación del riesgo en la Infraestructura de Servidores de la Nube en CEDIA

4.2.2. TRATAMIENTO DE RIESGOS EN SERVIDORES DE LA NUBE DE CEDIA

Para realizar el tratamiento de riesgos se debe tomar en cuenta la información de la tabla 3 donde se encuentran todos los riesgos identificados como no aceptables o residuales.

El tratamiento de riesgos es realizado por el área Técnica de CEDIA.

Activos / amenazas / vulnerabilidades						*Valores antes del tratamiento*		
No	**Nombre del activo**	**Propietario del activo**	**Amenaza**	**Vulnerabilidad**	**Propietario del riesgo**	**Consecuencia**	**Probabilidad**	**Riesgo**
1	Infraestructura de Servidores	Especialistas en Servidores	Acceso no controlados a la infraestructura física	Ubicación donde se encuentra la infraestructura no cumpla con normas de seguridad de ingreso de personal	Especialistas en Servidores	1	1	2
2	Infraestructura de Servidores	Especialistas en Servidores	Accesos no controlados a portales de administración	No cuenten con las seguridades debidas al ingreso de portales de administración	Especialistas en Servidores	2	1	**3**
3	Infraestructura de Servidores	Especialistas en Servidores	Fallas en la infraestructura física	No contar con equipamiento en alta disponibilidad	Especialistas en Servidores	1	1	2
4	Infraestructura de Servidores	Especialistas en Servidores	Ingreso de software mal intencionado	No cuente con políticas de parcheado de seguridad	Especialistas en Servidores	1	1	2

Activos / amenazas / vulnerabilidades						*Valores antes del tratamiento*		
No	**Nombre del activo**	**Propietario del activo**	**Amenaza**	**Vulnerabilidad**	**Propietario del riesgo**	**Consecuencia**	**Probabilidad**	**Riesgo**
5	Infraestructura de Servidores	Especialistas en Servidores	Amenazas de tipo secuestro o ransomware	Sistemas de respaldo deficiente o no protegidos adecuadamente	Especialistas en Servidores	1	1	2
6	Infraestructura de Servidores	Especialistas en Servidores	Autenticación simple con un factor (password)	El atacante pueda ingresar a las cuentas de usuarios privilegiados en permisos y realizar ataques a infraestructura critica	Especialistas en Servidores	2	1	3
7	Infraestructura de Servidores	Especialistas en Servidores	La falta de visibilidad de logs, alertas, equipamiento con problemas de	Los equipos pueden estar alertados y estando bajo ataque, se desconoce el tipo de servicio al cual está atacando y podría provocar	Especialistas en Servidores	1	1	2

Activos / amenazas / vulnerabilidades						*Valores antes del tratamiento*		
No	**Nombre del activo**	**Propietario del activo**	**Amenaza**	**Vulnerabilidad**	**Propietario del riesgo**	**Consecuencia**	**Probabilidad**	**Riesgo**
			hardware.	problemas graves				
8	Infraestructura de Servidores	Especialistas en Servidores	Incidentes provocados por humanos	Falta de política de uso del equipamiento da acceso a terceros para realizar un bypass a infraestructura critica afectando la integridad de la empresa	Especialistas en Servidores	2	2	**4**

Tabla 4 Evaluación del riesgo en la Infraestructura de Servidores de la Nube en CEDIA antes del tratamiento

Tratamiento del riesgo			*Valores después del tratamiento*		
No	**Elección de opciones**	**Medios de implementación**	**Consecuencia**	**Probabilidad**	**Riesgo**
1	2. Transferencia de riesgos a terceros	Contrato a proveedores	0	1	0
2	1. Elección de controles	A9.4.2 Procedimientos seguros de inicio de sesión	0	0	0
3	3. Evitar el riesgo	Se encuentran en estado gestionado los siguientes controles: A11.1.1 Perímetro de seguridad física	0	1	1

Tratamiento del riesgo			*Valores después del tratamiento*		
No	**Elección de opciones**	**Medios de implementación**	**Consecuencia**	**Probabilidad**	**Riesgo**
		A11.1.2 Controles físicos de entrada A11.2.1 Emplazamiento y protección de equipos A11.2.4 Mantenimiento de los equipos A11.2.6 Seguridad de los equipos fuera de las instalaciones			
4	3. Evitar el riesgo	A9.4.4 Uso de utilidades con privilegios del sistema A12.5.1 Instalación del software en explotación A12.6.2 Restricción en la instalación de software	0	1	1
5	2. Transferencia de riesgos a terceros	Contrato a proveedores	0	0	0
6	1. Elección de controles	A9.4.3 Sistema de gestión de contraseñas	1	0	1
7	1. Elección de controles	A12.4.1 Registro de eventos Se encuentran en estado gestionado los siguientes controles: A16.1.2 Notificación de los eventos de seguridad de la información A16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	0	0	0

Tratamiento del riesgo			*Valores después del tratamiento*		
No	**Elección de opciones**	**Medios de implementación**	**Consecuencia**	**Probabilidad**	**Riesgo**
		A16.1.5 Respuesta a incidentes de seguridad de la información			
8	1. Elección de controles	A9.4.1 Restricción del acceso a la información A9.4.2 Procedimientos seguros de inicio de sesión A9.4.3 Sistema de gestión de contraseñas A9.4.4 Uso de utilidades con privilegios del sistema	1	1	2

Tabla 5 Tratamiento de los riesgos en la Infraestructura de Servidores de la Nube en CEDIA

La elección de opciones se implementa a través de la tabla 5 de tratamiento de los riesgos en la Infraestructura de Servidores de la Nube en CEDIA. Generalmente, la norma ISO 27001 indica que se debe escoge la opción 1: Elección de uno o más controles de seguridad.

El tratamiento de riesgos relacionados con procesos externalizados será atendido por medio de contratos con los terceros responsables que en el caso de CEDIA se les llama “Proveedores”, como se especifica en la Política de seguridad para proveedores.

En el caso de la opción 1 que corresponde a la elección de controles de seguridad, será necesario evaluar el nuevo valor de consecuencia y probabilidad en el cuadro de tratamiento de riesgos, para evaluar la efectividad de los controles planificados.

Los propietarios de riesgos revisarán los riesgos vigentes y deben actualizar el Cuadro 3 de evaluación de riesgos y el Cuadro 5 de tratamiento de riesgos de acuerdo con los nuevos riesgos identificados. La revisión se debe realizar al menos una vez por año, o con mayor frecuencia en caso de cambios organizacionales significativos, cambios importantes en tecnología, en los objetivos de negocios, en el entorno empresarial, etc. (27001Academy, 2015)

ELABORAR LA DECLARACIÓN DE APLICABILIDAD SEGÚN EL ANÁLISIS DE BRECHAS PARA CEDIA EN BASE AL ANEXO A (NORMATIVO) OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA DE LA NORMA ISO/IEC 27002:2013

4.3. DAR A CONOCER LA RESEÑA HISTÓRICA DE LA ORGANIZACIÓN (CEDIA)

El día 25 de marzo de 2002 se reunieron los delegados de ocho instituciones de educación superior nacionales y los representantes de las redes avanzadas de México (CUDI), Brasil (RNP) y Estados Unidos (Internet2) para la creación de un Consorcio Nacional para el Desarrollo de Internet Avanzado (CEDIA).

La creación oficial de CEDIA fue el 17 de Septiembre del 2002 ante la presencia del Vicepresidente de la República del Ecuador y el Secretario Nacional de Ciencia y Tecnología firmando los representantes de la Escuela Superior Politécnica de Chimborazo, Escuela Politécnica Nacional, Escuela Superior Politécnica del Litoral, Universidad de las Fuerzas Armadas, Universidad Católica Santiago de Guayaquil, Universidad Nacional de Loja, Universidad Técnica Particular de Loja, Instituto Nacional de pesca y el Instituto Oceanográfico de la Armada del Ecuador más las firmas de los representantes legales de la SENACYT (Secretaría Nacional de Ciencia y Tecnología), el CONATEL (Consejo Nacional de Telecomunicaciones) y la Vicepresidencia Constitucional de la República del Ecuador.

El estatuto de CEDIA fue aprobado por el Subsecretario de Educación del Ecuador y registrado oficialmente el 6 de enero de 2003. (CORPORACION ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA - CEDIA, 2021)

El 09 de junio de 2003 CEDIA se constituye en la Cooperación Latinoamericana de Redes Avanzadas (Red CLARA) como proveedor único en el Ecuador.

En junio de 2015, CEDIA implementa con nuevos servicios de innovación y la incorporación a la red de instituciones, públicas y privadas, como: universidades, escuelas politécnicas, institutos de investigación, institutos tecnológicos y colegios.

CEDIA implementa su propia red IP/MPLS misma que está conectada con Estados Unidos y por la que cursa el tráfico de Red Avanzada e Internet Comercial.

El 31 de Julio de 2017 CEDIA se constituye como Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia para fomentar, promover y coordinar el desarrollo de la investigación científica y la academia; y ofrecer servicios relacionados a las tecnologías de la información enfocadas al desarrollo científico, tecnológico, innovador y educativo en el Ecuador, por medio del Proyecto de Redes Avanzadas. (CORPORACION ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA - CEDIA, 2021)

4.4. ESPECIFICACIÓN DE LA ESTRUCTURA ORGANIZACIONAL

El 06 de febrero de 2020 el Ministerio de Educación resuelve aprobar la reforma integral al Estatuto de la CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y ACADEMIA - CEDIA que consta de 48 artículos, en uno de los cuales indica la Misión de la Organización:

Artículo 4.- CEDIA es una organización privada sin fines de lucro que tiene por misión fomentar, promover y coordinar el desarrollo de la investigación científica, la academia, la innovación, transferencia tecnológica, emprendimiento, internacionalización y ofrecer servicios relacionados a estas áreas y otras afines, a sus miembros y a quienes la Asamblea lo autorice. Lo anterior podrá realizar de manera comercial o gratuita con actores del sector público, privado, nacional o internacional. (CEDIA, 2020)

CEDIA está constituida legalmente por miembros plenos y adherentes siendo un ente distinto a sus asociados. Sus miembros, donantes y participantes no adquieren personal, directa, indirecta, subsidiaria ni en forma solidaria, las obligaciones de la organización.

Los miembros plenos son las personas jurídicas como: Universidades, Escuelas Politécnicas, centros o institutos de investigación y de desarrollo científico que hayan suscrito el acta de constitución de CEDIA, o los que en el futuro soliciten serlo y que cumplan con ciertos requisitos que constan en el Estatuto de la organización.

Los miembros adherentes son las personas jurídicas como: Institutos tecnológicos, unidades educativas, centros de educación continua y otras instituciones aun cuando no cuenten con una plataforma de servicios a través de una infraestructura de servidores pero que estén comprometidas con el desarrollo, evolución y utilización de aplicaciones educativas y de tecnología avanzada, redes de telecomunicaciones e informática, investigación, innovación,

transferencia tecnológica, emprendimiento, internacionalización y afines, que de igual forma cumplan con ciertos requisitos. (CEDIA, 2020)

Tanto los miembros plenos como los adherentes tienen derechos y obligaciones que deben cumplir, mismos que constan en el Estatuto de CEDIA.

El funcionamiento de CEDIA como lo indican desde el artículo 17 al 36 del Estatuto, cuenta con la siguiente forma de gobierno:

- La Asamblea General
- El Presidente
- El Consejo Ejecutivo
- El Director Ejecutivo
- Comisiones

4.4.1. ASAMBLEA GENERAL

La Asamblea General es el máximo órgano de decisión política y estratégica de CEDIA, se constituye como un espacio parlamentario y legislativo, que es responsable de la definición, seguimiento y control de las estrategias generales para la consecución de los fines organizacionales y que son aplicadas por los niveles táctico-ejecutivo y operativo de la organización. Las decisiones son obligatorias, siempre que no contradiga el Estatuto vigente o las leyes conexas.

La Asamblea General está conformada por:

1. El representante legal (rector) o un delegado Ad-Hoc por cada miembro pleno con derecho a voz y voto.
2. El representante legal o un delegado Ad-Hoc por cada miembro adherente con derecho a voz.
3. El Presidente quien convoca y preside las reuniones de la Asamblea y
4. El Director Ejecutivo quién actúa como Secretario de la Asamblea.
5. La Asamblea General pudiendo ser ordinaria o extraordinaria.

4.4.2. PRESIDENTE

El Presidente de la Asamblea a su vez es el Presidente de CEDIA tiene un período de vigencia de 3 años pudiendo ser reelegido una sola vez y tiene las siguientes funciones:

1. *Preside las reuniones de la Asamblea General.*
2. *Preside las reuniones del Consejo Ejecutivo.*
3. *Convoca a las reuniones ordinarias y extraordinarias de la Asamblea General.*
4. *Convoca a las reuniones ordinarias y extraordinarias del Consejo Ejecutivo y*
5. *Otras delegadas o definidas por la Asamblea General, siempre que lo permita el Estatuto vigente.* (CEDIA, 2020)

4.4.3. CONSEJO EJECUTIVO

El Consejo Ejecutivo es un organismo que está conformado por 5 miembros que son elegidos por la Asamblea General, teniendo una vigencia de 3 años y está compuesto de *la siguiente manera:*

1. *El Presidente de CEDIA quien lo presidirá;*
2. *Tres representantes de los miembros plenos de CEDIA*
3. *El representante legal de un miembro adherente de CEDIA*. (CEDIA, 2020)

El Consejo Ejecutivo cuenta con un Secretario quien es el Director Ejecutivo de la organización actuando con voz y sin voto.

4.4.4. DIRECTOR EJECUTIVO

El Director Ejecutivo de CEDIA es la persona designada por la Asamblea General y responsable de la ejecución de acuerdos y estrategias que define la Asamblea General. Siendo esta persona quién ejerce la representación legal, judicial y extrajudicial de CEDIA y tiene a su cargo la administración del personal, su organización, selección, contratación y remoción.

4.4.5. COMISIONES

CEDIA cuenta con 4 comisiones asesoras permanentes:

1. Técnica
2. Académica e Investigación

3. Innovación y Vinculación
4. Internalización

Están integradas por 3 miembros plenos, quienes designan a un delegado especialista en la materia de la comisión a conformarse. (CEDIA, 2020)

4.4.6. ORGANIGRAMA A NIVEL ADMINISTRATIVO DE CEDIA

En el área administrativa de CEDIA el organigrama se encuentra compuesto por: la Dirección Ejecutiva y nueve departamentos estructurados de la siguiente manera:

Figura 12 Estructura organizacional de CEDIA

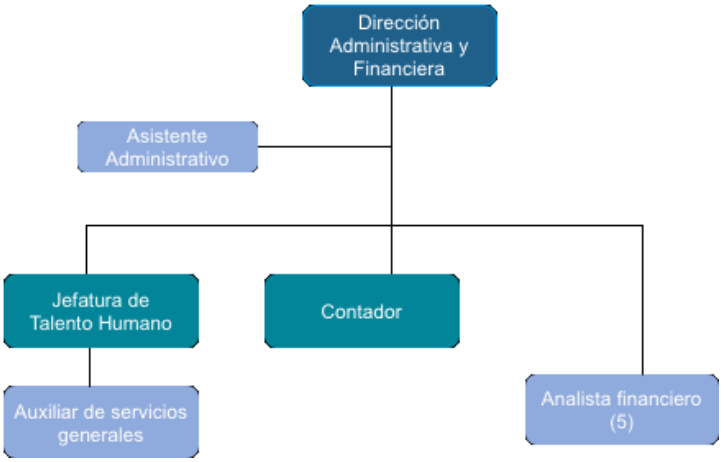


Figura 13 Dirección Administrativa y Financiera

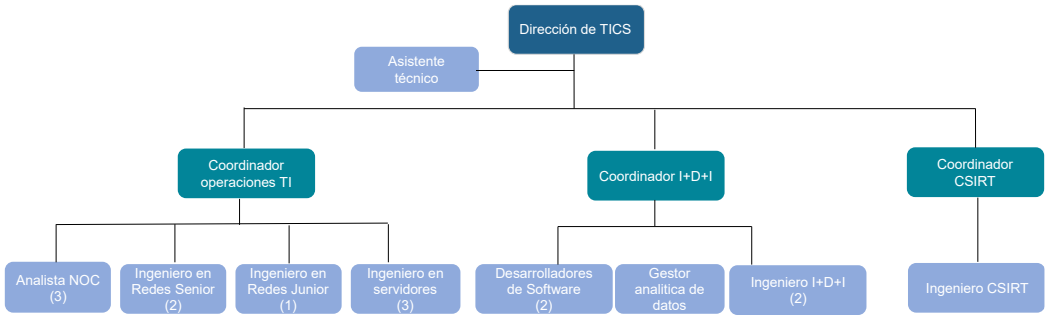


Figura 14 Dirección de TICs

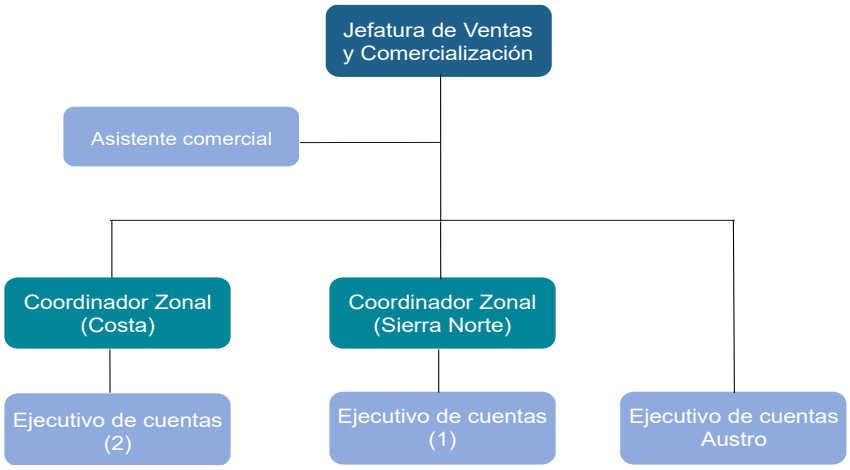


Figura 15 Jefatura de Ventas y Comercialización

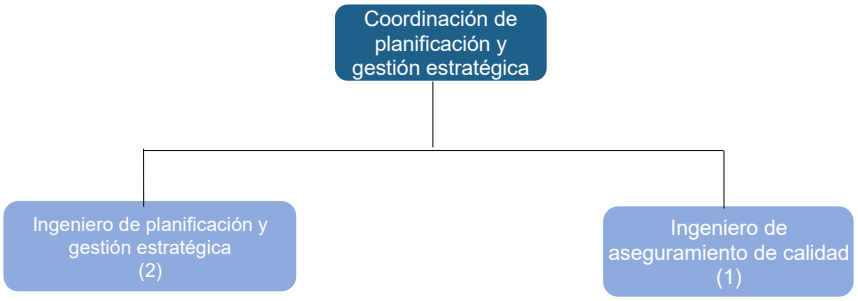


Figura 16 Coordinación de planificación y gestión estratégica

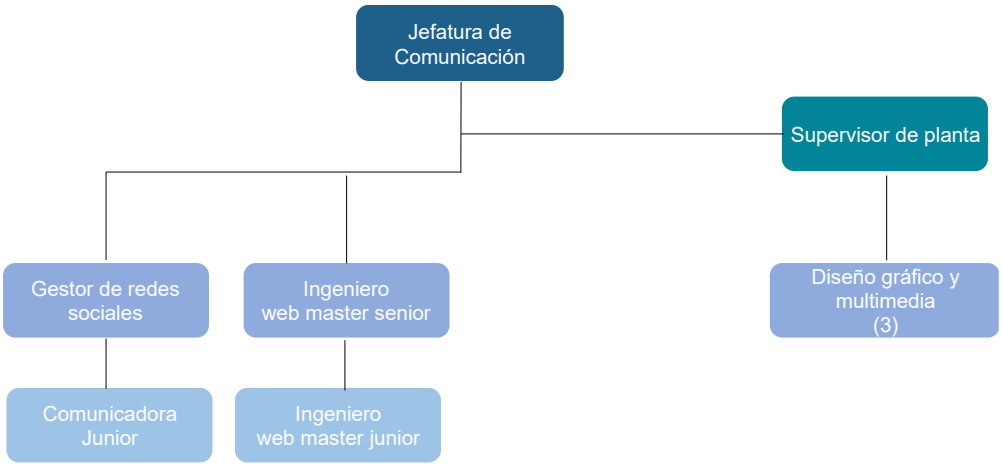


Figura 17 Jefatura de Comunicación

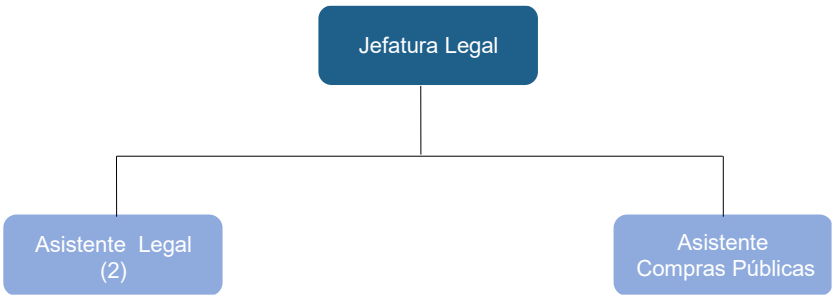


Figura 18 Jefatura Legal

Figura 19 Coordinación Académica y de Formación Continua

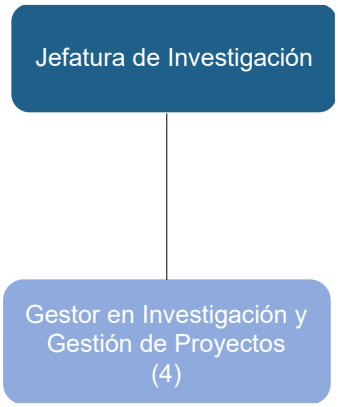


Figura 20 Jefatura de Investigación

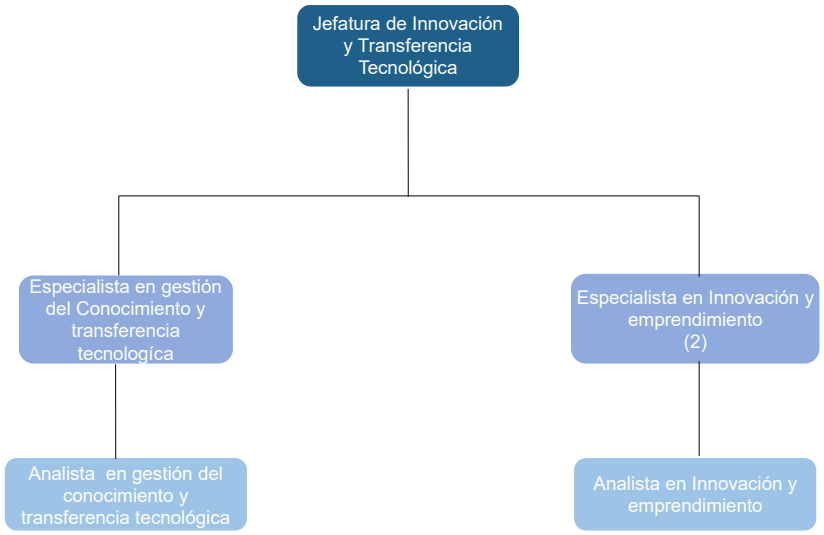


Figura 21 Jefatura de Innovación y Transferencia Tecnológica

4.5. ELABORACIÓN DEL ANÁLISIS DE LA SITUACIÓN ACTUAL DE CEDIA

CEDIA cuenta con varias políticas implementadas de acuerdo a su reglamento interno y estatuto aprobado por el Ministerio de Educación, además, se analiza junto con el departamento del Área Técnica de la Corporación los controles y objetivos de control del Anexo A de la ISO/IEC 27002 cumple CEDIA.

CEDIA al ser una organización sin fines de lucro que fomenta, promueve y coordina el desarrollo de la investigación, academia, innovación transferencia tecnológica y demás servicios se encuentra trabajando en las políticas de control del Anexo y actualmente está entre

un estado definido y administrado, esto se puede evidenciar en el análisis GAP que se estudia en el siguiente numeral del presente capítulo.

4.6. ANÁLISIS DE BRECHA (GAP)

Un análisis de brechas GAP es un método para evaluar las diferencias de rendimiento entre los sistemas de información de una empresa o las aplicaciones de software para determinar si se cumplen los requisitos del negocio y, de no ser así, qué pasos se deben tomar para garantizar que se cumplan con éxito. Gap se refiere al espacio entre "donde estamos" (el presente) y "donde queremos estar" (el objetivo a alcanzar). Un análisis de deficiencias también puede denominarse análisis de necesidades, permitiéndonos determinar lo que nos falta y los recursos necesarios para alcanzar los objetivos. (NORMAISO27001.es, 2021)

A continuación, se presenta el análisis de brecha para CEDIA de acuerdo al Anexo A de la ISO/IEC 27002:

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información	Inicial	Existe un manual de políticas de seguridad de la información sobre temas puntuales incluidas las políticas de Equipo de Respuesta a Incidentes de Seguridad (CSIRT), sin embargo, aún se encuentra en desarrollo otras políticas.
A5.1.2	Revisión de las políticas	Inicial	Cada política tiene un propietario designado que debe iniciar la revisión del documento según un intervalo planificado.
A6	**Organización de la seguridad de la información**		

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información	Limitado	Las responsabilidades sobre seguridad de la información se detallan en varios documentos del SGSI Si es necesario, el Oficial de Seguridad de la Información define responsabilidades adicionales
A6.1.2	Segregación de tareas	Definido	Cualquier actividad que incluya información sensible es aprobada por una persona e implementada por otra
A6.1.3	Contacto con las autoridades	Gestionado	Plan de Comunicaciones, Plan de respuesta ante incidentes
A6.1.4	Contacto con grupos de interés especial	Gestionado	El Oficial de Seguridad de la Información con el CSIRT son los responsable de supervisar el contacto con EcuCERT, FIRST,
A6.1.5	Seguridad de la información en la gestión de proyectos	Limitado	El área de investigación incluye las reglas correspondientes sobre seguridad de la información en cada proyecto
A6.2	**Dispositivos móviles y teletrabajo**		
A6.2.1	Política de dispositivos móviles	Inicial	No existe una política formal sobre el uso de dispositivos móviles, aún se está desarrollando
A6.2.2	Teletrabajo	Inicial	Para acceder a la información de la red de CEDIA, se debe conectar a

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
			una VPN, aún se está desarrollando la política
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes	Definido	La Jefatura de Talento Humano verifica a cada candidato a través de los procesos de selección, entrevistas y validación de referencias, Política de seguridad para proveedores
A7.1.2	Términos y condiciones del empleo	Definido	Todos los empleados firman la Declaración de aceptación de los documentos del SGSI y la Declaración de confidencialidad; Política de seguridad para proveedores
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	Limitado	Establecimiento de políticas y procedimientos en la organización
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Definido	Política de seguridad de la información, Plan de capacitación y concienciación, Política de seguridad para proveedores
A7.2.3	Proceso disciplinario	Inicial	Procedimiento para gestión de incidentes, Declaración de aceptación de los documentos del SGSI

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	Inicial	Todos los acuerdos con proveedores y socios contienen cláusulas que siguen vigentes después de finalizado el empleo o contrato, como también las [Declaraciones de confidencialidad] firmadas con los empleados.
A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		
A8.1.1	Inventario de activos	Limitado	Inventario de activos. El área financiera se encarga del balance de los activos físicos.
A8.1.2	Propiedad de los activos	Definido	El área financiera se encarga del balance de los activos físicos y asignar un propietario
A8.1.3	Uso aceptable de los activos	Inicial	Se tiene conocimiento del uso aceptable de los activos, sin embargo, se está desarrollando la política
A8.1.4	Devolución de activos	Gestionado	Política de seguridad para proveedores, Política de administración de activos
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	Limitado	Se tiene claramente identificados los niveles para la clasificación de

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
			la información, es estándar y consistente a lo largo de CEDIA
A8.2.2	Etiquetado de la información	Limitado	Existe un procedimiento para el etiquetado de los activos, se está desarrollando una política. El etiquetado de la información maneja cada departamento que se diferencia por las siglas y tipo de información, por ejemplo del área legal un contrato se etiquetaría de la siguiente manera: JLE-CT-2022-0001
A8.2.3	Manipulado de la información	Limitado	Existe la descripción del tratamiento de la información según su clasificación, así como los responsables por su manejo
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	Inicial	Se conoce el esquema de clasificación adoptado por CEDIA, sin embargo, se está desarrollando la política
A8.3.2	Eliminación de soportes	Inicial	Procedimientos operativos para tecnología de la información y de la comunicación
A8.3.3	Soportes físicos en tránsito	Definido	Cada equipo cuenta con usuario y contraseña, se cuenta con protección física adecuada
A9	**Control de acceso**		

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	Gestionado	Política de control de acceso
A9.1.2	Acceso a las redes y a los servicios de red	Gestionado	Política de control de acceso
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario	Definido	Se realiza un proceso de registro de usuario para cada empleado con perfiles y permisos asignados según justifique el caso. Política de control de acceso / Política de claves
A9.2.2	Provisión de acceso de usuario	Definido	Política de control de acceso / Política de claves
A9.2.3	Gestión de privilegios de acceso	Definido	Política de control de acceso
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Limitado	Política de control de acceso / Política de claves
A9.2.5	Revisión de los derechos de acceso de usuario	Limitado	Política de control de acceso
A9.2.6	Retirada o reasignación de los derechos de acceso	Definido	Se retira o reasigna derechos de acceso con autorización de cada jefe de área so
A9.3	**Responsabilidades del usuario**		

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A9.3.1	Uso de la información secreta de autenticación	Limitado	Política de uso aceptable, Política de claves
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	Gestionado	Política de control de acceso
A9.4.2	Procedimientos seguros de inicio de sesión	Definido	Existe un proceso de registro seguro para todos los ordenadores de la red
A9.4.3	Sistema de gestión de contraseñas	Limitado	Política de directorio activo
A9.4.4	Uso de utilidades con privilegios del sistema	Definido	Se deben establecer procedimientos para la autorización de aplicaciones / utilidades especiales
A9.4.5	Control de acceso al código fuente de los programas	Definido	El código fuente del programa se archiva y se almacena de acuerdo a la Políticas de Clasificación de la Información
A10	**Criptografía**		
A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos	Inicial	CEDIA emplea controles criptográficos bajo requerimiento
A10.1.2	Gestión de claves	Definido	CEDIA emplea controles criptográficos bajo requerimiento
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A11.1.1	Perímetro de seguridad física	Gestionado	Las áreas con información sensible están protegidas a través de permisos de acceso restringidos de acuerdo a las funciones de los colaboradores
A11.1.2	Controles físicos de entrada	Gestionado	El acceso a las áreas seguras de CEDIA están controladas a través del uso de tarjetas de acceso, códigos de acceso y entrada principal con guardia.
A11.1.3	Seguridad de oficinas, despachos y recursos	Gestionado	No se puede acceder a las instalaciones desde áreas públicas y las áreas seguras no son visibles para personas ajenas a CEDIA
A11.1.4	Protección contra las amenazas externas y ambientales	Gestionado	Hay un sistema de alarma instalado y conectado al centro de monitoreo de la empresa Alta Tecnología en Seguridad (ATS); hay cámaras de vigilancia instaladas; está implementada la protección contra incendios en los DC. La estructura de los edificios es sismo resistente
A11.1.5	El trabajo en áreas seguras	Gestionado	Procedimientos para trabajo en áreas seguras
A11.1.6	Áreas de carga y descarga	Gestionado	Las áreas de acceso público son controladas a través de puertas de acceso con cámaras y las áreas de carga y descarga en los DataCenter están controladas con guardias de

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
			seguridad en la entrada, además de trámites para permisos de acceso
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	Gestionado	Todo el equipamiento está ubicado en un área físicamente protegida, y el equipamiento altamente sensible como equipos de red e infraestructura en operación se encuentran ubicados en DataCenter con políticas de control de acceso y repuestos de equipos de red están ubicados en bodegas de Telconet y bodega DTI de CEDIA
A11.2.2	Instalaciones de suministro	Gestionado	Los aparatos de alimentación continua UPS, generadores de electricidad están instalados para la operación de los equipos del DataCenter del edificio de CEDIA y para equipamiento de las oficinas. Los DataCenter de ETAPA y TELCONET cuentan con baterías, suministro alterno de energía, y generadores.
A11.2.3	Seguridad del cableado	Gestionado	Los cables de energía y de datos están instalados dentro de áreas seguras de la organización y, donde no fue posible, están

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
			protegidos a través del uso de canaletas dedicadas
A11.2.4	Mantenimiento de los equipos	Gestionado	El Oficial de Seguridad de la Información debe llevar un registro de mantenimiento de todos los equipos, según las instrucciones del fabricante; y debe garantizar el mantenimiento en tiempo y forma. Los propietarios de los equipos serán los encargados de gestionar los mantenimientos
A11.2.5	Retirada de materiales propiedad de la empresa	Gestionado	Política de Uso aceptable
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Gestionado	Política de uso aceptable. Para acceder a la información de la red de CEDIA, se debe conectar a una VPN. Política de teletrabajo
A11.2.7	Reutilización o eliminación segura de equipos	Gestionado	Procedimientos operativos de TI / Política de eliminación y destrucción
A11.2.8	Equipo de usuario desatendido	Gestionado	Política de uso aceptable
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Inicial	No se cuenta con una política formal de pantalla y escritorio limpio
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A12.1.1	Documentación de procedimientos operacionales	Definido	Procedimientos operativos de TI
A12.1.2	Gestión de cambios	Definido	Política de gestión de cambio
A12.1.3	Gestión de capacidades	Definido	El Director de TI y Coordinador de Operaciones son los responsables de supervisar el uso de los activos de TIC y de planificar la capacidad necesaria
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Gestionado	Los sistemas de desarrollo, de pruebas y operacionales están separados
A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso	Gestionado	La herramienta utilizada es Nessus (programa de escaneo de vulnerabilidades), Política de uso aceptable. Análisis de vulnerabilidades de CSIRT Capacitación de CSIRT
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	Gestionado	Procedimientos operativos de TI / Política de creación de copias de seguridad, Política de uso aceptable
A12.3	**Registros y supervisión**		

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A12.4.1	Registro de eventos	Gestionado	Procedimientos operativos de TI Registro de tickets Registros de ingreso / tarjeta magnética / códigos de acceso
A12.4.2	Protección de la información del registro	Gestionado	Los registros no pueden ser eliminados sin el permiso otorgado por la persona autorizada
A12.4.3	Registros de administración y operación	Gestionado	Procedimientos operativos de TI
A12.4.4	Sincronización del reloj	Gestionado	Los relojes de los sistemas en todos los ordenadores están sincronizados con un Servidor de protocolo de internet (NTP)
A12.5	**Control del software en explotación**		
A12.5.1	Instalación del software en explotación	Definido	Política de Uso aceptable / Políticas en proceso de implementación de adopción y uso de software
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Gestionado	El CSIRT es el responsable de supervisar todas las vulnerabilidades de las aplicaciones y de los demás sistemas, y el Coordinador de Operaciones debe escoger las medidas que se tomarán en caso que se identifiquen nuevas vulnerabilidades

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A12.6.2	Restricción en la instalación de software	Definido	Política de Uso aceptable / Políticas en proceso de implementación de adopción y uso de software
A12.7	**Consideraciones sobre la auditoría de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	Limitado	Cada auditoría se planifica y coordina con la dirección; las auditorías se realizan solamente con derechos de acceso de sólo lectura
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	Gestionado	Procedimientos operativos de TI
A13.1.2	Seguridad de los servicios de red	Gestionado	Procedimientos operativos de TI
A13.1.3	Segregación en redes	Gestionado	La red se separa de la siguiente manera: [indicar qué segmentos de la red están separados, indicar si la separación es física o lógica]
A13.2	**Intercambio de información**		
A13.2.1	Políticas y procedimientos de intercambio de información	Limitado	Política de transferencia de información y comunicaciones , Política Trae tu propio dispositivo (BYOD)
A13.2.2	Acuerdos de intercambio de información	Limitado	Política de transferencia de información y comunicaciones

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A13.2.3	Mensajería electrónica	Gestionado	Política de clasificación de la información, Política de uso aceptable
A13.2.4	Acuerdos de confidencialidad o no revelación	Definido	Política de clasificación de la información , Formato de Acuerdos de Confidencialidad
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Definido	Al adquirir nuevos sistemas de información o al cambiar los vigentes, el Oficial de Seguridad de la Información debe documentar los requisitos de seguridad en el documento de Especificaciones de requerimientos de seguridad
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Gestionado	Política de desarrollo seguro
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Gestionado	Política de desarrollo seguro
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro	Definido	Se cuenta con ambientes de Producción y Desarrollo separados. Los datos en el

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
			ambiente de desarrollo y pruebas son datos reales de Producción
A14.2.2	Procedimiento de control de cambios en sistemas	Gestionado	Política de desarrollo seguro
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Definido	Política de desarrollo seguro
A14.2.4	Restricciones a los cambios en los paquetes de software	Definido	Política de desarrollo seguro
A14.2.5	Principios de ingeniería de sistemas seguros	Limitado	Política de desarrollo seguro
A14.2.6	Entorno de desarrollo seguro	Definido	Política de desarrollo seguro
A14.2.7	Externalización del desarrollo de software	Gestionado	Política de seguridad para proveedores, Política de desarrollo seguro
A14.2.8	Pruebas funcionales de seguridad de sistemas	Gestionado	Política de desarrollo seguro
A14.2.9	Pruebas de aceptación de sistemas	Gestionado	Política de desarrollo seguro
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	Definido	Política de desarrollo seguro

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Definido	Política de seguridad para proveedores
A15.1.2	Requisitos de seguridad en contratos con terceros	Definido	Existe un contrato suscrito por CEDIA y el proveedor. Política de seguridad para proveedores
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Definido	Política de seguridad para proveedores
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Definido	Política de seguridad para proveedores, niveles de servicio (SLA)
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Definido	Política de seguridad para proveedores, niveles de servicio (SLA)
A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A16.1.1	Responsabilidades y procedimientos	Gestionado	Procedimiento para gestión de incidentes
A16.1.2	Notificación de los eventos de seguridad de la información	Gestionado	Procedimiento para gestión de incidentes

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A16.1.3	Notificación de puntos débiles de la seguridad	Definido	Procedimiento para gestión de incidentes
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Gestionado	Procedimiento para gestión de incidentes
A16.1.5	Respuesta a incidentes de seguridad de la información	Gestionado	Procedimiento para gestión de incidentes, Plan de respuesta ante incidentes
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Definido	Procedimiento para gestión de incidentes, Procedimiento para medidas correctivas
A16.1.7	Recopilación de evidencias	Limitado	Procedimiento para gestión de incidentes
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Definido	Procedimiento para identificación de requisitos, Metodología para el análisis del impacto en el negocio, Estrategia de continuidad del negocio
A17.1.2	Implementar la continuidad de la seguridad de la información	Definido	Plan de continuidad del negocio

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Definido	Plan de mantenimiento y revisión del Sistema de Gestión de Continuidad de Negocio, Plan de prueba y verificación, Formulario de revisión postincidente
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Gestionado	Estrategia de recuperación para infraestructura de TI
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales**		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Inicial	Lista de requisitos legales, normativos, contractuales y de otra índole
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Limitado	Se cuenta con una persona experta en Propiedad Intelectual encargada de los derechos de PI
A18.1.3	Protección de los registros de la organización	Inicial	Procedimiento para control de documentos y registros
A18.1.4	Protección y privacidad de la información de carácter personal	Inicial	El Departamento Jurídico es el responsable de implementar los requerimientos legales relacionados con la protección de datos personales

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A18.1.5	Regulación de los controles criptográficos	Definido	Lista de requisitos legales, normativos, contractuales y de otra índole / Política del uso de controles criptográficos
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	Inicial	Procedimiento para auditorías
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Limitado	Todos los propietarios de activos de información, como también la dirección, revisan periódicamente la implementación de los controles de seguridad
A18.2.3	Comprobación del cumplimiento técnico	Limitado	Existe un responsable de verificar que los sistemas de información cumplan técnicamente con los requerimientos de seguridad

Tabla 6 Estado Actual CEDIA

La siguiente tabla describe el significado de cada estado con su porcentaje de cumplimiento actual de los controles en CEDIA:

Estado	Significado	Porcentaje de controles de seguridad de la información
Desconocido	Ni siquiera ha sido revisado todavía	**0%**

Estado	Significado	Porcentaje de controles de seguridad de la información
No existente	Falta total de políticas reconocibles, procedimientos, controles, etc.	**0%**
Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para cumplir con los requisitos.	**13%**
Limitado	Progresando bien pero aún no completo	**17%**
Definido	El desarrollo está más o menos completado, a pesar de que faltan ciertos detalles y/o no todavía no están implementados, reforzados y activamente soportados por la alta dirección	**32%**
Gestionado	El desarrollo está completado, el proceso/control ha sido implementado y comenzó a operar recientemente	**38%**
Optimizado	El requerimiento se cumple completamente, está operando completamente como se esperaba, se está monitoreando y mejorando activamente, y hay evidencia sustancial para demostrar todo eso a los auditores.	**0%**
No aplica	SGSI va a ser certificado TODOS los requisitos en el cuerpo principal de ISO/IEC 27001 son obligatorios. De lo contrario, la gerencia puede ignorarlos.	**0%**
	Total	100%

Tabla 7 Estado con su respectivo significado y porcentaje de cumplimiento actual de CEDIA

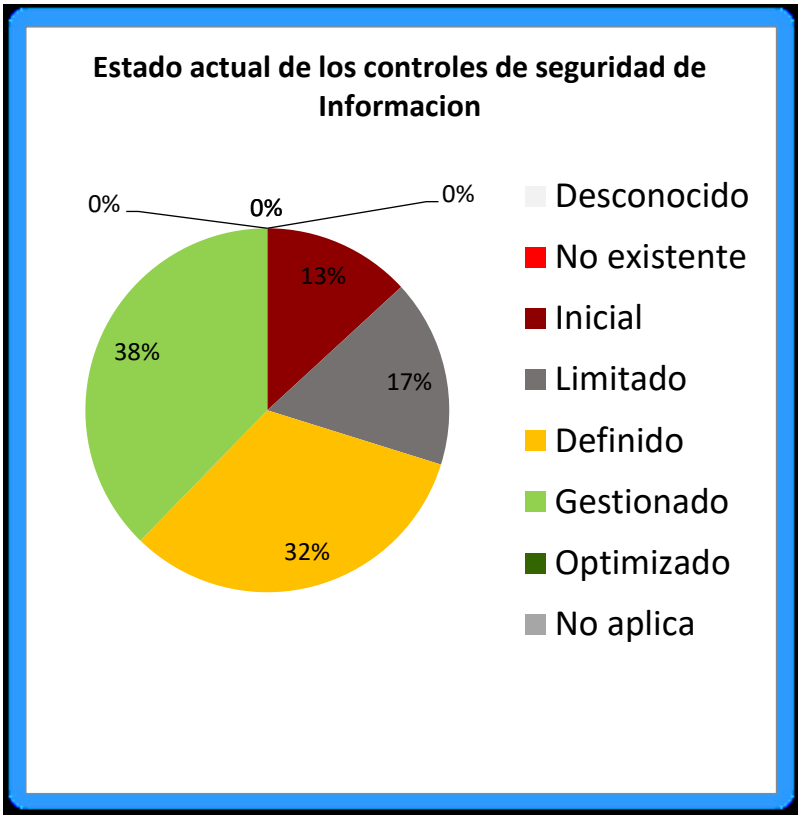


Figura 22 Estado actual de los controles de seguridad de Información de CEDIA

A continuación, se presenta el estado objetivo o deseado de CEDIA de acuerdo al ANEXO A de la ISO/IEC 27002:

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información	Gestionado	Documentar e implementar las políticas para la seguridad de la información incluyendo todos los objetivos de control y controles
A5.1.2	Revisión de las políticas	Gestionado	Mejora continua de la política de SGSI.
A6	**Organización de la seguridad de la información**		

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información	Optimizado	Política de responsabilidades en seguridad de la información que sean definidas y asignadas
A6.1.2	Segregación de tareas	Optimizado	Política de funciones y áreas de responsabilidad
A6.1.3	Contacto con las autoridades	Optimizado	Plan de Comunicaciones, Plan de respuesta ante incidentes
A6.1.4	Contacto con grupos de interés especial	Optimizado	El Oficial de Seguridad de la Información con el CSIRT son los responsables de supervisar el contacto con EcuCERT, FIRST,
A6.1.5	Seguridad de la información en la gestión de proyectos	Gestionado	Política de gestión de proyectos
A6.2	**Dispositivos móviles y teletrabajo**		
A6.2.1	Política de dispositivos móviles	Gestionado	Política de dispositivos móviles y medidas de seguridad
A6.2.2	Teletrabajo	Definido	Políticas de teletrabajo
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes	Gestionado	Mantener el control implementado y describir el procedimiento dentro del SGSI
A7.1.2	Términos y condiciones del empleo	Optimizado	Mantener el control implementado y describir el procedimiento dentro del SGSI

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	Gestionado	Plan de concienciación, educación y capacitación de la seguridad de la información a nivel del Director Ejecutivo
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Gestionado	Realizar el plan de concienciación, la capacitación adecuada a los colaboradores y la campaña completa de divulgación del SGSI
A7.2.3	Proceso disciplinario	Optimizado	Incluir el detalle formal de procesos disciplinarios y descargos dentro del manual de funciones y en el SGSI y comunicar a los colaboradores
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	Optimizado	Política de las responsabilidades en seguridad de la información y obligaciones vigentes de los colaboradores y/o proveedores que finalizaron el contrato, misma que debe ser comunicada a los involucrados
A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		
A8.1.1	Inventario de activos	Optimizado	Política de inventario de activos
A8.1.2	Propiedad de los activos	Optimizado	Política de propiedad de activos
A8.1.3	Uso aceptable de los activos	Gestionado	Política de uso aceptable

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A8.1.4	Devolución de activos	Gestionado	Política de seguridad para proveedores, Política de administración de activos
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	Gestionado	Política de clasificación de la información
A8.2.2	Etiquetado de la información	Gestionado	Política de etiquetado de la información
A8.2.3	Manipulado de la información	Gestionado	Políticas de manipulación de la información
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	Gestionado	Política de Clasificación de la Información
A8.3.2	Eliminación de soportes	Gestionado	Política eliminación y destrucción
A8.3.3	Soportes físicos en tránsito	Optimizado	Política de Clasificación de la Información
A9	**Control de acceso**		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	Optimizado	Política de control de acceso / Política de claves
A9.1.2	Acceso a las redes y a los servicios de red	Optimizado	Política de control de acceso / Política de claves
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario	Optimizado	Política de control de acceso / Política de claves
A9.2.2	Provisión de acceso de usuario	Optimizado	Política de control de acceso / Política de claves

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A9.2.3	Gestión de privilegios de acceso	Optimizado	Política de control de acceso
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Optimizado	Política de control de acceso / Política de claves
A9.2.5	Revisión de los derechos de acceso de usuario	Gestionado	Política de control de acceso
A9.2.6	Retirada o reasignación de los derechos de acceso	Optimizado	Política de control de acceso
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación	Gestionado	Política de uso aceptable, Política de claves
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	Optimizado	Política de control de acceso
A9.4.2	Procedimientos seguros de inicio de sesión	Optimizado	Política de control de acceso
A9.4.3	Sistema de gestión de contraseñas	Optimizado	Política de directorio activo y de control de acceso
A9.4.4	Uso de utilidades con privilegios del sistema	Gestionado	Mantener el esquema implementado, extender las restricciones en el dominio para todos los usuarios finales

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A9.4.5	Control de acceso al código fuente de los programas	Optimizado	Política de clasificación de la información
A10	**Criptografía**		
A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos	Gestionado	Los controles criptográficos deben ser obligatorios para el manejo y transporte de información por encima de "reservada" dentro de la clasificación de información. Este control debe ser formalmente descrito en una política dentro del SGSI
A10.1.2	Gestión de claves	Optimizado	Política de uso de los controles criptográficos
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		
A11.1.1	Perímetro de seguridad física	Optimizado	No descuidar la revisión periódica del funcionamiento de este control
A11.1.2	Controles físicos de entrada	Optimizado	No descuidar la revisión periódica del funcionamiento de este control
A11.1.3	Seguridad de oficinas, despachos y recursos	Gestionado	CEDIA cumple satisfactoriamente con este control
A11.1.4	Protección contra las amenazas externas y ambientales	Gestionado	CEDIA cumple satisfactoriamente con este control
A11.1.5	El trabajo en áreas seguras	Gestionado	No descuidar los controles de acompañamiento y registro de todos

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
			los usuarios que ingresan a las áreas restringidas
A11.1.6	Áreas de carga y descarga	Gestionado	Incluir la política de acceso por áreas de carga y descarga en el SGSI
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	Gestionado	CEDIA cumple satisfactoriamente con este control
A11.2.2	Instalaciones de suministro	Gestionado	Revisión periódica de UPS y plantas eléctricas para que se encuentren siempre en óptimas condiciones
A11.2.3	Seguridad del cableado	Gestionado	Dar de baja todo cableado obsoleto o en desuso y realizar una revisión periódica
A11.2.4	Mantenimiento de los equipos	Gestionado	Continuar con los mantenimientos constantes de los equipos tecnológicos
A11.2.5	Retirada de materiales propiedad de la empresa	Gestionado	Política de uso aceptable
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Gestionado	Política de uso aceptable
A11.2.7	Reutilización o eliminación segura de equipos	Gestionado	Procedimientos operativos de TI / Política de eliminación y destrucción
A11.2.8	Equipo de usuario desatendido	Gestionado	Política de uso aceptable
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Gestionado	Política de pantalla y escritorio limpio

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.1	Documentación de procedimientos operacionales	Gestionado	Política de documentación de procedimientos operacionales
A12.1.2	Gestión de cambios	Gestionado	Política de gestión de cambios
A12.1.3	Gestión de capacidades	Gestionado	Política de gestión de capacidades
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Optimizado	CEDIA cumple satisfactoriamente con este control
A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso	Optimizado	Política de uso aceptable. Análisis de vulnerabilidades de CSIRT Capacitación periódica de CSIRT
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	Optimizado	Política de creación de copias de seguridad, Política de uso aceptable
A12.3	**Registros y supervisión**		
A12.4.1	Registro de eventos	Optimizado	CEDIA cumple satisfactoriamente con este control
A12.4.2	Protección de la información del registro	Optimizado	CEDIA cumple satisfactoriamente con este control
A12.4.3	Registros de administración y operación	Optimizado	CEDIA cumple satisfactoriamente con este control
A12.4.4	Sincronización del reloj	Optimizado	CEDIA cumple satisfactoriamente con este control

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A12.5	**Control del software en explotación**		
A12.5.1	Instalación del software en explotación	Optimizado	Política de uso aceptable / Políticas de implementación de adopción y uso de software
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Optimizado	CEDIA cumple satisfactoriamente con este control
A12.6.2	Restricción en la instalación de software	Gestionado	Política de uso aceptable / Políticas de implementación de adopción y uso de software
A12.7	**Consideraciones sobre la auditoría de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	Gestionado	Capacitar a los auditores y enfocar las auditorías para que se incluyan en el SGSI y los indicadores de seguridad de la información
A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	Optimizado	CEDIA cumple satisfactoriamente con este control
A13.1.2	Seguridad de los servicios de red	Optimizado	CEDIA cumple satisfactoriamente con este control
A13.1.3	Segregación en redes	Optimizado	CEDIA cumple satisfactoriamente con este control
A13.2	**Intercambio de información**		
A13.2.1	Políticas y procedimientos de	Gestionado	Política de transferencia de información y comunicaciones ,

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
	intercambio de información		Política Trae tu propio dispositivo (BYOD)
A13.2.2	Acuerdos de intercambio de información	Gestionado	Política de transferencia de información y comunicaciones
A13.2.3	Mensajería electrónica	Optimizado	CEDIA cumple satisfactoriamente con este control
A13.2.4	Acuerdos de confidencialidad o no revelación	Gestionado	Política de clasificación de la información, Política de uso aceptable
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Gestionado	Política de requisitos y especificaciones de seguridad de la información
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Optimizado	Política de desarrollo seguro
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Optimizado	Política de desarrollo seguro
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro	Gestionado	Política de desarrollo seguro

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A14.2.2	Procedimiento de control de cambios en sistemas	Optimizado	Política de desarrollo seguro
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Gestionado	Política de desarrollo seguro
A14.2.4	Restricciones a los cambios en los paquetes de software	Gestionado	Política de desarrollo seguro
A14.2.5	Principios de ingeniería de sistemas seguros	Gestionado	Política de desarrollo seguro
A14.2.6	Entorno de desarrollo seguro	Gestionado	Política de desarrollo seguro
A14.2.7	Externalización del desarrollo de software	Optimizado	Política de seguridad para proveedores, Política de desarrollo seguro
A14.2.8	Pruebas funcionales de seguridad de sistemas	Definido	Política de desarrollo seguro
A14.2.9	Pruebas de aceptación de sistemas	Definido	Política de desarrollo seguro
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	Definido	Política de desarrollo seguro
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información en las	Gestionado	Política de seguridad para proveedores

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
	relaciones con los proveedores		
A15.1.2	Requisitos de seguridad en contratos con terceros	Gestionado	Política de seguridad para proveedores
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Gestionado	Política de seguridad para proveedores
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Gestionado	Política de seguridad para proveedores y Niveles de Servicio (SLA)
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Gestionado	Política de seguridad para proveedores y Niveles de Servicio (SLA)
A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A16.1.1	Responsabilidades y procedimientos	Optimizado	Procedimiento para gestión de incidentes
A16.1.2	Notificación de los eventos de seguridad de la información	Optimizado	Procedimiento para gestión de incidentes
A16.1.3	Notificación de puntos débiles de la seguridad	Optimizado	Procedimiento para gestión de incidentes
A16.1.4	Evaluación y decisión sobre los eventos de	Optimizado	Procedimiento para gestión de incidentes

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
	seguridad de información		
A16.1.5	Respuesta a incidentes de seguridad de la información	Optimizado	Procedimiento para gestión de incidentes, Plan de respuesta ante incidentes
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Optimizado	Procedimiento para gestión de incidentes, Plan de respuesta ante incidentes
A16.1.7	Recopilación de evidencias	Gestionado	Procedimiento para gestión de incidentes, Plan de respuesta ante incidentes
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Optimizado	Política de continuidad del negocio
A17.1.2	Implementar la continuidad de la seguridad de la información	Optimizado	Política de continuidad del negocio
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Optimizado	Política de continuidad del negocio
A17.2	**Redundancias**		

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Optimizado	Política para la estrategia de recuperación para la infraestructura de TI
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales**		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Optimizado	Extender la investigación de las leyes aplicables a temas de seguridad de la información
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Optimizado	Política de Derechos de Propiedad Intelectual
A18.1.3	Protección de los registros de la organización	Gestionado	Política de desarrollo control de cambios
A18.1.4	Protección y privacidad de la información de carácter personal	Gestionado	Política de protección de datos
A18.1.5	Regulación de los controles criptográficos	Optimizado	Política del uso de controles criptográficos
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	Gestionado	Política de seguridad de la información
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Optimizado	Una vez establecida e implementada la política de seguridad de la información, realizar los controles al cumplimiento de la misma

Sección	Control de la seguridad de la información	Estado	Justificación y referencias de CEDIA
A18.2.3	Comprobación del cumplimiento técnico	Gestionado	Reforzar las revisiones a los planes de mejoramiento y pruebas de vulnerabilidad a los sistemas de información.

Tabla 8 Estado objetivo o deseado de CEDIA

La siguiente tabla describe el significado de cada estado con su porcentaje de cumplimiento deseado de los controles en CEDIA:

Estado	Significado	Porcentaje de controles de seguridad de la información
Desconocido	Ni siquiera ha sido revisado todavía	**0%**
No existente	Falta total de políticas reconocibles, procedimientos, controles, etc.	**0%**
Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para cumplir con los requisitos.	**0%**
Limitado	Progresando bien pero aún no completo	**0%**
Definido	El desarrollo está más o menos completado, a pesar de que faltan ciertos detalles y/o no todavía no están implementados, reforzados y activamente soportados por la alta dirección	**4%**

Estado	Significado	Porcentaje de controles de seguridad de la información
Gestionado	El desarrollo está completado, el proceso/control ha sido implementado y comenzó a operar recientemente	**48%**
Optimizado	El requerimiento se cumple completamente, está operando completamente como se esperaba, se está monitoreando y mejorando activamente, y hay evidencia sustancial para demostrar todo eso a los auditores.	**48%**
No aplica	SGSI va a ser certificado TODOS los requisitos en el cuerpo principal de ISO/IEC 27001 son obligatorios. De lo contrario, la gerencia puede ignorarlos.	**0%**
	Total	100%

Tabla 9 Estado con su respectivo significado y porcentaje de cumplimiento objetivo o deseado de CEDIA

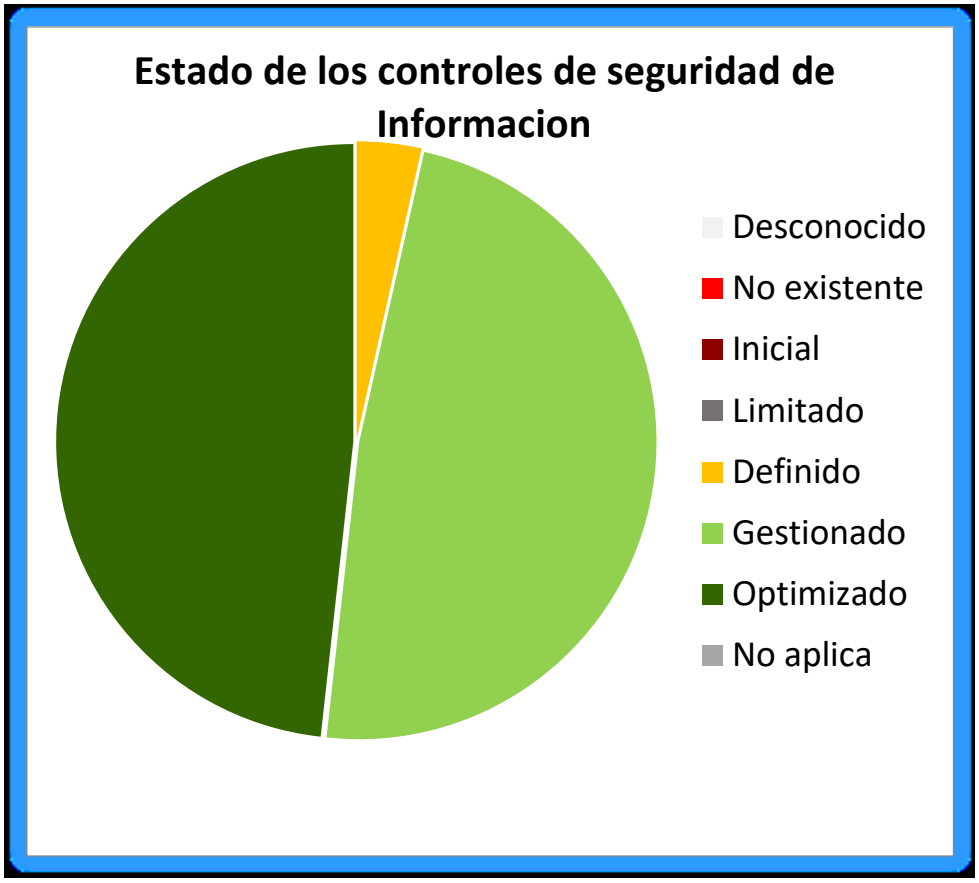


Figura 23 Estado objetivo o deseado de los controles de seguridad de Información de CEDIA

Para finalizar el análisis de brecha, se elaboró las gráficas entre el estado actual y el estado objetivo de CEDIA con sus respectivos valores, es decir:

DESCRIPCIÓN ESTADO	VALOR
Optimizado	100
Gestionado	80
Definido	50
Limitado	25
Inicial	10

Tabla 10 Estados con su respectivo valor

CONTROLES	VALOR ESTADO ACTUAL CEDIA	VALOR SOA
A5	**Valor Estado CEDIA**	**Valor SoA**

CONTROLES	VALOR ESTADO ACTUAL CEDIA	VALOR SOA
Políticas para la seguridad de la información	10	80
Revisión de las políticas	10	80
A6	**Valor Estado CEDIA**	**Valor SoA**
Roles y responsabilidades en seguridad de la información	25	100
Segregación de tareas	50	100
Contacto con las autoridades	80	100
Contacto con grupos de interés especial	80	100
Seguridad de la información en la gestión de proyectos	25	80
Política de dispositivos móviles	10	80
Teletrabajo	10	50
A7	**Valor Estado CEDIA**	**Valor SoA**
Investigación de antecedentes	50	80
Términos y condiciones del empleo	80	100
Responsabilidades de gestión	25	80
Concienciación, educación y capacitación en seguridad de la información	50	80
Proceso disciplinario	10	100
Responsabilidades ante la finalización o cambio	10	100
A8	**Valor Estado CEDIA**	**Valor SoA**
Inventario de activos	25	100
Propiedad de los activos	50	100
Uso aceptable de los activos	10	80
Devolución de activos	80	100
Clasificación de la información	25	80

CONTROLES	VALOR ESTADO ACTUAL CEDIA	VALOR SOA
Etiquetado de la información	25	80
Manipulado de la información	25	80
Gestión de soportes extraíbles	10	80
Eliminación de soportes	10	80
Soportes físicos en tránsito	50	100
A9	**Valor Estado CEDIA**	**Valor SoA**
Política de control de acceso	80	100
Acceso a las redes y a los servicios de red	80	100
Registro y baja de usuario	50	100
Provisión de acceso de usuario	50	100
Gestión de privilegios de acceso	50	100
Gestión de la información secreta de autenticación de los usuarios	25	100
Revisión de los derechos de acceso de usuario	25	80
Retirada o reasignación de los derechos de acceso	50	100
Uso de la información secreta de autenticación	25	80
Restricción del acceso a la información	80	100
Procedimientos seguros de inicio de sesión	50	100
Sistema de gestión de contraseñas	25	100
Uso de utilidades con privilegios del sistema	50	80
Control de acceso al código fuente de los programas	50	100
A10	**Valor Estado CEDIA**	**Valor SoA**

CONTROLES	VALOR ESTADO ACTUAL CEDIA	VALOR SOA
Política de uso de los controles criptográficos	10	80
Gestión de claves	50	100
A11	**Valor Estado CEDIA**	**Valor SoA**
Perímetro de seguridad física	80	100
Controles físicos de entrada	80	100
Seguridad de oficinas, despachos y recursos	80	80
Protección contra las amenazas externas y ambientales	80	80
El trabajo en áreas seguras	80	80
Áreas de carga y descarga	80	80
Emplazamiento y protección de equipos	80	80
Instalaciones de suministro	80	80
Seguridad del cableado	80	80
Mantenimiento de los equipos	50	80
Retirada de materiales propiedad de la empresa	80	80
Seguridad de los equipos fuera de las instalaciones	80	80
Reutilización o eliminación segura de equipos	80	80
Equipo de usuario desatendido	50	100
Política de puesto de trabajo despejado y pantalla limpia	10	80
A12	**Valor Estado CEDIA**	**Valor SoA**
Documentación de procedimientos operacionales	50	80
Gestión de cambios	50	80

CONTROLES	VALOR ESTADO ACTUAL CEDIA	VALOR SOA
Gestión de capacidades	50	80
Separación de los recursos de desarrollo, prueba y operación	80	100
Controles contra el código malicioso	80	100
Copias de seguridad de la información	80	100
Registro de eventos	80	100
Protección de la información del registro	80	100
Registros de administración y operación	80	100
Sincronización del reloj	80	100
Instalación del software en explotación	50	100
Gestión de las vulnerabilidades técnicas	80	100
Restricción en la instalación de software	50	80
Controles de auditoría de sistemas de información	25	80
A13	**Valor Estado CEDIA**	**Valor SoA**
Controles de red	80	100
Seguridad de los servicios de red	80	100
Segregación en redes	80	100
Políticas y procedimientos de intercambio de información	25	80
Acuerdos de intercambio de información	25	80
Mensajería electrónica	80	100
Acuerdos de confidencialidad o no revelación	50	80
A14	**Valor Estado CEDIA**	**Valor SoA**
Análisis de requisitos y especificaciones de seguridad de la información	50	80
Asegurar los servicios de aplicaciones en redes públicas	80	100

CONTROLES	VALOR ESTADO ACTUAL CEDIA	VALOR SOA
Protección de las transacciones de servicios de aplicaciones	80	100
Política de desarrollo seguro	50	80
Procedimiento de control de cambios en sistemas	80	100
Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	50	80
Restricciones a los cambios en los paquetes de software	50	80
Principios de ingeniería de sistemas seguros	25	80
Entorno de desarrollo seguro	50	80
Externalización del desarrollo de software	80	100
Pruebas funcionales de seguridad de sistemas	80	50
Pruebas de aceptación de sistemas	80	50
Protección de los datos de prueba	50	50
A15	**Valor Estado CEDIA**	**Valor SoA**
Política de seguridad de la información en las relaciones con los proveedores	50	80
Requisitos de seguridad en contratos con terceros	50	80
Cadena de suministro de tecnología de la información y de las comunicaciones	50	80
Control y revisión de la provisión de servicios del proveedor	50	80
Gestión de cambios en la provisión del servicio del proveedor	50	80

CONTROLES	VALOR ESTADO ACTUAL CEDIA	VALOR SOA
A16	**Valor Estado CEDIA**	**Valor SoA**
Responsabilidades y procedimientos	80	100
Notificación de los eventos de seguridad de la información	80	100
Notificación de puntos débiles de la seguridad	50	100
Evaluación y decisión sobre los eventos de seguridad de información	80	100
Respuesta a incidentes de seguridad de la información	80	100
Aprendizaje de los incidentes de seguridad de la información	50	100
Recopilación de evidencias	25	80
A17	**Valor Estado CEDIA**	**Valor SoA**
Planificación de la continuidad de la seguridad de la información	50	100
Implementar la continuidad de la seguridad de la información	50	100
Verificación, revisión y evaluación de la continuidad de la seguridad de la información	50	100
Disponibilidad de los recursos de tratamiento de la información	80	100
A18	**Valor Estado CEDIA**	**Valor SoA**
Identificación de la legislación aplicable y de los requisitos contractuales	10	100
Derechos de Propiedad Intelectual (DPI)	25	100
Protección de los registros de la organización	10	80

CONTROLES	VALOR ESTADO ACTUAL CEDIA	VALOR SOA
Protección y privacidad de la información de carácter personal	10	80
Regulación de los controles criptográficos	50	100
Revisión independiente de la seguridad de la información	10	80
Cumplimiento de las políticas y normas de seguridad	25	100
Comprobación del cumplimiento técnico	25	80

Tabla 11 Análisis de Brecha de CEDIA con el estado y su respectivo valor

A continuación, se presenta la comparación de lo indicado anteriormente en gráficos:

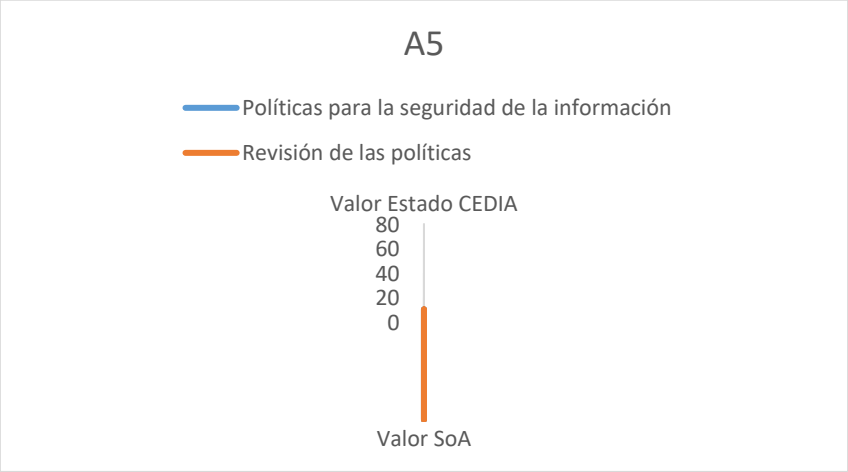


Figura 24 Control A5. Análisis de Brecha de CEDIA

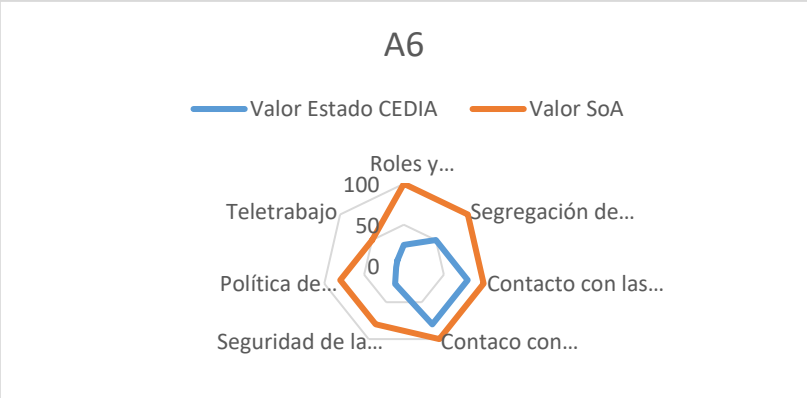


Figura 25 Control A6. Análisis de Brecha de CEDIA

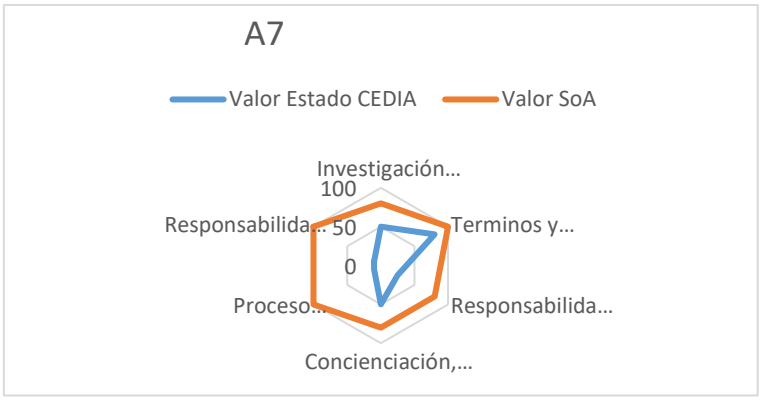


Figura 26 Control A7. Análisis de Brecha de CEDIA

Figura 27 Control A8. Análisis de Brecha de CEDIA

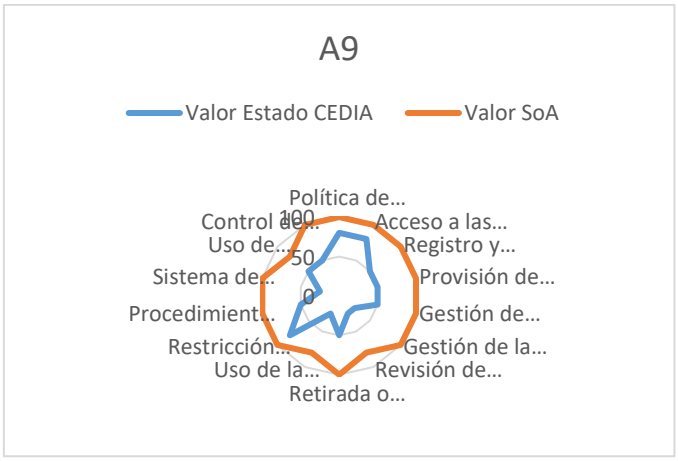


Figura 28 Control A9. Análisis de Brecha de CEDIA

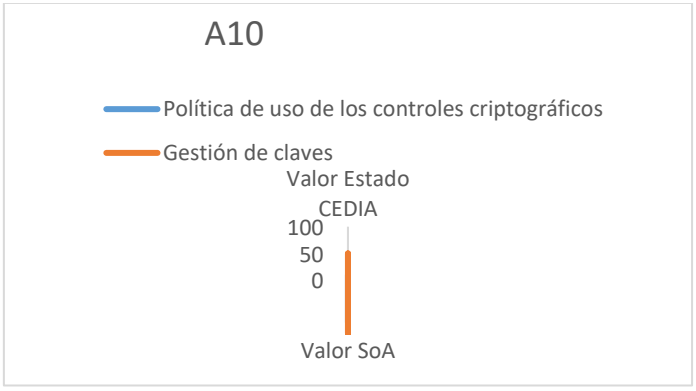


Figura 29 Control A10. Análisis de Brecha de CEDIA

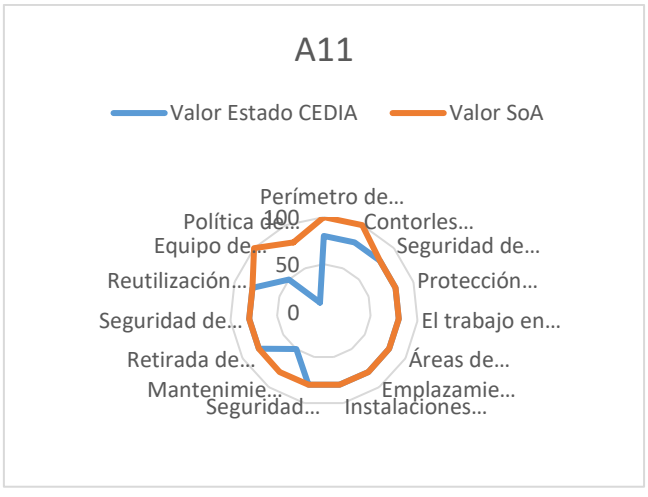


Figura 30 Control A11. Análisis de Brecha de CEDIA

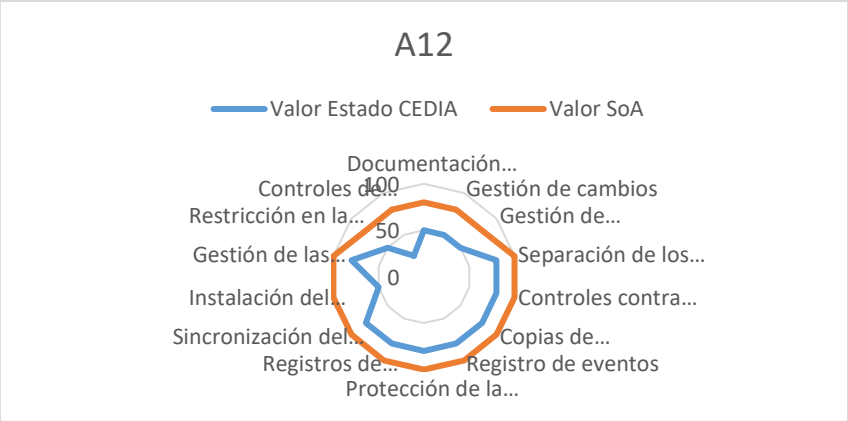


Figura 31 Control A12. Análisis de Brecha de CEDIA

Figura 32 Control A13. Análisis de Brecha de CEDIA

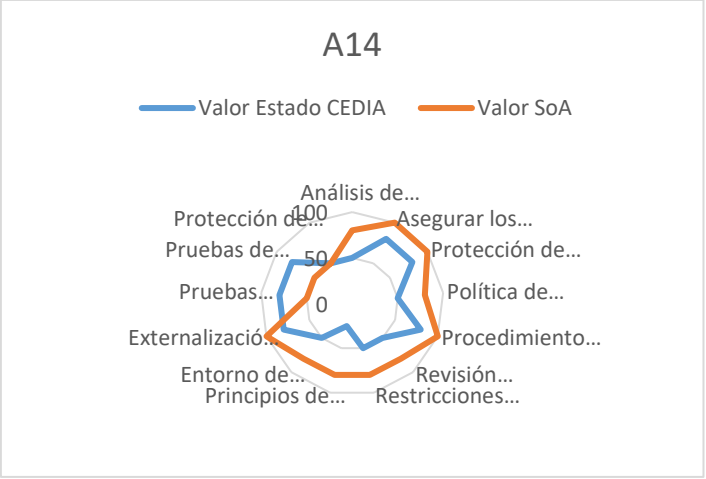


Figura 33 Control A14. Análisis de Brecha de CEDIA

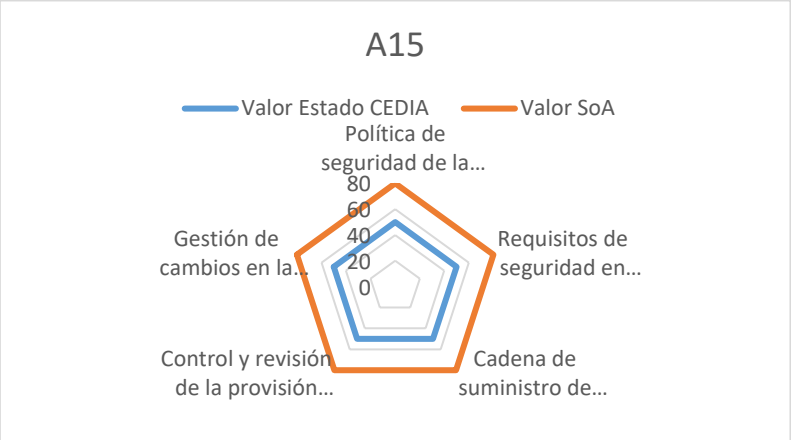


Figura 34 Control A15. Análisis de Brecha de CEDIA

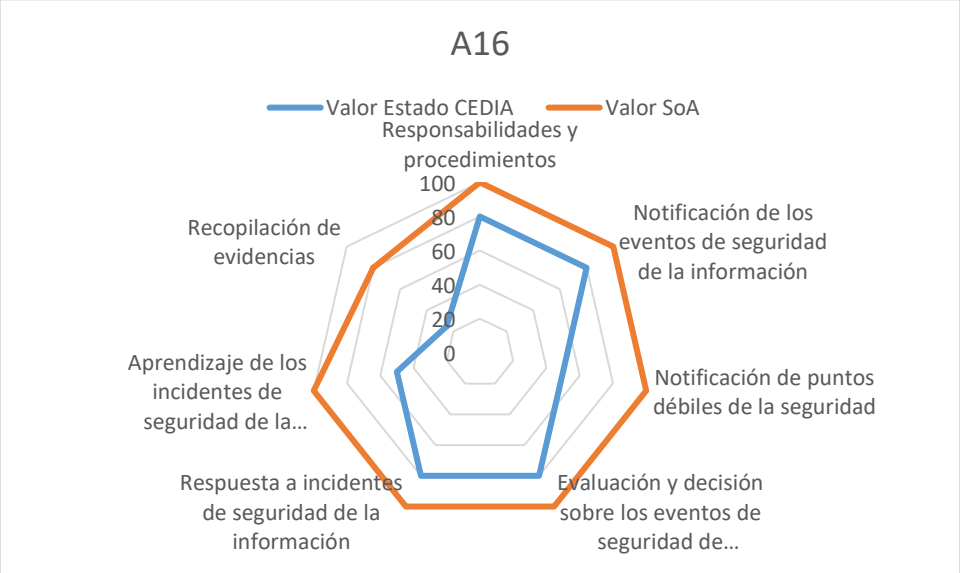


Figura 35 Control A16. Análisis de Brecha de CEDIA

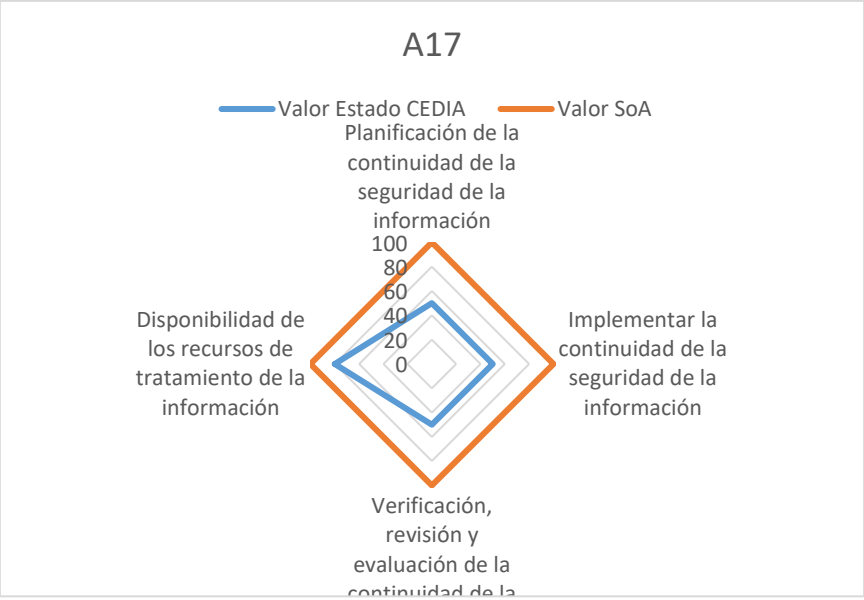


Figura 36 Control A17. Análisis de Brecha de CEDIA

Figura 37 Control A18. Análisis de Brecha de CEDIA

Como se puede evidenciar CEDIA actualmente cuenta con el 38% de los controles gestionados, 32% definidos, el 17% y 13% Limitados e Inicial respectivamente, es decir que cuenta con una buena implementación en varios controles y al tener apoyo de la Dirección Ejecutiva es posible cumplir con el estado deseado e implementar el SGSI en la Corporación.

Cabe mencionar que CEDIA cuenta con un equipo altamente calificado para las funciones asignadas y resulta conveniente garantizar y cumplir con el análisis de brecha.

Posterior al análisis realizado, se debe elaborar la declaración de aplicabilidad para CEDIA, dicha declaración es un documento o tabla que permite establecer los controles que debe cumplir e implementar para que la información se mantenga segura, confiable y disponible en la organización.

La declaración de aplicabilidad, establece qué controles y políticas ISO 27001 debe aplicar la organización con su respectiva justificación.

4.7. ELABORACIÓN DE LA DECLARACIÓN DE LA APLICABILIDAD PARA CEDIA EN BASE AL ANEXO A (NORMATIVO) OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA DE LA NORMA ISO/IEC 27002:2013

La tercera y última fase se refiere a la elaboración de la guía de implementación de un SGSI para la CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA - CEDIA basada en el ANEXO A (Normativo) Objetivos de control y controles de referencia de la norma ISO/IEC 27002:2013, es decir, que se establece el contexto actual de la organización, define el alcance, direccionar riesgos y oportunidades, proporcionar apoyo a las partes interesadas, operar y controlar y finalmente se evalúa el desempeño.

El objetivo de la elaboración de la Declaración de la Aplicabilidad es definir qué controles son adecuados para implementar en CEDIA con su respectiva justificación.

Los objetivos de control y los controles enumerados en la tabla 4 están alineados con aquellos enumerados en la ISO/IEC 27002:2013, es decir, las cláusulas 5 al 18 y se deben aplicar a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

A continuación, se detalla cada objetivo de control y controles para CEDIA:

Objetivos de control y controles			**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**
A.5 Políticas de seguridad de la información				
A.5.1 Directrices de gestión de la seguridad de la información				
Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes				
A.5.1.1	*Políticas para la seguridad de la información*	*Control* *Un conjunto de políticas para seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.*	SI	Se debe cumplir con los requisitos legales pertinentes, de acuerdo a la naturaleza de CEDIA y asegurar la integridad de la información
A.5.1.2	*Revisión de las políticas*	*Control* *Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.*	SI	Para el adecuado control y seguimiento enfocado a la mejora continua de la política de SGSI.
A.6 Organización de la seguridad de la información				
A.6.1 Organización interna				
Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				
A.6.1.1	*Roles y responsabilidades en seguridad de la información*	*Control* *Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas*	SI	Para toma de decisiones, escalabilidad y asignación de responsabilidades

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				relacionadas con seguridad de la información
A.6.1.2	*Segregación de tareas*	*Control* *Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.*	SI	Se debe asignar el perfil de acuerdo a las responsabilidades u objeto contractual, puesto que los obligaciones y/o funciones de cada área/cargo se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.
A.6.1.3	*Contacto con las autoridades*	*Control* *Deben mantenerse los contactos apropiados con las autoridades pertinentes.*	SI	Para reportar de manera oportuna los incidentes de seguridad que puedan afectar la continuidad de la operación del negocio.
A.6.1.4	*Contacto con grupos de interés especial*	*Control* *Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y*	SI	El Oficial de Seguridad de la Información con el CSIRT de CEDIA son los responsable de

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		asociaciones profesionales especializados en seguridad.		supervisar el contacto con EcuCERT, FIRST
A.6.1.5	*Seguridad de la información en la gestión de proyectos*	*Control* *La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.*	SI	El área de proyectos e investigación debe incluir las reglas correspondientes sobre seguridad de la información en cada proyecto
A.6.2 Los dispositivos móviles y el teletrabajo				
Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.				
A6.2.1	*Política de dispositivos móviles*	*Control* *Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.*	SI	Para reducir los riesgos de conexión de dispositivos móviles a la red de CEDIA
A.6.2.2	*Teletrabajo*	*Control* *Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.*	SI	CEDIA no ha establecido las disposiciones necesarias para dar cumplimiento a una política de teletrabajo
A.7 Seguridad relativa a los recursos humanos				
A.7.1 Antes del empleo				
Objetivo: Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.				
A.7.1.1	*Investigación de antecedentes*	*Control*	SI	Asegurar la idoneidad del colaborador para

Objetivos de control y controles			**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**
		La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.		asumir sus responsabilidades relacionadas con el manejo de la información en relación al acceso y riesgos identificados.
A.7.1.2	*Términos y condiciones del empleo*	*Control* *Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.*	SI	Asegurar que los colaboradores y proveedores acepten y cumplan las condiciones relacionadas con la seguridad de la información
A.7.2 Durante el empleo				
Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.				
A.7.2.1	*Responsabilidades de gestión*	*Control* *La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.*	SI	La dirección ejecutiva debe asegurar el cumplimiento de la seguridad de la información por parte de los colaboradores de CEDI mediante la

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				concientización del SGSI
A.7.2.2	*Concienciación, educación y capacitación en seguridad de la información*	*Control* *Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.*	SI	Todos los colaboradores de CEDIA deben aplicar seguridad de la información en su día a día para entender el impacto de su comportamiento en la Corporación
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.*	SI	Para aplicar el procedimiento disciplinario frente a acciones de colaboradores que cometan violaciones a la seguridad de la información
A.7.3 Finalización del empleo o cambio en el puesto de trabajo				
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.				
A.7.3.1	*Responsabilidades ante la finalización o cambio*	*Control* *Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al*	SI	Para asegurar que se cumplan los requisitos de seguridad de la información, es necesario r7ealizar un seguimiento de los activos de información

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		empleado o contratista y se deben cumplir.		y perfiles que son asignados a cada colaborador o proveedor dentro de la contratación
A.8 Gestión de activos				
A.8.1 Responsabilidad sobre los activos				
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.				
A.8.1.1	*Inventario de activos*	*Control* *La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.*	SI	Es necesario identificar los activos de información y sus niveles de importancia para gestionar los riesgos asociados a la Seguridad de la información
A.8.1.2	*Propiedad de los activos*	*Control* *Todos los activos que figuran en el inventario deben tener un propietario.*	SI	Para asegurar el manejo apropiado del activo de acuerdo a las políticas de seguridad establecidas
A.8.1.3	*Uso aceptable de los activos*	*Control* *Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.*	SI	Para dar el uso apropiado del activo en relación a las reglas establecidas a los requisitos de seguridad de la información

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
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.*	SI	Es necesario validar y controlar el estado del empleo, contrato y/o acuerdo en caso de finalización para formalizar la devolución del activo de forma segura
A.8.2 Calificación de la información				
Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.				
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.*	SI	Es necesario dar cumplimiento a la normativa de la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) con el fin de asegurar el manejo adecuado de los activos de tipo información
A.8.2.2	*Etiquetado de la información*	*Control* *Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.*	SI	Asegurar el manejo adecuado de los activos de tipo información

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
A.8.2.3	*Manipulado de la información*	*Control* *Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.*	SI	Se requiere garantizar la protección y el manejo óptimo del activo a través del procedimiento de gestión de activos
A.8.3 Manipulación de los soportes				
Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.				
A.8.3.1	*Gestión de soportes extraíbles*	*Control* *Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.*	SI	Se debe implementar una política para evitar la propagación de virus informáticos y/o fuga de información
A.8.3.2	*Eliminación de soportes*	*Control* *Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.*	SI	Con la política a implementar se asegura el borrado seguro de la información y estado del medio
A.8.3.3	*Soportes físicos en tránsito*	*Control* *Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.*	SI	Se requiere custodiar de manera segura la información para evitar acceso no autorizado o corrupción en el transporte

Objetivos de control y controles			**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**
A.9 Control de acceso				
A.9.1 Requisitos de negocio para el control de acceso				
Objetivo: Limitar el acceso a los recursos de tratamiento de la información y a la información.				
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.*	SI	CEDIA debe establecer roles y perfiles de acceso de acuerdo a las funciones del cargo dando cumplimiento a los acuerdos de confidencialidad
A.9.1.2	*Acceso a las redes y a los servicios de red*	*Control* *Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.*	SI	Es necesario que solo los usuarios y servicios de la red tengan permisos de acceso específicos a las conexiones de CEDIA
A.9.2 Gestión de acceso de usuario				
Objetivo: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.				
A.9.2.1	*Registro y baja de usuario*	*Control* *Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.*	SI	Se debe implementar un proceso que permita asignar y revocar los derechos de acceso, cuando el colaborador inicie o finalice su vinculación laboral
A.9.2.2	*Provisión de acceso de usuario*	*Control*	SI	Se debe implementar un proceso que

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.		permita asignar y revocar los derechos de acceso, cuando el colaborador inicie o finalice su vinculación laboral
A.9.2.3	*Gestión de privilegios de acceso*	*Control* *La asignación y el uso de privilegios de acceso debe estar restringida y controlada.*	SI	CEDIA establece roles y perfiles de acceso de acuerdo a las funciones del cargo dando cumplimiento a los acuerdos de confidencialidad
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.*	SI	Se requiere verificar la identidad de los usuarios que hacen uso de los sistemas de CEDIA por medio de autenticación
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.*	SI	Los responsables de los activos de información deben validar que los permisos estén acordes con las funciones del cargo, para asegurar que no hayan obtenido privilegios no autorizados

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
A.9.2.6	*Retirada o reasignación de los derechos de acceso*	*Control* *Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.*	SI	Los responsables de los activos de información deben validar que los permisos estén acordes con las funciones del cargo, para asegurar que no hayan obtenido privilegios no autorizados. En caso de finalización de contrato se deben revocar los permisos
A.9.3 Responsabilidades del usuario				
Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.				
A.9.3.1	*Uso de la información secreta de autenticación*	*Control* *Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.*	SI	Los usuarios deben cumplir con las directrices establecidas en la política para salvaguardar la información a través de la autenticación
A.9.4 Control de acceso a sistemas y aplicaciones				
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.				
A.9.4.1	*Restricción del acceso a la información*	*Control* *Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la*	SI	Los responsables de los activos de información deben validar que los derechos de acceso de

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		política de control de acceso definida.		los usuarios estén acordes con las funciones del cargo
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 se debe controlar por medio de un procedimiento seguro de inicio de sesión.*	SI	Los responsables de los activos de información deben validar que los derechos de acceso de los usuarios estén acordes con las funciones del cargo
A.9.4.3	*Sistema de gestión de contraseñas*	*Control* *Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.*	SI	Se requiere asegurar la calidad de las contraseñas para el ingreso confiable a los sistemas
A.9.4.4	*Uso de utilidades con privilegios del sistema*	*Control* *Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.*	SI	Se deben establecer procedimientos para la autorización de aplicaciones / utilidades especiales
A.9.4.5	*Control de acceso al código fuente de los programas*	*Control* *Se debe restringir el acceso al código fuente de los programas.*	SI	Se debe controlar el acceso a los códigos fuentes para reducir el riesgo de manipulación y divulgación de la fuente de los

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				programas y elementos asociados
A.10 Criptografía				
A.10.1 Controles criptográficos				
Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.				
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.*	SI	CEDIA debe establecer las normas para el uso de la criptografía y el tráfico de la información garantizando la protección de la misma
A.10.1.2	*Gestión de claves*	*Control* *Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.*	SI	Las normas de criptografía deben contener la gestión de las claves dentro de las cuales deben estar relacionadas a protección, tiempo de vida y ciclo de vida
A.11 Seguridad física y del entorno				
A.11.1 Áreas seguras				
Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.				
A.11.1.1	*Perímetro de seguridad física*	*Control* *Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible*	SI	Las áreas con información sensible deben estar protegidas a través de permisos de acceso restringidos de

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		así como los recursos de tratamiento de la información.		acuerdo a las funciones de los colaboradores
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.*	SI	El acceso a las áreas seguras de la organización deben estar controladas a través de un sistema físico, como por ejemplo: uso de tarjetas de acceso, códigos de acceso y entrada principal con guardia.
A.11.1.3	*Seguridad de oficinas, despachos y recursos*	*Control* *Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.*	SI	CEDIA maneja información confidencial por ende, se debe tomar las medidas para proteger las oficinas, recursos e instalación de la organización
A.11.1.4	*Protección contra las amenazas externas y ambientales*	*Control* *Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.*	SI	Para proteger a CEDIA se debe contar con el conocimiento adecuado del manejo de daños naturales o causados por el hombre

Objetivos de control y controles			**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**
A.11.1.5	*El trabajo en áreas seguras*	*Control* *Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.*	SI	Se debe proteger a CEDIA con procedimientos de seguridad que cubran el trabajo en áreas seguras y donde la información sea más sensible y susceptible
A.11.1.6	*Áreas de carga y descarga*	*Control* *Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.*	SI	Los puntos de acceso se deben aislar y controlar para evitar el acceso de personal ajeno a CEDIA sin el permiso correspondiente
A.11.2 Seguridad de los equipos				
Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.				
A.11.2.1	*Emplazamiento y protección de equipos*	*Control* *Los equipos deben situarse o 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.*	SI	Se debe establecer un área segura para la ubicación de los equipos y minimizar la exposición a peligro ambiental y accesos no autorizados

Objetivos de control y controles			**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**
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.*	SI	Se debe garantizar el servicio de potencia para los equipos de CEDIA
A.11.2.3	*Seguridad del cableado*	*Control* *El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.*	SI	El cableado de potencia y de telecomunicaciones debe estar debidamente identificado e implementado mediante una opción segura
A.11.2.4	*Mantenimiento de los equipos*	*Control* *Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.*	SI	Se debe implementar directrices de mantenimiento de equipos que garanticen su disponibilidad
A.11.2.5	*Retirada de materiales propiedad de la empresa*	*Control* *Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.*	SI	Las directrices para protección de los activos deben considerar la identificación del personal interno y externo que tiene la autorización de retiro de los activos, debe incluir el tiempo por el cual se retiran los

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				activos y verificar que cumplan con las devoluciones
A.11.2.6	*Seguridad de los equipos 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.*	SI	Para proteger los activos fuera de las instalaciones de CEDIA se deben generar directrices que estén enfocadas a la seguridad
A.11.2.7	*Reutilización o eliminación segura de equipos*	*Control* *Todos los soportes 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.*	SI	Se debe disponer de lineamientos para la disposición y reutilización de los equipos, los cuales garantizarán la eliminación de la información ya sea por destrucción o sobre escritura, de tal forma que esta información no sea recuperable
A.11.2.8	*Equipo de usuario desatendido*	*Control* *Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.*	SI	Los colaboradores de CEDIA deben tener clara y apropiada la directriz sobre el uso de los equipos, la confidencialidad de la información, el uso de

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				las contraseñas y manejo de las sesiones
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 desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.*	SI	Los colaboradores de CEDIA deben tener clara y apropiada la directriz sobre el uso de los equipos, la confidencialidad de la información, el uso de las contraseñas y manejo de las sesiones
A.12 Seguridad de las operaciones				
A.12.1 Procedimientos y responsabilidades operacionales				
Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.				
A.12.1.1	*Documentación de procedimientos operacionales*	*Control* *Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.*	SI	Se deben crear los procedimientos y documentarlos para las actividades de operaciones de tal forma que garanticen la seguridad
A.12.1.2	*Gestión de cambios*	*Control* *Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información deben ser controlados.*	SI	Los cambios en los procesos deben documentarse. La documentación debe contener aspectos como: identificación, planificación,

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				valoración del impacto, etc
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 garantizar el rendimiento requerido del sistema.*	SI	El Director de TI y Coordinador de Operaciones deben ser los responsables de supervisar el uso de los activos de TIC y de planificar la capacidad necesaria
A.12.1.4	*Separación de los recursos de desarrollo, prueba y operación*	*Control* *Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.*	SI	Se debe garantizar por parte de CEDIA la separación de ambiente de desarrollo pruebas y producción, de tal forma que se minimicen los riesgos de acceso o cambios no autorizados.
A.12.2 Protección contra el software malicioso (malware)				
Objetivo: Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.				
A.12.2.1	*Controles contra el código malicioso*	*Control* *Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.*	SI	Se debe garantizar la seguridad de la información creando políticas y controles que prohíban el uso de software no autorizado, hacer la detección de software

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				no autorizado, restringir el acceso a sitios web que se sospecha son malicioso
A.12.3 Copias de seguridad				
Objetivo: Evitar la pérdida de datos				
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 y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.*	SI	La política de respaldo de datos debe contener los requisitos para copias de información de CEDIA tanto de hardware como de software para preservar la disponibilidad de la información
A.12.4 Registros y supervisión				
Objetivo: Registrar eventos y generar evidencias.				
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.*	SI	Para dar un correcto manejo a las actividades se deben establecer las directrices para el registro, almacenamiento y consulta de los eventos
A.12.4.2	*Protección de la información del registro*	*Control* *Los dispositivos de registro y la información del registro deben estar*	SI	Para aplicar la protección de la información se

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		protegidos contra manipulaciones indebidas y accesos no autorizados.		requiere que a cada colaborador se le asigne un usuario y contraseña que le permita el ingreso de forma segura a la información , a las tareas asignadas y así establecer el control
A.12.4.3	*Registros de administración y operación*	*Control* *Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.*	SI	Se debe controlar y proteger los registros de los usuarios privilegiados que puedan afectar la seguridad de la información
A.12.4.4	*Sincronización del reloj*	*Control* *Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente de tiempo precisa y acordada.*	SI	Los relojes de los sistemas en todos los equipos de CEDIA deben estar sincronizados para cumplir con la reglamentación y mantener una medida estándar
A.12.5 Control del software en explotación				
Objetivo: Asegurar la integridad del software en explotación.				
A.12.5.1	*Instalación del software en explotación*	*Control* *Se deben implementar procedimientos para controlar la*	SI	Solo el personal autorizado dentro de CEDIA puede instalar

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		instalación del software en explotación.		o desinstalar software en los equipos de la organización
A.12.6 Gestión de la vulnerabilidad técnica				
Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.				
A.12.6.1	*Gestión de las 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.*	SI	Para la gestión de vulnerabilidades técnicas establecidas en la matriz de riesgos, se debe contar con los controles apropiados para el manejo
A.12.6.2	*Restricción en la instalación de software*	*Control* *Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.*	SI	Solo el personal autorizado dentro de CEDIA puede instalar o desinstalar software en los equipos de la organización
A.12.7 Consideraciones sobre la auditoria de sistemas de información				
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.				
A.12.7.1	*Controles de auditoría de 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*	SI	Cada auditoría se debe planificar y coordinar con la dirección ejecutiva; las auditorías se deberían realizar solamente con

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		de interrupciones en los procesos de negocio.		derechos de acceso de sólo lectura
A.13 Seguridad de las comunicaciones				
A.13.1 Gestión de la seguridad de las redes				
Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.				
A.13.1.1	*Controles de red*	*Control* *Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.*	SI	Para el adecuado uso de las redes de información se debe establecer controles y procedimientos para asegurar la configuración segura de los dispositivos y estar documentados
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.*	SI	Se debe determinar y gestionar los servicios de red mediante los mecanismos de control adecuados
A.13.1.3	*Segregación en redes*	*Control* *Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.*	SI	Para una mejor gestión y control de red se debe segmentar los dominios creando separación de red

Objetivos de control y controles			**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**
A.13.2 Intercambio de información				
Objetivo: Mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa.				
A.13.2.1	*Políticas y procedimientos de intercambio de información*	*Control* *Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.*	SI	Para garantizar la integridad, disponibilidad y confidencialidad de la información
A.13.2.2	*Acuerdos de intercambio de información*	*Control* *Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.*	SI	Para garantizar la integridad, disponibilidad y confidencialidad de la información
A.13.2.3	*Mensajería electrónica*	*Control* *La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.*	SI	Por el intercambio de datos con usuarios internos y externos se debe contar con un sistema de correo electrónico que permita: protección de información, confiabilidad y disponibilidad
A.13.2.4	*Acuerdos de confidencialidad o no revelación*	*Control* *Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación*	SI	Por aseguramiento de la información, se deben definir los lineamientos de los acuerdos de confidencialidad a

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				nivel interno para colaboradores y/o proveedores
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información				
A.14.1 Requisitos de seguridad en los sistemas de información				
Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.				
A.14.1.1	*Análisis de requisitos y especificaciones de seguridad de la información*	*Control* *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.*	SI	Al adquirir nuevos sistemas de información o al cambiar los vigentes, el Oficial de Seguridad de la Información debe documentar los requisitos de seguridad en el documento de Especificaciones de requerimientos de seguridad
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 autorizadas.*	SI	Para garantizar la integridad, disponibilidad y confidencialidad de la información
A.14.1.3	*Protección de las transacciones de*	*Control* *La información involucrada en las transacciones de servicios de*	SI	Por aseguramiento de accesos a las aplicaciones, se deben

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
	servicios de aplicaciones	*aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.*		instalar certificados de seguridad que involucren transacciones
A.14.2 Seguridad en el desarrollo y en los procesos de soporte				
Objetivo: Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información.				
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.*	SI	Mediante la implementación de mecanismos de control se debe aplicar técnicas de programación para garantizar el desarrollo seguro
A.14.2.2	*Procedimiento de control de cambios en sistemas*	*Control* *La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.*	SI	Para garantizar el desarrollo seguro se debe controlar las técnicas de programación
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 garantizar que no existen efectos adversos en las*	SI	Para asegurar el correcto funcionamiento de los sistemas, una vez aplicados los cambios se debe realizar

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		operaciones o la seguridad de la organización.		pruebas y así llevar el control de versiones debidamente documentadas
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.*	SI	Cada cambio en el software debe considerar riesgos y se debe documentar los controles que se aplicaron
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.*	SI	Porque la seguridad de desarrollo se debe establecer en todas las capas de desarrollo de los nuevos sistemas
A.14.2.6	*Entorno de desarrollo seguro*	*Control* *Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.*	SI	Se debe implementar el ambiente de desarrollo seguro de modo que proteja adecuadamente los procesos y procedimientos suministrados a todos los colaboradores considerando el carácter de los datos, los controles de

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				seguridad, el control de acceso, entre otros.
A.14.2.7	*Externalización del desarrollo de software*	*Control* *El desarrollo de software externalizado debe ser supervisado y controlado por la organización.*	SI	Se debe supervisar y controlar a los desarrollos contratados externamente
A.14.2.8	*Pruebas funcionales de seguridad de sistemas*	*Control* *Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.*	SI	Se requiere del desarrollo de pruebas en los sistemas para verificar y preparara de manera detallada las actividades que permitan asegurar el funcionamiento óptimo durante el proceso del ciclo de desarrollo
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.*	SI	Para asegurar que el sistema realice los procedimientos adecuados que mitigue los riesgos y controle o evite cualquier tipo de vulnerabilidades, el resultado de estas pruebas deberán tener criterios de aceptación y debe ser confiables
A.14.3 Datos de prueba				

Objetivos de control y controles			**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**
Objetivo: Asegurar la protección de los datos de prueba				
A.14.3.1	*Protección de los datos de prueba*	*Control* *Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.*	SI	Porque se debe asegurar los datos operacionales de información (datos personales o cualquier dato que se considere confidencial), los cuales serán utilizados con propósitos de pruebas
A.15 Relación con proveedores				
A.15.1 Seguridad en las relaciones con proveedores				
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
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.*	SI	Porque es necesario controlar el acceso de los proveedores a la información de CEDIA y se debe exigir el cumplimiento de las políticas de seguridad existentes y acuerdos de confidencialidad
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*	SI	Para garantizar la confidencialidad, integridad y disponibilidad de la información suministrada a los

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		proporcionar componentes de la infraestructura de Tecnología de la Información.		proveedores, de manera que exista claridad en los acuerdos para ambas partes
A.15.1.3	*Cadena de suministro de tecnología 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.*	SI	Se debe incluir en los acuerdos, procesos de seguimiento, herramientas y el uso de buenas prácticas para validar que bienes y/o servicios cumplan con los requisitos de seguridad establecidos
A.15.2 Gestión de la provisión de servicios del proveedor				
Objetivo: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores				
A.15.2.1	*Control y revisión de la provisión de servicios del proveedor*	*Control* *Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor*	SI	Para asegurar el cumplimiento de los términos y condiciones de los requisitos de seguridad de la información, así mismo la gestión adecuada de los incidentes y problemas que se ocasionen durante la prestación del servicio o entrega del bien

Objetivos de control y controles			**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**
A.15.2.2	*Gestión de cambios en la provisión del servicio del proveedor*	*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 existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.*	SI	Es necesario gestionar los cambios en el suministro del servicio por parte de los proveedores, con el uso de mejores prácticas y controles de seguridad, teniendo en cuenta la criticidad de la información y los procesos del negocio involucrados para realizar una adecuada revaloración de los riesgos
A.16 Gestión de incidentes de seguridad de la información				
A.16.1 Gestión de incidentes de seguridad de la información y mejoras				
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.				
A.16.1.1	*Responsabilidades y procedimientos*	*Control* *Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.*	SI	Para la gestión adecuada, de los incidentes de seguridad de la información, que permitan asegurar una respuesta oportuna y eficaz
A.16.1.2	*Notificación de los eventos de*	*Control* *Los eventos de seguridad de la información se deben notificar por*	SI	Todos los colaboradores de CEDIA deben conocer

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
	seguridad de la información	*los canales de gestión adecuados lo antes posible.*		el procedimiento para reportar eventos de seguridad de la información a través de los canales establecidos para tal fin.
A.16.1.3	*Notificación de puntos débiles de la seguridad*	*Control* *Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.*	SI	Todos los colaboradores de CEDIA deben reportar cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios, para anticipar un incidente de seguridad
A.16.1.4	*Evaluación y decisión sobre los eventos de seguridad de 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.*	SI	Para determinar si los eventos de seguridad se clasificaran como un incidente de seguridad de la información
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.*	SI	Porque es necesario dar una respuesta inmediata y oportuna a los eventos presentados en CEDIA, gestionando

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				adecuadamente los incidentes de seguridad de la información, por tanto se debe controlar de acuerdo a los implementado y/o procedimientos establecidos
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 incidentes en el futuro.*	SI	Se deben utilizar mecanismos o herramientas que permitan realizar análisis e identificación temprana de los eventos detectados, que permitan minimizar el impacto o probabilidad de un incidente futuro
A.16.1.7	*Recopilación de evidencias*	*Control* *La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de la información que puede servir de evidencia.*	SI	Se requiere mantener las evidencias y/o soportes de los elementos o herramientas que permitan la identificación, preservación y

Objetivos de control y controles			**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**
				recolección de la información
A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio				
A.17.1 Continuidad de la seguridad de la información				
Objetivo: La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de la continuidad de negocio de la organización.				
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 la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.*	SI	Es necesario mantener actualizado las guías que contienen el plan de contingencia para cada uno de los servicios de CEDIA, con el fin de preservar la continuidad del negocio en caso de siniestro
A.17.1.2	*Implementar la continuidad de la seguridad de la información*	*Control* *La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.*	SI	Para asegurar el nivel de continuidad requerido en caso de una situación adversa
A.17.1.3	*Verificación, revisión y evaluación de la continuidad de la seguridad de la información*	*Control* *La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son*	SI	Es necesario la realización de simulacros que permitan verificar, revisar y evaluar el plan de contingencia y

Objetivos de control y controles			**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**
		válidos y eficaces durante situaciones adversas.		continuidad, con el fin de asegurar que su implementación sea válida y eficaz
A.17.2 Redundancias.				
Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información.				
A.17.2.1	*Disponibilidad de los recursos de tratamiento de la información*	*Control* *Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.*	SI	Es necesario implementar herramientas o procesos que permitan asegurar la disponibilidad, integridad y confidencialidad de la información y los sistemas de información de modo que se reduzcan o se mitiguen los riesgos a través de componentes o arquitecturas redundantes
A.18 Cumplimiento				
A.18.1 Cumplimiento de los requisitos legales y contractuales				
Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.				
A.18.1.1	*Identificación de la Legislación aplicable y de los*	*Control* *Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el*	SI	Para mantener la seguridad de la información

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
	requisitos contractuales	*enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.*		
A.18.1.2	*Derechos de Propiedad Intelectual (DPI)*	*Control* *Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios 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.*	SI	Es necesario implementar procedimiento apropiado que permita asegurar el cumplimiento de los requisitos legales relacionados con la propiedad intelectual y uso legal de software
A.18.1.3	*Protección de los registros de la organización*	*Control* *Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.*	SI	Para asegurar su integridad y protección de la información contra pérdida debido a cambios futuros
A.18.1.4	*Protección y privacidad de la información de carácter personal*	*Control* *Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.*	SI	Para garantizar la gestión adecuada de la protección de los datos por medio de la política y/o procedimientos que se

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
				encuentren establecidos
A.18.1.5	*Regulación de los controles criptográficos*	*Control* *Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.*	SI	Para garantizar la gestión adecuada de la protección de los datos por medio de la política y/o procedimientos que se encuentren establecidos
A.18.2 Revisiones de la seguridad de la información				
Objetivo: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.				
A.18.2.1	*Revisión independiente de la seguridad de la información*	*Control* *El enfoque de la organización para la gestión de la seguridad de la información y su implantación, 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 en la implantación de la seguridad.*	SI	Porque es necesario establecer controles que aseguren la correcta implementación y operación de la gestión de seguridad de la información en CEDIA
A.18.2.2	*Cumplimiento de las políticas y normas de seguridad*	*Control* *Los directivos deben asegurarse que todos los procedimientos de seguridad dentro de su área de*	SI	Porque se requiere evaluar el cumplimiento de las políticas,

Objetivos de control y controles			Aplicabilidad (SI/NO)	Justificación de elección / no elección
		responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable		procedimientos y demás requisitos de seguridad de la información para verificar eficiencia y eficacia de su implementación
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 información de la organización.*	SI	Porque se requiere evaluar el cumplimiento de las políticas, procedimientos y demás requisitos de seguridad de la información realizando pruebas de manera periódica a través de herramientas que permitan la interpretación y valoración de vulnerabilidades que puedan comprometer la seguridad de los sistemas.

Tabla 12 Declaración de Aplicabilidad para CEDIA de acuerdo a los Objetivos de control y controles de la Norma ISO/IEC 27002:2013

A continuación, y como resultado final se presenta un contexto de la situación actual de CEDIA según todas las cláusulas de la Tabla 12:

- Cláusula A5. Políticas de seguridad de la información: CEDIA cuenta con políticas de seguridad de la información sobre temas puntuales y la Dirección Ejecutiva ha designado a varios departamentos para continuar trabajando en la revisión e implementación de todas las políticas.
- Cláusula A6. Organización de la seguridad de la información: CEDIA cuenta con su personal con cargos y funciones asignados como se detalla en el organigrama y por dicha razón se está desarrollando las políticas para dicha cláusula.
- Cláusula A7. Seguridad relativa a los recursos humanos: CEDIA cuenta con su departamento de Talento Humano, quienes se encargan actualmente de revisar los antecedentes de cada persona que está por ingresar a la organización y se encarga de velar por los derechos y obligaciones tanto de CEDIA como de cada colaborador y están trabajando por implementar y socializar las políticas.
- Cláusula A8. Gestión de Activos: Cada colaborador recibe los activos para su respectivo cargo, la encargada para este trámite es el departamento Financiero quién lleva el registro de todos los activos entregados y devueltos. Además, cada departamento cuenta con el etiquetado de la información de acuerdo a lo indicado por la Dirección Ejecutiva y el área de Planificación y Gestión Estratégica.
- Cláusula A9. Control de acceso: CEDIA cuenta con un Directorio Activo donde se encuentra todos los colaboradores con su respectivo usuario, contraseña y permisos de acceso a la información.
- Cláusula A10. Criptografía: CEDIA emplea controles criptográficos bajo requerimiento.
- Cláusula A11. Seguridad física y del entorno: CEDIA cuenta con una infraestructura física y equipos seguros para el bienestar de sus colaboradores y para la misma organización.
- Cláusula A12. Seguridad de las operaciones: CEDIA cuenta con el área técnica, misma que se encarga de implementar los procedimientos operacionales, protección contra software malicioso, realiza el respaldo de información. Y dentro del área técnica se encuentra el Centro de Operaciones de Red (Siglas en inglés NOC) que se encarga de la mesa de ayuda para registros y supervisión de eventos tanto internamente como para los miembros de CEDIA.

- Cláusula A13. Seguridad de las comunicaciones: CEDIA gestiona la seguridad de los servicios de red e intercambio de información por medio del área técnica.
- Cláusula A14. Adquisición, desarrollo y mantenimiento de los sistemas de información: Dentro del área técnica se encuentra la Coordinación de I+D+i (Investigación + Desarrollo + innovación) con personal interno y externo que se encarga de desarrollar varios sistemas y para asegurar los mismos, cuenta con la Política de desarrollo seguro tanto para el ambiente de pruebas como de producción.
- Cláusula A15. Relación con proveedores: Cada departamento de CEDIA cuenta con sus respectivos proveedores, quienes para ser parte del mismo suscriben un contrato y un acuerdo de confidencialidad dependiendo el caso, de esta manera se puede gestionar la provisión de los servicios a contratar o contratados.
- Cláusula A16. Gestión de incidentes de seguridad de la información: CEDIA cuenta dentro del área técnica a la Coordinación de CSIRT, quienes se encargan de gestionar los incidentes, ellos mantienen informados y capacitados a todo el personal ante posibles y/o futuros incidentes que se debe hacer en cada caso.
- Cláusula A17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio: CEDIA se encuentra en la implementación de los procedimientos para la identificación de requisitos y política de continuidad del negocio.
- Cláusula A18. Cumplimiento: CEDIA cuenta con el área legal, quienes se encargan de revisar los requisitos legales, normativos, contractuales y de otra índole. Para los derechos de propiedad intelectual se cuenta con una persona experta dentro del área de Innovación y Transferencia Tecnológica quien se encarga de la revisión y gestión de Propiedad Intelectual.

6. CRONOGRAMA

No.	Actividad desarrollada	Recursos/Materiales/ Conocimientos Requeridos	Fecha Inicio	Fecha Fin	Horas requeridas
1	Estudio de los conceptos, fundamentos requeridos por un Sistema de Gestión de Seguridad de la Información y los objetivos y controles de seguridad.	Computadora Servicio de Internet Norma ISO/IEC 27001	22/abril/2021	30/mayo/2021	Tutor: 50 Estudiante: 50
2	Estudiar las diferentes metodologías para el análisis del riesgo.	Computadora Servicio de Internet	01/junio/2021	14/julio/2021	Tutor: 38 Estudiante: 38
3	Evaluar el riesgo de la metodología de riesgos de la NORMA ISO/IEC 27001 en los Servidores de la Nube de CEDIA	Computadora Servicio de Internet Servidores de la Nube de CEDIA Área Técnica de CEDIA	15/julio/2021	17/Agosto/2021	Tutor: 51 Estudiante: 51
4	Tratar el riesgo de la metodología de riesgos de la NORMA ISO/IEC 27001 en los Servidores de la Nube de CEDIA	Computadora Servicio de Internet Servidores de la Nube de CEDIA Área Técnica de CEDIA	18/agosto/2021	06/septiembre/2021	Tutor: 30 Estudiante: 30
5	Elaboración del análisis de la situación actual de CEDIA.	Computadora Servicio de Internet Todos los departamentos de CEDIA	07/septiembre/2021	27/septiembre/2021	Tutor: 32 Estudiante: 32

No.	Actividad desarrollada	Recursos/Materiales/ Conocimientos Requeridos	Fecha Inicio	Fecha Fin	Horas requeridas
6	Elaborar la matriz actual de los controles y objetivos del ANEXO A de la Norma ISO/IEC 27002:2013 para CEDIA	Computadora Servicio de Internet Área Técnica de CEDIA	28/septiembre/2021	24/octubre/2021	Tutor: 34 Estudiante: 34
7	Elaborar la matriz deseada de los controles y objetivos del ANEXO A de la Norma ISO/IEC 27002:2013 para CEDIA	Computadora Servicio de Internet Área Técnica de CEDIA	25/octubre/2021	16/noviembre/2021	Tutor: 34 Estudiante: 34
8	Estructurar las gráficas de la matriz actual y deseada de los controles y objetivos del ANEXO A de la Norma ISO/IEC 27002:2013 para CEDIA para el análisis de brechas	Computadora Servicio de Internet ANEXO A de la Norma ISO/IEC 27002:2013	17/noviembre/2021	06/diciembre/2021	Tutor: 30 Estudiante: 30
9	Elaborar el análisis de brechas de los controles y objetivos del ANEXO A de la Norma ISO/IEC 27002:2013 para CEDIA	Computadora Servicio de Internet ANEXO A de la Norma ISO/IEC 27002:2013	07/diciembre/2021	06/enero/2022	Tutor: 31 Estudiante: 31
10	Analizar el Anexo A (Normativo) Objetivos de control y controles de referencia de la Norma ISO/IEC 27002:2013 que cumple CEDIA	Computadora Servicio de Internet Anexo A de la Norma ISO/IEC 27002:2013 Todos los departamentos de CEDIA	07/enero/2022	20/enero/2022	Tutor: 30 Estudiante: 30

No.	Actividad desarrollada	Recursos/Materiales/ Conocimientos Requeridos	Fecha Inicio	Fecha Fin	Horas requeridas
11	Elaboración de la Declaración de la Aplicabilidad para CEDIA en base al Anexo A (Normativo) Objetivos de control y controles de referencia de la Norma ISO/IEC 27002:2013.	Computadora Servicio de Internet Anexo A de la Norma ISO/IEC 27002:2013	21/enero/2022	04/febrero/2022	Tutor: 40 Estudiante: 40
Total de horas de trabajo:					Tutor: 400 horas Estudiante: 400 horas

Tabla 13 Cronograma de actividades

7. PRESUPUESTO

DENOMINACIÓN	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
	unidades	dólares	dólares
1. Bienes			
Copias	20	0,01	0,20
Impresiones	50	0,05	2,50
2. Tecnológico			
Computador Portátil	1	800,00	800,00
3. Servicios			
Servicios de Internet	10	35,00	350,00
4. Personal			
Estudiante Investigador	1	800,00	800,00
Asesoría especializada UPS	1	1500,00	1500,00
Asesoría especializada CEDIA	3	1200,00	3600,00
5. Otros			
Imprevistos	1	150,00	150,00
Total			**$7.202,70**

Tabla 14 Presupuesto del trabajo de titulación

8. CONCLUSIONES

- Se puede concluir que seguridad de la información no solo se refiere a ciberseguridad o seguridad informática, puesto que un SGSI abarca tanto ese tipo de información como la que se encuentra en formato físico y de todas las áreas de la organización.
- CEDIA cuenta con activos muy importantes como cualquier organización, mismos que pueden estar expuestos a riesgos, los cuales no se reducen provocarían un gran problema dentro de la organización.
- Para reducir los riesgos se debe implementar una metodología de análisis de riesgo, en este caso se analizó la metodología de la ISO/IEC 27001, puesto que cuenta con la evaluación y tratamientos de riesgos.
- Para conocer en qué estado se encuentra CEDIA se realizó el análisis de brecha, misma que ayuda a conocer hasta dónde puede llegar la organización con el cumplimiento de las cláusulas de la Norma ISO/IEC 27001.
- Para implementar un Sistema de Gestión de Seguridad de la Información se debe definir qué políticas son aplicables o no de acuerdo al giro de negocio de cada organización, en el caso de CEDIA todos los controles son aplicables.
- CEDIA cuenta con controles de seguridad implementados, sin embargo, no existe una evidencia formal de los mismos debido a que no se encuentran documentados, a pesar de esto, si fueron tomados en cuenta en el análisis de brecha actual.

9. RECOMENDACIONES

- Se recomienda que CEDIA por medio de la Coordinación de CSIRT continúe con la toma de acciones para prevenir y detectar a tiempo las vulnerabilidades a las que está expuesta los sistemas de información, así como la información que maneja y genera cada colaborador.
- Cada área debe ser la responsable de documentar las políticas correspondientes a sus funciones, puesto que se tiene el apoyo de la Dirección Ejecutiva para la implementación del Sistema de Gestión de la Seguridad de la Información.
- Se debe socializar a todo el personal sobre el cumplimiento de cada política, puesto que ellos son los responsables para que CEDIA pueda continuar con la implementación del Sistema de Gestión de la Seguridad de la Información y de esta manera se pueda certificar en la norma ISO/IEC 27001.

10. REFERENCIAS BIBLIOGRAFÍAS

27001Academy. (2015). Plantilla para clientes de EPPS Services Ltd - Metodología de evaluación y tratamiento de riesgos. New York, Estados Unidos.

CEDIA. (6 de Febrero de 2020). RESOLUCION ESTATUTO CEDIA. Cuenca, Azuay, Ecuador.

Colegio Oficial de Ingenieros de Telecomunicación. (2012). Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001. Madrid.

CORPORACION ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA - CEDIA. (2021). *CEDIA*. Obtenido de HISTORIA: https://www.cedia.edu.ec/sobre-nosotros

Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Escuela Europea de Excelencia. (10 de Enero de 2019). *Cómo se relacionan ISO 27001 e ISO 31000*. Obtenido de Cómo se relacionan ISO 27001 e ISO 31000: https://www.escuelaeuropeaexcelencia.com/2019/01/como-se-relacionan-iso-27001-e-iso-31000/

ESIC BUSINESS & MARKETING SCHOOL. (Junio de 2020). *Definición de la ciberseguridad y su riesgo*. Obtenido de Definición de la ciberseguridad y su riesgo: https://www.esic.edu/rethink/tecnologia/definicion-ciberseguridad-riesgo

Excellence, I. (28 de Julio de 2015). *SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/2015/07/que-es-sgsi/

Huerta, A. (30 de Marzo de 2012). *SECURITY A(r)TWORK*. Obtenido de SECURITY A(r)TWORK: https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

Ideas y proyectos promocionales. (Enero de 2019). Plan de Gestión del Riesgo en la Seguridad de la Información. Madrid.

ISO/IEC 27002:2013, N. (2013). ANEXO A (Normativo) Objetivos de control y controles de referencia. Madrid, España.

ISO27000.es. (2005). *ISO27000.es*. Obtenido de Serie "27000": https://www.iso27000.es/iso27000.html

ISOTool Excellence. (18 de Abril de 2019). *¿Cómo realizar el análisis de riesgos según la norma ISO 27001?* Obtenido de ¿Cómo realizar el análisis de riesgos según la norma ISO 27001?: https://www.pmg-ssi.com/2019/04/como-realizar-el-analisis-de-riesgos-segun-la-norma-iso-27001/

ISOTools Excellence. (05 de Diciembre de 2013). *ISO 27001. El inventario de activos en la implementación de la norma*. Obtenido de ISO 27001. El inventario de activos en la implementación de la norma: https://www.isotools.org/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-norma-iso-27001/

ISOTools Excellence. (10 de Diciembre de 2013). *SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Obtenido de SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información: https://www.pmg-ssi.com/2013/12/iso27001-origen/

ISOTools Excellence. (s.f.). Las Claves del Éxito para la Gestión de Riesgos. España.

LISOT. (14 de Mayo de 2018). *¿Qué es un Sistema de Gestión de la Seguridad de la Información (SGSI)?* Obtenido de https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/#

López Neira, A., & Ruiz Spohr, J. (2005). *ISO27000.ES*. Obtenido de https://www.iso27000.es/sgsi.html

NORMAISO27001.es. (14 de Enero de 2021). *ISO 27001 QUE ES UN ANÁLISIS DE BRECHAS GAP EN ISO 27001*. Obtenido de ISO 27001 QUE ES UN ANÁLISIS DE BRECHAS GAP EN ISO 27001: https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/#

Normalización, A. E. (Mayo de 2017). Norma Española UNE-EN ISO/IEC 27001. Madrid.

PECB Group Inc. (2005). Implementador Lider Certificado en la ISO 27001. Reino Unido.

Pineda, I. E. (2021). ANÁLISIS DE RIESGOS: PROCESO, REGULACIONES Y METODOLOGIAS. Bogotá, Colombia.

PINZÓN, I. D. (2017). Tesis Maestría METODOLOGÍA PARA LA SELECCIÓN DE HERRAMIENTAS EFICIENTES Y PROTOCOLOS ADECUADOS PARA MEJORAR LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES. Cuenca, Ecuador.

Prisma Consultoría SAS. (11 de Septiembre de 2017). *EN45 SEGURIDAD DE LA INFORMACIÓN ISO 27001*. Obtenido de EN45 SEGURIDAD DE LA INFORMACIÓN ISO 27001: https://www.prismaconsultoria.com/en45-seguridad-la-informacion-iso-27001/

Prof. Edward J. Humphreys. (2013). *ISO, New version of ISO/IEC 27001 to better tackle IT security risks*. Obtenido de ISO, New version of ISO/IEC 27001 to better tackle IT security risks: https://www.iso.org/news/2013/08/Ref1767.html

Sanchez Contreras, A., & Otero Gutierrez, R. F. (Septiembre de 2013). *METODOLOGIA O HERRAMIENTAS PARA EL ANALISIS Y GESTION DE RIESGOS CRAMM, UNIVERSIDAD FRANCISCO DE PAULA SANTANDER*. Obtenido de https://slideplayer.es/slide/5503051/

Silva Coelho, F. E., Segadas de Araújo, L. G., & Bezerra, E. K. (s.f.). Gestión de la Seguridad de la Información. Bogotá, Colombia.

Un blog editado por ISOTools Excellence. (28 de Julio de 2015). *SGSI Blog especializado en Sistemas de Gestión de Seguridad de la información*. Obtenido de ¿Qué es un SGSI?: https://www.pmg-ssi.com/2015/07/que-es-sgsi/

Welivesecurity by ESET - ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia. (16 de Junio de 2015). Obtenido de Welivesecurity by ESET - ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/