FACULTAD DE ARQUITECTURA E INGENIERIAS

Trabajo de fin de carrera titulado:

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE GESTIÓN ECONÓMICA DE LA ARCOTEL, BASADA EN LAS NORMAS ISO 27002:2013 Y EGSI"

Realizado por:

Ing. María Luisa Perugachi Betancourt

Director del proyecto:

Ing. Verónica Rodríguez Arboleda, MBA.

Como requisito para la obtención del título de

MASTER EN CIBERSEGURIDAD

Quito, abril de 2020

DECLARACIÓN JURAMENTADA

Por la presente, yo, MARIA LUISA PERUGACHI BETANCOURT, con cédula de ciudadanía Nro. 1001886678, declaro bajo juramento, que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de esta declaración cedo mis derechos de propiedad intelectual de autora a la UNIVERSIDAD INTERNACIONAL SEK UISEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

MARIA LUISA PERUGACHI BETANCOURT

CC: 1001886678

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro que el presente trabajo de investigación titulado:

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE GESTIÓN ECONÓMICA DE LA ARCOTEL, BASADA EN LAS NORMAS ISO 27002:2013 Y EGSI"

Realizado por:

MARIA LUISA PERUGACHI BETANCOURT

Como requisito para la obtención del Título de

MASTER EN CIBERSEGURIDAD

Ha sido dirigido por mi persona a través de reuniones periódicas con la estudiante y cumple con todas las disposiciones que rigen los trabajos de titulación.

_____

Ing. Verónica Rodríguez Arboleda, MBA.

DIRECTORA DEL PROYECTO

CC: 1707522312

LOS PROFESORES INFORMANTES

Los profesores informantes:

Diego Riofrío Luzcando.

Christian Pazmiño Flores.

Después de revisar el trabajo han calificado

como apto para su defensa oral ante el tribunal examinador

_____	_____
Ing. Diego Riofrío, PhD	Ing. Christian Pazmiño, Msc.

Quito, abril de 2020

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es de mi autoría, que se han citado las fuentes correspondientes y que en su desarrollo se respetaron las disposiciones legales vigente, que protegen los derechos de autor.

_____

María Luisa Perugachi Betancourt

CC:1001886678

AGRADECIMIENTO

Al personal de la Universidad Internacional SEK, en la figura de los docentes de la Maestría de Ciberseguridad, por haberme impartido sus conocimientos, guiarme en la actualización tecnológica y brindarme la oportunidad de volver a las aulas y obtener nuevos conocimientos, que aspiro los pondré en beneficio de la sociedad ecuatoriana.

Un especial agradecimiento, a la Ing. Verónica Rodríguez, por dedicar su tiempo y conocimientos para el desarrollo de este trabajo de titulación.

DEDICATORIA

Este trabajo está dedicado a mis hijos Mateo, Pamela y Thomás quienes ofrecieron su tiempo para que pueda educarme, fueron mi inspiración y motivación en los momentos difíciles para cumplir mis objetivos académicos y profesionales.

Una especial dedicatoria a mi esposo Javier por su apoyo incondicional para la culminación de este proyecto.

A Dios por darme la oportunidad de cumplir mis metas, a mis padres y hermanos por incentivarme a continuar con mis estudios

RESUMEN

Este proyecto diseña una política de seguridad de la información para la Dirección de Gestión Económica de la Agencia de Regulación y Control de las Telecomunicaciones (Arcotel), con base en la norma ISO 27002:2013 y el EGSI, puesto que la entidad maneja información sensible de los operadores de servicios de telecomunicaciones, generando informes económicos, que son susceptibles de intrusiones, por ende, se requiere minimizar los riesgos a los que está expuesta la información; se analizó el estado actual de la seguridad de la información en la Dirección de Gestión Económica, se revisó la norma ISO 27002 y seleccionó la metodología Magerit de gestión de riesgos sugerida en el EGSI, para determinar los activos de la información y valorarlos respecto a la degradación de las características de confidencialidad, integridad y disponibilidad; como siguiente paso se identifican las amenazas y se valoran en cuanto a la probabilidad de ocurrencia y al impacto que causaría si las amenazas se materializan, debido a las vulnerabilidades que poseen los activos. Posteriormente, se evalúa el riesgo y se realiza el tratamiento de los mismos con las salvaguardas y controles de la ISO 27002:2013. Finalmente, se elabora la política de seguridad propuesta, que incluye aspectos generales y específicos para la mitigación de los riesgos de los activos, lo cual, se espera la aprobación por la ARCOTEL como parte del cumplimiento del EGSI v2.

Pablabras claves: Seguridad de la información, Magerit, Norma ISO 27002:2013, EGSI.

ABSTRACT

The objective of this thesis project is to design an Information Security Policy for the Directorate of Economic Management of the Telecommunications Regulation and Control Agency, based on ISO 27002: 2013 and the EGSI, due to information is managed sensitive of telecommunications service operators, which are susceptible to intrusions, in order to minimize the risks that information is exposed. It begins with the revision of the ISO 27002 standard, analysis of risk management Magerit methodology suggested in the EGSI, to determine the assets of the information and assess them regarding the degradation of the characteristics of confidentiality, integrity and availability; As a next step, threats are identified and assessed as to the probability of occurrence, the impact they would cause if the threats materialize is also evaluated, due to the vulnerabilities of the assets; Next, the irrigation is evaluated and its treatment is carried out with the safeguards, selecting the appropriate controls provided by ISO 27002: 2013. Finally, the proposed policy is elaborated, which includes general and specific aspects for the mitigation of the risks of the assets, with this it is expected to be approved by ARCOTEL as part of the compliance with EGSI v2.

Keywords: Security information, Magerit methodology, Standard ISO 27002:2013, EGSI.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

1 El problema de investigación

1.1 Planteamiento del problema

La Dirección Técnica de Gestión Económica es parte de la Coordinación Técnica de Títulos Habilitantes en la Agencia de Regulación y Control de las Telecomunicaciones y es responsable del manejo de la información sensible y confidencial que entregan los operadores de servicios de telecomunicaciones (ARCOTEL, 2017).

Dicha información constituye la base para la generación de informes con los cuales se establecen obligaciones económicas de los prestadores de servicios de telecomunicaciones, por lo cual es necesario conservar las características de confidencialidad, integridad y disponibilidad para mejorar su gestión.

La información es procesada, manipulada y analizada de forma manual por diferentes funcionarios de la Dirección de Gestión Económica de la ARCOTEL, siendo susceptible de intrusiones debido al fácil acceso por parte de todos los funcionarios de esa área; ya que no existen niveles de accesos priorizados, contraseñas en los archivos, lo que genera vulnerabilidad y alto riesgo de amenazas a la información que se gestiona. No existen mecanismos que protejan las

características de la información, generando procesos de liquidación de valores, complicaciones en la administración y reclamos por parte de los operadores de telecomunicaciones.

Con el crecimiento de nuevos prestadores de servicios de telecomunicaciones, cada vez es mayor la información a ser procesada y analizada, la gestión de seguridad de la información por parte de los funcionarios de la Dirección de Gestión Económica de la ARCOTEL no garantiza la conservación de las dimensiones de la información, debido a que pueden producirse cambios en los datos de los informes generados con afectación de recursos para el Estado y los operadores de telecomunicaciones, por lo que de persistir el fácil acceso a la información y la manipulación de la misma, aumenta el riesgo y la vulnerabilidad de alterar sus características; afectando a los informes que son el resultado de su gestión y de la institución.

A fin de evitar esta problemática y mejorar la gestión y seguridad de la información enviada por los prestadores de telecomunicaciones, se requieren controles que permitan conservar su integridad, puesto que los informes económicos que se elaboran, requieren que la información sea confiable y no esté modificada. Los controles serán parte de una política de seguridad que se desarrolla bajo el estándar ISO/IEC 27002:2013.

1.2 Objetivos

1.2.1 Objetivo general

Diseñar una política de seguridad de la información para la Dirección de Gestión Económica de la ARCOTEL basada en las normas ISO 27002:2013 y en el EGSI, que permita la disponibilidad, integridad y confidencialidad de los datos.

1.2.2 Objetivos específicos

- Identificar el estado actual de los procesos de recolección de información en la Dirección de Gestión Económica de la ARCOTEL, mediante entrevistas y encuestas a los funcionarios de diferente nivel jerárquico, que permitan la identificación de vulnerabilidades en la seguridad de la información.
- Analizar las vulnerabilidades de la información de la Dirección de Gestión Económica, mediante la aplicación de una matriz de gestión de riesgos, identificando y valorando los activos; además categorizando las amenazas y el impacto causado.
- Establecer los controles de seguridad mediante el análisis de la norma ISO 27002: 2013 que servirán para el diseño de la política de seguridad de la información de la Dirección de Gestión Económica de la ARCOTEL.
- Elaborar la política de seguridad de la información de la Dirección de Gestión Económica de la ARCOTEL, mediante los controles seleccionados de la norma ISO 27002: 2013 y del Esquema Gubernamental de Seguridad de la Información EGSI, que permitan conservar la integridad, confidencialidad y disponibilidad de la información.

1.3 Formulación del problema

En la Dirección de Gestión Económica de ARCOTEL se elaboran informes económicos para que los operadores de telecomunicaciones paguen al Estado sus obligaciones; pero, debido a controles insuficientes y a los niveles de acceso y procedimientos inadecuados para salvaguardar la información, los datos para elaborar los informes han presentado fallas de seguridad informática, así como inconsistencias en las diferentes aplicaciones que posee la institución.

1.4 Justificación

La Dirección de Gestión Económica – DGE de la ARCOTEL, se encarga de recopilar, procesar y analizar la información financiera, entregada por los operadores de telecomunicaciones, misma que debe ser confiable, integra y disponible, pues es la base de los estudios sobre los cuales se determinan los informes de obligaciones de pago para el Estado, que son susceptibles de procesos de revisión por parte de la Contraloría General del Estado.

Además, al ser una entidad pública, está obligada a cumplir con el Esquema de Gestión de Seguridad de la Información EGSI versión 2, emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL, mediante acuerdo Nro. 25 de 10 de enero de 2020.

El disponer de una política de seguridad de la información en la Dirección de Gestión Económica en ARCOTEL, ésta permitirá mitigar las vulnerabilidades y disminuir el impacto de los riesgos que presenta la gestión de la información, evitando la intrusión de agentes internos y externos a la organización, reduciendo futuros reclamos de operadores de telecomunicaciones y evitando egresos para el Estado.

Para desarrollar la política se gestionarán los riesgos de los activos de información críticos para lo cual se escogió la norma ISO 27002:2013, ya que esta versión se adapta al tamaño de la organización, proporcionando directrices y buenas prácticas para la seguridad de la información. La particularidad de esta norma es permitir seleccionar controles para implementar un Sistema de Gestión de Seguridad de la Información SGSI, lo cual facilitará el desarrollo de la política de seguridad de la información de la Dirección de Gestión Económica de la ARCOTEL.

1.5 Estado del Arte

Existe literatura sobre la seguridad de la información y su importancia en las organizaciones, así como documentos y directrices de la alta dirección sobre este tema para entidades públicas y privadas.

En las entidades del Estado que dependen del poder Ejecutivo, se dispone del Acuerdo Ministerial Nro. 25 emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información -MINTEL, que reemplazó al Acuerdo Nro. 166 emitido por la Secretaría Nacional de la Presidencia que define al esquema gubernamental de seguridad de la información EGSI, para las entidades ecuatorianas que dependan de la Función Ejecutiva (Secretaría Nacional, 2013), instrumento que señala el uso de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información y su implementación, la cual dependerá de cada institución, su tamaño, estructura orgánica, ámbito de acción, nivel de madurez en gestión de seguridad de la información.

Algunos trabajos sobre políticas de la seguridad de la información, en entidades públicas o gubernamentales, se basan en la norma ISO 27002. Según Ledezma (2015) las instituciones que requieren proteger la gestión institucional y su información emiten políticas de seguridad sobre las plataformas tecnológicas y los sistemas de información; según Gallardo (2018) el diseño de una política de seguridad de la información en una institución pública debe basarse en el esquema gubernamental de seguridad de la información.

Para algunas entidades del sector educativo, que gestionan gran cantidad de información de alumnos y plataformas virtuales, se han diseñado políticas de seguridad de la información basada

en la Norma ISO 27002 versión 2013, como el Departamento de Tecnología de la Información y la Comunicación de la Universidad Técnica de Ambato (Torres & López, 2015).

De manera análoga, la política de seguridad para el departamento de TICS del Instituto Tecnológico Superior Central Técnico (ITSCT), tiene como referencia la norma ISO/IEC 27002:2013 MAGERIT como metodología para identificar y gestionar los riesgos de la información (Cevallos, 2019).

De acuerdo a Sangoluisa (2015) para el establecimiento de políticas de seguridad de la información para el servicio de correo electrónico y de videoconferencia de la Presidencia de la República se ha realizado el análisis de algunas metodologías para gestión de riesgos de la seguridad de la información como: MAGERIT, FRAAP, OCTAVE-ALLEGRO; que ayudan a distinguir áreas de impacto y activos críticos de la organización.

Para las entidades del sector salud, Puga (2019) en la propuesta de la política de seguridad en un área específica de un hospital, resalta el uso de las referencias de las normas ISO 27000 e ISO 27799, que permiten identificar amenazas de la información en el área sanitaria, para lo cual se deben establecer controles para mitigar riesgos y su impacto.

En el sector de telecomunicaciones, la política de seguridad de la información del Ministerio de Telecomunicaciones y de la Sociedad de la Información, está basada en el Acuerdo Ministerial 166, con base en la norma ISO/IEC 27000 y en la norma de Gestión del Riesgo de Seguridad de la Información INEN ISO/IEC 27005, aspecto que deberá ser actualizado sobre la base del Acuerdo Ministerial Nro, 25 con la emisión del EGSI v2 (MINTEL, 2016).

Respecto a los objetivos de una política de seguridad de la información, según LSE (2019) *Information Security Policy*, que se utiliza en la Escuela de Economía de Londres (LSE), la política debe englobar a todos los dispositivos que almacenan información, hardware, software, tanto a nivel de estudiantes como información que está en la nube. Con la política de seguridad de la información se protegerá la confidencialidad, la integridad y la disponibilidad en un entorno de trabajo de sistemas de información.

CAPÍTULO II

MARCO TEÓRICO

2.1 Seguridad de la Información

Se define seguridad de la información, a la protección de la información de un amplio espectro de amenazas, que permitan asegurar la continuidad del negocio, reduciendo el riesgo e incrementando el retorno de la inversión y oportunidades comerciales (ISO27002, 2013).

Se define seguridad de la información a las medidas y controles que protegen la información y sistemas de información del acceso no autorizado, uso o modificación, conservando su confidencialidad, integridad y disponibilidad de los sistemas de información, durante el procesamiento, almacenamiento y manipulación (CNSSI- Committee on National Security Systems, 2015).

2.1.1 Dimensiones de la información

Las propiedades o dimensiones de la información, corresponde a la denominada triada de seguridad CIA por sus siglas en inglés *confidentiality*, *integrity*, *availability*, confidencialidad, integridad y disponibilidad, además del no repudio y responsabilidad ante terceros, los cuales son fundamentales para guiar las directrices de seguridad de la información de cualquier institución (SSCI-Certified Information Systems Security Professional, 2012).

Según MAGERIT Ministerio de Hacienda y Administraciones Públicas (2012), se definen así:

2.1.2 Confidencialidad

Es la dimensión que limita el acceso a la información, para ser accesible únicamente al personal autorizado, si ésta se pierde se ve afectada la confianza en la organización.

2.1.3 Integridad

Es la dimensión que garantiza que la información no sea manipulada o modificada, que se encuentre en las condiciones en las que fue creada.

2.1.4 Disponibilidad

Esta característica indica que la información y servicios estén siempre accesibles y disponibles en el tiempo cuando se requieran.

2.2 Riesgos de los sistemas informáticos

2.2.1 Administración del Riesgo

En las guías para la certificación profesional del sistema de seguridad de la administración *Certified Information System Security Professional* – CISSP, "los riesgos primero deben evitarse o mitigarse, evitarlo implica implementar controles de seguridad de la información". (Krause & Tipton, 2007, pág. 32)

Según Baud (2015) el riesgo, es el análisis de una situación que le puede ocurrir a un activo, es una amenaza o vulnerabilidad, a fin de entender los efectos y posibles consecuencias para la

organización o sociedad en general. Otro concepto asociado al riesgo es el análisis del impacto en el negocio, *Business Impact Analysis* que constituye el documento que va a identificar los efectos o impactos de una catástrofe en la organización; para lo cual se debe listar las actividades indispensables de la organización para desarrollar su negocio (Baud, 2015, pág. 208).

Un efecto del riesgo se explica como una desviación de lo "esperado" sin explicar si ésta es una expectativa matemática, una mejor suposición, pronóstico o una vista sobre lo que debería suceder (Leitch, 2010).

2.2.2 Vulnerabilidad

La vulnerabilidad es la probabilidad que una amenaza suceda en un activo de la organización, consecuentemente es el porcentaje de riesgo asociado a cada activo del servicio, lo cual es complicado y subjetivo" (Baud, 2015, pág. 208).

Conocer dónde existen las vulnerabilidades permitirá a una organización utilizar un enfoque basado en el riesgo para gestionar éstas y reducirlas (O'Hanley & Tiller, 2013).

2.2.3 Amenazas

Según Baud (2015), una amenaza es una acción, situación o hecho que puede obstaculizar el buen funcionamiento de un activo de servicio o de un conjunto de activos de servicios.

En los sistemas de información, amenaza es un evento capaz de provocar un impacto negativo en la organización (Estado, personas o activos) a través del acceso no autorizado, denegación de servicios, modificación, destrucción o divulgación de información (Kiseel, 2013).

2.3 Las normas ISO

Utilizando la metodología de lo general a lo particular, previo a describir la Norma ISO/IEC 27002:2013, se revisó en contexto las normas ISO, las cuales corresponden a normas creadas por la Organización Internacional de Normalización ISO y Comisión Electrotécnica Internacional IEC (ISO27000, 2005).

Son estándares internacionales, que están orientadas para ser utilizadas en entidades y organizaciones de diferente tamaño, tipo y jerarquía, sin embargo, hay que precisar el dominio que abarcan en cada una de las organizaciones.

Para referirse a la versión de una norma, es necesario conocer que en la nomenclatura el año que está adjunto al estándar corresponde de la publicación de la revisión más reciente de la norma, en este sentido se utilizó la norma ISO 27002 que viene de la familia de las normas ISO 27000, versión 2013. A continuación, se resume estas normas.

2.3.1 La familia de la norma ISO 27000.

La familia de normas ISO 27000, están orientadas a la seguridad de la información, que incluye aspectos de técnicas de seguridad, así como las tecnologías y gestión de seguridad de la información, ayudando a entidades y organizaciones de diferente tamaño a implementar su sistema de gestión de seguridad de la información (ISO27000, 2005).

2.3.1.1 La norma ISO 27001:2013

Este estándar especifica los requisitos genéricos aplicables a cualquier organización, para establecer y mantener un sistema de gestión de seguridad de la información, incluyendo la evaluación y el tratamiento de los riesgos de su seguridad (ISO27001, 2013).

2.3.1.2 La norma ISO 27002:2013

La norma ISO/IEC 27002:2013, está relacionada con la guía de buenas prácticas para la seguridad de la información de las organizaciones, proporcionando controles para la gestión de sus riesgos (ISO27002, 2013).

El estándar puede utilizarse en cualquier tipo de organización que tenga como objetivo desarrollar o implementar un SGSI. La versión 2013 del estándar describe 14 áreas o dominios principales para la seguridad de la información de una organización, posee 35 objetivos de control y 114 controles, de los cuales se debe elegir los que más se ajusten a la organización, a continuación, se resume estos dominios de seguridad (ISO27002, 2013).

1. Políticas de Seguridad: son la directrices, políticas o decisiones de alto nivel adoptadas por el nivel jerárquico de una organización para la seguridad de la información.
2. Organización de la Seguridad de la Información: se refiere a la organización interna y como se asigna funciones y responsabilidades de los roles que están vinculados a la seguridad de la información.
3. Seguridad en Recursos Humanos: concientizar, capacitar y educar al personal, durante su contratación; y en la fase previa, investigar sus antecedentes; en la desvinculación del personal se debe deshabilitar sus privilegios y accesos.

4. Gestión de los Activos: se refiere a la información exclusivamente, ya que es un activo y es uno de los más importantes en la organización, sugiere revisar su clasificación, el inventario, la responsabilidad sobre dichos activos, así como los soportes para su almacenamiento.
5. Control de Accesos: este dominio se asocia a los requisitos que una organización debe adoptar para el control de accesos de los usuarios a la información y los sistemas, asignar los privilegios correspondientes, así como las responsabilidades de estos usuarios.
6. Cifrado: es la gestión de claves o uso de criptografía para proteger la información que posee una entidad.
7. Seguridad Física y Ambiental: se refiere a establecer áreas seguras para proteger la información, por ejemplo, delimitar el área de los datacenter y añadir controles físicos para su ingreso; así como establecer zonas de oficina restringidas y públicas; además de definir políticas para bloqueo de pantalla.
8. Seguridad de las Operaciones: se basa en los procedimientos que se deben adoptar en la organización para proteger contra malware o software malicioso; este dominio sugiere realizar auditorías a los sistemas de información, software y aplicaciones, sus respaldos.
9. Seguridad de las Comunicaciones: se refiere a la seguridad que deben cumplir las redes de comunicación, de datos, cableado.
10. Adquisición de sistemas, desarrollo y mantenimiento: es la seguridad de la información en el desarrollo de software y aplicaciones informáticas de la organización.
11. Relaciones con los Proveedores: se refiere a las medidas de seguridad de la información que debe existir en las relaciones de la organización con terceros, para conservar el sigilo de la información con proveedores y cadena de suministros.

12. Gestión de Incidencias que afectan la Seguridad de la Información: es la gestión que realiza la organización cuando se produce un incidente relacionado con la seguridad de su información, incluyendo el tratamiento y plan de mejoras.
13. Gestión para continuidad del negocio: se basa en la capacidad de la organización para volver a su ritmo de trabajo habitual, luego de haber sufrido un incidente de seguridad de la información, para lo cual deben aplicar planes de continuidad.
14. Conformidad: se refiere a la socialización y concienciación, que debe tener el personal de una organización al conocer y aplicar conforme a las exigencias legales y políticas que existan en torno a la seguridad de su información.

2.3.1.3 La norma ISO/IEC 27003:2017

Este estándar inicialmente fue publicado en 2010 y la versión corregida actual es 2017; es un estándar que se utiliza en cualquier tipo de organización, refiere aspectos de ciberseguridad, seguridad de la información, sus activos críticos e incluye protección a la privacidad n (ISO27003, 2017).

2.3.1.4 La norma ISO/IEC 27004:2016

Este estándar es aplicable a una organización de cualquier tamaño e índole, proporciona pautas destinadas a evaluar el desempeño, así como hace seguimiento al SGSI que una organización tenga implementado (ISO27004, 2016).

2.3.1.5 La norma ISO/IEC 27005

Este estándar está orientado a la gestión del riesgo en la seguridad de la información, incluye actualizaciones de requisitos y conceptos generales basados en la norma ISO/IEC 27001:2013 y no se trata de una metodología para gestión de riesgos (ISO27005, 2018).

2.4 Esquema gubernamental de seguridad de la información EGSI v2

Con Acuerdo Ministerial Nro. 25, emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, publicado el 10 de enero de 2020, se expide el Esquema Gubernamental de Seguridad de la Información EGSI versión 2, señalando que su implementación es obligatoria en las instituciones de la administración pública (MINTEL, 2020). Este decreto derogó el Acuerdo 166 emitido el 25 de septiembre de 2013, en el cual se estableció en su artículo uno el "*uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información en las entidades de la administración pública*." (Secretaría Nacional, 2013).

2.5 Política de Seguridad

La política de seguridad es un documento administrativo de alto nivel y de carácter obligatorio, en el cual se establecen los objetivos estratégicos y principios de seguridad de la información que deben ser seguidos en cualquier actividad que afecte el entorno de la organización y en donde se definen las responsabilidades y roles para todos los actores involucrados (ISACA, 2016).

Políticas de seguridad son entendidas como la normativa de diferente jerarquía que se encargan de custodiar la seguridad informática de una organización (Agencia Europea Ciberseguridad, 2019).

2.6 Metodologías para la Gestión del Riesgo

Una vez que se ha analizado las normas ISO familia 27000, en este trabajo se propone utilizar los controles de la norma 27002 con base a lo señalado en el Estado del Arte y trabajos revisados anteriormente, previo a ello es necesario contar con el análisis de la gestión de los riesgos de la información basados en una determinada metodología. Existen algunas metodologías para la gestión de riesgos en sistema de información, como MAGERIT, CRAMM, NIST 800-30, OCTAVE, normas ISO 31000, ISO 27005 (Leitch, 2010).

Las fases de análisis de los riesgos dependen de la metodología utilizada, de acuerdo a INCIBE (2005) existen pasos del proceso que son comunes, independientemente de la metodología aplicada, lo cual se muestra en la figura 1.

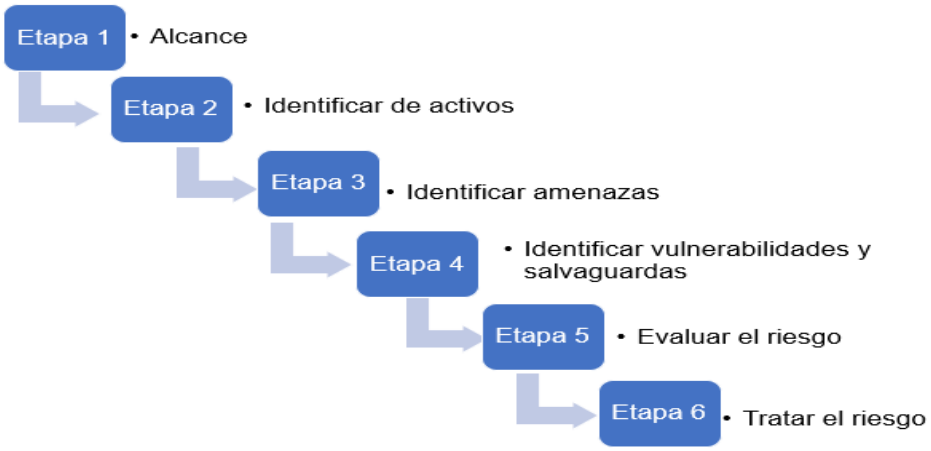

*Figura 1.*Etapas del análisis de riesgo.
Fuente: INCIBE (2015)

2.6.1 MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas - MAGERIT, desarrollada por el Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales del Gobierno Español (Ministerio de Hacienda y Administraciones Públicas, 2012).

Consiste en analizar y gestionar el riesgo, iniciando con la definición del alcance, clasificando los activos de la información de la organización, identificando amenazas y vulnerabilidades, proponiendo salvaguardas, evaluando el impacto del riesgo y proponiendo medidas oportunas para mantener el riesgo bajo control con la selección de los controles adecuados de la norma ISO 27002:2013, de modo que la organización esté en las mejores condiciones para someterse a procesos de auditoría y certificación.

La secuencia del proceso de análisis de riesgo de la metodología MAGERIT, se describe en la figura 2, que inicia con la identificación de los activos.

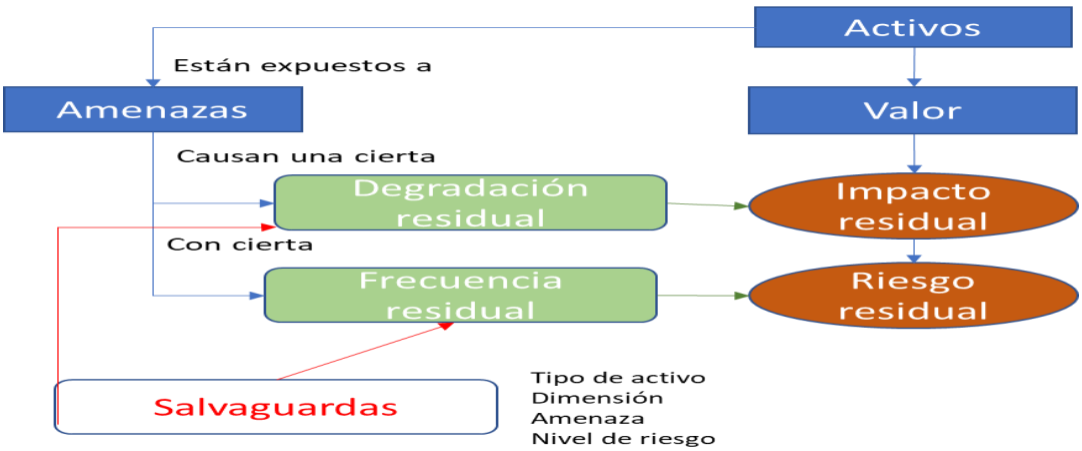

Figura 2 Análisis de riesgo de MAGERIT.
Fuente: Ministerio de Hacienda y Administraciones Públicas (2012).

2.6.1.1 Activos

El primer paso consiste en la identificación de todos los activos relevantes para la organización, clasificados por: servicios, datos, sistemas de información, software, aplicaciones, hardware, respaldos, equipamiento, instalaciones, redes de comunicaciones, climatización, sistemas de energía, como se muestra en la tabla 1.

Tabla 1 *Clasificación de activos según MAGERIT*

Activo	Descripción
[S] Servicio	Los servicios, se pueden determinar internamente cuando se producen dentro del reparto y se determinan como externos cuando se consume de otras unidades o proveedores.
[D] Datos/información	Los datos son soportes de información que los usuarios los deben valorar. Su clasificación debe determinar los niveles de confidencialidad y el valor que los califica.
[SW] Aplicaciones (software)	Las aplicaciones se refieren a programas, aplicativos, desarrollos, entre otros. Estos van ligados con la automatización de los procesos actividades y tareas.
[HW] Equipos informáticos (hardware)	Se refiere a los bienes materiales o físicos que son de utilidad para la unidad y que pueden ser reemplazados si fuera así la necesidad.
[COM] Redes de comunicaciones	Se refiere a la infraestructura de comunicaciones sobre redes.
[SI] Soporte de información	Se refiere a los dispositivos de almacenamiento de datos.
[AUX] Equipamiento auxiliar	Se refiere al equipamiento que complementa el material informático, apoyando la infraestructura de la unidad.

Activo	Descripción
[L] Instalaciones	Las instalaciones, son los lugares donde se encuentra la infraestructura tecnológica.
[P] Personal	Corresponde al talento humano involucrado con los procesos y tareas de sistemas de información dentro de la organización.

Elaborado por la autora de la investigación.
Fuente: Ministerio de Hacienda y Administraciones Públicas (2012), págs. 16-26.

Identificados y clasificados los activos, se los evalúa en función del impacto de la pérdida de las dimensiones de la información: confidencialidad, integridad, disponibilidad, utilizando los valores que se muestran en la tabla 2, definidos con base al EGSI v2, criterios que serán analizados en la valoración de los activos en la Dirección Técnica de Gestión Económica de la ARCOTEL.

Tabla 2 *Criterios de valoración de activos*

VALOR	CONFIDENCIALIDAD
Bajo (1)	La información puede ser utilizada por todos, su divulgación no tiene efecto.
Medio (2)	La información puede ser conocida y utilizada por un grupo de personas que la necesiten para realizar su trabajo, su divulgación tiene efecto limitado para la institución.
Alto (3)	La información puede ser conocida y utilizada por un grupo limitado de personas, su divulgación podría causar efecto crítico en la institución.
VALOR	**INTEGRIDAD**
Bajo (1)	La modificación no autorizada o destrucción de la información, podría causar un daño leve a la institución; puede repararse.
Medio (2)	La modificación no autorizada o destrucción de la información, podría causar un daño significativo a la institución, es difícil reparar.
Alto (3)	La modificación no autorizada o destrucción de la información, no podría repararse, ocasiona perjuicio severo a la institución.

VALOR	CONFIDENCIALIDAD

VALOR	DISPONIBILIDAD
Bajo (1)	La inaccesibilidad a la información o sistemas tiene un efecto leve para la institución.
Medio (2)	La inaccesibilidad a la información o sistemas tiene un efecto significativo para la institución.
Alto (3)	La inaccesibilidad a la información o sistemas tienen un efecto severo a la institución.

Elaborado por la autora de la investigación.
Fuente: MINTEL (2020)

El valor referencial del activo será:

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

Donde: C es confidencialidad.

I es integridad.

D es disponibilidad.

2.6.1.2 Amenazas

Posteriormente se describe las amenazas, que son aquellas situaciones que puede afectar a los activos de la información, causando un impacto o perjuicio a la institución, se escoge de un catálogo de amenazas que se muestra en la tabla 3 del libro de MAGERIT (Ministerio de Hacienda y Administraciones Públicas, 2012).

Tabla 3. *Clasificación de amenazas del catálogo de MAGERIT*

Amenazas	Tipo
Desastres naturales	- Fuego, daños por agua, desastres naturales

Amenazas	Tipo
De origen industrial	- Avería de origen físico o lógico - Suspensión del servicio eléctrico - Condiciones inadecuadas de temperatura o humedad - Interrupción de los servicios de comunicaciones - Interrupción de otros servicios y suministros esenciales - Fallas en el respaldo de la información.
Errores y fallos no intencionados	-Errores de usuarios, del administrador, de monitorización -Errores de configuración; de mantenimiento - Fuga de información - Vulnerabilidades de software - Actualización de software y hardware
Ataques intencionados	- Abuso de privilegios de acceso - Difusión de software dañino - Redireccionamiento de mensajes - Acceso no autorizado - Interceptación de información - Destrucción, divulgación de información - Manipulación de programas, de equipos - Denegación de servicio - Robo - Indisponibilidad del personal - Ingeniería social
Nuevas amenazas XML	-Sintaxis -Esquema

Elaborado por la autora de la investigación.
Fuente: Ministerio de Hacienda y Administraciones Públicas (2012)

Las amenazas deben ser valoradas en degradación de las dimensiones de la información, por cada activo, en la frecuencia de ocurrencia y en el impacto que puede causar la amenaza al activo de información. La frecuencia puede ser muy frecuente, poco frecuente, diario, semanal, mensual; una misma amenaza puede afectar a uno o varios activos. Para cuantificar la probabilidad de ocurrencia de las amenazas se utiliza la tabla 4.

Tabla 4 *Criterios de valoración de la probabilidad de ocurrencia de las amenazas*

VALOR	PROBABILIDAD DE OCURRENCIA
Bajo (1)	La probabilidad que la amenaza se materialice es poco frecuente (>0 y <50%).
Medio (2)	La probabilidad que la amenaza se materialice es medianamente frecuente (-50%).
Alto (3)	La probabilidad que la amenaza se materialice es muy frecuentemente, es probable (> 50%).

Elaborado por la autora de la investigación.
Fuente: MINTEL (2020)

2.6.1.3 Estimación del Impacto

Considerando que el impacto es una medida del daño causado a un activo, debido a la materialización de la amenaza, cuando es explotada una vulnerabilidad, es necesario estimar el impacto sobre el activo de información. (Ministerio de Hacienda y Administraciones Públicas, 2012) Para cuantificar se utiliza la valoración de la tabla 5.

Tabla 5 *Criterios de valoración del impacto causado por la explotación de las amenazas*

VALOR	IMPACTO
Bajo (1)	Si la amenaza se materializa, no hay consecuencias relevantes
Medio (2)	Si la amenaza se materializa, las consecuencias son relevantes.
Alto (3)	Si la amenaza se materializa, hay consecuencias graves

Elaborado por la autora de la investigación:
Fuente: Ministerio de Hacienda y Administraciones Públicas (2012)

En la figura 3, se representa la relación entre amenazas, vulnerabilidades y el impacto que causan en los activos.

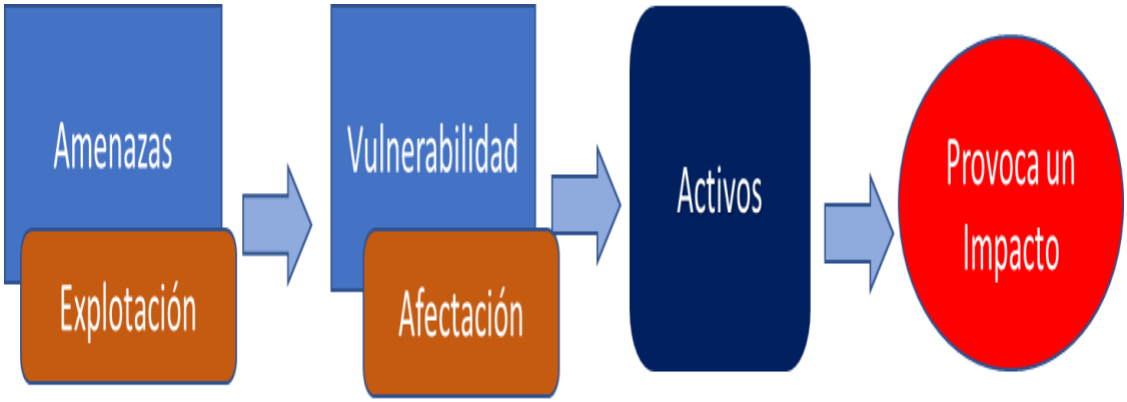

Figura 3 Interrelación de amenaza, vulnerabilidad, activo e impacto.
Fuente: INCIBE (2015).

2.6.1.4 Determinación y cuantificación del riesgo

La cuantificación del riesgo de los activos identificados depende de la degradación causada al activo por cada amenaza y según la frecuencia de ocurrencia, es una estimación de lo que puede suceder (Ministerio de Hacienda y Administraciones Públicas, 2012).

La valoración del nivel del riesgo se calcula:

Riesgo = Probabilidad (amenaza) * Impacto (causado)

Para su cuantificación puede utilizarse la tabla 6 donde se representa cinco niveles cualitativos de riesgo, que serán el resultado de la multiplicación del valor de la probabilidad de ocurrencia de la amenaza multiplicado por el valor del impacto.

Tabla 6 Valoración cualitativa del riesgo de MAGERIT

PROBABILIDAD	IMPACTO	RIESGO
Alto	Alto	Muy Alto
Alto	Medio	Alto
Alta	Bajo	Medio

PROBABILIDAD	IMPACTO	RIESGO
Media	Alto	Medio
Medio	Medio	Medio
Medio	Bajo	Bajo
Bajo	Alto	Medio
Bajo	Medio	Bajo
Bajo	Bajo	Muy Bajo

Elaborado por la autora de la investigación.
Fuente: Ministerio de Hacienda y Administraciones Públicas (2012)

Otra forma de cuantificar el riesgo se muestra en la tabla 7, donde la valoración de 9 corresponde a un riesgo muy alto cuando la probabilidad de ocurrencia es alta y el impacto que cause en el activo es alto, mientras que el valor de 1 corresponde a un riesgo muy bajo, cuando la probabilidad de ocurrencia es baja y el impacto que causa en el activo también es bajo.

Tabla 7 *Resumen de valoración cuantitativa y cualitativa del riesgo*

TABLA DE RIESGO				
		PROBABILIDAD		
		Bajo	Medio	Alto
IMPACTO	Alto	Medio (3)	Alto (2)	Muy alto (9)
	Medio	Bajo (2)	Medio (4)	Alto (6)
	Bajo	Muy bajo (1)	Bajo (2)	Medio (3)

Elaborado por la autora de la investigación.
Fuente: Ministerio de Hacienda y Administraciones Públicas (2012).

2.6.1.5 Salvaguardas o contramedidas

Constituye otro paso en la gestión de riesgos, una vez estimado los riesgos, las salvaguardas son los elementos de defensa tecnológicos tendientes a reducir riesgos, para que las amenazas no causen tanto daño en la organización. Las salvaguardas se realizan para el tratamiento de los riesgos y son para mitigar, reducir, transferir o aceptar el riesgo.

Posteriormente, se deberá revisar impacto residual que se produce cuando hay tareas por completar como salvaguardas inadecuadas o insuficientes controles, así como gestionar el riesgo residual que es aquel que continua degradando el activo, una vez que se tomaron las salvaguardas y se realiza nuevamente los cálculos del riesgo con el impacto residual y la nueva frecuencia (Ministerio de Hacienda y Administraciones Públicas, 2012).

2.6.2 Otras metodologías para análisis de gestión de riesgos.

2.6.2.1 CRAMM

CRAMM: *Risk Analysis and Management Method* Metodología para Análisis y Gestión de Riesgos, desarrollada por la *Central Communication and Telecommunication Agency* del Reino Unido, la metodología de la gestión de riesgo consiste en tres fases: en la primera se identifican los activos físicos y el software valorando en relación al impacto en la organización; en la segunda se identifica las amenazas y vulnerabilidades que afectan al sistema; en la tercera fase de evaluación, se seleccionan las medidas de seguridad (El Fray, 2012).

Según El Fray (2012) la metodología CRAMM incluye una librería con medidas de seguridad orientadas a proteger los sistemas de información, esta metodología se resume en la figura 4.

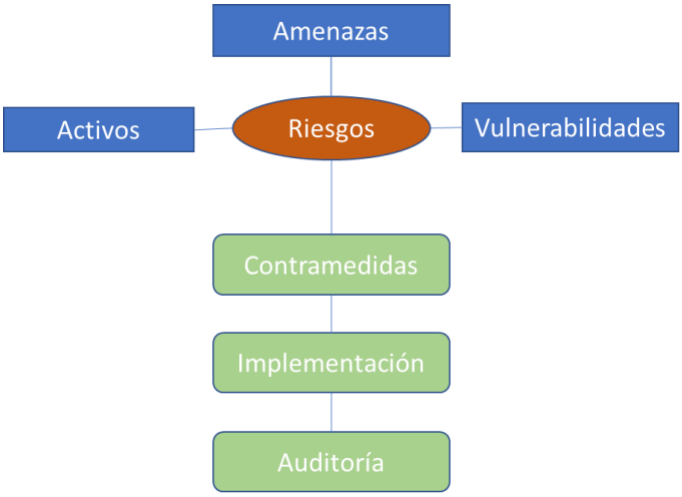

Figura 4 Enfoque metodología CRAMM.
Fuente: El Fray (2012).

2.6.2.2 OCTAVE

Esta metodología para gestión de riesgos denominada *Operationally Critical, Threat, Asset and Vulnerability Evaluation* OCTAVE, desarrollada por el *Software Engineering Institute - SEI*, consiste en analizar varios criterios para evaluar los riesgos tecnológicos de la organización con el factor de riesgo; incluye la situación de la organización, planificación de medidas y reducción de riesgos, combinando un argumento comercial para la gestión de los riesgos cibernéticos; posee una herramienta denominada OCTAVE-FORTE (Alberts, Dorofee, Stevens, & Woody, 2003).

2.6.2.3 NIST 800-30

Esta guía para evaluación del riesgo es desarrollada por el *National Institute of Standards and Technology* del Departamento de Comercio de Estados Unidos, consiste en analizar el riesgo utilizando el concepto de amenaza en sistemas de información, considerando cualquier evento como un acceso no autorizado, denegación de servicios, modificación o pérdida de información;

sin embargo el modelo no contempla los procesos, los activos y dependencias (National Institute of Standars and Technology-NIST, 2012). En la tabla 8 se muestran las fases de esta metodología.

Tabla 8 *Pasos de la metodología NIST SP 800-30:*

Pasos	**Descripción**
Enmarcar el riesgo	Identificar el propósito y alcance de la evaluación, los supuestos, limitaciones y prioridades bajo los cuales se evalúa los riesgos; Identificar fuentes de información y el impacto si ésta es usada.
Evaluar el riesgo	Identificar las amenazas (activos o personas) y vulnerabilidades (internas y externas) a la organización, determinando la probabilidad del daño causado.
Responder el riesgo	Desarrollando y evaluando cursos de acción alternativos y apropiados de tolerancia al riesgo.
Seguimiento del riesgo	Monitorear los factores de riesgo, sus cambios y actualizar la evaluación del riesgo basado en el monitoreo de resultados.

Elaborado por la autora de la investigación.
Fuente: National Institute of Standars and Technology-NIST (2012)

CAPÍTULO III

SITUACIÓN ACTUAL

3.1 Agencia de Regulación y Control de las Telecomunicaciones.

Es una entidad pública creada por la Ley Orgánica de Telecomunicaciones el 18 de febrero de 2015, publicada en el Registro Oficial Nro.439, su gestión está anexa al Ministerio de las Telecomunicaciones y de la Sociedad de la Información (Ley 439, 2015).

> La Agencia de Regulación y Control de las Telecomunicaciones, es la entidad encargada de la administración, regulación y control de las telecomunicaciones y del espectro radioeléctrico y su gestión, así como de los aspectos técnicos de la gestión de medios de comunicación social que usen frecuencias del espectro radioeléctrico o que instalen y operen redes. (Ley 439, 2015, artículo 142)

La gestión de la Agencia de Regulación y Control de las Telecomunicaciones, es muy importante en el entorno digital en el Ecuador, puesto que es la entidad que autoriza los permisos para prestación de servicios de telecomunicaciones, estaciones de radio y televisión, audio & video por suscripción, operación de redes privadas, posibilitando que los ciudadanos accedan a la tecnología y los servicios, potenciando los ingresos de los ciudadanos y del país a través de la recaudación de ingresos por dichas autorizaciones.

Según el Estatuto Organizacional por Procesos emitido en el año 2016, que asigna las atribuciones y responsabilidades para la gestión de la Agencia, tiene como misión y visión lo siguiente:

Misión:

> Regular y controlar, el uso del espectro radioeléctrico y los servicios de telecomunicaciones, garantizando el derecho de los usuarios a acceder a servicios de calidad, convergentes, con precios y tarifas equitativas; así como gestionar los recursos inherentes a las telecomunicaciones mediante su asignación transparente, equitativa, eficiente y ambientalmente sostenible. (ARCOTEL, 2017, pág. 4).

Visión:

> Ser la Institución que garantice la gestión y desarrollo soberano y efectivo del régimen general de las telecomunicaciones y del espectro radioeléctrico, a través de la administración, regulación y control de las telecomunicaciones como sector estratégico, que contribuya al buen vivir. (ARCOTEL, 2017, pág. 4).

3.1.1 La Dirección de Gestión Económica DGE

La Dirección de Gestión Económica es parte de la Coordinación Técnica de Títulos Habilitantes, misma que es considerada un área que agrega valor a los procesos de la Institución, parte de la estructura de ARCOTEL se muestra en la figura 5; en el Estatuto de la Agencia, consta la misión de la Dirección de Gestión Económica la siguiente:

"Ejecutar y controlar los procesos para la liquidación, reliquidación de las obligaciones económicas y la gestión económica financiera de títulos habilitantes, mediante el cumplimiento del ordenamiento jurídico vigente, las políticas y lineamientos emitidos para optimizar la recaudación de los ingresos" (ARCOTEL, 2017, pág. 33).

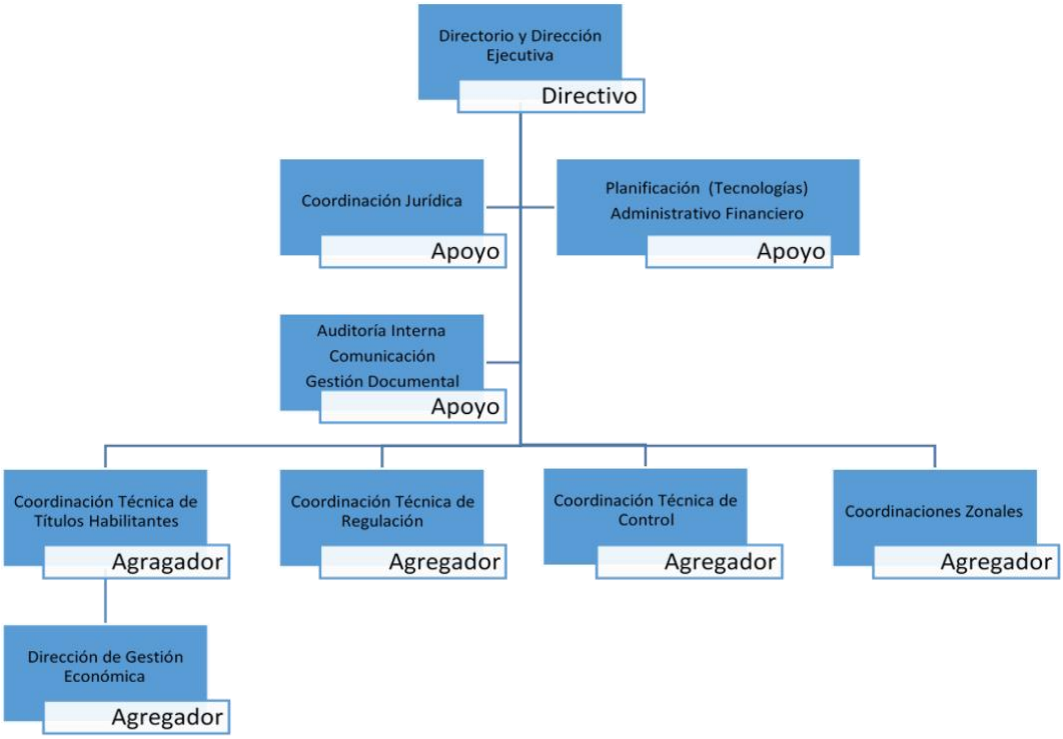

Figura 5 Organigrama resumido de ARCOTEL, donde consta la DGE.
Fuente: ARCOTEL (2017).

Con la emisión del EGSI v2 a través del Acuerdo 25 de 2020, que reemplaza al Acuerdo Ministerial Nro. 166, es necesario emitir una política de seguridad de la información acorde al Esquema Gubernamental de Seguridad de la Información. La Dirección Técnica de Gestión Económica motivo de este estudio, no posee una política de seguridad de su información, sin embargo, la organización ha emitido un proceso basado en el Acuerdo Ministerial 166 de 2013,

que refiere a las Normas ISO/IEC 27002, el cual no ha sido actualizado, con socialización insuficiente a los funcionarios y su implementación es parcial.

Por tal situación, en este trabajo se presenta una propuesta de política o directrices para asegurar su información, basada en la norma técnica ISO/IEC 27002:2013, la cual viene acompañada previamente del análisis de riesgo de los activos, con relación a las amenazas y vulnerabilidades de la información, que se genera en los procesos de la Dirección Técnica de Gestión Económica de la ARCOTEL, área escogida por la relevancia del trabajo que realiza para cumplir con la misión de la organización.

Debe mencionarse que el EGSI v2 dispone que en el plazo de cinco meses se realizó una evaluación de los riesgos en cada institución que dependen del gobierno central y en siete meses la actualización o implementación de los controles de los riesgos que se identificaron, razón por la cual, este trabajo contribuirá a que la ARCOTEL cumpla con el Acuerdo 25.

3.2 De los servicios de telecomunicaciones que deben cumplir obligaciones de pago

La Dirección Técnica de Gestión Económica de la ARCOTEL, debe realizar los informes, de la gestión económica financiera de los títulos habilitantes, los cuales se clasifican en servicios de telecomunicaciones, radiodifusión, entidades de certificación.

Con el incremento de prestadores de servicios de telecomunicaciones a través del otorgamiento de nuevos títulos habilitantes, la elaboración de los informes económicos va en crecimiento y el consiguiente volumen de trabajo. En la tabla 9 de muestra los títulos habilitantes de telecomunicaciones y audio y vídeo por suscripción que están vigentes a diciembre de 2019.

Tabla 9 *Títulos habilitantes de telecomunicaciones 2019*

SERVICIOS DE TELECOMUNICACIONES	**AUTORIZACIONES**
Servicio Móvil Avanzado-SMA (telefonía móvil)	3
Telefonía Fija-STF	6
Servicio Portador-SP	22
Servicio de Acceso a Internet-SAI	587
Servicio Comunal	472
Servicio Troncalizado	3
Transporte Internacional-TI	14
Cable Submarino-CS	3
Telecomunicaciones Móviles por Satélite-TMS	17
Audio y Video A&V	277

Elaborado por la autora de la investigación.
Fuente: ARCOTEL (2020).

El número de informes que deben ser elaborados ha incrementado en el período 2015 - 2019, razón por la cual es necesario realizar una planificación conforme clasificación de servicios, de acuerdo con el volumen de ingresos que representan los pagos para el Estado, concentrando su esfuerzo en el servicio móvil avanzado que ha sido sujeto de exámenes especiales por parte de la Contraloría General del Estado.

En la figura 6, se muestra una proporción del crecimiento de información en función del número de títulos habilitantes de los servicios, otorgados en el período 2015 al 2020, representado un 9,6% de incremento en el período.

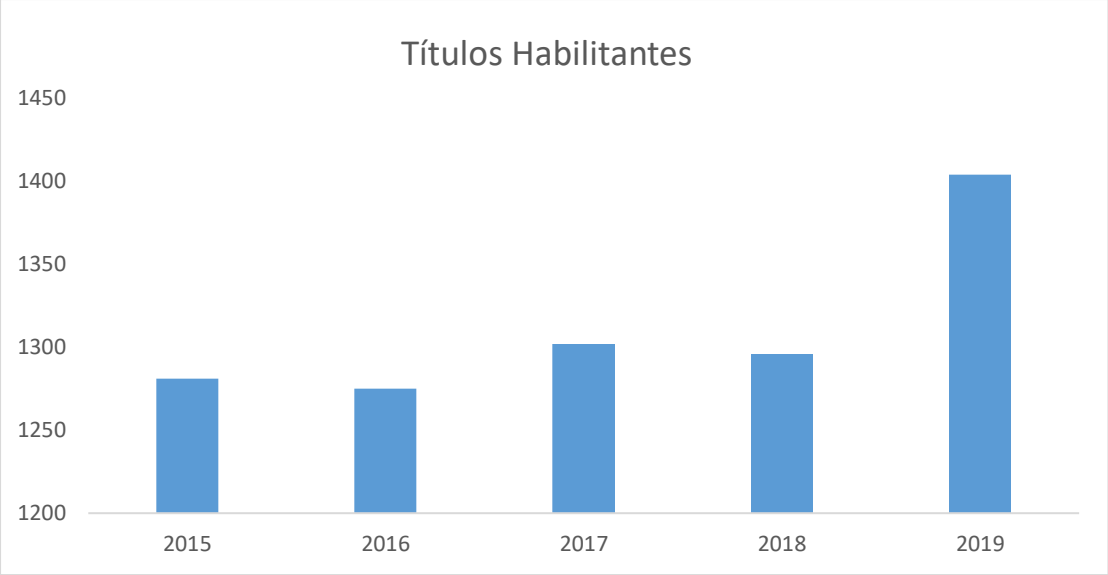

Figura 6 Títulos habilitantes de telecomunicaciones emitidos en el período 2015-2019

Fuente: ARCOTEL (2020)

3.3 La Seguridad de la información en la DGE

Para identificar el estado de seguridad que posee la información de los activos en la Dirección Técnica de Gestión Económica DGE, información tanto física como digital, se aplicó una encuesta a 13 funcionarios de la DGE, 4 de la Dirección Técnica de Títulos de Servicios de Telecomunicaciones, 1 de la Dirección de Tecnologías de la Información; contando con la autorización de la máxima autoridad de la organización, en este caso del Director Ejecutivo de la ARCOTEL que se encontraba ejerciendo el cargo en agosto de 2019, así como el seguimiento de las actividades por parte de la Asesora Institucional, lo cual se encuentra documentado a través de los memorandos ARCOTEL-CRDM-2019- 0143-M de 27 de agosto de 2019 y ARCOTEL-CRDM-2019- 0184-M de 8 de noviembre de 2019, adjuntos en el Anexo 1; dentro de la DGE se entrevistó al Director y a tres funcionarios con roles operativo y experto; en la Dirección de Tecnologías de la Información se entrevistó a un funcionario responsable del proceso denominado

infraestructura donde está el data center; se realizó inspección física de los equipos informáticos, visita al data center del edificio matriz.

De las encuestas cuyo formato está en el anexo 2 y entrevistas se obtuvo los siguientes resultados.

- El personal desconoce que existe un documento procedimental relacionado con la política de seguridad de la información en aplicación del EGSI Acuerdo 166 de 2013, el cual no ha sido difundido y tampoco aplicado, sin embargo, señalan que es necesaria emitir una política de seguridad para minimizar los riesgos internos y externos de fuga de información y mantener sigilo de la información.
- Los archivos físicos son de fácil acceso, se encuentran en archivadores a los cuales pueden acceder todos los funcionarios.
- El acceso físico a las instalaciones de la DGE no está restringido con control de acceso, puesto que, si bien existen los dispositivos al ingreso principal de las oficinas, éstos no funcionan.
- Falta implementar un proceso adecuado y organizado del archivo de la información digital, las carpetas no están codificadas con una nomenclatura determinada y son de fácil acceso para el personal de dicha Dirección.
- No se han implementado procesos o metodologías adecuadas para el respaldo de la información digital.
- No se han implementado procesos o metodologías para almacenar la información digital en el servidor NAS, en los computadores, en discos y dispositivos externos.
- Falta implementar un procedimiento para el tratamiento de la información considerada como confidencial o restringida.

- No existe cambios de contraseñas del computador con una frecuencia determinada.
- Ocasionalmente, las computadoras no están bloqueadas para su acceso durante el receso del almuerzo o ausencia temporal en la jornada de trabajo.
- No existen procesos automáticos de recolección de información para evitar modificaciones y manipulaciones.
- Las claves de acceso al computador a veces son compartidas entre funcionarios para continuar realizando los trabajos diarios.

3.4 Aplicación de metodología para análisis y gestión de riesgos

Para el análisis de la gestión de riesgos de la información de la Dirección de Gestión Económica de la ARCOTEL, tanto la física como la digital, se utilizará la metodología MAGERIT descrita en el capítulo anterior, así mismo, con base en la Guía para la gestión de riesgo, dispuesto en el Acuerdo Ministerial Nro. 25 del EGSI v2, por ser una entidad pública de la administración central.

3.4.1 Alcance

El análisis de riesgos se enfocará en las amenazas y vulnerabilidades que puede sufrir la información que se genera en los procesos de la Dirección Técnica de Gestión Económica de la ARCOTEL, de forma que se garantice la confidencialidad, integridad y disponibilidad de dicha información, para lo cual se analizará también la infraestructura informática del edificio matriz donde funciona la Dirección Técnica de Gestión Económica.

3.4.2 Reconocimiento de los activos

Se identificaron los activos de información más relevantes y críticos que posee la Dirección de Gestión Económica DGE, utilizando la clasificación del catálogo de elementos, libro 1 y libro 2 de

MAGERIT, con el uso de las plantillas de INCIBE (INCIBE - Instituto Nacional de Ciberseguridad, 2015).

- **Servicios (S)**: Facturación y obligaciones económicas; Gestión asignación de frecuencias; Registro Público; Respaldos y digitalización, Gestión parque informático; Correo Institucional; Almacenamiento información; Registro Público, Internet.
- **Datos e información (D)**: Bases de datos, Documentos internos; documentos confidenciales;
- **Aplicaciones (Software) (SW)**: SIFAF, OnBase, ESPECTRA, Quipux, SACOF; Windows.
- **Equipos informáticos (HW):** Equipos PCs -Laptops, access point AP, Servidores de rack HP, routers, firewall, switchs de piso, switchs de core, scaners, impresoras.
- **Redes de comunicaciones (COM):** red local LAN estructurada, privada virtual-VPN, inalámbrica, red telefónica (VoIP).
- **Soporte de información (SI):** almacenamiento en NAS de red, cintas, discos duros externos.
- **Equipo auxiliar (AUX)**: generador eléctrico, fuentes de alimentación.
- **Instalaciones (L)**: Data center, oficinas.
- **Personal (P)**: funcionarios roles operativo y jerárquico de la DGE y analista de tecnología TI del edificio matriz.

Cada activo se asociará a un proceso informático definido en el Estatuto Orgánico por Procesos de la ARCOTEL, siendo: Soporte Técnico; Desarrollo/aplicaciones; Infraestructura.

Posteriormente se aplicará la valoración según la confidencialidad C, integridad I, disponibilidad D y finalmente obtener el nivel de criticidad mediante (C+I+D)/3, lo cual se muestra en las tablas 10 a la 18.

En la tabla 10 se muestra la valoración de los activos clasificados en Servicios, aquellos que tienen valor igual a 3, constituyen los activos más críticos; se determina que el respaldo y digitalización; facturación y obligaciones económicas; y la gestión de asignación de frecuencias son los activos críticos que posee la ARCOTEL en esta clasificación.

Tabla 10 *Activo: Servicios*

TIPO	ID.	ACTIVO	PROCESO	C	I	D	CRITICIDAD
Servicios	S1	Respaldo y digitalización	Soporte Técnico	3	3	3	3,0
	S2	Facturación y obligaciones económicas	Desarrollo/aplicaciones	3	3	3	3,0
	S3	Gestión asignación de frecuencias	Infraestructura	3	3	3	3,0
	S4	Gestión parque informático	Soporte Técnico	2	3	3	2,7
	S5	Correo Institucional	Infraestructura	3	2	3	2,7
	S6	Almacenamiento información	Infraestructura	2	2	3	2,3
	S7	Registro Público	Desarrollo/aplicaciones	2	3	2	2,3
	S8	Internet	Infraestructura	2	2	3	2,3

Elaborado por la autora de la investigación.

En la tabla 11 se muestra la cuantificación de los activos clasificados en datos e información; los que tienen valor igual a 3, constituyen los activos más críticos que posee la DGE en esta clasificación, se determina que son: bases de datos y documentos internos.

Tabla 11 *Datos e información*

TIPO	IDENT.	ACTIVO	PROCESO	C	I	D	CRITI-CIDAD

Datos e	D1	Bases de datos	Desarrollo/aplicaciones	3	3	3	3
Informa-ción	D2	Documentos internos	Infraestructura	3	3	3	3
	D3	Documentos Confidenciales	Infraestructura	3	2	3	2,7
	D4	Documentos Públicos	Infraestructura	1	2	3	2

Elaborado por la autora de la investigación.

En la tabla 12 se establece la cuantificación de los activos clasificados en aplicaciones y software; los que tienen valor igual a 3, constituyen los activos más críticos que posee la DGE en esta clasificación, se determina que son: el sistema SIFAF y SPECTRA.

Tabla 12 *Aplicaciones*

TIPO	IDENT.	ACTIVO	PROCESO	C	I	D	CRITI-CIDAD
Aplicaciones (Software)	SW1	SIFAF	Desarrollo/aplicaciones	3	3	3	3,0
	SW2	SPECTRA	Mantenimiento	3	3	3	3,0
	SW4	OnBase	Mantenimiento	2	3	3	2,7
	SW5	Quipux	Desarrollo/aplicaciones	2	3	3	2,7
	SW6	SACOF	Desarrollo/aplicaciones	2	3	3	2,7
	SW7	Windows	Soporte Usuario	2	3	3	2,7

Elaborado por la autora de la investigación.

La tabla 13 indica la cuantificación de los activos clasificados en equipos informáticos, los que tienen valor igual a 3, constituyen los activos más críticos que posee la DGE en esta clasificación, se determina que son: computadoras y laptos, access point y servidores de rack.

Tabla 13 *Equipos informáticos*

TIPO	ID.	ACTIVO	PROCESO	C	I	D	CRITICI-DAD
Equipos Informáticos	HW1	Computadoras y laptops	Mantenimiento	3	3	3	3,0
	HW2	Access point	Mantenimiento	3	3	3	3,0
	HW3	Servidores de rack	Mantenimiento	3	3	3	3,0
	HW4	Router	Infraestructura	2	3	3	2,7
	HW5	Switchs de piso y de core	Infraestructura	2	3	3	2,7
	HW6	Escaners e impresoras	Infraestructura	2	3	2	2,3

Elaborado por la autora de la investigación.

La tabla 14 indica la cuantificación de los activos clasificados en redes de comunicaciones, los que tienen valor igual a 3, constituyen los activos más críticos que posee la DGE en esta clasificación, se determina que es la red LAN.

Tabla 14 *Redes de Comunicaciones*

TIPO	ID.	ACTIVO	PROCESO	C	I	D	CRITICI-DAD
Redes de Comunicaciones	COM 1	Red LAN	Infraestructura	3	3	3	3,0
	COM 2	Red inalámbrica	Infraestructura	2	3	3	2,7
	COM 3	Red VPN	Infraestructura	2	3	3	2,7
	COM 4	Red telefónica	Infraestructura	2	2	3	2,3

Elaborado por la autora de la investigación.

En la tabla 15 se muestra la valoración de los activos clasificados en soporte de información, los que tienen valor igual a 3, constituyen los activos más críticos que posee la DGE en esta

clasificación se encuentran los respaldos en el servidor de almacenamiento de red (NAS) y en cintas.

Tabla 15 *Soporte de información*

TIPO	ID.	ACTIVO	PROCESO	C	I	D	CRITICI-DAD
Soporte de Información	SI1	Almacenamiento en red -nas	Mantenimiento	3	3	3	3,0
	SI2	Cintas	Mantenimiento	3	3	3	3,0

Elaborado por la autora de la investigación.

En la tabla 16 se muestra la valoración de los activos clasificados en equipamiento auxiliar, los que tienen valor igual a 3, constituyen los activos más críticos que posee la DGE en esta clasificación, sin determinarse activos que correspondan a este nivel de criticidad.

Tabla 16 *Equipo auxiliar*

TIPO	ID.	ACTIVO	PROCESO	C	I	D	CRITICI-DAD
Equipamiento Auxiliar	AUX 1	Generador eléctrico	Mantenimiento	2	3	3	2,7
	AUX 2	Fuentes de alimentación	Mantenimiento	2	3	3	2,7

Elaborado por la autora de la investigación

En la tabla 17 se muestra la valoración de los activos clasificados en instalaciones, los que tienen valor igual a 3, constituyen los activos más críticos que posee la DGE en esta clasificación, se determina que es el data center.

Tabla 17 *Instalaciones*

TIPO	ID.	ACTIVO	PROCESO	C	I	D	CRITICIDAD
Instalaciones	L1	Data Center	Infraestructura	3	3	3	3,0
	L2	Oficinas	Infraestructura	2	3	3	2,7

Elaborado por la autora de la investigación.

En la tabla 18 se muestra la valoración de los activos clasificados en personal, los que tienen valor igual a 3, constituyen los activos más críticos que posee la DGE en esta clasificación, se determina que son: el personal con rol de jefe y analistas del edificio matriz.

Tabla 18 *Personal*

TIPO	ID.	ACTIVO	PROCESO	C	I	D	CRITICI-DAD
Personal	P1	Analistas DGE y TI edificio matriz	Rol operativo	3	3	3	3,0
	P2	Jefe DGE	Rol jerárquico	3	3	3	3,0

Elaborado por la autora de la investigación.

3.4.3 Matriz de amenazas a las que están expuestos los activos

Se construye la matriz de amenazas a las que están expuestos los activos, utilizando el catálogo de amenazas de MAGERIT, descritas en el capítulo II, las escogidas serán valoradas en degradación de las dimensiones de la información, asociada con la frecuencia de ocurrencia, para determinar qué tan probable es que se materialice la amenaza. Se puede escoger una amenaza para uno o varios activos de la información de la Dirección de Gestión Económica. La tabla 19 indica la valoración cualitativa y cuantitativa de cuan probable es que una amenaza ocurra; la valoración cuantitativa por cada activo se muestra en las tablas de la 20 a la 28.

Tabla 19 *Valoración de la probabilidad de amenazas*

Valor	Probabilidad ocurrencia de amenaza
Bajo (1)	Poco frecuente (año)
Medio (2)	Medianamente frecuente (mes)
Alto (3)	Muy frecuente (semanal)

Elaborado por la autora de la investigación basado en el EGSI v2

La tabla 20 muestra la valoración de las amenazas en los activos de la clasificación denominada Servicios, para lo cual se utiliza la nomenclatura S1 (respaldo y digitalización), S2 (facturación y obligaciones económicas), S3 (gestión asignación de frecuencias), S4 (gestión parque informático), S5 (correo institucional), S6 (almacenamiento de información).

Tabla 20 *Valoración de probabilidad de amenazas del activo Servicios*

N°	**AMENAZA**	**SERVICIOS**					
		S1	S2	S3	S4	S5	S6
1	Fuego	1					1
2	Daños por agua	2					2
3	Suspensión del servicio eléctrico	2	2	2	2	2	2
4	Inadecuadas condiciones de temperatura	1	1		1	1	1
5	Interrupción de los servicios de comunicaciones	2	2	2	2	2	2
6	Averías por fallos físicos o lógicos	1	1	1	1	1	1
7	Fuga de información	2	1	2			
8	Acceso no autorizado		2	2			
9	Corrupción de la información	1	1				
10	Errores de los usuarios	2	2	2	2	2	2
11	Errores de configuración	1					
12	Fallas en el respaldo de la información	3	3	3			3

Elaborado por la autora de la investigación.

La tabla 21 indica las amenazas a los que están expuestos los activos clasificados como Datos e Información, D1 (bases de datos), D2 (documentos internos), D3 (documentos confidenciales), D4 (documentos públicos).

Tabla 21 *Valoración de probabilidad de amenazas del activo Datos e Información*

N°	AMENAZA	DATOS			
		D1	D2	D3	D4
1	Daños por agua	1	1	1	1
2	Suspensión del servicio eléctrico	2	2	2	2
3	Inadecuadas condiciones de temperatura	1	1	1	1
4	Interrupción de los servicios de comunicaciones	3	3	3	3
5	Desastres industriales	1	1	1	1
6	Fuga de información	1	1	1	1
7	Fallas en el respaldo de la información	3	3	3	3

Elaborado por la autora de la investigación.

La tabla 22 indica las amenazas a los que están expuestos los activos clasificados como Aplicaciones, SW1 (SIFAF), SW2 (OnBase), SW3 (SPECTRA), SW4 (Quipux), SW5 (SACOF), SW6 (Windows).

Tabla 22 *Valoración de probabilidad de amenazas del activo Aplicaciones.*

N°	AMENAZA	APLICACIONES					
		SW1	SW2	SW3	SW4	SW5	SW6
1	Suspensión del servicio eléctrico	2	2	2	2	2	2
2	Interrupción de los servicios de comunicaciones	2	2	2	2	2	2
3	Desastres industriales	2	2	2	2	3	2
4	Errores de los usuarios	3	1	3	1	2	2
5	Errores del administrador					1	1
6	Errores de configuración	2	1	1	1	2	2
7	Fallas en el respaldo de la información	2	3	2	2	3	3
8	Errores de mantenimiento / actualización de programas (software)	2				2	

Elaborado por la autora de la investigación.

La tabla 23 indica las amenazas a los que están expuestos los activos clasificados en Equipos informáticos, HW1 (computadoras y laptops), HW2 (access point), HW3 (servidores de rack), HW4 (router), HW5 (switchs de piso y de core), HW6 (escaners e impresoras).

Tabla 23 *Valoración de probabilidad de amenazas del activo Equipos Informáticos*

N°	AMENAZA	EQUIPOS INFORMÁTICOS					
		HW1	HW2	HW3	HW4	HW5	HW6
1	Fuego	1	1	1	1	1	1
2	Daños por agua	2	2	2	2	2	2
3	Suspensión del servicio eléctrico	1	1	1	1	1	1
4	Condiciones inadecuadas de temperatura o humedad	1	1	1	1	1	1
5	Interrupción de los servicios de comunicaciones	2	2	2	2	2	2
6	Desastres industriales	1	1	1	1	1	1
7	Fuga de información	2	1	1	1	1	1
8	Vulnerabilidad de programas (software)	3	3				
9	Corrupción de la información	3	2	1	1	1	1
10	Fallas en el respaldo de la información	3					

Elaborado por la autora de la investigación

La tabla 24 indica las amenazas a los que están expuestos los activos clasificados en Redes de comunicaciones, COM1 (red LAN), COM2 (red inalámbrica), COM3 (red privada virtual VPN), COM4 (red telefónica).

Tabla 24 *Valoración de probabilidad de amenazas del activo Redes de comunicaciones*

N°	AMENAZA	REDES DE COMUNICACIONES			
		COM1	COM2	COM3	COM4
1	Fuego	1	1	1	1
2	Daños por agua	1	1	1	1
3	Desastres naturales	1	1	1	1
4	Suspensión del servicio eléctrico	1	2	1	1
5	Condiciones inadecuadas de temperatura	1	1	1	1
6	Interrupción de los servicios de comunicaciones	1	1	1	1
7	Averías por fallo físico o lógico	1	1	1	1

Elaborado por la autora de la investigación.

En la tabla 25 se muestran las amenazas de los activos clasificados en Soporte de información, SI1 (almacenamiento en NAS), SI2 (cintas).

Tabla 25 *Valoración de probabilidad de amenazas del activo Soporte de información*

N°	AMENAZA	SOPORTE DE INFORMACIÓN	
		SI1	SI2
1	Daños por agua	1	1
2	Suspensión del servicio eléctrico	3	
3	Inadecuadas condiciones de humedad		2
4	Interrupción de los servicios de comunicaciones	1	1
5	Desastres industriales	2	1
6	Fallas en el respaldo de la información	3	3

Elaborado por la autora de la investigación.

La tabla 26 indica las amenazas a las que están expuestas los activos clasificados en Equipos auxiliar, AUX1 (generador eléctrico), AUX2 (fuentes de alimentación).

Tabla 26 *Valoración de probabilidad de amenazas del activo Equipamiento auxiliar*

N°	AMENAZA	EQUIPAMIENTO AUXILIAR	
		AUX1	AUX2
1	Fuego	1	1
2	Daños por agua	1	1
3	Desastres naturales	1	1
4	Suspensión del servicio eléctrico	2	2
5	Condiciones inadecuadas de temperatura o humedad	2	2
6	Desastres industriales	2	2

Elaborado por la autora de la investigación.

La tabla 27 indica las amenazas a las que están expuestas los activos clasificados en Instalaciones: L1(data center), L2 (oficinas).

Tabla 27 *Valoración de probabilidad de amenazas del activo Instalaciones*

N°	AMENAZA	INSTALACIONES	
		L1	L2
1	Fuego	1	1
2	Daños por agua	1	1
3	Desastres naturales	1	1
4	Suspensión del servicio eléctrico	2	2
5	Inadecuadas condiciones de temperatura	1	1
6	Interrupción de los servicios de comunicaciones	2	2

Elaborado por la autora de la investigación.

La tabla 28 muestra las amenazas a las que están expuestos los activos clasificados en Personal; P1(rol analistas de la DGE y TI oficina matriz), P2 (rol jefe DGE).

Tabla 28 *Valoración de probabilidad de amenazas del activo Personal*

N°	AMENAZA	PERSONAL	
		P1	P2
1	Indisponibilidad del personal	3	3
2	Agotamiento de recursos	1	1
3	Errores de los usuarios	3	3
4	Ingeniería social	3	3

Elaborado por la autora de la investigación.

3.4.4 Matriz de estimación del impacto

La estimación del impacto se realiza valorando las respuestas de las preguntas ¿qué consecuencias causaría en cada activo si la amenaza se materializa? y ¿que ocasionaría en la ARCOTEL o en la Dirección de Gestión Económica? La valoración dependerá de las respuestas, pudiendo ser que no hay consecuencias relevantes o por el contrario las consecuencias son graves o muy graves.

Para la estimación del impacto de forma cuantitativa y cualitativa, se utilizará los datos de la tabla 29 con base a los criterios de valoración descritos en el capítulo II:

Tabla 29 *Valoración del impacto causado por la explotación de las amenazas*

VALOR	IMPACTO EN EL ACTIVO
Bajo (1)	No hay consecuencias relevantes
Medio (2)	Las consecuencias son relevantes.
Alto (3)	Hay consecuencias graves

Elaborado por la autora de la investigación con base a lo descrito en el capítulo II.

A partir de la tabla 30 hasta la 37, se muestra la valoración de la estimación del impacto si se materializa la amenaza, para cada clasificación de los activos; aquellos que tienen valoración igual a 3 se estima que tienen consecuencias graves para el activo, dependiendo de la amenaza analizada.

La tabla 30 indica la estimación del impacto para los activos clasificados como servicios.

Tabla 30 *Estimación del impacto para los activos Servicios.*

No.	AMENAZA	SI	S2	S3	S4	S5	S6
1	Fuego	3					3
2	Daños por agua	3					2
3	Suspensión del servicio eléctrico	2	3	2	3	2	2
4	Inadecuadas condicione de temperatura	2	2		2	3	3
5	Interrupción de los servicios de comunicaciones	2	3	3	3	3	3
6	Averías por fallos físicos o lógicos	3	3	3	3	3	3
7	Fuga de información	3	3	3			
8	Acceso no autorizado		3	3			
9	Corrupción de la información	3	3				
10	Errores de los usuarios	2	3	2	2	2	2
11	Errores de configuración	2					
12	Fallas en el respaldo de la información	3	3	2			3

Elaborado por la autora de la investigación.

La tabla 31 indica la estimación del impacto que causaría las amenazas en los activos datos e información.

Tabla 31 *Estimación del impacto para los activos: Datos e información*.

N°	AMENAZAS	D1	D2	D3	D4
1	Desastres naturales	3	3	3	3
2	Suspensión del servicio eléctrico	3	2	2	2
3	Condiciones inadecuadas de temperatura o humedad	3	2	2	2
4	Interrupción de los servicios de comunicaciones	2	2	2	2
5	Desastres industriales	3	3	3	2
6	Fuga de información	3	3	3	1
7	Fallas en el respaldo de la información	3	3	3	3

Elaborado por la autora de la investigación.

La tabla 32 indica la estimación del impacto que causarían las amenazas en los activos software y aplicaciones:

Tabla 32 *Estimación del impacto para los activos Software y aplicaciones*.

N°	AMENAZA	SW1	SW2	SW3	SW4	SW5	SW6
1	Suspensión del servicio eléctrico	2	2	2	2	2	2
2	Interrupción de los servicios de comunicaciones	3	3	2	3	3	2
3	Desastres industriales	3	2	2	2	2	3
4	Errores causados por los usuarios	3	3	2	2	3	2
5	Errores del administrador					3	2
6	Errores en la configuración	3	2	2	3	3	2
7	Fallas en el respaldo de la información	3	3	3	3	3	3
8	Errores de mantenimiento / actualización de programas (software)	3				3	

Elaborado por la autora de la investigación.

La tabla 33 indica la estimación del impacto para los activos equipos informáticos:

Tabla 33 *Estimación del impacto para los activos Equipos informáticos*

N°	AMENAZA	HW1	HW2	HW3	HW4	HW5	HW6
1	Fuego	3	3	3	3	3	3
2	Daños por agua	3	3	3	3	3	3
3	Suspensión del servicio eléctrico	2	2	2	2	2	2
4	Condiciones inadecuadas de temperatura o humedad	2	2	2	2	2	2
5	Interrupción de los servicios de comunicaciones	1	1	1	1	2	2
6	Desastres industriales	2	2	2	2	2	2
7	Fuga de información	3	3	3	2	2	2
8	Vulnerabilidad de programas (software)	2	2				
9	Corrupción de la información	3	3	3	3	3	3

N°	AMENAZA	HW1	HW2	HW3	HW4	HW5	HW6
10	Fallas en el respaldo de la información	3					

Elaborado por la autora de la investigación.

La tabla 34 indica la estimación del impacto para los activos redes de comunicaciones.

Tabla 34 *Estimación del impacto para los activos Redes de comunicaciones*.

N°	AMENAZA	COM1	COM2	COM3	COM4
1	Fuego	3	3	3	3
2	Daños por agua	3	3	3	3
3	Desastres naturales	3	3	3	3
4	Suspensión del servicio eléctrico	2	2	2	2
5	Inadecuadas condiciones de temperatura	2	2	2	2
6	Interrupción de los servicios de comunicaciones	1	1	1	1
7	Avería por daño físico o lógico	3	3	3	3

Elaborado por la autora de la investigación.

La tabla 35 indica la estimación del impacto para los activos soporte de información.

Tabla 35 *Estimación del impacto para los activos Soporte de información.*

N°	AMENAZA	SI1	SI2
1	Desastres naturales	3	3
2	Suspensión de servicio eléctrico	3	
3	Inadecuadas condiciones de temperatura		3
4	Interrupción en los servicios de comunicación	3	2
5	Desastres industriales	1	1
6	Fallas en el respaldo de la información	3	3

Elaborado por la autora de la investigación.

La tabla 36 indica la estimación del impacto para los activos equipamiento auxiliar

Tabla 36 *Estimación del impacto para los activos Equipamiento auxiliar*

N°	AMENAZA	AUX1	AUX2
1	Fuego	3	3
2	Daños por agua	3	3
3	Desastres naturales	3	3
4	Suspensión del servicio eléctrico	3	3
5	Condiciones inadecuadas de temperatura o humedad	2	2
6	Averías por fallos físicos o lógicos	3	3

Elaborado por la autora de la investigación

La tabla 37 indica la estimación del impacto para los activos instalaciones.

Tabla 37 *Estimación del impacto para los activos Instalaciones*.

N°	AMENAZAS	INSTALACIONES	
		L1	L2
1	Fuego	3	3
2	Daños por agua	3	3
3	Desastres naturales	3	3
4	Suspensión del servicio eléctrico	3	3
5	Inadecuadas condiciones de temperatura	1	1
6	Interrupción de los servicios de comunicación	3	1

Elaborado por la autora de la investigación.

La tabla 38 indica la estimación del impacto para los activos personal.

Tabla 38 *Estimación del impacto para los activos Personal.*

N°	AMENAZAS	PERSONAL	
		P1	P2
1	Indisponibilidad del personal	2	2
2	Agotamiento de recursos	1	1
3	Errores de los usuarios	3	3
4	Ingeniería social	3	3

Elaborado por la autora de la investigación.

3.4.5 Matriz de gestión de riesgos

Una vez que se obtiene las matrices de probabilidad de ocurrencia del riesgo, así como el impacto que causaría si es que las amenazas se materializan en cada activo, se construye la matriz de gestión de riesgos utilizando la siguiente fórmula:

Gestión del Riesgo = Probabilidad (ocurrencia de la amenaza) * Impacto

De manera cualitativa la valoración de la gestión de riesgo que se utilizará está enfocada en los cinco niveles que se muestran en la tabla 39, que son el resultado de la multiplicación del valor de

la probabilidad de ocurrencia de la amenaza multiplicada por el valor del impacto que la amenaza causaría sobre el activo de información.

Tabla 39 *Resumen de la estimación del riesgo (probabilidad por impacto)*

CUANTIFICACIÓN DEL RIESGO (NIVEL)	
1 (MB)	El riesgo es MUY BAJO
2 (B)	El riesgo es BAJO
3-4 (M)	El riesgo es MEDIO
6 (A)	El riesgo es ALTO
9 (MA)	El riesgo es MUY ALTO

Elaborado por la autora de la investigación con base a la tabla 7.

Los niveles del riesgo son cuantificados en una matriz, donde un valor igual a 9 significará que el riesgo es muy alto, este será cuando las amenazas tienen alta probabilidad de materializarse y el impacto que causan también es alto; valores entre 3 y 4 significan riesgo medio y valores de 1 significará que el riesgo es muy bajo, esto se representa en la tabla 40.

Tabla 40 *Matriz de valoración del riesgo*

TABLA DE RIESGO				
		PROBABILIDAD		
		Bajo	Medio	Alto
IMPACTO	Alto	3	6	9
	Medio	2	4	6
	Bajo	1	2	3

Elaborado por la autora de la investigación
Fuente: INCIBE (2015).

Con base a la matriz de la tabla 40, se calcula la estimación del riesgo que tendrían los activos clasificados en las nueve categorías de información de la DGE de ARCOTEL.

En la tabla 41 se muestra la cuantificación del valor del riesgo dispuesta en EGSI v2, existen tres escalas, la más alta corresponde al riesgo alto, en la cual coindice con la metodología MAGERIT, para cuando los riesgos son muy altos con valor 9.

Tabla 41 *Nivel de riesgo del EGSI*

VALOR	**CUANTIFICACIÓN DEL RIESGO (NIVEL)**
1-3 (B)	El riesgo es BAJO
4-8 (M)	El riesgo es MEDIO
9 -27 (A)	El riesgo es ALTO

Elaborado por la autora de la investigación.:
Fuente: MINTEL (2020).

La tabla 42 indica la evaluación de los riesgos del activo con la clasificación servicios, identificándose un valor 9, es decir riesgo alto para los activos S1, S2 y S6 si ocurriera la amenaza de Fallas en el respaldo de la información.

Tabla 42 *Evaluación de riesgos del activo Servicios*

N°	AMENAZAS	SI	S2	S3	S4	S5	S6
1	Fuego	3	0	0	0	0	3
2	Daños por agua	6	0	0	0	0	4
3	Suspensión del servicio eléctrico	4	6	4	6	4	4
4	Condiciones inadecuadas de temperatura o humedad	2	2	0	2	3	3
5	Interrupción de los servicios de comunicaciones	4	6	6	6	6	6
6	Averías por fallos físicos y lógicos	3	3	3	3	3	3
7	Fuga de información	6	3	6	0	0	0
8	Acceso no autorizado		6	6	0	0	0
9	Corrupción de la información	3	3				

N°	AMENAZAS	SI	S2	S3	S4	S5	S6
10	Errores de los usuarios	4	6	4	4	4	4
11	Errores de configuración	2					
12	Fallas en el respaldo de la información	9	9	6	0	0	9

Elaborado por la autora de la investigación.

La tabla 43 indica la evaluación de los riesgos del activo datos, identificándose valores entre 1 y 3, sin establecer valores de riesgo alto para las diferentes amenazas.

Tabla 43 *Evaluación de riesgos del activo Datos*.

N°	AMENAZA	D1	D2	D3	D4
1	Daños por agua	3	3	3	3
2	Suspensión del servicio eléctrico	3	2	2	2
3	Inadecuadas condiciones de temperatura	3	2	2	2
4	Interrupción de los servicios de comunicaciones	2	2	2	2
5	Desastres industriales	3	3	3	2
6	Fuga de información	3	3	3	1
7	Fallas en el respaldo de la información	3	3	3	3

Elaborado por la autora de la investigación.

La tabla 44 indica la evaluación de los riesgos del activo con la clasificación aplicaciones, identificándose valores entre 2 y 6, es decir riesgos bajos y medios para las diferentes amenazas.

Tabla 44 *Evaluación de riesgos del activo Aplicaciones*

N°	AMENAZA	SW1	SW2	SW3	SW4	SW5	SW6
1	Suspensión del servicio eléctrico	4	4	4	4	4	4
2	Interrupción de los servicios de comunicaciones	6	6	4	6	6	4
3	Desastres industriales	6	4	4	4	6	6
4	Errores de los usuarios	0	0	0	0	3	2
5	Errores del administrador	3	2	2	3	3	2
6	Errores de configuración	3	3	3	3	3	3
7	Fallas en el respaldo de la información	3	0	0	0	3	0
8	Errores de mantenimiento / actualización de programas (software)	6	0	0	0	6	0

Elaborado por la autora de la investigación.

La tabla 45 indica la evaluación de los riesgos del activo con la clasificación Equipos informáticos, identificándose un valor de 9, es decir riesgo alto para el activo HW1 con las amenazas de corrupción de la información y fallas en el respaldo de la información.

Tabla 45 *Evaluación de riesgos del activo Equipos informáticos*

N°	AMENAZA	HW1	HW2	HW3	HW4	HW5	HW6
1	Fuego	3	3	3	3	3	3
2	Daños por agua	6	6	6	6	6	6
3	Suspensión del servicio eléctrico	2	2	2	2	2	2
4	Condiciones inadecuadas de temperatura o humedad	2	2	2	2	2	2
5	Interrupción de los servicios de comunicaciones	2	2	2	2	4	4
6	Desastres industriales	2	2	2	2	2	2
7	Fuga de información	6	3	3	2	2	2
8	Vulnerabilidad de programas (software)	6	6				
9	Corrupción de la información	9	6	3	3	3	3
10	Fallas en el respaldo de la información	9					

Elaborado por la autora de la investigación.

La tabla 46 indica la evaluación de los riesgos del activo con la clasificación redes de comunicaciones, identificándose valores entre 1 y 4, sin establecer valores de riesgo alto para las diferentes amenazas.

Tabla 46 *Evaluación de riesgos del activo Redes de comunicaciones*

N°	AMENAZA	COM1	COM2	COM3	COM4
1	Fuego	3	3	3	3
2	Daños por agua	3	3	3	3
3	Desastres naturales	3	3	3	3
4	Suspensión del servicio eléctrico	2	4	2	2
5	Condiciones inadecuadas de temperatura o humedad	2	2	2	2
6	Interrupción de los servicios de comunicaciones	1	1	1	1
7	Averías por fallo físico o lógico	3	3	3	3

Elaborado por la autora de la investigación.

La tabla 47 indica la evaluación de los riesgos del activo con la clasificación soporte de información, identificándose valores entre 1 y 3, sin establecer valores de riesgo alto para las diferentes amenazas.

Tabla 47 *Evaluación de riesgos del activo Soporte de información*

N°	AMENAZA	SI1	SI2
1	Desastres naturales	3	3
2	Suspensión del servicio eléctrico	3	
3	Condiciones inadecuadas de temperatura o humedad		3
4	Interrupción de los servicios de comunicaciones	3	2
5	Desastres industriales	1	1
6	Fallas en el respaldo de la información	3	3

Elaborado por la autora de la investigación.

La tabla 48 indica la evaluación de los riesgos del activo con la clasificación equipo auxiliar, identificándose valores entre 3 y 6, sin establecer valores de riesgo alto para las diferentes amenazas.

Tabla 48 *Evaluación de riesgos del activo Equipo auxiliar*

N°	AMENAZA	AUX1	AUX2
1	Fuego	3	3
2	Daños por agua	3	3
3	Desastres naturales	3	3
4	Suspensión del servicio eléctrico	6	6
5	Condiciones inadecuadas de temperatura o humedad	4	4
6	Desastres industriales	6	6

Elaborado por la autora de la investigación.

La tabla 49 indica la evaluación de los riesgos del activo instalaciones, identificándose valores entre 1 y 6, sin establecer valores de riesgo alto para las diferentes amenazas.

Tabla 49 *Evaluación de riesgos del activo Instalaciones*

Nro.	AMENAZA	L1	L2
1	Fuego	3	3
2	Daños por agua	3	3
3	Desastres naturales	3	3
4	Suspensión del servicio eléctrico	6	6
5	Condiciones inadecuadas de temperatura o humedad	1	1
6	Interrupción de los servicios de comunicaciones	6	2

Elaborado por la autora de la investigación.

La tabla 50 indica la evaluación de los riesgos del activo con la clasificación personal, identificándose valores de 9, es decir riesgo alto para los activos P1 y P2 con la amenaza de ingeniería social.

Tabla 50 *Evaluación del riesgo del activo Personal*

N°	AMENAZA	P1	P2
1	Indisponibilidad del personal	6	6
2	Agotamiento de recursos	1	1
3	Errores de los usuarios	6	6
4	Ingeniería social	9	9

Elaborado por la autora de la investigación.

Una vez que se realizó la evaluación de riesgos por activo, amenaza, probabilidad e impacto, en la figura 7 se visualiza el mapa de calor de la gestión de riesgos de la Dirección de Gestión Económica de la ARCOTEL y su entorno de sistemas informáticos del edificio matriz de la ARCOTEL.

El color rojo significa que el riesgo sobrepasa un nivel aceptable es decir el riesgo de la seguridad de la información es alto, mientras que el color marrón y amarillo significa que el riesgo es medio y el color verde significa que el riesgo es bajo y aceptable.

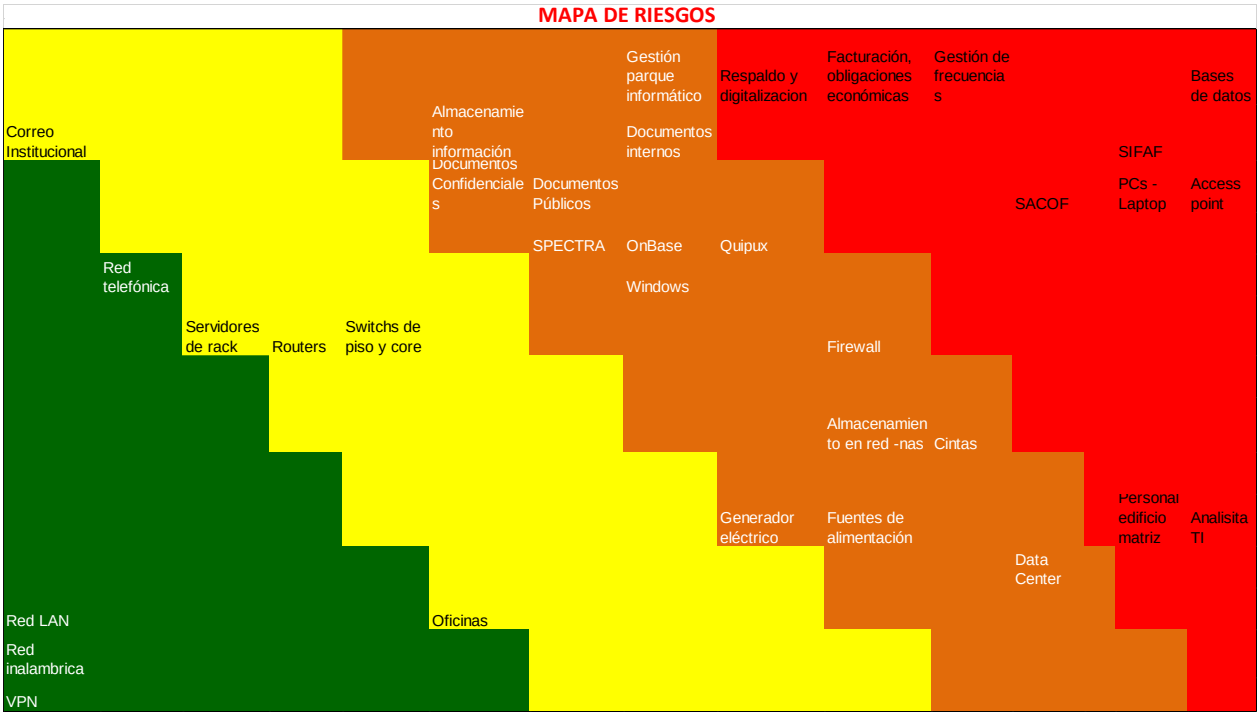

Figura 7 Mapa de calor de la gestión de riesgos de la DGE.

Se han identificado los activos con riesgo que sobrepasa un nivel aceptable, razón por la cual es necesario realizar el tratamiento del riesgo para estos activos considerados críticos, los cuales son: respaldo y digitalización; facturación y obligaciones económicas; equipos y laptops; bases de datos, access point; gestión de espectro; SIFAF Sistema de Facturación de Frecuencias; SACOF Sistema que administra información de las concesiones, títulos habilitantes; personal.

3.4.6.- Tratamiento de riesgos

Para cada uno de los riesgos identificados, y que superen un nivel aceptable, es necesario realizar un tratamiento. Para este tratamiento, principalmente se tiene cuatro opciones: reducir los riesgos, evitarlos, transferirlos y aceptarlos (Ministerio de Hacienda y Administraciones Públicas, 2012).

Se propone reducir los riesgos de los activos de la información con la implementación de controles y diseño de la política de seguridad de la información.

3.5 Selección de los controles

Para el tratamiento de riesgos de los activos identificados como críticos o relevantes, en la Dirección de Gestión Económica DGE de la ARCOTEL, se seleccionaron minuciosamente algunos controles de los disponibles en la norma ISO 27002:2013 que se incluye como Anexo.

Los controles seleccionados, para el tratamiento de los riesgos de los activos críticos son:

- 5.1 Directrices en seguridad de la información
- 7.2.1 Responsabilidades de gestión
- 7.2.2 Concienciación, educación y capacitación en seguridad de la información
- 8.3.1 Gestión de soportes extraíbles
- 8.3.3 Soporte físico en tránsito
- 9.1.1 Política de control de accesos
- 9.3.1 Uso de información confidencial para autenticación
- 9.2.3 Gestión de los derechos de acceso con privilegio especial
- 9.2.5 Revisión de los derechos de acceso de los usuarios (contraseñas)
- 11.1.2 Controles físicos de entrada
- 11.1.3 Seguridad de oficinas, despachos y recursos
- 11.2.4 Mantenimiento de los equipos
- 12.1.1 Documentación de procedimientos de operación
- 12.1.3 Gestión de capacidades
- 12.3.1 Copias de seguridad de la información

- 12.4.1 Registro y gestión de eventos de actividad
- 13.1.1 Controles de red
- 13.1.2 Mecanismos de seguridad asociados a servicios en red

La tabla 51 muestra el resumen de la gestión de riesgos elaborada, así como las vulnerabilidades asociadas a los activos críticos o relevantes de la DGE y los controles seleccionados para su tratamiento.

Tabla 51 *Resumen de gestión de riesgos de los activos críticos y selección de controles*

Activos críticos	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**	**Número de Control**
Respaldo y digitalización	Degradación de los soportes de almacenamiento	Pérdida en la información, falta de procesos e implementación de respaldos de información	3	3	9	8.3.1 8.3.3 12.3.1
	Daños por agua	Archivos físicos ubicados junto a tomas de agua, daño material de los archivos	2	3	6	11.1.3 12.3.1
	Fuga de información	Falta de procedimientos que impidan que el personal divulgue información, falta definición de perfiles	2	3	6	7.2.2 9.3.1 11.1.2
Facturación y obligaciones económicas	Suspensión del servicio eléctrico	Equipo insuficiente de respaldo de energía; perdidas de información	2	3	6	12.1.3 11.2.4
	Interrupción de los servicios de comunicaciones	Un único proveedor de comunicaciones, pérdida de información	2	3	6	12.1.1
	Errores de los usuarios	Implementar y actualizar manuales de usuarios; controles de ingreso de datos.	2	3	6	7.2.2. 12.1.1
	Fallas en el respaldo de la información	Pérdida en la información, falta de procesos e implementación de respaldos	3	3	9	8.3.1 8.3.3 12.3.1

Activos críticos	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo	Número de Control
	Acceso no autorizado	Falta de contraseñas robustas o contraseñas permanentes	2	3	6	9.1.1 9.2.3 9.2.5
Bases de datos	Equipo insuficiente de respaldo de energía; pérdidas de información	Fallo en los equipos de redundancia	2	3	6	11.2.4 12.1.3
	Conexiones interrumpidas, insuficiente revisión de puertos abiertos	Pérdida, robo de información	3	2	6	13.1.1 13.1.2
	Insuficientes procesos de respaldos de información	Pérdida en la información, falta de procesos e implementación de respaldos	3	3	9	8.3.1 8.3.3
Gestión de espectro - frecuencias	Interrupción de los servicios de comunicaciones	Pérdida, robo de información	2	3	6	13.1.1 13.1.2

Activos críticos	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo	Número de Control
	Fuga de información	Falta de procedimientos que impidan que el personal divulgue información, falta definición de perfiles	2	3	6	9.3.1 11.1.2
	Fallas en el respaldo de la información	Falla o pérdida en la información	3	2	6	8.3.1 8.3.3 12.3.1
- SIFAF (Sistema de Facturación de Frecuencias)	Interrupción de los servicios de comunicaciones	Pérdida de información	2	3	6	13.1.1 13.1.2
	Averías por fallos físicos o lógicos	Pérdida de información	2	2	4	11.2.4
	Errores de los usuarios	Insuficientes manuales de usuarios, sin actualizar; controles de ingreso de datos	3	3	9	7.2.2 12.1.1
	Errores de configuración	Falta de actualización del software acorde a regulación vigente	2	3	6	12.1.1 12.1.3

Activos críticos	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo	Número de Control
	Acceso no autorizado	Falta de contraseñas robustas o contraseñas permanentes	2	3	6	9.1.1 9.2.3 9.2.5
	Fallas en el respaldo de la información	Falla o pérdida en la información, falta de procesos de respaldos de información	2	2	4	8.3.1 8.3.3 12.3.1
	Errores de mantenimiento / actualización de programas (software)	Insuficiente actualización de las aplicaciones, datos equivocados en informes	2	3	6	12.4.1
SACOF (Sistema Administrativo de Concesiones, Otros títulos y Frecuencias)	Suspensión del servicio eléctrico	Fallo en los equipos de redundancia	2	2	4	11.2.4
	Interrupción de los servicios de comunicaciones	Pérdida de información	2	3	6	13.1.1 Controles de red 13.1.2 Mecanismos de seguridad asociados a servicios en red
	Averías por fallos físicos o lógicos	Pérdida de información	3	2	6	11.2.4 Mantenimiento de los equipos

Activos críticos	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo	Número de Control
	Errores de los usuarios	Implementar y actualizar manuales de usuarios; sin controles de ingreso de datos	2	3	6	7.2.1 7.2.2 12.1.1
	Errores del administrador	Falta de implementación de manuales o la actualización de procesos	1	3	3	12.1.1
	Errores de configuración	Software incompatible con la nueva regulación de telecomunicaciones	2	3	6	12.1.1 12.1.3
	Fallas en el respaldo de la información	Pérdida en la información, falta de procesos e implementación de respaldos	3	3	9	8.3.1 8.3.3 12.3.1
	Errores de mantenimiento / actualización de programas (software)	Falta de actualizaciones, datos equivocados en informes	2	3	6	12.4.1
Equipos y laptops	Daños por agua	Archivos físicos ubicados junto a tomas de agua, daño material de los archivos	2	3	6	11.2.4 11.1.3

Activos críticos	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo	Número de Control
	Fuga de información	Fácil ingreso a instalaciones y datos, falta definición de perfiles.	2	3	6	9.3.1 11.1.2
	Vulnerabilidad de programas (software)	Fácil acceso a instalación de software no existe listado de software autorizado, versiones de sistemas operativos antiguas.	3	2	6	12.2.2
	Acceso no autorizado	Falta de contraseñas robustas, o contraseñas permanentes	2	3	6	9.1.1 9.2.3 9.2.5
	Corrupción de información	Daño en la integridad de la información, falta de implementación de políticas	3	3	9	9.2.3 9.2.5
	Fallas en el respaldo de la información	Pérdida en la información, falta de procesos e implementación de respaldos	3	3	9	8.3.1 8.3.3 12.3.1
Access point	Daños por agua	Ubicación de equipos inadecuada	2	3	6	11.1.3

Activos críticos	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo	Número de Control
	Vulnerabilidad de programas (software)	Fácil acceso a la información a través de dispositivos móviles, código malicioso	3	2	6	9.2.3 12.2.2
	Corrupción de información	Pérdida de la información	2	3	6	9.2.3 9.2.5
Almacenamiento en NAS	Suspensión del servicio eléctrico	Fallo en los equipos de redundancia	3	3	9	11.2.4
	Fallas en el respaldo de la información	Pérdida en la información, falta de procesos e implementación de respaldos	3	3	9	8.3.1 8.3.3 12.3.1
Cintas	Condiciones inadecuadas de temperatura o humedad	Fallo en los respaldos de la información, pérdida de esta.	2	3	6	8.3.1 8.3.3 12.3.1
	Fallas en el respaldo de la información	Falla o pérdida en la información, falta de procesos de respaldos de información	3	3	9	8.3.1 8.3.3 12.3.1
Data Center	Suspensión del servicio eléctrico	Fallo en los equipos de redundancia	2	3	6	11.2.4

Activos críticos	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo	Número de Control
	Interrupción de los servicios de comunicaciones	Pérdida de información	2	3	6	13.1.1 13.1.2
Personal DGE edificio matriz	Indisponibilidad del personal	Falta de continuidad y transferencia de conocimientos	3	2	6	5.1 7.2.1
	Errores de los usuarios	Implementar y actualizar manuales de usuarios; controles de ingreso de datos.	2	3	6	7.2.2 12.1.1 18.2.2
	Ingeniería social	No existe conocimiento de seguridad de información	3	3	9	7.2.1 7.2.2

Elaboración propia autora de la investigación

CAPÍTULO IV

PROPUESTA DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4.1 Introducción

En esta sección se desarrolla la política de seguridad de la información para la Dirección de Gestión Económica de la ARCOTEL, con el fin de proteger la confidencialidad, integridad y disponibilidad de su información, basada en la gestión de riesgos de los activos considerados críticos. La política se desarrolla en dos secciones, la primera parte de aspectos generales en los que se señala, la autoridad competente para aprobar la política, el objeto, ámbito, responsabilidades, términos y definiciones; la segunda sección detalla la política específica de acuerdo a los controles escogidos de la norma ISO 27002:2013, para minimizar los riesgos identificados en los activos.

4.2 Aspectos generales de la política

4.2.1. Autoridad que aprueba

La Dirección de Gestión Económica de la ARCOTEL tiene como máxima autoridad al Director Ejecutivo de la Institución, quién aprobará la política de seguridad propuesta.

4.2.2 Objeto

Emitir una política de seguridad de la información para la Dirección de Gestión Económica de la ARCOTEL, basada en las normas ISO 27002:2013 y EGSI v2, para proteger las características de confidencialidad, integridad y disponibilidad de su información.

4.2.3 Alcance

La política de seguridad de la información se ha diseñado para un área particular la Agencia de Regulación de las Telecomunicaciones, la Dirección de Gestión Económica, ubicada en el edificio matriz de la Institución, en la ciudad de Quito, sin embargo, la política puede hacerse extensiva para todas las áreas de ARCOTEL.

4.2.4.- Base legal

- Considerando que esta política de seguridad de la información está diseñada para ser aplicada en una institución pública, es mandatorio basarse en la guía emitida en el Esquema de Gestión de Seguridad de la Información, versión 2 EGSI v2 emitido con Acuerdo Ministerial Nro. 25 de 10 de enero de 2020.
- Normas ISO 27002 versión 2013, que contiene los controles para minimizar los riesgos de la seguridad de la información, encontrados en la Dirección de Gestión Económica de la ARCOTEL.
- Estatuto Orgánico de Gestión Organizacional por Procesos Reformado de la ARCOTEL, actualizado para la gestión de la seguridad de la información, emitido con resolución 13-13-ARCOTEL-2019 de 30 de agosto de 2019.

4.2.5 Términos y Definiciones

Los términos y definiciones utilizados en la política de seguridad de la información serán los indicados en el EGSI v2, aquello términos que no han sido definidos se adoptarán de la norma internacional ISO 27002:2013 o versiones superiores, también se utilizarán referencias internacionales como los libros de MAGERIT e INCIBE.

- **Activo:** corresponde a cualquier recurso que posee y agrega valor a la institución, le permite cumplir sus actividades (INCIBE, 2015).
- **Activo de información:** es cualquier elemento, sistema, soporte, edificio, personas, hardware, software, redes de comunicaciones, que tienen un valor para la institución (MINTEL, 2020).
- **Amenaza:** es una acción, situación o hecho que puede obstaculizar el buen funcionamiento de un activo de servicio o de un conjunto de activos de servicios (Baud, 2015).
- **Confidencialidad**: es la dimensión que limita el acceso a la información, para ser accesible únicamente al personal autorizado (Ministerio de Hacienda y Administraciones Públicas, 2012).
- **Disponibilidad:** esta característica indica que la información esté siempre accesible y disponible en el tiempo para el personal autorizado, cuando lo requiera (Ministerio de Hacienda y Administraciones Públicas, 2012).
- **Integridad:** es la dimensión que garantiza que la información no sea manipulada, alterada o modificada, que se encuentre en las condiciones en las que fue creada (Ministerio de Hacienda y Administraciones Públicas, 2012).

- **Política de seguridad:** es el documento que contiene directrices o decisiones de alto nivel adoptadas por la máxima autoridad de ua organización para la seguridad de la información (ISACA, 2016).
- **Riesgo:** es el análisis de una situación que le puede ocurrir a un activo, es una amenaza o vulnerabilidad, a fin de entender los efectos y posibles consecuencias para la organización o sociedad en general (Baud, 2015).
- **Seguridad de la información:** es la protección de la información de un amplio espectro de amenazas, que permitan asegurar la continuidad del negocio, reduciendo el riesgo e incrementando el retorno de la inversión y oportunidades comerciales (ISO27002, 2013).
- **Vulnerabilidad:** es la probabilidad que una amenaza suceda en un activo de la organización, consecuentemente es el porcentaje de riesgo asociado a cada activo del servicio, lo cual es complicado y subjetivo (Baud, 2015).

4.3 Responsabilidades

- **Máxima autoridad o su delegado:** corresponde al rol del Director Ejecutivo de la ARCOTEL o a su delegado, es el encargado de aprobar la política de seguridad de la información.
- **Coordinador General de Planificación y Gestión Estratégica o su delegado:** es el encargado de presentar la propuesta de política de seguridad de la información de la Dirección de Gestión Económica de la ARCOTEL.
    - Además, es el responsable de informar la implementación del esquema de gestión de seguridad de la información EGSI v2.

- **Oficial de Seguridad de la información:** es un funcionario designado por el Comité de Seguridad que será implementado por la ARCOTEL, será el responsable de la unidad de la seguridad de la información. Elabora propuestas de la documentación requerida en el Esquema Gubernamental de Seguridad de la Información (EGSI); también elabora el plan de concienciación al personal basado en el EGSI.
- **Comité de Seguridad de la información**: es el comité designado por el director ejecutivo de la ARCOTEL; estará integrado por los responsables de las Coordinaciones Generales Administrativa Financiera, Planificación y Gestión Estratégica, Coordinación Técnica de Regulación, Técnica de Gestión de Títulos Habilitantes, Direcciones de Talento Humano, Administrativa, Tecnologías de la Información, Unidad de Comunicación Social y en calidad de asesor el Coordinador General Jurídico.
- **Aplicación y concienciación**: corresponde a los funcionarios de la Dirección de la Gestión Económica de la ARCOTEL.

4.4 Tiempo de revisión de la política

La política de seguridad de la información deberá ser documentada y actualizada por lo menos una (1) vez al año; será socializada con todos los funcionarios de la ARCOTEL, con especial énfasis al personal de la Dirección de Gestión Económica. Si existieran cambios en la estructura de la ARCOTEL también deberá ser documentada y revisada.

4.5 Aplicación de los controles

Área:	**Políticas de seguridad**
Objetivo:	Asegurar que la Dirección de Gestión Económica de la ARCOTEL, cuente con una política de seguridad de la información, con directrices y responsabilidades claras para sus funcionarios
Control:	ISO/IEC 27002: 5, 5.1 Directrices de la Dirección Ejecutiva de ARCOTEL en seguridad de la información.

Artículo 1. La Dirección Ejecutiva de la ARCOTEL aprobará la política de seguridad para la Dirección de Gestión Económica, que se describe en este documento, en aplicación al EGSI emitido por MINTEL con Acuerdo Ministerial Nro. 25 del año 2020. Esta normativa reemplazará procesos y políticas de seguridad que existan con anterioridad.

Artículo 2. La actualización y revisión de la política requerirá un nuevo análisis de gestión de riesgos de los activos de información y sus controles en las normas ISO 27002:2013 y EGSI, y se realizará por lo menos una (1) vez en el año.

Artículo 3. La política será socializada a todos los funcionarios de la ARCOTEL, con énfasis en la Dirección de Gestión Económica, para su implementación.

Área:	**Organización de la seguridad de la información**
Objetivo:	Asegurar que la ARCOTEL cuente con una organización interna y operativa que permita documentar e implementar estas directrices, incluyendo la creación formal de la unidad exclusiva de seguridad de la información.
Control:	ISO/IEC 27002: 6, 6.1 Organización interna, 6.2 Dispositivos para movilidad y teletrabajo.

Artículo 4. Se conformará la Unidad de Seguridad de la información en la ARCOTEL, que estará liderada por el Oficial de Seguridad de la información, funcionario designado por el Comité de Seguridad que será implementado por la ARCOTEL y descrito en la sección de aspectos generales.

Artículo 5. La Unidad de seguridad de la información tendrá como responsabilidades las que refiere el EGSI v2, así como de la revisión de la política de seguridad, el análisis de activos y la gestión de riesgos de la Dirección de Gestión Económica.

Dispositivos para movilidad

Artículo 6. Al ingreso a las instalaciones de la institución se contará obligatoriamente con el registro de dispositivos móviles que incluirán teléfonos móviles inteligentes, *iPad, tablets, laptops*, entre otros, para su autorización.

Artículo 7. En el teletrabajo, se contará con conexiones seguras de comunicaciones, para el ingreso remoto a los sistemas y servicios.

Artículo 8. Los dispositivos móviles de personas ajenas a la institución que requieran navegación web no deben tener acceso a la red LAN, su conexión será con un grupo de direcciones IP diferentes a las de la institución y en un número limitado.

Área:	**Política de seguridad asociada al talento humano**
Objetivo:	Asegurar que los funcionarios de la ARCOTEL conozcan, implementen y cumplan con la responsabilidad asociada a la seguridad de la información en la etapa de concienciación preventiva.
Control:	ISO/IEC 27002: 7, 7.1, 7.2, 7.3 .

Antes de la contratación

Artículo 9.- Previo la contratación de un funcionario para laborar en la Agencia de Regulación y Control de las Telecomunicaciones, se deberá contar con un informe de antecedentes personales, otorgado por autoridad pública competente y que el candidato deberá adjuntar como un requisito con declaración juramentada, para verificar que el candidato no esté inmerso en ningún incidente de seguridad de la información.

La investigación de antecedentes personales estará además relacionados con el tipo de información al que tendrán acceso.

Durante la contratación

Artículo 10. La Dirección de Talento Humano de la ARCOTEL deberá informar al personal a contratar, que las charlas de inducción incluirán una socialización en materia de seguridad de la información, protección de datos, derechos de propiedad intelectual, esta

inducción estará a cargo de la Unidad de Seguridad de la Información, que formará parte de la Coordinación General de Planificación Estratégica.

Artículo 11. El personal que ingresa a laborar en la institución deberá tener pleno conocimiento de sus funciones, roles, responsabilidades, derechos y obligaciones respecto de la seguridad de la información.

Artículo 12. El personal deberá ser informado de las consecuencias de no cumplir políticas y procedimientos de la seguridad de la información.

Artículo 13. El personal tiene derecho y está obligado a cumplir con estas directrices.

Artículo 14. La institución organizará y dictará charlas de socialización y capacitación sobre seguridad de la información al menos una vez en el año, tendientes a motivar a los funcionarios sobre su cumplimiento, incluido el uso de la Norma de Gestión de Incidentes y Vulnerabilidades.

Cese de funciones o cambio de actividades laborales

Artículo 15. Una vez que el personal se desvincule de la Dirección de Gestión Económica, no podrán llevarse la información generada y de propiedad de la Institución, en dispositivos externos o en la nube, tampoco podrán divulgar la información, esto constará en cláusulas específicas de la contratación del personal.

Artículo 16. El personal que deja de laborar en la institución deberá realizar la transferencia de información al nuevo personal o a quien sustituya en sus labores, como consecuencia del

cese de sus funciones o cambio de actividades laborales, deberá entregar un documento al jefe inmediato y al Oficial de seguridad de la información.

Área:	**Gestión efectiva de los activos**
Objetivo:	Proteger los activos de la información de la Dirección de Gestión Económica, mediante la gestión efectiva de los activos de información a través de su clasificación de la información y administración de los soportes de almacenamiento.
Control:	ISO/IEC 27002: 8.3.1; 8.3.3

Gestión de soportes extraíbles

Artículo 17. El respaldo de la información extraíble en medios deberá ser almacenada en varias locaciones.

Artículo 18. Los medios extraíbles utilizaran técnicas criptográficas para protección de los datos y así conservar la confidencialidad e integridad de los mismos.

Artículos 19. Los medios de soporte extraíble deberán ser almacenados en sitios seguros con las especificaciones de los fabricantes y procurando utilizar equipamiento de última tecnología.

Artículo 20. En los casos en los cuales no sea necesario conservar la información, por motivos de caducidad o tiempo, ésta deberá borrarse de manera permanente de los medios extraíbles.

Soporte físico en tránsito

Artículo 21. Se deberá contratar los servicios de una empresa que transporte los medios extraíbles hacia otro lugar fuera de la institución, que responda por la seguridad de la transportación de modo que se conserve la cadena de custodia segura; se deberá verificar la identidad de los empleados de la empresa que realiza el transporte.

Artículo 22. El empaquetado para la transportación física en tránsito deberá ser cumpliendo las especificaciones del fabricante.

Área:	**Política de seguridad asociada al control de acceso**
Objetivo:	Establecer directrices que permitan proteger los activos de información de la institución, a través de requisitos, responsabilidades y gestión para el control de acceso a los usuarios de la Dirección de Gestión Económica de la ARCOTEL.
Control:	ISO/IEC 27002: 9.1; 9.2.3; 9.2.5; 9.3 .

Política de control de accesos

Artículo 23. Se establecerá requisitos para la autorización formal de pedidos para ingresar a los sistemas de información que corresponda, evitando accesos no autorizados.

Artículo 24. Los permisos otorgados para acceso a la información deberán ser revisados de manera periódica al menos dos (2) veces en el año, de manera de identificar y mantener los perfiles de los funcionarios custodios y generadores de información.

Artículo 25. Se deberá retirar el acceso a la información a aquellos funcionarios que no la requieran debido a sus roles y responsabilidades.

Artículo 26. El Director de la Dirección de Gestión Económica deberá otorgar la autorización para que sus funcionarios tengan acceso a la información, de acuerdo con la clasificación, pudiendo ser pública o confidencial.

Artículo 27- Para el acceso se deberá aplicar la regla de menor privilegio, todo está prohibido hasta que se de autorización expresa.

Artículo 28. El Director de Gestión Económica a través de un documento, autorizará a los funcionarios para el acceso a las redes, VPN, redes inalámbricas y servicios de red de acuerdo al rol y responsabilidades de sus funciones, lo cual será enviado a la Unidad de Seguridad de la información.

Artículo 29. Se deberá identificar y documentar los equipos que se encuentran en las redes y a los cuales pueden tener acceso los funcionarios, para relacionar la identificación del equipo con la autenticación del usuario.

Gestión de los derechos de acceso con privilegio especial

Artículo 30. Se entregarán contraseñas para acceso con privilegio especial, únicamente a aquellos funcionarios que por sus roles y funciones así lo requieran, para lo cual serán expresamente autorizados por el Director de la unidad a través de un documento formal de control de acceso, cuya copia será entregada a la Unidad de Seguridad de la Información.

Artículo 31. Deberá contarse con un listado de funcionarios que poseen autorización y registro de privilegios especiales, clasificados por sistema operativo, servicio, bases de datos y aplicaciones, mismo que será actualizado periódicamente.

Artículo 32. Se establecerán requisitos tanto para la autorización y terminación de acceso con privilegios a los sistemas, servicios y bases de datos.

Uso de información confidencial para autenticación

Artículo 33. Para los casos que requieren utilizar información confidencial para autenticación, se debe asignar una autenticación temporal, única, que no pueda predecirse y que será cambiada obligatoriamente con el primer uso. La clave proporcionada deberá entregarse a través de correo seguro cifrado con técnicas criptográficas.

Artículo 34. Los funcionarios que requieren información confidencial para autenticarse deberán suscribir un acuerdo de confidencialidad para mantener confidencial la autenticación personal y la del grupo cuando se requiera el acceso a carpetas compartidas.

Contraseñas

Artículo 35. Las contraseñas de acceso de los usuarios deberán cambiarse al menos cada 90 días, mientras que la asignación de privilegios deberá revisarse cada 30 días o cuando las necesidades de la Dirección lo requieran.

Artículo 36. Se deberá registrar en los logs de los sistemas de información los cambios realizados en las cuentas de los usuarios.

Responsabilidades de los usuarios en el acceso

Artículo 37. Deberán cambiar las contraseñas para autenticación y acceso a los sistemas de información en el plazo establecido para el efecto y siempre que se sospeche de su divulgación.

Artículo 38. Mantendrán las contraseñas confidenciales, evitando que esté escrita en un papel a disposición de otros funcionarios o sujetos a divulgación.

Artículo 39. Las contraseñas confidenciales para autenticación deberán tener al menos las siguientes características:

- Longitud mínima de ocho (8) caracteres.
- Incluir al menos un carácter especial.
- De fácil recordación para el usuario.
- Debe contener números, letras mayúsculas y minúsculas.
- No incluir información de su nombre o fecha de nacimiento.
- No incluir información susceptible de ataques por diccionario.

Área:	**Política asociada a la seguridad física y ambiental**
Objetivo:	Establecer directrices para gestionar áreas seguras de trabajo para los funcionarios de la ARCOTEL y para el equipamiento informático utilizado en sus labores diarias.
Control:	ISO/IEC 27002: 11.1.2; 11.1.3; 11.2.

Controles físicos de entrada segura

Artículo 40. Se deberá revisar e implementar los controles físicos a través de la tarjeta magnética para ingresar a las oficinas, a fin de restringir el ingreso a las oficinas solo al personal autorizado.

Artículo 41. Establecer y delimitar un área exclusiva para recibir a personal externo a la institución, supervisar su cumplimiento.

Artículo 42. El ingreso principal a la institución deberá mantenerse cerrado, únicamente se abrirá con el uso de la tarjeta de identificación del funcionario o del visitante. Se deberá verificar su cumplimiento.

Seguridad de oficinas, despachos y recursos

Artículo 43. No se autorizará el ingreso físico a las instalaciones del datacenter a personal externo de la institución, salvo el caso de mantenimiento debidamente autorizado por el Director de la Unidad de Tecnologías.

Artículo 44. Reforzar la delimitación del acceso físico a las instalaciones del datacenter donde se encuentran los servidores que alojan las aplicaciones institucionales.

Mantenimiento de los equipos

Artículo 45. Se elaborará e implementará un plan de mantenimiento de los equipos informáticos de la institución, siguiendo las recomendaciones y especificaciones de los fabricantes.

Artículo 46. la Coordinación General de Planificación, dispondrá la inclusión en el presupuesto PAC-Plan Anual de adquisiciones, la contratación del mantenimiento anual de los equipos del parque informático, de manera prioritaria en los de la Dirección de Gestión Económica, con la supervisión de funcionarios de la Dirección de Tecnologías.

Artículo 47. Se levantará un registro de las fallas y novedades del manteamiento de los equipos, a fin de planificar la compra o reposición.

Artículo 48. Aquellos equipos que la institución ha declarado como críticos y sensibles, recibirán mantenimiento únicamente por personal propio de la Dirección de Tecnologías.

Artículo 49. La distribución de los equipos informáticos en las oficinas deberá ubicarse alejados en lo posible de las ventanas, objetos pesados o junto a los baños, para reducir riesgos por fugas de agua y desastres naturales.

Área:	**Política de seguridad asociada a la operatividad**
Objetivo:	Establecer directrices y procedimientos para la operatividad de las tareas realizadas en la ARCOTEL, a través de copias de seguridad de la información, controles del software en operación, actividades de supervisión, controles de la red, protección de los registros de información.
Control:	ISO/IEC 27002: 12.1; 12.1.3; 12.2; 12.3; 12.4

Documentación de procedimientos de operación

Artículo 50. La Dirección de Tecnologías deberá elaborar, actualizar y difundir manuales de operación de usuarios, para los sistemas y aplicaciones informáticas utilizadas en la Dirección de Gestión Económica.

Artículo 51. Se desarrollarán y difundirán manuales de usuario, para las aplicaciones informáticas desarrolladas externamente, así como del buen uso del correo electrónico y de la información que puede compartirse de manera segura.

Artículo 52. Se elaborará manuales de usuario de Seguridad Informática a través del Comité de Seguridad de la Información, para concientización del entorno de seguridad de la información.

Artículo 53. Se desarrollará manuales para el manejo, respaldo y restauración de la información de la DGE.

Gestión de capacidades

Artículo 54. La Dirección de Tecnologías deberá realizar el análisis de tráfico y consumo de ancho de banda de aquellos servicios que no son críticos para el desarrollo funcional de la institución, de modo que se puedan optimizar y priorizar estas aplicaciones.

Artículo 55. Se deberá realizar de manera periódica el monitoreo para adquirir y asignar nuevos recursos informáticos para asegurar la continuidad de las operaciones de la DGE.

Artículo 56. Se deberá contar con un plan de proyección de requerimientos futuros para solicitar recursos económicos con la antelación correspondiente y asegura el desempeño y continuidad de las operaciones de la DGE.

Protección contra código malicioso (malware)

Artículo 57. Se deberá elaborar e implementar un listado de software que está permitido utilizar en DGE y en general en la Institución, el cual deberá ser actualizado y socializado de forma periódica, al menos tres veces en el año, lo cual estará bajo responsabilidad del Comité de Seguridad Informático.

Artículo 58. Se deberá contar con un registro actualizado de la revisión del contenido de los equipos informáticos de la DGE respecto a software, aplicaciones y datos, la revisión se realizará periódicamente.

Artículo 59. Se difundirá y socializará a los funcionarios, información sobre nuevos malware o alguno específico, así como las acciones y recomendaciones a implementarse.

Artículo 60. Revisar y actualizar periódicamente controles para evitar navegación en sitios no autorizados (*Deep web*).

Artículo 61. Mantener siempre actualizado la base de datos del antivirus corporativo para protección de todo el parque informático.

Copias de seguridad de la información

Artículo 62. Se elaborará un procedimiento formal para el respaldo de la información, que incluirá la frecuencia, el resguardo y contención de la información.

Artículo 63. Para las copias de seguridad se establecerá un etiquetado, en el cual se identifique el contenido por tipo de información de acuerdo a su clasificación, la fecha y nombre de quien entrega la información. Si el contenido corresponde a información confidencial, el respaldo contará con cifrado.

Artículo 64. Los dispositivos donde se guardan los respaldos de información se almacenarán en un sitio distinto a la oficina matriz donde está la DGE, libre de humedad y disminuyendo los riesgos ambientales.

Artículo 65. Se deberá realizar la revisión periódica de los medios de respaldos de la información, para verificar que su estado sea el adecuado y se pueda recuperar la información.

Registro y gestión de eventos de actividad

Artículo 66. Se elaborará e implementará un procedimiento para registrar los eventos de las aplicaciones institucionales que son requeridos en la DGE, identificando al usuario y la IP del equipo, incluyendo la fecha, hora de conexión y desconexión.

Artículo 67. Para los sistemas y aplicaciones categorizadas como críticos para la institución, se registrará los eventos de registro fallidos y exitosos con una determinada periodicidad.

Artículo 68. Se registrará el acceso a los archivos y las fechas de modificación de los mismos.

Área:	**Política asociada a las telecomunicaciones**
Objetivo:	Establecer directrices para asegurar las redes de comunicaciones que posee el edificio matriz de la ARCOTEL donde funciona la Dirección de Gestión Económica.
Control:	ISO/IEC 27002: 13.1; 13.2

Controles en la red

Artículo 69. Se establecerá políticas de seguridad para controlar la red y preservar la confidencialidad e integridad de la información y disponibilidad de la información de los equipos conectados.

Artículo 70. Todos los equipos deberán tener autenticación para el acceso a la red institucional.

Artículo 71. Se establecerá responsabilidades separadas para la gestión de los equipos de infraestructura de red y del área de operación de los sistemas informáticos.

Mecanismos de seguridad asociados a servicios en red

Artículo 72. Se deberá incorporar tecnología aplicada a los servicios en red, para lo cual todos los equipos informáticos de la DGE deberán estar configurados para políticas de seguridad de red como sistemas de detección de intrusión IDS, sistemas de prevención de intrusos IPS.

Artículo 73. Todos los equipos informáticos de la DGE deberán estar asociados o pertenecer a la red de datos y de comunicaciones institucional.

Artículo 74. Todos los equipos informáticos de la DGE deberán estar configurados para que se sujeten a las políticas, configuraciones y normativas de seguridad de la Dirección de Tecnologías.

Artículo 75. Todos los equipos informáticos de la DGE deberán estar configurados para tener el mínimo número de puertos abiertos para tener un control en las conexiones.

Área:	**Cumplimiento de las políticas de seguridad, conformidad**
Objetivo:	Asegurar que se cumplan las políticas de seguridad que se están estableciendo, por parte de los funcionarios de la ARCOTEL, a través del cumplimiento de la normativa vigente.
Control:	ISO/IEC 27002: 18.2

Cumplimiento de las políticas y normas de seguridad

Artículo 76. Los funcionarios de la DGE deberán conocer, concientizar y aplicar la presente política de seguridad, desarrollada de conformidad con la normativa vigente para la seguridad de la información.

Artículo 77. La política de seguridad de la información debe revisarse y actualizarse de forma periódica al menos una vez al año, el encargado de la revisión será el comité de seguridad de la información.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- La identificación de los activos de información en la Dirección de Gestión Económica de la ARCOTEL se realizó utilizando la metodología de gestión de riesgos denominada MAGERIT, determinando nueve activos críticos, clasificados según la alta probabilidad de ocurrencia de las amenazas, así como al alto impacto que causaría en los activos de la Dirección.
- Para reducir el riesgo de los activos de la información se identificó las vulnerabilidades que tenían los activos críticos de información y se escogió los controles de la norma ISO/IEC 27002 versión 2013, así como los sugeridos en el Esquema Gubernamental de Seguridad de la Información versión 2, emitido para las entidades del sector público del país que dependen del poder ejecutivo, como es el caso de la Dirección de Gestión Económica de la ARCOTEL.
- La valoración de los activos de información, el análisis de las vulnerabilidades, categorización de amenazas y el impacto en la información de la Dirección de Gestión Económica, se realizó aplicando la metodología MAGERIT a través de las matrices de gestión de riesgos, con base a la experiencia de las actividades de valor agregado

que genera esta Dirección a la institución, así como a la estimación del riesgo sugerida por el EGSI versión 2 para las entidades del sector público.

- Esta política se desarrolló para la Dirección de Gestión Económica de la ARCOTEL, seleccionando 22 controles en 9 áreas que proporciona la norma internacional ISO/IEC: 27002:2013, también se utilizó la guía para la implementación de los controles que ofrece el Esquema Gubernamental de Seguridad de la Información EGSI v2, tendientes a preservar y asegurar las dimensiones de la información.
- La política de seguridad de la información propuesta permitirá reducir los riesgos de los activos de información a los que están sometidos la Dirección de Gestión Económica y en general el resto de las áreas de la ARCOTEL, contribuyendo a mejorar la gestión pública, la calidad de los informes, reduciendo futuros reclamos de operadores de telecomunicaciones, evitando egresos para el Estado y salvaguardando la confidencialidad, integridad y disponibilidad de la información.

5.2 Recomendaciones

- Se recomienda documentar todas las acciones efectuadas en torno a la seguridad de la información, desde el inicio del análisis pormenorizado del levantamiento de los activos, el desarrollo de la gestión de sus riesgos y resultados de la implementación de las directrices para asegurar la información, causando el menor impacto a la entidad ante la ocurrencia de una amenaza.
- Se recomienda socializar la política de seguridad de la información propuesta y actualizarla al menos una vez en el año y concientizar a todos los funcionarios de la

institución con énfasis en el personal que no tiene vinculación con las áreas de tecnologías y comunicación.

- La Seguridad de la información es un eje de acción de la política pública Ecuador Digital y como tal es mandatorio que las entidades públicas cuenten con Políticas de Seguridad de su información o las actualicen; por lo que se recomienda que la máxima autoridad de la ARCOTEL, apruebe mediante una resolución esta política a fin de que este trabajo contribuya a la implementación del EGSI según el Acuerdo Ministerial Nro. 25 emitido por el MINTEL y publicado en el registro oficial Nro. 228.

REFERENCIAS

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). *Introduction to the OCTAVE Approach*. Carnegie Mellon University Software Engineering Institute. Pittsburgh PA, USA.

Agencia Europea para la Ciberseguridad. (2019). *Reglamento sobre la Ciberseguridad.* Madrid, España: BOE.

ARCOTEL. (2017). *Estatuto Orgánico de Gestion Organizacional por Procesos* (13 ed.). Quito. Obtenido de http://www.arcotel.gob.ec

ARCOTEL. (2020). *Estadísticas telecomunicaciones*. Obtenido el 25 de febrero de 2020 de https://www.arcotel.gob.ec/estadisticas-de-telecomunicaciones2/.

Baud, J.L. (2015). *Preparación para la certificación ITIL Foundation V3* (Vol. 3). Barcelona, España: Eni Ediciones.

Cevallos, H. (2019). *Diseño de una política de seguridad de la información para el área de TICS del Instituto Técnológico Superior Central Técnico, basado en la norma de seguridad ISO/IEC 27002:2013.* Quito: Universidad Internacional SEK. Obtenido de http://repositorio.uisek.edu.ec/handle/123456789/3320

CNSSI- Committee on National Security Systems. (2015). *Glosario de Ciberseguridad 4009.* Glasario, Committee on National Security Systems, Seatle. Obtenido de https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

El Fray, I. (2012). *A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in information systems.* In IFIP International Conference on Computer Information Systems and Industrial Management (pp. 428-442). Springer, Berlin, Heidelberg.

Gallardo, M. (2018). *Elaboración de una política de seguridad de la información para una institución pública basado en el esquema gubernamental de seguridad de la información.* Quito: Universidad Internacional SEK.

INCIBE (2015). *Gestión de riesgos. Una guía de gestión para el empresario*. (pp. 1-28). Obtenido de https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf

ISACA - Information Systems Audit and Control Association. (2016). *Journal ISACA, 1*, 1-5. Obtenido de https://www.isaca.org/Journal/archives/2017/Volume-1/Pages/smashing-the-information-security-policy-for-fun-and-profit-spanish.aspx

ISO/IEC. (2013). *Controles ISO 27002:2013.* Obtenido de http://iso27000.es/download/ControlesISO27002-2013.pdf

ISO27000. (2005). *Sistemas de Gestión de Seguridad de la Información SGSI, Fundamentos y Vocabulario.* Madrid, España: Alianza.

ISO27001. (2013). Requisitos para implementación de un Sistema de Gestión de Seguridad de la Información. Obtenido de https://www.iso.org

ISO27002. (2013). *Buenas prácticas para Gestión de Seguridad de la Información, Estándar y Dominios.* Madrid, España: Alianza.

ISO27003. (2017). Guia para la implementación de un Sistema de Gestión de Seguridad de la Información. Obtenido de https://www.iso.org

ISO27004. (2016). En *Evalución de la Gestión de Seguridad de la Información.* Obtenido de https://www.iso.org

ISO27005. (2018). Administración del Riesgo de la Seguridad de la Información. Obtenido de https://www.iso.org

Kiseel, R. (2013). *Glossary of Key Information Security Terms*. (D. Publishing, Ed.) *NISTIR 7298, 2*. Obtenido de http://nvlpubs. nist. gov/nistpubs/ir/2013/NIST. IR. 7298r2. pdf.

Krause, M., & Tipton, H. F. (2007). *Information Security Management Handbook* (6ta ed.). New York, Estados Unidod: Auerbach Publications.

Ledezma, D. (2015). *Desarrollo de políticas de seguridad de la información basada en las normas ISO 27002 para una coodinación zonal del INEC.* Ambato: Pontificia Universidad Católica del Ecuador. Obtenido de https://repositorio.pucesa.edu.ec/handle/123456789/1555

Leitch, M. (2010). ISO 31000;2009- The new international standard on risk management. *Risk Analysis: An International Journal 30 (6)*, 887-892. doi:DOI: 10.1111/j.1539-6924.2010.01397.x

LSE. (2019). *Information Security Policy.* Londres: The London School Economic and Political Science. Obtenido de https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecPol.pdf

Ley Orgánica de Telecomunicaciones. Registro Oficial 449, Quito, Ecuador, 18 de febrero de 2015.

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT Metodología de análisis y gestión de riesgos de los sistemas de información*. En Administración Electrónica C.S. (Libro III). Madrid, España. Obtenido de https://administracionelectronica.gob.es

MINTEL. (2016). *Política de Seguridad de la Información del Ministerio de Telecomunicaciones* (Vol. 755). Quito: Registro Oficial. Obtenido de www.lexis.com.ec

MINTEL. (2020). *Esquema Gubernamental de Seguridad de la Información EGSI v2* (Vol. 2). Quito: Registro Oficial 228. Obtenido de http://www.lexis.com

National Institute of Standars and Technology-NIST. (Septiembre de 2012). *Guide for Conducting Risk Assessment. Information Security*. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

O'Hanley, R., & Tiller, J. S. (2013). *Information Security Management Handbook* (Vol. 7). (T. Group, Ed.) New York, Estados Unidos: CRC Press, AUERBACH.

Puga, C. (2019). *Diseño de una política de gestión de seguridad de la información para el área de imagenología del Hospital General Docente de Calderón utilizando los estándares ISO 27001 E ISO 27799.* Quito, Ecuador: Universidad Internacional SEK.

Sangoluisa, D. (2015). *Definición de las políticas de seguridad de la información para la red de la Presidencia de la República del Ecuador.* Quito, Ecuador: Escuela Politécnica Nacional.

Secretaría Nacional, A. (2013). *Esquema Gubernamental de Seguridad de la Información EGSI.* Quito: Registro Oficial Nro.88.

SSCI-Certified Information Systems Security Professional. (2012). *www.pmg-ssi.com.* Obtenido de Triada de Seguridad: https://www.pmg-ssi.com/quienes-somos/

Torres, E., & López, G. (2015). *Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y*

Comunicación. Ambato, Ecuador: Univesidad Técnica de Ambato. Obtenido de http://repositorio.uta.edu.ec/jspui/handle/123456789/13057

UIT, U. I. (2012). *M.1224 : Vocabulario de términos de las telecomunicaciones.* Obtenido de https://www.itu.int/rec/R-REC-M.1224-1-201203-I/es

Anexo1. Documentos de autorización de ARCOTEL

AGENCIA DE REGULACIÓN Y CONTROL
DE LAS TELECOMUNICACIONES
Agencia de Regulación y Control de las Telecomunicaciones
DIRECCIÓN EJECUTIVA
DESPACHO
FECHA 27 AGO 2019 HORA 16:30 x 2.
RECEPCION DE DOCUMENTOS
ANEXO: SI ☐ NO ☐
RECIBIDO POR

Memorando Nro. ARCOTEL-CRDM-2019-0143-M

Quito, D.M., 27 de agosto de 2019

PARA: Sr. Mgs. Ricardo Augusto Freire Granja
Director Ejecutivo

ASUNTO: Solicitud de autorización para elaboración de Plan de Titulación para la Universidad Internacional SEK-UISEK, en relación a los Estudios de Postgrado

De mi consideración:

Pongo en su conocimiento que con memorando ARCOTEL-CRDM-2018-0149-M de 2 de octubre de 2018, se solicitó autorización a la Dirección de Talento Humano, para que se conceda una Comisión de Servicios para Estudios de Postgrado a la Ing. María Luisa Perugachi Betancourt, servidora de la Dirección Técnica de Estudios, Análisis Estadístico y de Mercado considerando que había sido admitida para cursar estudios en el Programa de Maestría en Tecnologías de la Información y Comunicación de la Universidad Internacional SEK (UISEK), luego de haber cumplido con el proceso de selección respectivo, actualmente homologada a la Maestría de Ciberseguridad, lo cual fue concedido con Acción de Personal Nro.552 de 15 de octubre de 2018.

El programa de maestría semipresencial, se encuentra relacionado con la formación académica de la funcionaria y coadyuvará en el ámbito de desarrollo y necesidades en el área que actualmente se desenvuelve, esto es la Dirección de Estudios, Análisis Estadístico y de Mercado.

Considerando que en el semestre que corresponde al período octubre 2019- marzo 2020, es necesario plantear y desarrollar un estudio para el Plan de Titulación, se solicita su autorización como máxima autoridad de la Agencia de Regulación y Control de las Telecomunicaciones, para desarrollar el trabajo en la ARCOTEL, que consiste en: "DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE GESTIÓN ECONÓMICA DE LA ARCOTEL, BASADA EN LAS NORMAS ISO 272002:2013/O EN EGSI", lo cual considero será en beneficio de la Institución.

La razón por la cual se ha escogido a la Dirección de Gestión Económica, para realizar el estudio, es por considerar que en dicha unidad se utiliza información sensible proveniente de los poseedores de títulos habilitantes de telecomunicaciones y radiodifusión, en base a la cual se establecen obligaciones económicas para con el Estado.

Por lo expuesto, mucho agradeceré a Usted, se me conceda la autorización para desarrollar el trabajo de titulación, tendiente a obtener el grado de Magister en Ciberseguridad que otorga la Universidad Internacional SEK sede Ecuador.

Recibido CRDM 16h33 27/Ago/2019

AGENCIA DE REGULACIÓN Y CONTROL
DE LAS TELECOMUNICACIONES

Memorando Nro. ARCOTEL-CRDM-2019-0143-M

Quito, D.M., 27 de agosto de 2019

Por la favorable atención que dé al presente requerimiento, le expreso mi agradecimiento.

Con sentimientos de distinguida consideración, me despido.

Atentamente,

Mgs. Maria Luisa Perugachi Betancourt
JEFE DE DIVISIÓN

Copia:
Sra. Mgs. Jenny Belén Carrillo Auquilla
Asesor 4

Sr. Ing. Carlos Javier Cevallos Manzano
Director Técnico de Estudios, Análisis Estadístico y Mercado

Sr. Mgs. Galo Cristóbal Procel Ruiz
Coordinador Técnico de Títulos Habilitantes

Reporte del quipux de la autorización del Director Ejecutivo

Información del Documento			
No. Documento:	ARCOTEL-CRDM-2019-0143-M	**Doc. Referencia:**	--
De:	Sra. Mgs. Maria Luisa Perugachi Betancourt, Jefe de Division, Agencia de Regulacion y Control de las Telecommunicaciones	**Para:**	Sr. Mgs. Ricardo Augusto Freire Granja, Director Ejecutivo, Agencia de Regulacion y Control de las Telecommunicaciones
Asunto:	Solicitud de autorizacion para elaboracion de Plan de Titulacion para la Universidad Internacional SEK-UISEK, en relacion a los Estudios de Postgrado	**Descripción Anexos:**	--
Fecha Documento:	2019-08-27 (GMT-5)	**Fecha Registro:**	2019-08-27 (GMT-5)

Ruta del documento

Area	De	Fecha/Hora	Acción	Para	No. Dias	Comentario
DIRECCIÓN EJECUTIVA	Ricardo Augusto Freire Granja (ARCOTEL)	2019-08-30 18:45:45 (GMT-5)	Reasignar	Carlos Javier Cevallos Manzano (ARCOTEL)	3	Autorizo realizar en la ARCOTEL el trabajo de titulación de la servidora pública a su cargo Mgs. Maria Luisa Pertugachi. Por favor informar periodicamente el avance, novedades y observaciones de la tesis con respecto a la institución a la asesora técnica.
DIRECCIÓN EJECUTIVA	Jenny Belén Carrillo Auquilla (ARCOTEL)	2019-08-30 18:40:55 (GMT-5)	Reasignar	Ricardo Augusto Freire Granja (ARCOTEL)	3	Se ha revisado el contenido, beneficios e implicaciones del Plan de Tesis, comprobando que es procedente y aporta a los procesos dentro de la gestión de la institución y no requiere de información confidencial. Por favor aprobar.
DIRECCIÓN EJECUTIVA	Ricardo Augusto Freire Granja (ARCOTEL)	2019-08-27 17:31:17 (GMT-5)	Reasignar	Jenny Belén Carrillo Auquilla (ARCOTEL)	0	Trámite correspondiente.
DIRECCIÓN TÉCNICA DE ESTUDIOS, ANÁLISIS ESTADÍSTICO Y DE MERCADO	Maria Luisa Perugachi Betancourt (ARCOTEL)	2019-08-27 16:25:00 (GMT-5)	Envío Manual del Documento		0	
DIRECCIÓN TÉCNICA DE ESTUDIOS, ANÁLISIS ESTADÍSTICO Y DE MERCADO	Maria Luisa Perugachi Betancourt (ARCOTEL)	2019-08-27 16:21:40 (GMT-5)	Registro	Ricardo Augusto Freire Granja (ARCOTEL)	0	-

Autorización para realización de la encuesta

AGENCIA DE REGULACIÓN Y CONTROL
DE LAS TELECOMUNICACIONES

Por favor aplicar encuesta
a la CTBE - CTHB y continuar
con el trabajo de titulación

Memorando Nro. ARCOTEL-CRDM-2019-0184-M

Quito, D.M., 08 de noviembre de 2019

PARA: Sra. Mgs. Jenny Belén Carrillo Auquilla
Coordinadora del Grupo de Aspectos Técnicos y Regulatorios de la TDT

ASUNTO: Aplicación de encuesta

De mi consideración:

Con base en la sumilla del quipux en el memorando ARCOTEL-CRDM-2019-0143-M de 27 de agosto de 2019, mediante el cual se me autoriza realizar en la ARCOTEL el trabajo de titulación denominado *"DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN DE GESTIÓN ECONÓMICA DE LA ARCOTEL, BASADA EN LAS NORMAS ISO 27002:2013/O EN EGSI"*, para obtener el título de magíster en la Universidad Internacional SEK, como un avance del trabajo realizado, comunico a Usted que se ha diseñado una encuesta a ser aplicada en la Dirección de G stión Económica, a fin de conocer el estado actual de la seguridad de la información que permita la identificación de vulnerabilidades en las características de confidencialidad, integridad, disponibilidad.

Por lo expuesto, agradeceré si sirva autorizar la aplicación de dicha encuesta en la unidad motivo de estudio.

Con sentimientos de distinguida consideración, expreso mi agradecimiento.

Atentamente,

Mgs. María Luisa Perugachi Betancourt
JEFE DE DIVISIÓN

Copia:
Sr. Mgs. Roberto Fernando Morcano Viteri
Director Técnico de Estudios, Análisis Estadístico y de Mercado Encargado

08-11-2019 16:13

RMV

08-11-2019

Anexo 2: Formato de la encuesta

Objetivo de la encuesta:

Identificar el estado actual de la seguridad de la información en la Dirección Técnica de Gestión Económica. Este estudio permitirá la identificación de vulnerabilidades en la seguridad de la información.

Preguntas

SECCIÓN: Politica de seguridad

1. La ARCOTEL posee un manual de políticas de seguridad de la información?

SÍ ..... NO ..... NO SABE ..X..

2. La Dirección Técnica de Gestión Económica posee un manual de políticas de seguridad de la información?

SÍ ..... NO ..X..... NO SABE .....

3. Tiene contraseña en su computador:

SÍ ..X..... NO .....

4. Cada que tiempo cambia la contraseña del computador :

Menos de cada mes ..... Cada mes..X.....

Entre 2 a 6 meses ..... Entre 6 a 12 meses.....

Más de 12 meses..... Nunca .....

5. Tienen contraseña los archivos a los que usted accede, diferente a la del computador.

SÍ ..... NO ..X.....

6. En caso que la respuesta sea afirmativa responda lo siguiente:

Cada que tiempo cambia esta contraseña

Menos de cada mes ..... Cada mes.....

Entre 2 a 6 meses ..... Entre 6 a 12 meses.....

Más de 12 meses..... Nunca .....

7. Tienen contraseña los archivos que usted genera:

SÍ ..... NO ..X.....

8. Cada que tiempo cambia la contraseña de los archivos

Menos de cada mes ..... Cada mes.....

Entre 2 a 6 meses ..... Entre 6 a 12 meses.....

Más de 12 meses..... Nunca .....

9. Cuál es el nombre del antivirus que tiene su computador?

..... NOD 32 ..... No sabe .....

10. Seleccione lo que usted considera es más importante en la seguridad de la información y ponga el número: Muy importante (5), Importante (4), Regular (3), Poco importante (2), Nada importante (1)

5 ..... Política de seguridad de la información

4 ..... Contraseñas fuertes

5 ..... Respaldos periódicos de la información

4 ..... Información en la nube

4 ..... Capacitación en seguridad

11. Porqué cree Usted que se debe tener una política de seguridad de la información

..... Para mejor un mismo estandar .....

SECCIÓN PROCESAMIENTO

Esta sección se refiere a la forma como se capta u obtiene la información que se gestiona en la Unidad.

12. Como es la captación o recolección de la información que se procesa y analiza.

Utiliza algún programa de automatización .....

La recibe a través de un Excel ..... X .....

Ingresa la información utilizando un portal web ..... X .....

La información que obtiene de los usuarios está en la intranet .....

13.- En la Dirección de Gestión Económica-CTDG se cuenta con algún procedimiento documentado de recolección de información.

Sí ..... No ..... X ..... No sabe .....

14.-Roles de quienes tienen acceso a la información para su procesamiento

Rol directivo CTDG .....

Rol ejecución de la CTDG ..... X .....

Rol de coordinación de la CTDG .....

Otros funcionarios .....

15. Respecto de la información que usted utiliza /procesa, escoja:

Que perjuicio causaría a la Institución el no disponer de la información:

Muy alto ..... Alto ..X.. Medio ..... Bajo .....No sabe

16. Que perjuicio causaría a la Institución si la información estuviera modificada:

Muy alto ..... Alto ..X.. Medio ..... Bajo .....No sabe

17. Que perjuicio causaría a la Institución si la información fuera conocida por quien no debe:

Muy alto ..X.. Alto ..... Medio ..... Bajo .....No sabe

18. Como realiza el procesamiento de la "información"

Manual ..X.. Automática .....

19.-Tiene algún nivel de clasificación la información que procesa, escoja.

Confidencial ..X..

Pública ..X..

No clasificada .....

20.- Escoja el mecanismo que utiliza como respaldo (control) para verificar las modificaciones de un archivo o documento.

Firma física del documento .....

Firma electrónica .....

No conoce ..X..

Otros .....

21.- Posee usted firma electrónica

Sí ..... No ..X..... No sabe .....

22.- Indique donde se almacena los informes que son generados en su Dirección.

Archivos físicos .....

Archivos digitales ..X..

Nube (cloud) .....

No conoce con precisión .....

23. Existe una organización del archivo de la información digital, por ejemplo las carpetas están codificadas u organizadas con una nomenclatura determinada.

Si ..... No ..... No conoce ..X..

Anexo 3. Controles de la norma ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

6. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

8. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta. Octubre-2013