RESUMEN – TRABAJO DE GRADO

AUTORES	ERIKA LORENA MOLINA RINCÓN OSCAR HUMBERTO RODRIGUEZ ALVAREZ YALIDE SANCHEZ DELGADO JOHN ALEXANDER VERGEL NÚÑEZ
FACULTAD	INGENIERÍAS
PLAN DE ESTUDIOS	ESPECIALIZACIÓN AUDITORIA DE SISTEMAS
DIRECTOR	ANTÓN GARCÍA BARRETO
TÍTULO DE LA TESIS	GUÍA PARA LA SEGURIDAD BASADA EN LA NORMA ISO/IEC 27002, PARA LA DEPENDENCIA DIVISIÓN DE SISTEMAS DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

RESUMEN

(70 palabras aproximadamente)

LA INFORMACIÓN ES UNO DE LOS ACTIVOS MÁS IMPORTANTES DE TODA ORGANIZACIÓN MODERNA, REQUIERE SER PROTEGIDA FRENTE AMENAZAS QUE PUEDAN PONER EN PELIGRO SU CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD, PARA ELLO SE PRESENTA LA GUÍA DE BUENAS PRÁCTICAS COMO UN INSTRUMENTO QUE DESCRIBE DE MANERA DETALLADA, UNA SERIE DE ACTIVIDADES O ACCIONES NECESARIAS A FIN DE CUMPLIR CON LOS REQUERIMIENTOS DE SEGURIDAD ESTABLECIDOS EN LA ISO/IEC 27002 “CÓDIGO DE BUENAS PRÁCTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN”.

CARACTERÍSTICAS

PÁGINAS: 227	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

GUÍA PARA LA SEGURIDAD BASADA EN LA NORMA ISO/IEC 27002, PARA LA DEPENDENCIA DIVISIÓN DE SISTEMAS DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

ERIKA LORENA MOLINA RINCÓN
OSCAR HUMBERTO RODRIGUEZ ALVAREZ
YALIDE SANCHEZ DELGADO
JOHN ALEXANDER VERGEL NÚÑEZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
OCAÑA
2014

GUÍA PARA LA SEGURIDAD BASADA EN LA NORMA ISO/IEC 27002, PARA LA DEPENDENCIA DIVISIÓN DE SISTEMAS DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

ERIKA LORENA MOLINA RINCÓN
OSCAR HUMBERTO RODRIGUEZ ALVAREZ
YALIDE SANCHEZ DELGADO
JOHN ALEXANDER VERGEL NÚÑEZ

Proyecto de grado presentado como requisito parcial para optar el título de Especialista en Auditoria de Sistemas

Director
ANTÓN GARCÍA BARRETO
ESP. MSC. Software Libre

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
OCAÑA
2014

DEDICATORIA

Dedico este logro principalmente a Dios por darme la sabiduría para alcanzar cada una de las metas y objetivos propuestos.

A mi madre Bertha Delgado y mi padre Alfonso Sánchez a ellos por su apoyo y ser mi motor que día a día me impulsa a seguir adelante, gracias por permitir de mis sueños una realidad.

A mis hermanos Maryi Liliana, Suli Milena, Einer A, por apoyarme incondicionalmente y compartir conmigo cada momento de mi vida.

A mis sobrinos Andrea Camila, José María y Laura Sofía, porque hoy soy un ejemplo para ellos de esfuerzo, entrega, dedicación y superación, para que nunca desmayen y alcancen sus sueños.

A mi novio Elver Álvarez por su amor, dedicación y comprensión por darme fuerzas para seguir adelante.

Y demás familiares y amigos quienes han compartido conmigo en este largo camino y hoy ven este sueño realidad.

YALIDE SÁNCHEZ DELGADO

AGRADECIMIENTOS

Agradezco a Dios por darme la sabiduría y entendimiento que me permiten alcanzar cada una de mis metas propuestas y hacer realidad este gran sueño.

A mis padres por haberme brindado la oportunidad de optar a la realización de una carrera con esfuerzo y dedicación.
A la Msc. Torcoroma Velásquez Pérez por el gran apoyo que me brindó durante mi carrera profesional y en la especialización.

Elver Álvarez, por su apoyo, colaboración y estar ahí cuando más lo necesite.

Al Msc. Antón García Barreto por su colaboración, tiempo y aportes que nos brindó para hacer de este logro una realidad.

A mis compañeros Erika L. Molina, Oscar H. Rodríguez, John A. Vergel, a ustedes mil y mil gracias por ser un grupo selecto y comprometido, por su apoyo y entrega en este proyecto que hace unos meses emprendimos y que hoy nos permite el paso una vez más alcanzar una meta.

YALIDE SÁNCHEZ DELGADO

DEDICATORIA

Este trabajo es dedicado en primer lugar a Dios, quien es la guía y soporte.

Agradezco a mis padres, ya que sin su apoyo constante habría sido imposible alcanzar esta meta, a mi hermana que siempre estuvo impulsándome y apoyándome.

OSCAR HUMBERTO RODRÍGUEZ ÁLVAREZ

DEDICATORIA

Doy gracias a Dios por todas sus bendiciones, a mis hermosos padres por todos los esfuerzos que hicieron para llevarme a donde estoy el día de hoy, a mi adorado hermano por su incondicional apoyo. A toda mi familia y a mi novia por apoyarme siempre y darme esa voz de aliento y ganas de seguir adelante para cumplir mis metas.

AGRADECIMIENTOS

Agradezco a los profesores por sus enseñanzas y a todos mis compañeros de la especialización, en especial a mis compañeros de trabajo de grado Erika, Yalide y Oscar que gracias a esos días de trabajo arduo y constante hoy podemos sentirnos orgullosos de haber cumplido nuestras metas.

Al Ing. Msc. Antón García Barreto quién nos dio los lineamientos necesarios y nos brindó toda su colaboración, apoyo y tiempo para hacer posible nuestro proyecto.

A la Ing. Msc. Torcoroma Velásquez y el Ing. Msc. Andrés Mauricio Puentes por su asistencia, tiempo y apoyo durante la especialización.

JOHN ALEXANDER VERGEL NÚÑEZ

DEDICATORIA

Doy gracias a Dios por brindarme la sabiduría, tolerancia y disciplina, gracias a esto se pudo alcanzar un logro más; además agradecerle por brindarme la oportunidad de realizar satisfactoriamente la especialización.

A mis padres por la comprensión y vos de aliento en cada momento de desánimo, por estar ahí en cada uno de los momentos de mi vida.

AGRADECIMIENTOS

Al Ingeniero Antón Gracía Barreto por brindarnos la oportunidad de realizar nuestro trabajo de grado en la División de Sistemas, por brindarnos información relevante e importante en el momento que se requería.

A la Universidad por crear estos espacios de aprendizaje que nos enriquecen en la formación profesional.

ERIKA LORENA MOLINA RINCÓN

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE CUADROS

LISTA DE ANEXOS

RESUMEN

La información es uno de los activos más importantes que se encuentra presente en una organización, por esto se hace necesario que los procesos y sistemas que la gestionan a diario deban ser protegidos de amenazas que afectan la continuidad del negocio; para ello se debe establecer unos procedimientos adecuados e implementar controles de seguridad de la información basados en la evaluación de los riesgos y en la medición de su eficacia.

Este documento se presenta como una serie de recomendaciones, que oriente la implementación de políticas, procedimientos y controles de seguridad de la información, que permita mantener el riesgo en un nivel aceptable.

INTRODUCCIÓN

Los sistemas de información se han constituido como una base imprescindible para el desarrollo de cualquier actividad empresarial; estos sistemas han evolucionado de forma extraordinariamente veloz, aumentando la capacidad de gestión y almacenamiento. Esta evolución tecnológica también ha generado nuevas amenazas y vulnerabilidades para las organizaciones.

Cuando se aborda la problemática de la seguridad, la organización analiza habitualmente aspectos relacionados con la disponibilidad de los datos, copias de seguridad, mantenimiento de los equipos de cómputo y servidores, mantenimiento de las redes de telecomunicaciones, etc., todos ellos orientados a la disponibilidad de los datos, olvidando otras características que se deben cuidar igualmente como son la integridad y la confidencialidad.

Esto implica la implementación de estrategias que involucren procesos en donde la información es un activo (es esencial para las actividades de la organización) primordial, necesita una protección adecuada.

Esta guía tiene como propósito instruir en la implementación de controles, para proteger y salvaguardar tanto la información como los sistemas que la almacenan y administran. Sustentado en un marco teórico basado en el estándar ISO/IEC 27002 código de buenas para la gestión de la seguridad de la información y los reglamentos internos de la institución.

La investigación aplicada es de tipo descriptivo, pues permite conocer las características predominantes a través de la descripción exacta de las actividades, procesos y aspectos fundamentales para la gestión de la seguridad y el instrumento para la recolección de la información a aplicar es la realización de encuesta, entrevista y lista de chequeo.

El trabajo de investigación está compuesto por: el primer capítulo que contiene el problema, donde se especifica el título, el planteamiento del problema a tratar, los objetivos que se pretenden alcanzar con la investigación, la justificación e importancia, las limitaciones que se pueden presentar así como los alcances para el desarrollo de la misma.

El segundo capítulo el cual contiene el marco teórico conformado por los antecedentes de la investigación, bases teóricas y legales con las cuales se fundamenta la investigación.

El tercer capítulo se establece la metodología para la realización de la investigación determinando el tipo de investigación que se va a realizar, la población y muestra a la cual se dirige la investigación, los instrumentos a utilizar para la recolección de la información (encuesta, entrevista y lista de chequeo) la forma como se recolectaran los datos y las técnicas para su análisis.
El cuarto Capítulo el cual contiene los resultados obtenidos de la investigación, análisis de controles existentes y una guía de buenas prácticas para la seguridad basada en la ISO/IEC

27002 código de buenas prácticas para la administración de la seguridad de la información y finalmente se incluye un capítulo de conclusiones y recomendaciones.

1. TÍTULO

Guía para la seguridad basada en la norma ISO/ICE 27002, para la dependencia división de sistemas de la universidad francisco de Paula Santander Ocaña.

1.1 PLANTEAMIENTO DEL PROBLEMA

La seguridad es el conjunto de métodos y herramientas destinados a proteger los sistemas, los datos y los activos que los almacenan ante cualquier amenaza, desde un punto de vista físico y lógico.

Actualmente las políticas de seguridad existentes en el área de sistemas de la UFPSO no se ajustan a los estándares internacionales de seguridad información, generando un mayor riesgo de que las amenazas puedan explotar las vulnerabilidades con efectos inesperados en los activos y la continuidad de las operaciones del negocio.

El uso de una guía para la seguridad basada en el código de buenas prácticas para la gestión de la seguridad de la información ISO/IEC 27002 orientará a la seguridad de la información en la división de sistemas, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo.

En caso de que la división de sistemas no actualice las políticas de seguridad existentes, de acuerdo a los estándares de seguridad de la información, se corre el riesgo de que las amenazas puedan explotar las vulnerabilidades y que pongan en peligro la protección de la información y de los activos relacionados con ella.

1.2 FORMULACIÓN DEL PROBLEMA

¿La creación de una guía de principios para la seguridad contribuirá a la protección física y lógica de los datos?

1.3 OBJETIVOS

1.3.1 Objetivo general

Diseñar una guía para la seguridad basada en la Norma ISO/IEC 27002 para la dependencia División de Sistemas de la Universidad Francisco de Paula Santander Ocaña.

1.3.2 Objetivos Específicos

- Identificar los controles implementados para gestionar la seguridad en la dependencia división de sistemas.

● Comparar los controles de seguridad de la norma ISO/IEC 27002 con los controles implementados en la división de sistemas.

● Elaborar una guía para seguridad que contenga los controles de acuerdo a la norma internacional para la seguridad de la información.

1.4 JUSTIFICACIÓN

"La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades"[1]

La dependencia División de sistemas tiene como objetivo diseñar, administrar y mantener los sistemas de información, las telecomunicaciones y la infraestructura tecnológica utilizados para el desarrollo de los procesos de la UFPSO de manera eficaz, efectiva y oportuna para satisfacción de los clientes y el uso eficiente de los recursos tecnológicos minimizando el impacto ambiental y bajo un ambiente laboral propicio para los trabajadores.

La División de Sistemas representa el soporte tecnológico de la Universidad Francisco de Paula Santander Ocaña, por esta razón se origina la necesidad de identificar controles apropiados que se deben implementar para asegurar que minimicen las amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación, código malicioso, pirateo computarizado o negación de ataques de servicios.

Con el diseño de una guía para la seguridad, se contribuirá al mejoramiento de las políticas de seguridad, con el propósito de potenciar las capacidades institucionales reduciendo la vulnerabilidad y limitando las amenazas con la intención de reducir el riesgo.

1.5 HIPÓTESIS

Al crear guías para la seguridad basada en la Norma ISO/IEC 27002: 2005, se contará con un recurso de fácil comprensión, especificado las actividades que guie la implementación de controles para fortalecer la seguridad en la dependencia de División de Sistemas de la Universidad Francisco de Paula Santander Ocaña.

1.6 DELIMITACIONES

1.6.1 Conceptual. En el presente trabajo se manejarán temas y conceptos de manera general sobre: seguridad de la información, seguridad informática, seguridad física, seguridad lógica y norma ISO/IEC 27002: 2005 estándar para la seguridad de la información.

[1]El estándar internacional ISO/IEC 17799 en su segunda edición (2005, p.8)

1.6.2 Temporal. El tiempo estipulado para la realización de la propuesta comenzará después de ser aceptada como se muestra en el cronograma de actividades.

1.6.3 Geográfica. El proyecto se desarrollará en la División de Sistemas de la Universidad Francisco de Paula Santander, Ocaña.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

2.1.1 Historia y evolución de la norma ISO/IEC 27002

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British StandardsInstitution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

- ISO 9001: BS 5750. Publicada en 1979.
- ISO 14001: BS 7750. Publicada en 1992.
- OHSAS 18001: BS 8800. Publicada en 1996.

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación.

La segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

Cinco Años después, se empezó a gestar la Familia de normas ISO-27000, apareciendo la ISO-27001, cuyo origen lo tenía en la BS-7799-2.

A continuación se revisó la ISO-17799 y lo llamaron ISO-27002.

A partir de ahí y gracias a unos grupos de trabajo muy especializados se han ido creando proyectos de normativas para la Familia ISO-27000.[2]

ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

SO/IEC 27002: El Estándar Internacional nace bajo la coordinación de dos organizaciones:

ISO: International Organization for Standardization.

IEC: International Electrotechnical Commission.

ISO e IEC hanestablecido un comitétécnicoconjuntodenominado ISO/IEC JTC1 (ISO/IEC Joint Technical Committee). Este comité trata con todos los asuntos de tecnología de información. La mayoría del trabajo de ISO/IEC JTC1 es hecho por subcomités que tratan con un campo o área en particular. Específicamente el subcomité SC 27 es el que se encarga de las técnicas de seguridad de las tecnologías de información, que es en esencia de lo que trata el Estándar Internacional ISO/IEC 27002 (antiguamente llamado ISO/IEC 17799, pero a partir de julio de 2007, adoptó un nuevo esquema de numeración y actualmente es ISO/IEC 27002.[3]

Los siguientes son algunos de los trabajos encontrados a fin con la investigación de una guía para la seguridad:

DANIEL ROMO VILLAFUERTE Y JOFFRE VALAREZCO CONSTANTE:
"Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la universidad politécnica salesiana sede Guayaquil".

CORONEL ORTIZ YENY ANDREA, GUEVARA GELVES ROCIO ALEXANDRA, JAIMES FERNANDEZ JUAN CAMILO, SALAZAR RINCÓN RAMÓN DAVID:
"Formulación de un documento que de soporte a la gestión de la seguridad física basado en

[2] [En línea] Disponible desde Internet en: http://www.iso27000.es/download/doc_iso27000_all.pdf[con acceso el 07-12-2013]
[3] [En línea] Disponible desde Internet en: http://www.iso27000.es/iso27000.html#section3a [con acceso el 07-12-2013]

la norma NTC-ISO/IEC 27002 en el Centro de Investigación Tecnológico (CDIT) DE LA VAN Ocaña". La información es uno de los activos más significativos de una organización, la cual representa una ventaja estratégica y para la cual se invierte grandes cantidades de tiempo y dinero con el fin de mantener la mayor productividad posible.

La gestión de la seguridad física es una herramienta enfocada en la protección de la información. Debe estar basada en normas o estándares evitando que usuarios no autorizados accedan a ella alterando la infraestructura tecnológica.

ANGELA MARÍA GUERRERO BAYONA, GERARDO ALFONSO VERJEL CLAVIJO, JAIME ENRIQUE RIPOLL CARVAJAL, JOHN FREDDY MELO ECHAVEZ." Desarrollo de una Guía con Políticas para Garantizar la Seguridad de la Información que se maneja en la Unidad de Presupuesto de la Universidad Francisco de Paula Santander Ocaña"**.** La unidad de presupuesto de la Universidad Francisco de Paula Santander Ocaña, no lleva un control adecuado de la información que se manipula en esta dependencia, por tal razón hay pérdida de información entre las unidades a fines. Después de una investigación exhaustiva se presenta una guía con políticas para garantizar la seguridad de la información, basados en la norma técnica Colombiana NTC-ISO/IEC 27002.

2.2 MARCO CONTEXTUAL

2.2.1 Universidad Francisco de Paula Santander Ocaña. Nace como institución de educación superior pública a través del Acuerdo 003 del 18 julio de 1974, brindando a los estudiantes de la Provincia de Ocaña y sus alrededores la alternativa de realizar sus estudios en esta institución. El "Alma Mater" tiene como misión "La Universidad Francisco de Paula Santander Ocaña, institución pública de educación superior, es una comunidad de aprendizaje y autoevaluación en mejoramiento continuo, comprometida con la formación de profesionales idóneos en las áreas del conocimiento, a través de estrategias pedagógicas innovadoras y el uso de las tecnologías; contribuyendo al desarrollo nacional e internacional con pertinencia y responsabilidad social".

Actualmente la universidad tiene cuatro facultades como son; facultad de ciencias administrativas y económicas, facultad de ingenierías, facultad de ciencias agrarias y del ambiente, facultad de educación artes y humanidades, las cuales tienen veinte nueve programas de pregrado adscritos; y adicionalmente ofrece ocho técnicos, veintiún programas a distancia y siete posgrados (especialización). Con estos programas ofertados es reconocida a nivel nacional y regional como una de las mejores universidades públicas del país y busca a través de la aplicación de normas de calidad contribuir con el crecimiento continuo de la institución. En su visión se deja claro que "La Universidad Francisco de Paula Santander Ocaña para el 2019, será reconocida por su excelencia académica, cobertura y calidad, a través de la investigación como eje transversal de la formación y el uso permanente de plataformas de aprendizaje; soportada mediante su capacidad de gestión, la sostenibilidad institucional, el bienestar de su comunidad académica, el desarrollo físico y tecnológico, la innovación y la generación de conocimiento, bajo un marco de responsabilidad social y ambiental hacia la proyección nacional e internacional".

2.2.2 División de Sistemas. Hace parte de la Universidad Francisco de Paula Santander Ocaña como proceso de apoyo, conocido como Sistema de Información, telecomunicaciones y tecnología (SITT), su objetivo principal es diseñar, administrar y mantener los sistemas de información, las telecomunicaciones y la infraestructura tecnológica utilizados para el desarrollo de los procesos de la Universidad de manera eficaz, efectiva y oportuna para satisfacción de los clientes y el uso eficiente de los recursos tecnológicos minimizando el impacto ambiental y bajo un ambiente laboral propicio para los trabajadores.

Esta dependencia es la encargada de brindar soporte tecnológico a la Universidad Francisco de Paula Santander Ocaña; por lo tanto, los procesos tecnológicos, de telecomunicaciones y sistemas de información se centran en dicha dependencia.

La misión de la División de Sistemas "Es una dependencia administrativa encargada de la implementación de sistemas de información que estén acorde a solucionar los problemas de información académica y administrativa, soporte técnico del software y hardware de la Universidad y fijación de pautas de desarrollo e implementación de nuevas tecnologías".

2.3 MARCO CONCEPTUAL

Figura 1. Marco conceptual

Fuente: Autores del Proyecto

La información es toda aquella documentación en poder de una organización, independiente de la forma que adquiera o los medios por los cuales se distribuya o almacene (cintas, papel, audio u otras alternativas), que como otros de los activos, tiene un valor para la organización y por consiguiente debe ser protegida en debida forma, de los diferentes amenazas que la pongan en riesgo. Ante esta premisa, la seguridad de la información entra a jugar un papel

predomínate en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

La ISO 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información, por esta razón es el primer paso a seguir en la protección de la información.

Por consiguiente, la seguridad de la información abarca la seguridad informática, siendo esta el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, incluyendo la información obtenida. Luego, su finalidad es asegurar que los recursos del sistema de información de una organización sean empleados de forma correcta, de acuerdo a las políticas establecidas, y que el acceso a la información, así como su modificación, sólo le sea permitida a las personas capacitadas y autorizadas.

La seguridad en la informática contiene los conceptos de seguridad física y seguridad lógica. La seguridad física, se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, entre otras, y la seguridad lógica, se refiere a la seguridad mediante el uso de software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Si bien los términos de seguridad de la información y seguridad física tienen distintos significados, es necesario que converjan con el propósito de proteger las características básicas de la información.

2.4 MARCO TEÓRICO

Una de las alternativas de análisis para el problema, la creación de una guía de principios para la seguridad contribuirá a la protección física y lógica de los datos, para proporcionar seguridad de la información a la Institución de Educación Superior.

Según la ISO/IEC 17799:2005, seguridad de la información es la preservación de la confidencialidad, la integridad y la disponibilidad de la información; pudiendo además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio[4].

Según laISO/IEC 13335-1:2004[5]

[4]AENORediciones, Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes). [En línea] Disponible desde Internet en:<file:///D:/Downloads/PUB_DOC_Tabla_AEN_9551_1%20(1).pdf>[con acceso el 08-07-2014]

[5]AENORediciones, Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes). [En línea] Disponible desde Internet en:<file:///D:/Downloads/PUB_DOC_Tabla_AEN_9551_1%20(1).pdf>[con acceso el 08-07-2014]

Confidencialidad es la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.

Disponibilidad es la propiedad de ser accesible y utilizable por una entidad autorizada.

Integridad es la propiedad de salvaguardar la exactitud y completitud de los activos.

Chamorro afirma que la seguridad informática de define como el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas[6].

Actualmente las organizaciones le apuntan a proteger el activo más importante de la organización, cuyo activo es la Información, Czinkota y Kotabedicen que consiste en un conjunto de datos que han sido clasificados y ordenados con un propósito determinado.

Gestión de seguridad de la información. "El Sistema de Gestión de la Seguridad de la Información (SGSI) en las empresas ayuda a establecer estas políticas, procedimientos y controles en relación a los objetivos de negocio de la organización, con objeto de mantener siempre el riesgo por debajo del nivel asumible por la propia organización"[7].

Por medio de un SGSI se le brinda a la organización una visión global sobre el estado de sus sistemas de información, los controles que tienen asociados y la manera como operan, para poder determinar si se están obteniendo los resultados deseados, permitiendo así, tomar decisiones para garantizar la seguridad de la información.

ISO 27002. "La ISO 27002 viene a ser un código de buenas prácticas en el que se recoge un catálogo de los controles de seguridad y una guía para la implantación de un SGSI. Al igual que el Anexo A de la ISO 27001, se compone de 11 dominios, 39 objetivos de seguridad y 133 controles de seguridad. Cada uno de los dominios conforma un capítulo de la norma y se centra en un determinado aspecto de la seguridad de la información"[8]

[6] Escuela Politécnica Nacional, plan de seguridad de la información basado en el estándar ISO 13335 aplicado a un caso de estudio. [En línea] <http://bibdigital.epn.edu.ec/bitstream/15000/5617/1/CD-4645.pdf>[con acceso el 08-07-2014]

[7] OfisegConsulting, S.L. ¿Qué es un SGSI? [En línea] <http://www.ofisegconsulting.com/iso27000.htm> [citado en 09 de julio de 2014]

[8] Inteco. Normativa. [En línea] <http://www.inteco.es/Formacion_gl/SGSI_gl/Conceptos_Basicos_gl/Normativa_SGSI_gl/> [citado en 09 de julio de 2014]

Figura 2. Distribución de los dominios de la Norma ISO 27002

Fuente: Instituto Nacional de Tecnologías de la Comunicación, INTECO – España. Normativa de un SGSI. [En línea] <http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI> [citado en 08 de julio de 2014]

ISO 27002 (Documentación). Todas las medidas que se hayan decidido implantar para la protección de la información deben quedar documentadas, la estructura de la documentación generada seguirá la siguiente forma:

Figura 3. Tipos de documentación

Fuente: Instituto Nacional de Tecnologías de la Comunicación, INTECO – España. Normativa de un SGSI. [En línea] <http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI> [citado en 08 de julio de 2014]

Donde las Políticas sientan las bases de la seguridad constituyendo la redacción de los objetivos generales y las implantaciones que ha llevado a cabo la organización. Pretenden indicar las líneas generales para conseguir los objetivos marcados sin entrar en detalles técnicos. Deben ser conocidas por todo el personal de la organización.

Los Procedimientos desarrollan los objetivos marcados en la Políticas. En ellos sí que aparecerían detalles más técnicos y se concreta cómo conseguir los objetivos expuestos en las Políticas. No es necesario que los conozcan todas las personas de la organización sino, únicamente, aquellas que lo requieran para el desarrollo de sus funciones.

Las Instrucciones constituyen el desarrollo de los Procedimientos. En ellos se llega hasta describir los comandos técnicos que se deben realizar para la ejecución de dichos Procedimientos.

Y por último los Registros evidencian la efectiva implantación del SGSI y el cumplimiento de los requisitos. En este punto también es importante el contar con una serie de indicadores o métricas de seguridad que permitan evaluar la consecución de los objetivos de seguridad establecidos.[9]

2.5 MARCO LEGAL

2.5.1 Constitución Política de Colombia. Artículo 61[10]. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

2.5.2Ley 1273 DE 2009 (enero 5)[11]. El Congreso de la República de Colombia, establece la ley 1273 por medio de la cual se modifica el Código Penal, creando un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

El proyecto tendrá como bases legales la ley 1273 de 2009, en sus Capítulos:

CAPITULO I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

[9]Inteco. Normativa. [En línea] <http://www.inteco.es/Formacion_gl/SGSI_gl/Conceptos_Basicos_gl/Normativa_SGSI_gl/> [citado en 08 de julio de 2014]

[10] REPÚBLICA DE COLOMBIA, Constitución Política De La República De Colombia De 1991,Actualizada hasta el Decreto 2576 del 27 de Julio de 2005

[11]CONGRESO DE LA REPÚBLICA, Ley 1273 de 2009 (enero 5). [En línea] Disponible desde Internet en: <http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html>[con acceso el 02-12-2013]

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II
De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad[12].

2.5.3 Ley 599 de 2000.[1] Por la cual se expide el Código Penal, título VIII de los delitos contra los derechos de autor capítulo único:

Artículo 270. Violación a los derechos morales de autor. Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a doscientos (200) salarios mínimos legales mensuales vigentes quien:

1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.

2. Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

Parágrafo. Si en el soporte material, carátula o presentación de una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, en los casos de cambio, supresión, alteración, modificación o mutilación del título o del texto de la obra, las penas anteriores se aumentarán hasta en la mitad.

Artículo 271. Defraudación a los derechos patrimoniales de autor. Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a mil (1.000) salarios mínimos legales mensuales vigentes quien, salvo las excepciones previstas en la ley:

1. Por cualquier medio o procedimiento, sin autorización previa y expresa del titular, reproduzca obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador, o transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución, o suministre a cualquier título dichas reproducciones.

3. Alquile o de cualquier otro modo comercialice fonogramas, videogramas, programas de ordenador o soportes lógicos u obras cinematográficas, sin autorización previa y expresa del titular de los derechos correspondientes.

[12]CONGRESO DE COLOMBIA. Ley 599 de 2000 (Julio 24). [En línea] Disponible desde Internet en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388>[con acceso el 02-12-2013]

5. Disponga, realice o utilice, por cualquier medio o procedimiento, la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución y representación de una obra de las protegidas en este título, sin autorización previa y expresa de su titular.

Parágrafo. Si como consecuencia de las conductas contempladas en los numerales 1, 3 y 4 de este artículo resulta un número no mayor de cien (100) unidades, la pena se rebajará hasta en la mitad.

Artículo 272. Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones. Incurrirá en multa quien:

1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados.

2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada.

3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal, o de cualquier forma de eludir, evadir, inutilizar o suprimir un dispositivo o sistema que permita a los titulares del derecho controlar la utilización de sus obras o producciones, o impedir o restringir cualquier uso no autorizado de éstos.

3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal, o de cualquier forma de eludir, evadir, inutilizar o suprimir un dispositivo o sistema que permita a los titulares del derecho controlar la utilización de sus obras o producciones, o impedir o restringir cualquier uso no autorizado de éstos.

2.5.4 Ley 1581 de 2012[13]La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20

2.5.5 Norma ISO/IEC 27002:2005. Tecnología de la información, técnicas de seguridad[14]**.** Código de práctica para la gestión de la información. Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

[13]CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
[14]Norma Técnica Colombiana ISO 27002:2005.

Esta norma puede servir como guía práctica para el desarrollo de normas de seguridad de la organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

La investigación correspondiente al análisis de la seguridad de la División de Sistemas de la Universidad Francisco de Paula Santander Ocaña es:

De enfoque; cuantitativo porque a través de la investigación se pretende estudiar, cuantificar y analizar estadísticamente los datos e información obtenidos mediante los instrumentos de recolección de información aplicadas, teniendo en cuenta las necesidades y opiniones de la población objeto del estudio.

El método a utilizar es de tipo descriptivo, porque se quiere llegar a conocer las características predominantes a través de la descripción exacta de las actividades, procesos y aspectos fundamentales de la División de Sistemas.

3.2 POBLACIÓN

En el presente proyecto el universo está conformado por la Universidad Francisco de Paula Santander Ocaña y la población se tomará del capital humano que labora en la División de Sistemas, para un total de 12 personas.

La población está compuesta por:

Perfil del cargo	Cantidad
Jefe de la dependencia; Ingeniero de Sistemas, Especialista en Práctica Docencia Universitaria, Especialista en Informática Educativa, Magister en Software Libre.	1
Coordinador SIF, Especialista en Práctica Docencia Universitaria, Especialista en Informática Educativa, Magister en Software Libre.	1
Apoyo al SIF, Ingeniero de Sistemas, Especialista en Auditoría de Sistemas	2
Apoyo al SIA, Ingeniero de Sistemas	1
Apoyo a Servicios WEB, Ingeniero de Sistemas	1
Apoyo de calidad y autoevaluación del SIG, Ingeniero de Sistemas, Especialista en Auditoria de Sistemas	1
Apoyo a Telecomunicaciones, Ingeniero de Sistemas	1
Apoyo a Servidores, Ingeniero de Sistemas	1
Apoyo al SID, Ingeniero de Sistemas, Especialista en Auditoría de Sistemas	1
Coordinador tecnológico e-learning. ingeniera de sistemas, Especialista en Administración de la Informática Educativa, Especialista en Práctica Docencia Universitaria	1

Secretaría	1
Total	**12**
Fuente: División de Sistemas UFPSO	

3.3 MUESTRA

Como se cuenta con una población objeto de estudio reducida, se ha determinado aplicar a todos el instrumento de recolección de información, siendo entonces esta la muestra. Esto con la finalidad de detectar con mayor precisión lo que puede aportar los encuestados, es decir el personal que labora directamente en la dependencia de sistemas.

3.4 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

La recopilación de la información necesaria para la estructuración del proyecto se fundamentó en las técnicas de observación, revisión documental, encuesta, entrevista y lista de chequeo aplicadas al personal que allí labora.

3.5 ANÁLISIS DE LA INFORMACIÓN

La recopilación de información de la dependencia División de Sistemas se analizará en base a la norma ISO/IEC 27002 de 2005.

Para el análisis de la información se cree necesario tomar como referencia los datos principales de los instrumentos de información aplicados, el conocimiento que tiene cada uno de los funcionarios que labora en la oficina acerca de los controles de la seguridad de la información.

3.6 SEGUIMIENTO METODOLÓGICO DE ACTIDADES

Cuadro 1. Seguimiento metodológico

OBJETIVO ESPECÍFICO	ACTIVIDAD	INDICADOR
Identificar los controles implementados para gestionar la seguridad en la dependencia división de sistemas	Revisión documental de los controles implementados en el área	Listar los documentos hallados en la división de sistemas para el desarrollo de las operaciones
	Diseño de las técnicas e instrumentos de recolección de la información	Instrumentos de recolección de la información
	Aplicación de los instrumentos de recolección de la información	Análisis de la información recolectada
Comparar los controles de seguridad de la norma ISO/IEC 27002 con los controles implementados en la división de sistemas	Identificar los controles de la Norma ISO/IEC 27002 para aplicar los que tienen relación con la dependencia.	Matriz comparativa
	Comparación de los controles existentes vs controles establecidos en la ISO/IEC 27002	
Elaborar una guía para la seguridad que contenga los controles de acuerdo a la norma internacional para la seguridad de la información.	Diseñar una guía que permita la implementación de los controles	Crear la guía mediante una serie de lineamientos ordenados y comprensibles que garanticen la implementación de los controles para la gestión de la seguridad de la UFPSO
	Establecer las actividades que guie la implementación de los controles	

Fuente: Autores del Proyecto

4. PRESENTACIÓN DE RESULTADOS

4.1 IDENTIFICACIÓN DE LOS CONTROLES IMPLEMENTADOS PARA GESTIONAR LA SEGURIDAD EN LA DEPENDENCIA DIVISIÓN DE SISTEMAS

4.1.1 Revisión documental: Mediante la exploración, observación e investigación documental, se pudo constatar que la división de sistemas cuenta con una serie de instrumentos los cuales se enunciaran a continuación:

- **Política**

Política de seguridad de la información institucional

- **Procedimientos**

R-TT-DSS-001 – Procedimiento soporte y atención al usuario_rev C
R-TT-DSS-002 – Procedimiento administración de los recursos informáticos_rev C
R-TT-DSS-001 – Procedimiento gestión de los sistemas de TI_rev A

- **Instructivos**

I-TT-DSS-001 – Instructivo servicio técnico y tencológico_rev A
I-TT-DSS-002 – Instructivo gestión de la configuración_rev B
I-TT-DSS-001 – Instructivo parametrización de los sistemas informáticos_rev A

- **Manuales**

M-TT-DSS-001 – Manual de usuario (SIF) – modulo contabilidad cxp_rev A
M-TT-DSS-002 – Manual de usuario (SIF) – modulo almacen cxp_rev A
M-TT-DSS-009 – Manual de usuario (SIB) – administración módulo de circulación _rev A
M-TT-DSS-010 – Manual de usuario (SIB) – módulo jefe _rev A
M-TT-DSS-028 – Manual especifico proceso de sistemas de información, telecomunicaciones y tecnología_rev D

- **Formatos**

F-TT-DSS-001- Formato solicitud y ejecución de requerimientos_rev C
F-TT-DSS-002- Formato mantenimiento correctivo de los equipos de computo_rev A
F-TT-DSS-004- Formato administración de usuarios y cuentas de correo_rev A
F-TT-DSS-005- Formato administración de usuarios en la bd_rev A
F-TT-DSS-007- Formato control de préstamo de salas_rev B
F-TT-DSS-008- Formato bitácora manejo de errores sitt_rev A
F-TT-DSS-010- Formato entrega de carnés_rev A
F-TT-DSS-011- Formato inventario de equipos de computo_rev A
F-TT-DSS-012- Formato ficha técnica de servidores_rev A
F-TT-DSS-013- Formato ficha técnica de redes_rev B
F-TT-DSS-014- Formato bitácora de monitoreo a servidores_rev B
F-TT-DSS-015- Formato ficha técnica de hardware_rev A
F-TT-DSS-016- Formato ficha técnica de impresoras_rev A

F-TT-DSS-017- Formato ficha técnica de software_rev A
F-TT-DSS-018- Formato inventario de telecomunicaciones_rev A
F-TT-DSS-019- Formato infraestructura de red_rev A
F-TT-DSS-021- Formato levantamiento de informacion_rev A
F-TT-DSS-002- Formato diagrama de flujo_rev A
F-TT-DSS-023- Formato modelo de datos_rev A
F-TT-DSS-024- Formato diseño preliminar de software_rev A
F-TT-DSS-025- Formato ficha técnica de si_rev A
F-TT-DSS-026- Formato control de capacitación al usuario_rev B
F-TT-DSS-027- Formato solicitud de creación de programas de educación continuada con apoyo virtual_rev A
F-TT-DSS-030- Formato seguimiento de la atención al usuario_rev A
F-TT-DSS-031- Formato mantenimiento preventivo de equipos de computo_rev A
F-TT-DSS-032- Formato mantenimiento preventivo de las salas de computo_rev A
F-TT-DSS-033- Formato control de copias de seguridad_rev B
F-TT-DSS-035- Formato bitácora de monitoreo de camaras_rev A
F-TT-DSS-039- Formato inscripción para capacitación_rev A
F-TT-DSS-040- Formato mantenimiento correctivo de servidores_rev A
F-TT-DSS-042- Formato de registro acceso a la sala de servidores_rev A

- **Otros**

L-TT-DSS-001 – Plan de mantenimiento preventivo de equipos de computo_rev A
L-TT-DSS-002 – Plan de contingencia de TI_rev A

4.1.2 Análisis de la información recolectada. Con la información recolectada se pudo evidenciar que la dependencia división de sistemas cuenta con una política de seguridad la cual discrepa de lo preceptuado en la ISO 27002 lo cual hace engorroso la efectividad que pueda brindar a la seguridad de la información y activos relacionados con ella.

De otro lado es de mencionar la escasa comunicación para dar a conocer las medidas adoptadas en dicho documento a los demás procesos, lo cual genera un escenario propicio para que amenazas atenten contra la seguridad y se aprovechen de las vulnerabilidades.

Debido a la escasa difusión, el personal que labora dentro de la división de sistemas no emplea ciertos controles descritos dentro de la política de seguridad, un claro ejemplo de esto es el consumo constante de alimentos cerca de los equipos informáticos.

Se observó la escasa comunicación entre el área de sistemas y recursos humanos en cuanto al proceso de dar de alta o de baja y asignación de privilegios en los sistemas a empleados que ingresan, dejan de laborar o es trasladado a otra área.

Se evidenció la des actualización y el desconocimiento del plan de emergencia. El personal que labora en la división de sistemas desconoce el manejo apropiado de extintores que ayuden a eliminar cualquier tipo de conflagración que se presente en dicha área, causando así la pérdida total de los recursos tecnológicos que se encuentren allí. Por consiguiente,

siendo esta área de gran importancia dentro de la institución debería poseer una mejor infraestructura física, la cual evite el ingreso abrupto y daños inesperados por cualquier tipo de eventualidad; además, no cuenta con tecnología de punta (detector de humo, alarmas y sistemas biométricos) que brinden la seguridad adecuada.

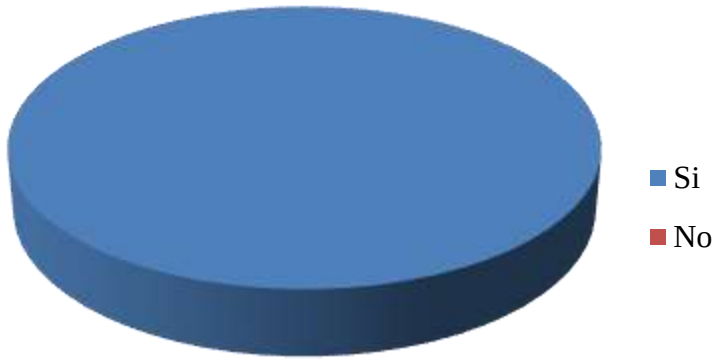
4.1.3 Aplicación de los instrumentos de recolección de la información

Tabla 1. ¿Conoce y entiende la política de seguridad, su propósito e implicaciones?

ALTERNATIVA	CANTIDAD	PORCENTAJE
Si	11	100%
No	0	0%
Total	11	100%

Fuente: Autores del Proyecto

Figura 4. Conocimiento de la política de seguridad



Fuente: Autores del Proyecto

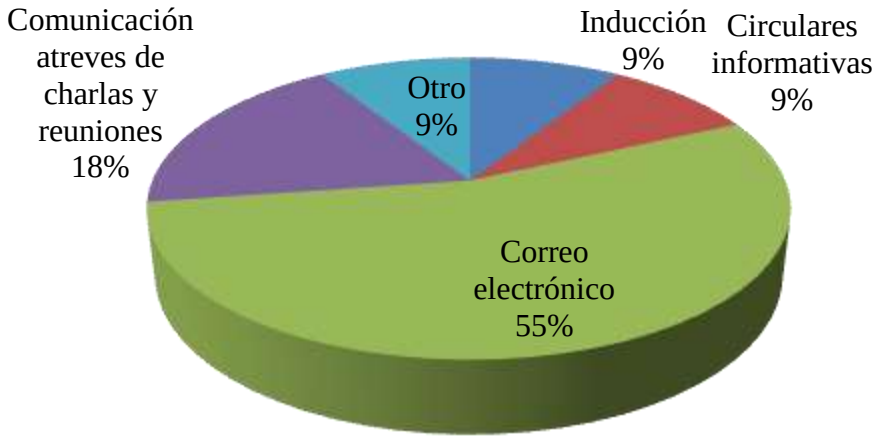
Interpretación: el 100% de las personas encuestadas manifiesta conocer y entender la política de seguridad de la información, su propósito e implicaciones.

Tabla 2. ¿Atreves de qué medios se le dieron a conocer la política?

ALTERNATIVA	CANTIDAD	PORCENTAJE
Inducción	1	9%
Circulares informativas	1	9%
Correo electrónico	6	55%
Comunicación atreves de charlas y reuniones	2	18%
Otro	1	9%
Total	11	100%

Fuente: Autores del Proyecto

Figura 5. Medios de comunicación de la política de seguridad



Fuente: Autores del Proyecto

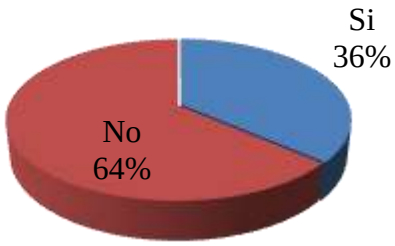
Interpretación: El 55 % de los encuestados manifiesta que se le dio a conocer la política a través de correo electrónico, dejando entrever que al momento de recibir el cargo en la inducción no se tuvo en cuenta la socialización de la política de seguridad poniendo en riesgo la seguridad de la información de la institución. En el cual no se verifica la apropiación de la política de seguridad por parte del personal encargado de la Seguridad de la Información.

Tabla 3. ¿Conoce algún Plan de Emergencia que organice y defina las actuaciones, (quien debe actuar, con qué medios, que se debe hacer, qué no se debe hacer, como se debe hacer), frente a una catástrofe natural que pueda presentarse en la dependencia?

ALTERNATIVA	CANTIDAD	PORCENTAJE
SI	4	36%
NO	7	64%
Total	11	100%

Fuente: Autores del Proyecto

Figura 6. Conocimiento de la existencia de plan de emergencia



Fuente: Autores del Proyecto

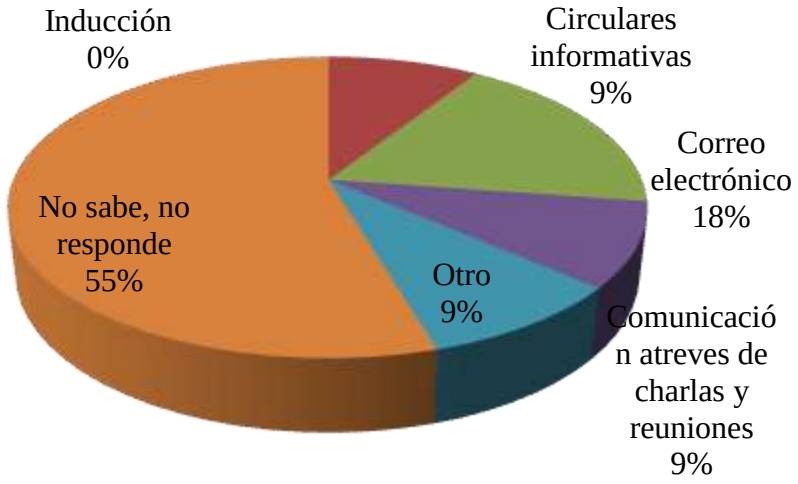
Interpretación: El64% de las personas encuestadas no conoce ningún plan de emergencia lo cual pone en riesgo la seguridad integral de las personas que laboran en el departamento de TI.

Tabla 4. ¿Atreves de qué medios se le dieron a conocer el Plan de Emergencia?

ALTERNATIVA	CANTIDAD	PORCENTAJE
Inducción	0	0%
Circulares informativas	1	9%
Correo electrónico	2	18%
Comunicación atreves de charlas y reuniones	1	9%
Otro	1	9%
No sabe, no responde	6	55%
Total	11	100%

Fuente: Autores del Proyecto

Figura 7. Medios de comunicación para dar a conocer plan de emergencia



Fuente: Autores del Proyecto

Interpretación: El 55% del personal al cual fue aplicada la encuesta manifiesta no conocer acerca de un plan emergencia que esté definido por la organización.

Tabla 5. ¿Cuándo fue la última vez que recibió una capacitación en el uso de equipos contra-incendios?

ALTERNATIVA	CANTIDAD	PORCENTAJE
Hace dos años	1	9%
Hace un año	1	9%
Hace seis meses	0	0%
Nunca	9	82%
Otro	0	0%
Total	11	100%

Fuente: Autores del Proyecto

Figura 8. Capacitación en el manejo de medios de lucha contra incendios

Fuente: Autores del Proyecto

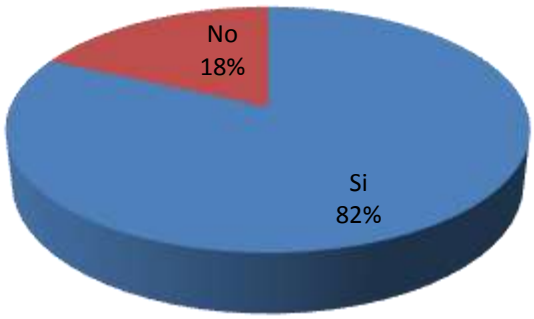
Interpretación: El 82% del personal encuestado no ha recibido capacitación en el uso de equipos contra incendios, lo cual se está colocando en riesgo la seguridad de las personas y la infraestructura tecnológica de la dependencia.

Tabla 6. ¿Conoce la existencia de un Plan de Contingencia y su propósito?

ALTERNATIVA	CANTIDAD	PORCENTAJE
Si	9	82%
No	2	18%
Total	11	100%

Fuente: Autores del Proyecto

Figura 9. Conocimiento de la existencia de plan de contingencia



Fuente: Autores del Proyecto

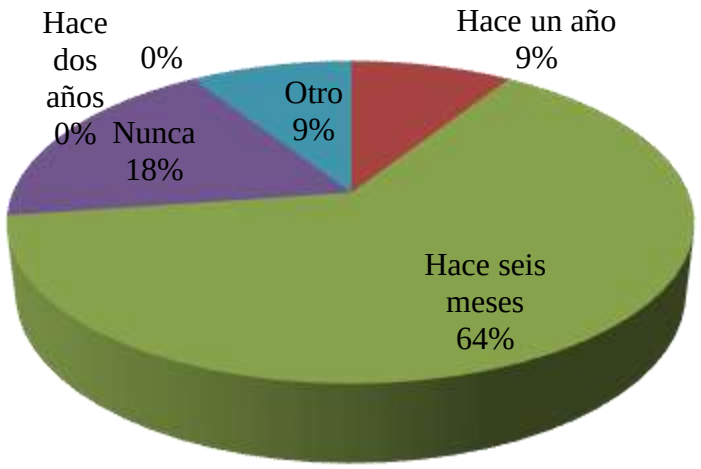
Interpretación: El 82% del personal encuestado manifiesta conocer acerca de la existencia de un plan de contingencia y su propósito.

Tabla 7. ¿Cuándo fue la última vez que recibió una capacitación en seguridad informática y/o seguridad de la información?

ALTERNATIVA	CANTIDAD	PORCENTAJE
Hace dos años	0	0%
Hace un año	1	9%
Hace seis meses	7	64%
Nunca	2	18%
Otro	1	9%
Total	11	100%

Fuente: Autores del Proyecto

Figura 10. Capacitación impartida capacitación en seguridad informática y/o seguridad de la información



Fuente: Autores del Proyecto

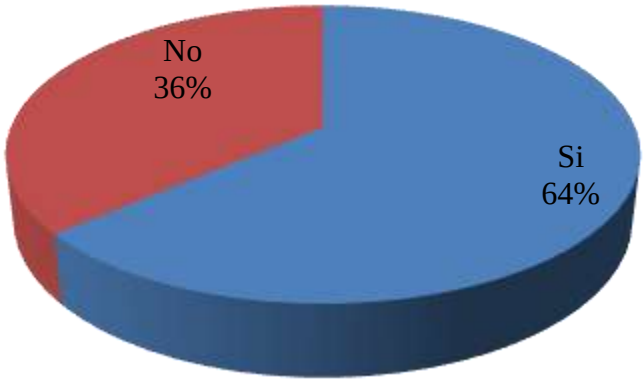
Interpretación: El 64 % del personal encuestado ha recibido capacitación en seguridad informática y/o seguridad de la información, es de resaltar el compromiso por parte de la institución en brindar capacitación a sus empleados en las posibles amenazas que puedan colocar en riesgo la seguridad de la información.

Tabla 8. ¿Usted ha laborado en horarios fuera de su trabajo en el departamento de cómputo?

ALTERNATIVA	CANTIDAD	PORCENTAJE
Si	7	64%
No	4	36%
Total	11	100%

Fuente: Autores del Proyecto

Figura 11. Trabajo fuera de horarios laborales



Fuente: Autores del Proyecto

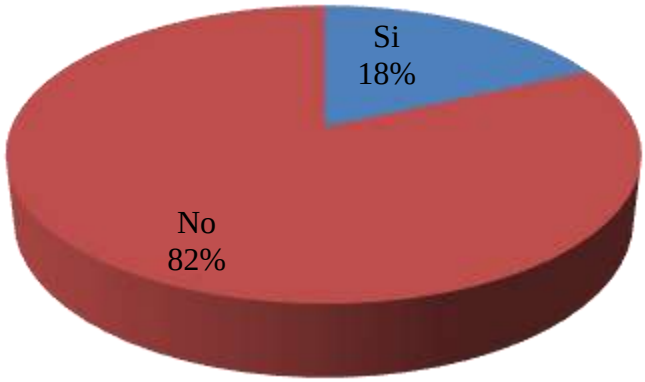
Interpretación: El 64% del personal encuestado manifiesta haber laborado en horarios fuera de su trabajo en el departamento de cómputo por cumplimiento de algunas actividades laborales.

Tabla 9. ¿Ha recibido capacitación en el desempeño de sus funciones, para saber cómo actuar luego de presentarse incidentes o crisis?

ALTERNATIVA	CANTIDAD	PORCENTAJE
Si	2	18%
No	9	82%
Total	11	100%

Fuente: Autores del Proyecto

Figura 12. Capacitación en la reacción de incidentes



Fuente: Autores del Proyecto

Interpretación: El 82% de los encuestados manifiestan no haber recibido capacitación para saber cómo reaccionar frente a un incidente que amenace la seguridad de la información.

Tabla 10. ¿Cada vez que se desatiende o se retira del puesto de trabajo utiliza un mecanismo de bloqueo adecuado?

ALTERNATIVA	CANTIDAD	PORCENTAJE
Si	11	100%
No	0	0%
Total	11	100%

Fuente: Autores del Proyecto

Figura 13. Utilización de medidas para el bloqueo de estaciones de trabajo

Fuente: Autores del Proyecto

Interpretación: El 100 % de los encuestados manifiesta utilizar un mecanismo de bloqueo adecuado en el momento que se desatiende su lugar de trabajo.

4.2COMPARACIÓN DE LOS CONTROLES DE SEGURIDAD DE LA NORMA ISO/IEC 27002 CON LOS CONTROLES IMPLEMENTADOS EN LA DIVISIÓN DE SISTEMAS

Se realizó una comparación entre la actual política de seguridad de la división de sistemas contra la norma ISO 27002.

La Política de seguridad de la división de sistemas se encuentra divida por objetivos, por lo cual se tomó fragmentos de texto de cada uno de los objetivos de la política de seguridad y se comparó con los diferentes controles que posee la norma ISO/IEC 27002.

Los fragmentos de texto se encuentran textualmente en la columna **política de seguridad de la información institucional** y los controles inmersos en el fragmento de texto se mencionan en la columna **controles ISO/IEC 27002,** por último en la columna **comentarios** se realizó una descripción de lo encontrado que hace referencia a dicho texto.

Cuadro2. Matriz de comparación

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN INSTITUCIONAL	CONTROLES ISO/IEC 27002	COMENTARIOS
El personal con cualquier tipo de vinculación al que se ha concedido acceso a los sistemas de información y sus módulos, servicios Web, espacio en servidores, acceso a las bases de datos, dispositivos de telecomunicación y redes, no debe extralimitarse en sus funciones y permisos, por el contrario debe propender por la integridad de la información, confidencialidad y el manejo prudente y reservado de la misma, limitando su accionar a lo contemplado en sus funciones	11.1.1 Política de control del acceso	La División de Sistemas limita las funciones de sus empleados en el documento "Manual Especifico de Funciones y Competencias Laborales" cuyo código de identificación es M-GH-DRH-001, acceder a través de http://ufpsonew.ufpso.edu.co/ftp/pdf/manuales/gh/M-GH-DRH-001BII.pdf. Por otra parte dentro de la clausula 3 del contrato se establece "Guardar estricta reserva total de lo que llegue a su conocimiento en razón de su oficio y que sea de naturaleza reservada o cuya divulgación pueda

		causar perjuicios al empleador".
En el caso de personal ajeno que suministre soporte técnico a la institución, que requieran acceder a las instalaciones físicas o equipo de telecomunicaciones, computadores, servidores y demás elementos relacionados con el área de la división de sistemas, así como proveedores de servicios e infraestructura, el responsable de autorizar su ingreso y generar información requerida por dicho personal, debe permitir solo acceso indispensable de acuerdo con el trabajo a ejecutar, dejando justificación escrita, de su ingreso, hora fecha de entrada y salida, especificando las funciones y actividades que debe realizar. Debe contar con las condiciones de acceso favorables para el desempeño de sus funciones solo y durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas; esto aplica para personal que labora en la institución (personal de servicios generales, de soporte técnico, electricistas entre otros) y que temporal u ocasionalmente suministre algún tipo de servicio.	6.2.1 Identificación de los riesgos relacionados con los grupos externos 9.1.2 Controles de ingreso físico 9.1.5 Trabajo en áreas aseguradas 11.1.1 Política de control del acceso 11.2.1 Registro del usuario	La universidad no lleva a cabo una evaluación de los riesgos para la información y los medios de procesamiento de la información de la organización en caso de que personal ajeno ingrese al área donde estos se encuentren; pero si se lleva un registro en el área de sistemas mediante el formato F-TT-DSS-042-Formato de registro de acceso a sala de servidores_rev A para el control de acceso físico.
Todo cambio (creación, modificación o eliminación de datos, campos, tablas, fechas, formularios, reportes, modificación de registros, usuarios, contraseñas, accesos, entre otros) que involucre o afecte los recursos informáticos, debe ser anunciado y registrado de forma explícita por los usuarios de la información y aprobado formalmente por el responsable de la administración de la misma, al nivel	10.1.2 Gestión del cambio	La división de sistemas cuenta con el formato F-TT-DSS-008A-Formato bitácora manejo de errores sitt_rev A, donde se registra fecha (D/M/AA), dependencia / origen del error, código / tipo de error, descripción del error, causas, procedimiento realizado, responsable. El cual sirve

de jefe inmediato o a quienes estos formalmente deleguen. Cualquier manipulación que se realice a la información, módulos, sistemas de información, archivos fuente, registros y demás, debe quedar formalmente registrada en los formatos aprobados correspondientes a cada proceso y actividad determinando fechas y responsables, describiendo el tipo de acción realizada desde su solicitud hasta su implementación,		de control a los cambios en cuanto al código e información de los sistemas de información. Por otra parte, cuando se realizan cambios a usuario o contraseñas se registra dichos cambios en el formato F-TT-DSS-005 - Formato administración de usuarios en la bd_rev A
Debe establecerse mecanismos que permitan el seguimiento y control. (Documentos de soporte: formato de registro control de cambios. Todo cambio, actualización o modificación realizada a un recurso informático relacionado con modificación de accesos y/o permisos, mantenimiento de software o hardware, equipos de telecomunicación, servidores, modificación de parámetros entre otros, debe realizarse de tal forma que no vulnere, exponga o disminuya el nivel de seguridad existente y la robustez actual de dicha infraestructura, así mismo debe documentarse en los formatos establecidos y/o determinar mecanismos que permitan controlar y dar seguimiento a éstas acciones.	12.5.1 Procedimientos del control del cambio	La División de Sistemas utiliza el formato F-TT-DSS-008 - Formato bitácora manejo de errores sitt_rev A para realizar el seguimiento y control de cambios, actualización o modificación realizada a un recurso informático relacionado con modificación de accesos y/o permisos, mantenimiento de software. F-TT-DSS-002 - Formato mantenimiento correctivo de equipos de computo_rev A F-TT-DSS-040 - Formato mantenimiento correctivo de servidores_rev A
El jefe de la División de Sistemas y administrador la base de datos, velarán por la seguridad en el uso de las contraseñas para acceder a los aplicativos institucionales. Para ello se contempla un período semestral, sincronizando el calendario	11.2.1 Registro del usuario 11.2.2 Gestión de privilegios 11.5.3 Sistema de gestión de claves secretas	Existe una política de gestión de contraseñas sincronizado, el cual vence cada 3 meses, dichas contraseñas deben cumplir con un parámetro (13 caracteres como

académico y los períodos de contratación para funcionarios administrativos, estableciendo la respectiva actualización de contraseñas. Se aclara que la división de sistemas requiere el apoyo necesario de la división de personal, para bloquear contraseñas a funcionarios que han culminado contratación o han sido removidos o rotados de su cargo. Bajo conocimiento de estas circunstancias, en todo caso, se aplica la restricción de contraseñas a personal sin vinculación laboral.		mínimo, letras, números y caracteres especiales). No hay una comunicación fluida entre el área de recursos humanos y la división de sistemas que permita informar la desvinculación, rotación o ingreso de nuevo personal. Por otra parte, cuando se realizan cambios a usuario o contraseñas se registra dichos cambios en el formato F-TT-DSS-005 - Formato administración de usuarios en la bd_rev A
Los funcionarios de la Universidad Francisco de Paula Santander Ocaña, se consideran responsables de la información a la que tienen acceso y/o manipulan, al hacer parte de la institución asumen el compromiso de dar uso reservado, prudente y adecuado de la información que conocen, por lo tanto deberán cumplir los lineamientos generales y especiales establecidos por la Universidad Francisco de Paula Santander Ocaña y por la ley colombiana, para protegerla, evitar pérdidas, daños, accesos no autorizados, exposición y utilización indebida de la misma.	6.1.5 Acuerdos de confidencialidad	El contrato laboral establece en la cláusula 3. Guardar estricta reserva total de lo que llegue a su conocimiento en razón de su oficio y que sea de naturaleza reservada o cuya divulgación pueda causar perjuicios al empleador
Cada funcionario de la Universidad debe firmar y renovar semestralmente o anualmente (según contratación), un acuerdo de cumplimiento donde exprese su responsabilidad de contribuir con la seguridad de la información, la confidencialidad y el buen manejo de la información.	8.1.3 Términos y condiciones laborales	

Si el trabajador deja de prestar sus servicios a la Institución, se compromete entregar toda la información y documentación respectiva de su trabajo realizado, contraseñas y usuarios tanto para el acceso a módulos, sistemas de información, correos electrónicos y equipos de cómputo o telecomunicaciones asignados y a no divulgarla directamente o a través de terceros bajo ninguna circunstancia.	8.3.1 Responsabilidades en la terminación 8.3.2 Devolución de activos	El proceso Gestión Humana dentro de sus formatos establece el formato F-GH-DRH-029 - Formato entrega del puesto de trabajo_rev A el cual establece en el índice 3. informe detallado de actividades y recursos utilizados
La información clasificada como pública puede ser entregada o publicada sin restricciones a cualquier persona advirtiendo que su uso no debe causar daños a terceros ni a los sistemas y procesos académicos o administrativos de la Universidad.	7.1.1 Inventario de activos 7.2.1 Directrices de clasificación	No se tiene implementado un procedimiento que permita la clasificación de la información.
La información clasificada como confidencial y almacenable (Los equipos, archivos o distintos medios físicos o Digitales) debe tener una marcación o etiquetado con la siguiente información: "Información para uso exclusivo del personal autorizado UFPSO".Su almacenamiento debe hacerse en lugares específicos de almacenamiento de información con las condiciones mínimas de preservación documental. Generar una codificación del grado de confidencialidad de la información.	7.2.1 Directrices de clasificación 7.2.2 Etiquetado y manejo de la información	No se tiene implementado un procedimiento que permita la clasificación de la información.
Tanto personal externo como funcionarios de cualquier estamento y con cualquier tipo de contratación así como estudiantes de la Universidad no deben intentar sobrepasar los controles de los sistemas, examinar los	7.1.3 Uso aceptable de los activos	La Universidad contiene reglamento, normas y procedimientos estipulados para el uso correcto de la infraestructura tecnológica; pero dichas

computadores y redes en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.		medidas no se han dado conocer al personal interesado. La División de Sistemas tiene implementado controles que permiten restringir páginas web inapropiadas.
Todo funcionario de la Universidad que utilice los recursos de los Sistemas, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.	7.1.3 Uso aceptable de los activos	Existen normas y procedimientos estipulados para el uso correcto de los recursos de los sistemas y de la información que se almacene en ellos. Además, el contrato laboral establece en la cláusula 3. Guardar estricta reserva total de lo que llegue a su conocimiento en razón de su oficio y que sea de naturaleza reservada o cuya divulgación pueda causar perjuicios al empleador
Es responsabilidad de los usuarios tener máximo secreto de la palabra clave; sobre todo la mantendrá secreta, usará clave que no sean triviales o simples de averiguar. Si requiere el cambio de la clave de ingreso a red o a sistemas de información debe notificar de manera personal para el cambio de contraseña siempre que crea o sospeche que su confidencialidad pueda ser vulnerada.	11.2.3 gestión de contraseñas para usuarios	El contrato laboral establece en la cláusula 3. Guardar estricta reserva total de lo que llegue a su conocimiento en razón de su oficio y que sea de naturaleza reservada o cuya divulgación pueda causar perjuicios al empleador. Existe una política de gestión de contraseñas sincronizado, el cual vence cada 3 meses, dichas contraseñas deben

		cumplir con un parámetro (13 caracteres como mínimo, letras, números y caracteres especiales). A través de este formato F-TT-DSS-001 - Formato solicitud y ejecución de requerimientos_rev C se realiza las solicitudes de los usuarios o a través de la página web http://divisis.ufpso.edu.co/contenido/18/solicita-nuestro-servicio.html
Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Universidad Francisco de Paula Santander Ocaña, deberán ser consideradas y tratadas como información confidencial.	7.1.1 Inventario de activos 7.1.3 Uso aceptable de los activos 7.2.1 Directrices de clasificación	Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Universidad Francisco de Paula Santander Ocaña solo son conocidas por el personal encargado de la administración de dichos recursos.
Cualquier cambio que se requiera realizar en los equipos de cómputo de esta institución (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable (Control registrado en los formatos estipulados para tal fin).	10.1.2 Gestión del cambio	Procedimiento soporte y atención al usuario http://www.ufpso.edu.co/ftp/pdf/procedimientos/sitt/R-TT-DSS-001CII.pdf
La reparación técnica de los equipos de cómputo y telecomunicaciones, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.	9.2.4 Mantenimiento de los equipos	Se tiene establecido un plan de acción en el cual se establece la actividad mantenimiento preventivo, cuya

		actividad se registra en el formato F-TT-DSS-031 - Formato mantenimiento preventivo de equipos de computo_rev A F-TT-DSS-040 - Formato mantenimiento correctivo de servidores_rev A, realizado por el administrador de servidores.
Los equipos de cómputo (PC, servidores, equipos de telecomunicación, cableado LAN y wireless entre otros) no deben moverse o reubicarse sin la aprobación previa del jefe del área involucrada.	9.2.1 Ubicación y protección de los equipos	
La universidad definirá la custodia de los respaldos de la información que se realizará externamente con una compañía especializada en este tema. La responsabilidad operativa en el cumplimiento de esta labor está a cargo de la División de Sistemas, quienes procesarán y vigilarán las copias de seguridad y respaldo de la información de cada aplicación Web (SIA, SIF, SID, SIB, Uvirtual, sitio web institucional). El almacenamiento de copias de seguridad de la información se realizará interna y/o externamente a la Universidad y las personas responsables de este procedimiento, serán definidas por el jefe de la dependencia (División de Sistemas), quien conocerá los estados finales de dichos respaldos y su ubicación definitiva.	10.5.1 copias de seguridad	La división de sistemas dentro del procedimiento R-TT-DSS-002 - Procedimiento administración de los recursos informaticos_rev C, numeral 5 se encuentra estipulado el procedimiento copias de seguridad; además, el personal encargado de los servidores realiza el registro de dichas copias de seguridad mediante el formato F-TT-DSS-033 - Formato control de copias de seguridad_rev B
Cámaras de Seguridad. Con el fin de implementar estrategias tecnológicas que apoyen las estrategias de seguridad en la	9.1.1 Perímetro de seguridad física	Se tienen implementados en varios puntos geográficos del campus

institución, se hace uso de cámaras de seguridad en distintos puntos geográficos del campus universitario.		universitario cámaras de seguridad.
En los centros de cómputo o áreas que la entidad considere criticas deberán existir elementos de control de incendio y alarmas.	9.1.4 Protección contra amenazas externas y ambientales	Se tiene extintores como elementos de extinción de fuego, pero no se cuenta con alarmas que permiten detectar incendios en áreas donde se encuentran recursos tecnológicos e información en documentos físicos.
Los centros de cómputo o áreas que la entidad considere criticas deberán estar demarcados con zonas de circulación y zonas restringidas	9.1.1 Perímetro de seguridad física	La Universidad no tiene demarcada las áreas críticas como zonas restringidas**.** La zona critica de la universidad se encuentra separa por paredes de las zonas de circulación sin restricción.
Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso	9.1.1 Perímetro de seguridad física 9.1.2 Controles de acceso físico	La Universidad cuenta con un área donde se centra la información (área de servidores) dicha área está separada de los sitios concurridos; además los centros de conexión cuenta con cerraduras que solo se pueden abrir con llaves. Sin embargo la zona de alto riesgo no es la adecuada, los equipos se encuentran expuestos a una intención de ingreso abrupta.
Todos los computadores portátiles, módems y equipos de comunicación se deben registrar su ingreso y salida y no debe abandonar la entidad a menos que esté acompañado por la	9.2.7 Retiro de activos	Todos los computadores portátiles, módems y equipos de comunicación ingresan a almacén quien

autorización respectiva y la validación de supervisión de la oficina de informática.		se realiza la entrega al área destino. El área destino se encarga de mantener en buenas condiciones el equipo asignado. No se realiza el registro del equipo saliente.
Toda persona que se encuentre dentro de la entidad deberá portar su identificación	9.1.2 Control de acceso físico	No se porta el carnet de forma visible.
Los centros de cómputo o áreas que la universidad considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares	9.1.1 Perímetro de seguridad física 9.1.2 Controles físicos de entrada	F-TT-DSS-042 - Formato de registro acceso a sala de servidores_rev A
En lo referente a la ubicación de computadores y hardware en general, se debe tener especial cuidado contra fallas del sistema de control del medio ambiente, y otras amenazas que puedan afectar la normal operación del sistema.	9.2.1 Ubicación y protección de los equipos	La infraestructura es asignada por planeación cuya dependencia es la encargada de realizar los diferentes estudios, de tal forma que el área asignada no presente riegos para los recursos tecnológicos.
En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo indicio de incendio. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses.	9.1.4 Protección contra amenazas externas y ambientales	Actualmente no se cuenta con detectores de calor ni de humo.

Se deben tener extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico especiales		Cada dependencia o área cuenta con extintores de acuerdo a los recursos manejados, estos son revisados periódicamente con el fin de mantener extintores en buen estado.
El cableado de la red debe ser protegido de interferencias usando canaletas que lo protejan. Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.	9.2.3 Seguridad del cableado	Se encuentran separados de acuerdo a las normas técnicas.
Las áreas en donde se tenga equipos de procesamiento de información, no se permitirá fumar, tomar ningún tipo de bebidas o consumir alimentos.	9.2.1 Ubicación y protección de los equipos	Con frecuencia se toman alimentos cerca de los equipos de cómputo.
Seguridad Física en el área de servidores. Control en el acceso físico: el acceso físico a la sala de servidores de la UFPSO se hace mediante llave. Las personas autorizadas para posesión de una copia de dicha llave, son específicamente el jefe de la división de sistemas, el administrador de dicha sala y las personas que ellos bajo previa solicitud autoricen. En ningún caso se permite a personas diferentes a las mencionadas obtener copia de dicha llave de forma abusiva y sin consentimiento. En todo caso, el funcionario debe permanecer bajo supervisión del uno o ambos funcionarios mencionados anteriormente.	9.1.2 Controles de acceso físico	Solo ingresa el personal autorizado por el jefe de la dependencia, el cual se registra su ingreso en el formato F-TT-DSS-042 - Formato de registro acceso a sala de servidores_rev A y permanece con el administrador de servidores.
Autorización de acciones a ejecutar: las acciones que se ejecuten en la sala de servidores, pueden variar de acuerdo a la solicitud que solventen, siendo posible que se requiera apoyo	9.1.2 Controles de acceso físico	

técnico de terceros donde las acciones a realizar serán específicamente autorizadas, vigiladas y controladas por el jefe de la división de sistemas y el administrador de dicha sala.		
Registro del acceso de terceros a las sala de servidores: se debe registrar el acceso a la sala de servidores, de personas ajenas a la universidad diferentes a las autorizadas, discriminando el nombre del funcionario que realiza la operación, fecha, hora de entrada, de salida, acción a ejecutar y nombre del funcionario que autoriza el acceso. En todo caso, las personas que permanezcan en la sala y operen con los servidores, deben actuar con prudencia procurando la protección de los mismos, evitando producir cortes de energía, reinicio o apagado de servidores o daño en los mismos.	9.1.2 Controles de acceso físico 9.1.5 Trabajo en áreas seguras	
Escritorios Limpios Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD's, USB, disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.	11.3.3 Política de escritorio despejado y de pantalla despejada	Estaciones desatendidas bloqueadas No se encuentra clasificada la información

Fuente: Autores del Proyecto

4.3 GUÍA DE BUENAS PRÁCTICAS

ISO/IEC 17799 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

Esta guía no pretende ser de obligatorio cumplimiento, sino informativa, proporcionando los requisitos de la norma y orientando respecto a la manera en que se pueden cumplir esos requerimientos.

Generalmente, una primera aproximación a la norma puede infundir desconfianza en cuanto a la capacidad de la empresa para poder llevar a cabo todos los requerimientos que expresa, debido a que la norma específica una amplia gama de controles de seguridad a implementar en numerosos casos con una gran carga de contenido técnico. Los objetivos, controles y lineamientos de implementación contenidos en la norma ISO/IEC 27002 pueden ser muy difíciles de valorar por una persona que no cuente con la información o formación adecuada, hecho que le impediría decidir cabalmente sobre cuál es su importancia para la empresa y las consecuencias de la implementación o no de un determinado control en ella.

Esta guía pretende suplir semejantes carencias, proporcionando información detallada sobre las posibles actividades a desarrollar para cumplir y alcanzar dicho control.

Objetivo: Contemplar las recomendaciones generales y actividades para la implantación de la seguridad de la información, utilizando la norma internacional para ello, la norma ISO/IEC 27002.

Alcance: El trabajo se presenta como una guía de buenas prácticas para la Seguridad, con la cual se pretende formular una serie de actividades que Instruyan la implementación de controles. Las actividades formuladas no serán desarrolladas, solo se presentarán Como una parte necesaria de los controles.

DESCRIPCIÓN DEL ESQUEMA O FORMATO DE LA GUÍA: el desarrollo de las medidas de seguridad se realizara mediante fichas, las cuales disponen los siguientes campos:

Dominio: Comprende las áreas de control o actuación

Objetivo: Conjunto de controles son una serie de consideraciones (controles) y un conjunto de sugerencias para cada uno de los controles.
Control: medios para manejar el riesgo, incluyen políticas, procedimiento, lineamientos, práctica; las cuales pueden ser administrativas, técnicas, de gestión o naturaleza legal.

DESARROLLO

Propósito: Hace referencia al control de la ISO 27002, el cual describe lo que se pretende proteger con su implementación.

Recomendación: Es un conjunto de sugerencias que permite llevar a cabo de una forma adecuada las acciones que orienten la implementación de los controles.

Actividades: son las acciones necesarias que se recomiendan para lograr la materialización del control, no todas serán desarrolladas debido a que no lo requieren, para ello se formula una serie de estrategias como son:

- Políticas
- Procedimientos
- Formularios o formatos
- Uso de tecnologías (Hardware y Software)

DOMINIO	Política de seguridad	OBJETIVO	Política de seguridad de la información
CONTROL	**5.1.1 Documento política de seguridad de la información**		
DESARROLLO			

Propósito: Establecer una política de seguridad con el fin de informar y concienciar a todos los empleados sobre la estrategia de seguridad de la Institución y definir las directrices generales de actuación para evitar amenazas ante incidentes que pongan en riesgo la seguridad.

La política debe obedecer a los objetivos del negocio como un requisito imprescindible para la planificación de la gestión de la seguridad de la información y a los requerimientos legales y estatutarios.

Recomendación: La política de seguridad requiere un alto compromiso de la dirección, para que las medidas adoptadas sean efectivas, entre las principales actuaciones que han de tener respaldo directo están:

- Establecer una política
- Asegurar que se establezcan controles
- Establecer roles y responsabilidades para la seguridad de la información
- Comunicar al interior de la institución la importancia de lograr los controles de seguridad de la información y cumplir la política de seguridad de la información, del cumplimiento de la ley y la necesidad de un mejoramiento continuo.
- Decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptable
- Realizar revisiones a la política

Estructura del documento

- Una definición de seguridad de la información, objetivos y alcance generales
- Establecer los objetivos de control y los controles
- Definir la estructura de la evaluación del riesgo. Definiruna metodología de análisis y evaluación de riesgos de los sistemas de información que provea un enfoque sistemático adecuado para identificar, cuantificar y priorizar los riesgos de seguridad de la información.
- La gestión de riesgo. Definir los controles de seguridad necesarios para manejar los riesgos identificados y caracterizados en el control de análisis y evaluación de riesgos.
- Una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información (incluyendo el reporte de incidentes de seguridad de la información).

- Referencias a la documentación que fundamenta la política, por ejemplo, políticas y procedimientos de seguridad más detallados

Actividades

- Difusión de la política a usuarios relevantes y una socialización con el resto de usuarios
- Mantener una comunicación interna entre las diversas dependencias de la institución acerca de la seguridad de la información, para mantener adecuadamente su funcionamiento y por ende asegurar el cumplimiento de la política y sus objetivos.

La política debiera darse a conocer r a través de los siguientes medios:

- Publicación en sitios de acceso al personal
- Inducción a nuevos funcionarios
- Comunicaciones a través de charlas y reuniones
- Intranet y plataforma para el Sistema Gestión Calidad
- Correo electrónico
- Oficios y circulares
- Inducción a partes externas relevantes

DOMINIO	Política de seguridad	**OBJETIVO**	Política de seguridad de la información
CONTROL	**5.1.2 Revisión política de seguridad de la información**		
DESARROLLO			

Propósito: La política de seguridad de la información debiera ser revisada a intervalos tiempos planeados, con la finalidad de asegurarse de su continua idoneidad, conveniencia y efectividad; dicha revisión incluye las oportunidades de evaluación para el mejoramiento así como la necesidad de cambios en el sistema, incluyendo la política de seguridad y los objetivos de seguridad de la información.

Recomendación: La revisión de la política de seguridad de la información, debiera estar reflejada en un informe de revisión el cual contenga los siguientes aspectos:
a) Mejoramiento de la efectividad.
b) Actualización de la evaluación del riesgo y el plan de tratamiento de riesgo.
c) Modificaciones a procedimientos y controles que afecten la seguridad de la información.
d) Detectar las necesidades de recursos para que en la medida de lo posible se puedan administrar de acuerdo a las prioridades y presupuesto disponible.

Actividades: El Comité de Seguridad de la Información debe revisarla a intervalos planeados y prever el tratamiento de caso de los cambios no planeados, a efectos de mantener actualizada la política.

Efectuar toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.
El Comité de Seguridad de la Información debiera aprobar las modificaciones de la política revisada

DOMINIO	Organización de la seguridad de la información	**OBJETIVO**	Manejar la seguridad de la información dentro de la organización.
CONTROL	**6.1.1 Compromiso de la gerencia con la seguridad de la información**		
DESARROLLO			

Propósito: Establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

Aprobar la política de seguridad de la información por parte de la dirección o a quien corresponda, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización.

Recomendación: La dirección debe apoyar la seguridad de la información a través de una dirección clara, mostrando compromiso, asignando roles y reconociendo responsabilidades explícitas.
Debe formular, revisar y aprobar la política de seguridad de la información, como asimismo revisar los beneficios de la implementación de la misma.

La dirección debiera:

- Asegurar que los objetivos de seguridad de la información estén identificados, cumplan con los requerimientos organizacionales y estén integrados en los procesos relevantes.
- Formular, revisar y aprobar la política de seguridad de la información.
- Revisar la efectividad de la implementación de la política de seguridad de la información.
- Proporcionar una dirección clara y un apoyo gerencial visible para las iniciativas de seguridad.
- Proporcionar los recursos necesarios para la seguridad de la información.
- Aprobar la asignación de roles y responsabilidades específicas para la seguridad de la información a lo largo de toda la Universidad.
- Iniciar planes y programas para mantener la conciencia de seguridad de la información.
- Asegurar que la implementación de los controles de seguridad de la información sea coordinado en toda la Universidad.

Actividades:
- Creación de los objetivos de la seguridad de la Información de acuerdo a los requerimientos de la Universidad e integrarlos a los procesos; además asegurase que los objetivos sean claramente identificados e implantados en los procesos institucionales de la Universidad.
- Planeación y asignación de recursos necesarios para la seguridad de la información

- Creación, aprobación y aplicación de planes de capacitación y sensibilización para los funcionarios.
- Monitoreo y vigilancia sobre la implementación de los controles de seguridad en toda la Universidad.

Estructura del documento:
Conformación del Comité de Seguridad de la Información

Área / Dirección	Representante
---	---
---	---

Estipular las funciones del Comité de Seguridad de la Información, tal y como se describe a continuación:
Este Comité tendrá entre sus funciones:

1. Revisar y proponer a la máxima autoridad de la Universidad para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
2. Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
3. Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
4. Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
5. Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
6. Garantizar que la seguridad sea parte del proceso de planificación informática de la Universidad.
7. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
8. Promover la difusión y apoyo a la seguridad de la información dentro de la Universidad.
9. Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información de la Universidad frente a interrupciones imprevistas.

DOMINIO	Organización de la seguridad de la información	**OBJETIVO**	Manejar la seguridad de la información dentro de la organización.
CONTROL	**6.1.2 Coordinación de la seguridad de la información**		
DESARROLLO			

Propósito: Involucrar la cooperación y colaboración del Director, usuarios, administradores, docentes, diseñadores de aplicación, auditores y personal de seguridad, y capacidades especializadas en áreas como seguros, temas legales, recursos humanos, TI o gestión del riesgo.

Recomendación:

- Asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información.
- Identificar cómo manejar las no-conformidades.
- Aprobar las metodologías y procesos para la seguridad de la información; por ejemplo, la evaluación del riesgo, la clasificación de la información.
- Identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas.
- Evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de información.
- Promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización.
- Evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados.

Si la Universidad no utiliza grupos inter-funcionales separados; por ejemplo, porque dichogrupono es apropiado para el tamaño de la Universidad; las acciones arriba descritasdebieran ser realizadas por otro organismo gerencial adecuado o un gerente individual.

DOMINIO	Organización de la seguridad de la información	**OBJETIVO**	Manejar la seguridad de la información dentro de la organización.
CONTROL	**6.1.3 Asignación de responsabilidades de la seguridad de la información**		
DESARROLLO			

Propósito: Definir claramente las responsabilidades para la protección de los activos individuales y llevar acabo los procesos de seguridad específicos.

Definir claramente las responsabilidades locales para la protección de activos y para llevar a cabo procesos de seguridad específicos, como la planeación de la continuidad del negocio.

Recomendación: Las personas con responsabilidades de seguridad asignadas pueden delegar las tareas de seguridad a otros. No obstante, ellos siguen siendo responsables y debieran determinar si cualquier tarea delegada ha sido realizada correctamente.

La responsabilidad de asignar los recursos e implementar los controles con frecuencia permanece con los gerentes individuales. Una práctica común es nombrar a un propietario para cada activo quien entonces se volverá responsable por su protección diaria.

Actividades:

- Identificación de los procesos y activos de información relevantes y los distintos niveles de autorización para los activos de información identificados.
- Formalización a los responsables por cada proceso/activo de información identificado.

Estructura del documento:

La asignación de responsabilidades de la seguridad de la información debe ejecutarse en forma alineada a la política de seguridad de la información de acuerdo a lo estipulado en la cláusula 5 política de seguridad.

El Magíster EDGAR A. SÁNCHEZ ORTIZ, Director y Representante Legal de la UFPSO, asigna las funciones relativas a la Seguridad Informática de la Universidad Francisco de Paula Santander Ocaña a _____ (indicar el cargo), en adelante el "Responsable de Seguridad de la Información", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la Universidad Francisco de Paula Santander Ocaña, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente.

A continuación se detallan los procesos de seguridad, indicándose en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Proceso	Responsable
Seguridad de Recursos Humanos	---------
Seguridad Física y Ambiental	---------
Gestión de las Comunicaciones y Operaciones	---------
Control de Acceso	---------
---------	---------
---------	---------

De igual forma, seguidamente se detallan los propietarios de la información, quienes serán los Responsables de las Unidades Organizativas a cargo del manejo de la misma:

Información	Recursos asociados (activos)	Procesos involucrados	Propietario	Nivel de autorización
Inventario	Sistema de información, bases de datos, datos, documentos físicos, ---------	---------	---------	---------
---------	---------	---------	---------	---------

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.

DOMINIO	Organización de la seguridad de la información	**OBJETIVO**	Manejar la seguridad de la información dentro de la organización.
CONTROL	**6.1.4 Proceso de autorización de recursos para el tratamiento de la información**		

DESARROLLO

Propósito: Definir e implantar un proceso de autorización por parte de la dirección para las nuevas instalaciones de procesamiento de información.

Recomendación: Los nuevos recursos de procesamiento de información deberán ser autorizados por el Responsable de Seguridad de la Información, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.
Las siguientes guías deben ser consideradas para el proceso de autorización:

- Cumplir con los niveles de aprobación vigentes de la Universidad, incluso el responsable del ambiente de seguridad de la información, asegurando el cumplimiento de las políticas y requerimientos.
- Verificar el hardware y software cuando corresponda, para garantizar su compatibilidad con los componentes de otros sistemas de la Universidad.
- El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso deberá ser evaluado en cada caso por el Responsable de Seguridad de la Información y debe ser autorizado por el Responsable del Área Informática.

Actividades:

- Las nuevas instalaciones deberán poseer un mecanismo apropiado de identificación de usuarios, la que debe ser otorgada por el Responsable de Seguridad de la Información, verificando el cumplimiento con las políticas de seguridad.
- Chequear cuando sea necesario el hardware y software para garantizar su compatibilidad con la infraestructura actual.
- El uso de dispositivos de carácter personal como laptops o dispositivos de mano, que sean utilizados para procesar información de la institución, podrían introducir nuevas vulnerabilidades, por lo tanto deben considerarse controles adicionales.

DOMINIO	Organización de la seguridad de la información	**OBJETIVO**	Manejar la seguridad de la información dentro de la organización.
CONTROL	**6.1.5 Acuerdos de confidencialidad**		

DESARROLLO
Propósito: Identificar y revisar regularmente que los requerimientos de confidencialidad o acuerdos de no-divulgación reflejan las necesidades de la organización para proteger la información. **Recomendación:** Se deberá definir, implementar y revisar regularmente los acuerdos de confidencialidad o de no-divulgación para la protección de la información de la Universidad. Dichos acuerdos deberán responder a los requerimientos de confidencialidad o no-divulgación de la información de la UFPSO; además, deberán ser revisados de acuerdo a la fecha estipulada en el control. Asimismo, deberá cumplir con toda legislación o normativa que alcance alaUniversidad en materia de confidencialidad de la información. Dichos acuerdos deben celebrarse tanto con el personal del organismo como con aquellos terceros que se relacionen de alguna manera con su información. **Actividades:** • Clasificación de la información (pública-secreta). • Definición de la duración del acuerdo, incluyendo la duración indefinida. • Estipulación de las acciones necesarias una vez que el acuerdo haya terminado. • Asignación de responsabilidades para evitar la divulgación no-autorizada de la información. • Describir el derecho de auditar y supervisar actividades que involucren información secreta. • Estipular el procedimiento a seguir frente a una divulgación no autorizada o violaciones de la información secreta. • Definición de los términos de devolución o destrucción de la información, una vez finaliza un acuerdo. • Describir las acciones necesarias en el caso de no cumplir con el acuerdo.

DOMINIO	Organización de la seguridad de la información	**OBJETIVO**	Manejar la seguridad de la información dentro de la organización.
CONTROL	**6.1.6 Contacto con las autoridades**		
DESARROLLO			
Propósito: Mantener los contactos apropiados con las autoridades relevantes. **Recomendación:** Mantener los contactos puede ser un requerimiento para apoyar el manejo de un incidente de seguridad o la continuidad del negocio y el proceso de planeación de contingencia. Los contactos con organismos reguladores también son útiles para anticipar y prepararse para cambios en la ley o las regulaciones que la organización debiera cumplir. Los contactos con otras autoridades incluyen servicios públicos,			

servicios de emergencia, salud y seguridad; por ejemplo, departamento de bomberos (en conexión con la continuidad del negocio), proveedores de telecomunicaciones (en conexión con el routing de la línea) y los proveedores de agua (en conexión con los medios de enfriamientos del equipo).

Actividades:

- Mantener un registro de las empresas prestadoras de servicio tales como bomberos, hospital, defensa civil, proveedores de servicio, entre otros; donde se identifique claramente la persona de contacto, dirección y número telefónico.

DOMINIO	Aspectos Organizativos de la Seguridad de la Información	**OBJETIVO**	Manejar la seguridad de la información dentro de la organización.
CONTROL	**6.1.7 Contacto con Grupos de Especial Interés**		

DESARROLLO

Propósito: La organización interna de la institución debiera mantener Contactos apropiados con grupos de interés especial o grupos de seguridad externos, incluyendo las autoridades relevantes, para mantenerse actualizado, monitorear los estándares, evaluar los métodos y proporcionar vínculos adecuados para el manejo de los incidentes de seguridad de la información.

Recomendación: El contacto con grupos de especial interés debe considerarse como un medio para

- Adquirir y mejorar conocimientos acerca de las mejores prácticas y estar actualizado con la información de seguridad relevante
- Asegurar que la concientización acerca de la seguridad de la información esté actualizada y completa
- Recibir advertencias de alertas tempranas, asesorías, avisos y recomendaciones ante ataques y vulnerabilidades
- Proporcionar vínculos adecuados durante el tratamiento de los incidentes de seguridad de la información.
- obtener acceso a consultoría especializada de seguridad de la información
- compartir e intercambiar información sobre tecnologías, productos, amenazas o vulnerabilidades;

Actividades

Se debe nombrar un responsable de Seguridad de la Información quien será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad.

Se debe establecer acuerdos de intercambio de información para mejorar la cooperación y

Coordinación de temas de seguridad. Tales acuerdos debieran identificar los requerimientos de Protección de información sensible.

DOMINIO	Aspectos Organizativos de la Seguridad de la Información	**OBJETIVO**	Manejar la seguridad de la información dentro de la organización.
CONTROL	**6.1.8Revisión independiente de la seguridad de la información**		
DESARROLLO			

Propósito: La seguridad de la información debe ser revisada de una manera independiente a intervalos planeado o cuando ocurran cambios significativos en la implementación de la seguridad, esto se hace con el fin de manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información).

Recomendación

- La revisión independiente es necesaria para asegurar la continua idoneidad, eficiencia y efectividad del enfoque de la organización para manejar la seguridad de la información.
- La revisión debiera incluir las oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el enfoque por seguridad, incluyendo políticas y objetivos de control.
- La revisión debe ser llevada a cabo por personas independientes al área de revisión; por ejemplo, la función de la auditoria interna, un gerente independiente o una tercera organización especializada en revisiones.
- Las personas que llevan a cabo estas revisiones debieran tener la capacidad y experiencia apropiada.
- Los resultados de la revisión independiente se debieran registrar y reportar a la gerencia que inició la revisión y deben mantener los registros.
- Si la revisión independiente identifica que el enfoque y la implementación de la organización para manejar la seguridad de la información no son adecuadas o no cumplen con la dirección para la seguridad de la información establecida en el documento de la política de seguridad dela información, la gerencia debiera considerar acciones correctivas.
- se debe realizar una revisión de las actividades de implantación al menos 1 vez al año

Actividades: El Comité de Seguridad de la Información debe proponer un auditor interno o consultor externo para realizar revisiones independientes sobre la vigencia, implementación y gestión de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas del Organismo reflejan adecuadamente sus disposiciones.
Las revisiones deben incluir las oportunidades de evaluación de mejoras y las necesidades de cambios de enfoque en la seguridad, incluyendo políticas y objetivos de control.

DOMINIO	Aspectos Organizativos de la Seguridad de la Información	**OBJETIVO**	Mantener la seguridad de la información y los medios de

			procesamiento de información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos.
CONTROL	**6.2.1Identificación de los riesgos derivados del acceso de terceros**		
DESARROLLO			

Propósito: Identificar los riesgos asociados a la información, los medios de procesamiento de la información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos y mantener la seguridad de esta misma.

Recomendación: Se debe identificar los riesgos asociados con terceros teniendo en cuenta:

- Los medios de procesamiento de información a los cuales necesita tener acceso el grupo externo.
- El tipo de acceso que tendrá el grupo externo a la información y los medios de procesamiento de la información.
    - acceso físico: oficinas, edificios de cómputo, archivadores
    - acceso lógico: bases de datos o sistemas de información de la organización;
    - conectividad de red entre las redes de la organización y el grupo externo; por ejemplo, conexión permanente, acceso remoto;
    - si el acceso se da fuera o dentro del local;
- Los motivos para los cuales se solicita el acceso.
- El valor, sensibilidad y criticidad de la información involucrada.
- Los controles necesarios para proteger la información que no puede ser accesible por terceros.
- Como se identifican y verifican los controles.
- Diferentes medios y controles empleados por el grupo externo cuando almacena, procesar, transmitir e intercambia información.
- Impacto del acceso denegado al tercero, o que el tercero ingrese o reciba información inexacta o engañosa.
- El personal del grupo externo involucrado en el manejo de la información de la organización.
- Cómo se puede identificar a la organización y el personal autorizado que tiene acceso, cómo verificar la autorización, y con cuánta frecuencia se necesita reconfirmar esto.
- Los diferentes medios y controles empleados por el grupo externo cuando almacena, procesa, comunica, comparte e intercambia información.
- El impacto del acceso no disponible para el grupo externo cuando lo requiere, y el grupo externo que ingresa o recibe información inexacta o confusa.

- Prácticas y procedimientos para lidiar con los incidentes en la seguridad de la información y los daños potenciales, y los términos y condiciones para la continuación del acceso del grupo externo en caso de un incidente en la seguridad de la información.
- Requerimientos legales y reguladores y otras obligaciones contractuales relevantes que se debieran tomar en cuenta para el grupo externo.
- Los intereses de los clientes/usuarios/beneficiarios que pueden ser afectados por terceros.

No se debiera otorgar acceso a los grupos externos a la información de la organización hasta que se hayan implementado los controles apropiados y, cuando sea factible, se haya firmado un contrato definiendo los términos y condiciones para la conexión o acceso y el contrato de trabajo.
Se debiera asegurar que el grupo externo esté al tanto de sus obligaciones y acepte las responsabilidades involucradas en tener acceso, procesar, comunicar o manejar la información y los medios de procesamiento de información de la organización.
Las organizaciones pueden enfrentar riesgos asociados con procesos, gestión y comunicación inter-organizacional si se aplica un alto grado de abastecimiento externo, o cuando existen varios grupos externos involucrados.
Se otorga permiso a terceros solo si se han implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso, algunos permisos a terceros son:

- Personal de mantenimiento y soporte de hardware y software.
- Limpieza, "catering", guardia de seguridad y otros servicios de soporte por parte de terceros.
- Pasantías y otras designaciones de corto plazo.
- Consultores.
- Auditores

Actividades: Establecer e implementar controles, requerimientos de seguridad y compromisos de confidencialidad aplicables para otorgar permisos a terceros.
Cuando exista la necesidad de otorgar acceso a terceras partes a información del Organismo, el Responsable de Seguridad de la Información y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos.

Utilizar acuerdos de no-divulgación de la informaciónsi existe la necesidad de que terceros ingresen a los medios de procesamiento de la información.

DOMINIO	Aspectos Organizativos de la Seguridad de la Información	**OBJETIVO**	Mantener la seguridad de la información y los medios de procesamiento de

			información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos.
CONTROL	**6.2.2 Tratamiento de la seguridad en relación con los clientes**		
DESARROLLO			

Propósito: Tratar todos los requerimientos de seguridad identificados antes de proporcionar a los clientes acceso a la información o activos de la organización.

Recomendación: Para el tratamiento de la seguridad de los activos se debe considerar los siguientes controles antes de proporcionar a los clientes acceso a cualquier activo de la organización:

- Cumplimiento de la Política de seguridad de la información del Organismo.
- protección de activos del organismo, incluyendo:
  - Procedimientos para proteger los bienes del Organismo, abarcando los activos físicos, la información y el software.
  - procedimientos para determinar si algún activo está comprometido; por ejemplo, cuando ha ocurrido una pérdida o modificación de data;
  - Controles para proteger y garantizar integridad de la información.
  - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo
  - restricciones sobre el copiado y divulgación de información;
- Descripción de los servicios disponibles.
- las diferentes razones, requerimientos y beneficios para el acceso del cliente/usuarios/beneficiarios
- política de control de acceso, abarcando:
  - Métodos de acceso permitidos, y el control y uso de identificadores singulares como IDs del usuario y claves secretas;
  - Un proceso de autorización para el acceso y privilegios del usuario;
  - Un enunciado que establezca que está prohibido todo acceso que no esté explícitamente autorizado;
  - Un proceso para revocar los derechos de acceso o interrumpir la conexión entrelos sistemas;
- Acuerdos para el reporte, notificación e investigación de las inexactitudes de la información (por ejemplo, de detalles personales), incidentes de seguridad de información y fallas en la seguridad;
  Una descripción de cada servicio que va a estar disponible;
- El nivel a alcanzar del servicio y los niveles inaceptables del servicio;

- El derecho a monitoreo o seguimiento y a revocar, cualquier actividad relacionada con los activos de información del servicio.
- Las respectivas obligaciones de la organización y el cliente;
- Responsabilidades legales, contractuales y derechos de propiedad intelectual (IPRs).

Los requerimientos de seguridad relacionados con el acceso del cliente a los activos organizacionales pueden variar considerablemente dependiendo de los medios de procesamiento de la información y la información a la cual se tiene acceso.

Actividades

- Realizar acuerdos con el cliente, los cuales contengan todos los riesgos identificados y los requerimientos de seguridad.
- Establecer un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
- Llevar un Proceso claro y detallado de administración de cambios.
- Diseñar Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- Diseñar Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- Diseñar Controles que garanticen la protección contra software malicioso.

DOMINIO	Aspectos Organizativos de la Seguridad de la Información	**OBJETIVO**	Mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos.
CONTROL	**6.2.3 Tratamiento de la seguridad en contratos con terceros.**		
DESARROLLO			

Propósito: Los contratos o acuerdos con terceros que involucran el acceso, procesamiento, comunicación no manejo de la información o medios de procesamiento de información de la organización o agregan producto o servicios a los medios de procesamiento de información debieran abarcar todos los requerimientos de seguridad relevantes.

Recomendación: Dentro del contrato o acuerdo se debe considerar los siguientes términos a incluirse en el acuerdo para cumplir con los requerimientos de seguridad:

- La política de seguridad de la información.
- Controles para asegurar la protección de los activos, incluyendo:
    - Procedimientos para proteger los bienes del Organismo, abarcando los activos físicos, la información y el software.
    - cualquier control y mecanismo de protección física requerido
    - controles para asegurar la protección contra software malicioso
    - procedimientos para determinar si algún activo está comprometido; por ejemplo, cuando ha ocurrido una pérdida o modificación de data.
    - controles para asegurar el retorno o destrucción de información y los activos al final de, o en un punto de tiempo acordado durante el acuerdo.
    - confidencialidad, integridad, disponibilidad y cualquier otra propiedad relevante de los activos.
    - restricciones sobre el copiado y divulgación de información, y la utilización de acuerdos de confidencialidad.

- Capacitación del usuario y administrador en métodos, procedimientos y seguridad.
- Asegurar la conciencia del usuario para las responsabilidades y problemas de la seguridad de la información.
- Provisión para la transferencia de personal, cuando sea apropiado.
- Responsabilidades relacionadas con la instalación y mantenimiento de hardware y software.
- Una estructura de reporte clara y formatos de reporte acordados.

- Un proceso claro y especificado de gestión de cambio.
- Política de control de acceso, abarcando.
  - las diferentes razones, requerimientos y beneficios que hacen que sea necesario el acceso de terceros.
  - métodos de acceso permitidos, y el control y uso de identificadores singulares como IDs del usuario y claves secretas.
  - un proceso de autorización para el acceso y privilegios del usuario.
  - un requerimiento para mantener una lista de personas autorizadas a utilizar los servicios que se están poniendo a disposición, y los derechos y privilegios con respecto a este uso.
  - un enunciado que establezca que está prohibido todo acceso que no esté explícitamente autorizado.
  - un proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.

- Acuerdos para el reporte, notificación e investigación de las inexactitudes de la información (por ejemplo, de detalles personales), incidentes de seguridad de información y fallas en la seguridad.
- Una descripción de cada servicio que debiera estar disponible, y una descripción de la información que debiera estar disponible junto con su clasificación. El nivel objetivo del servicio y los niveles inaceptables del servicio.
- Una definición del criterio del desempeño verificable, su monitoreo y reporte.
- El derecho a monitoreo o seguimiento y a revocar, cualquier actividad relacionada con los activos de información del servicio.
- El derecho de auditar las responsabilidades definidas en el acuerdo, el derecho que un tercero lleve a cabo la auditoria, y enumerar los derechos estatutarios de los auditores.
- Requerimientos de continuidad del negocio, incluyendo las medidas de disponibilidad y confiabilidad, en concordancia con las prioridades comerciales de la organización.
- Las obligaciones respectivas de la organización y el cliente.
- Acuerdos para el manejo de incidentes de seguridad.
- Requerimientos de continuidad.
- Condiciones para la negociación/terminación de los acuerdos:
  - se debiera establecer un plan de contingencia en caso que alguna de las partes desee terminar la relación antes del fin del acuerdo;
  - renegociación de acuerdos si los requerimientos de seguridad de la organización cambian;
  - documentación actual de las listas de activos, licencias, acuerdos y derechos relacionados a ellos.

Actividades

- Organizar, planear y manejar la transición a un acuerdo de abastecimiento externo que cuente con los procesos adecuados para manejar los cambios y los acuerdos de negociación/terminación.
- Definir el acuerdo o contrato donde se considere procedimientos para continuar el procesamiento en el evento que la tercera persona no pueda suministrar los servicios para evitar cualquier demora en acordar el reemplazo de los servicios.

DOMINIO	Gestión de Activos	**OBJETIVO**	Lograr y mantener una apropiada protección de los activos organizacionales
CONTROL	**7.1.1 Inventario de Activos**		
DESARROLLO			

Propósito: Lograr y mantener una apropiada protección de los activos organizacionales. Los propietarios deben identificar todos los activos y se debe asignar la responsabilidad por el mantenimiento de los controles apropiados.

Recomendación: La organización debe identificar todos los activos y documentar la importancia de estos mismos algunos de ellos son:

- Información: bases de datos, archivos de datos, documentación, contratos, acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoría e información archivada.
- Activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilidades.
- Activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos, personas, y sus calificaciones, habilidades y experiencia.
- Activos intangibles, tales como la reputación y la imagen del Organismo.

El inventario de los activos debiera incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial.

El inventario no debiera duplicar innecesariamente otros inventarios, pero se debiera asegurar que el contenido esté alineado.

Los inventarios de los activos ayudan a asegurar que se realice una protección efectiva de los activos, y también puede requerir de otros propósitos comerciales; como planes de salud y seguridad, seguros o razones financieras (gestión de activos).

El inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.

Actividades:
Identificar todos los activos y elaborar y mantener actualizado un inventario de todos los activos importantes.

OMINIO	Gestión de Activos	**OBJETIVO**	Lograr y mantener una apropiada protección de los activos organizacionales
CONTROL	**7.1.2 Propiedad de los activos**		
DESARROLLO			

Propósito: Lograr mantener la protección adecuada de los activos de la organización identificando los dueños para todos los activos.

Asignar la responsabilidad para el mantenimiento de los controles adecuados.

Recomendación: Se debiera designar los Propietarios de los activos identificados, quienes deben cumplir sus funciones de propietario .Toda la información y los activos junto a sus medios de procesamiento de información deben ser propiedad de un responsable designado en el organismo.
Los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, pero conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de los activos debiera ser documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.
Se debiera asegurar que los activos de información sean debidamente clasificados considerando su criticidad, definiendo y revisando periódicamente los accesos de acuerdo a la política correspondiente.
La propiedad puede ser asignada a:
a) un proceso.
b) un conjunto de actividades definido.
c) una aplicación.
d) un conjunto de data definido.
Actividades:

- Asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente en función a su valor
- Definir y revisar periódicamente los requisitos de seguridad y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.

- Velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

DOMINIO	Gestión de Activos	**OBJETIVO**	Lograr y mantener una apropiada protección de los activos organizacionales
CONTROL	**7.1.3 Uso aceptable de los activos**		
DESARROLLO			

Propósito: Identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

Recomendación: Los empleados, contratistas y terceros que usan o tienen acceso a los activos debieran estar al tanto de los límites existentes para el uso de la información y los activos asociados con los medios y recursos del procesamiento de la información; debieran ser responsables por el uso que le den a cualquier recurso de procesamiento de información realizado bajo su responsabilidad.

Todos los empleados, contratistas y usuarios de terceras partes debieran seguir las reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la misma

Actividades: Se debe crear un procedimiento para el manejo y uso de los activos que incluyan:
a) Reglas para la utilización de correo electrónico e internet.
b) Medidas para sistemas de gestión y seguridad.
c) Normas para el uso de estaciones de trabajo.
d) Lineamientos para el uso de dispositivos móviles.

DOMINIO	Gestión de Activos	**OBJETIVO**	Asegurar que la información reciba un nivel de protección apropiado
CONTROL	**7.2.1 Directrices de clasificación**		
DESARROLLO			

Propósito: Asegurar que la información reciba un nivel de protección apropiado, clasificándola para indicar la necesidad, prioridades y grado de protección.

Evaluar las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.
Recomendación: Utilizar una metodología como la siguiente para la clasificación de la información en función a cada uno de los pilares fundamentales de la seguridad de la misma.

Confidencialidad:

0- Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del Organismo o no. PUBLICO
1- Información que puede ser conocida y utilizada por todos los empleados del Organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el Organismo, el Sector Público Nacional o terceros. RESERVADA – USO INTERNO
2- Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros. RESERVADA - CONFIDENCIAL
3- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del Organismo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA

Integridad:

0- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta las operaciones del organismo.
1- Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el organismo.
2- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el organismo.
3- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al organismo.

Disponibilidad:

0- Información cuya inaccesibilidad no afecta las operaciones del organismo.
1- Información cuya inaccesibilidad permanente durante (definir un plazo no menor a una semana) podría ocasionar pérdidas significativas para la división de sistemas.

2- Información cuya inaccesibilidad permanente durante (definir un plazo no menor a un día) podría ocasionar pérdidas significativas a la división de sistemas.
3- Información cuya inaccesibilidad permanente durante (definir un plazo no menor a una hora) podría ocasionar pérdidas significativas a la división de sistemas.

Actividades:

- Clasificar la información en una de las siguientes categorías:
  - **Criticidad Baja**: ninguno de los valores asignados supera el 1.
  - **Criticidad Media**: alguno de los valores asignados es 2
  - **Criticidad Alta**: alguno de los valores asignados es 3
- Asignarle una fecha de efectividad.
- Comunicárselo al propietario del recurso.
- Realizar los cambios cuando sean necesarios y comunicarlo para que los usuarios conozcan la nueva clasificación.

DOMINIO	Gestión de Activos	**OBJETIVO**	Asegurar que la información reciba un nivel de protección apropiado.
CONTROL	**7.2.2 Etiquetado y manipulado de la información**		
DESARROLLO			

Propósito: Desarrollar e implementar procedimientos apropiados para el etiquetado y manejo de la información en concordancia con el esquema de clasificación adoptado por el organismo

Recomendación: Los procedimientos para el etiquetado de la información necesitan abarcar los activos de información en formatos físicos y electrónicos.

El output de los sistemas conteniendo información que es clasificada como sensible acrítica debiera llevar la etiqueta de clasificación apropiada (en el output). El etiquetado debiera reflejar la clasificación de acuerdo a las reglas establecidas en Directrices de Clasificación.

Los ítems a considerarse incluyen reportes impresos, presentaciones en pantalla, medios de grabación (por ejemplo; cintas, discos, CDs), mensajes electrónicos y transferencia de archivos.

Para cada nivel de clasificación, se debiera definir los procedimientos de manejo seguros; incluyendo el procesamiento, almacenaje, transmisión, de-clasificación y destrucción. Esto también debiera incluir los procedimientos de la cadena de custodia y el registro de cualquier incidente de seguridad relevante.

Los acuerdos con otras organizaciones que incluyen intercambio de información debieran incluir procedimientos para identificar la clasificación de esa información e interpretar las etiquetas de clasificación de otras organizaciones.

Actividades: Se debe etiquetar los activos de información identificados, de acuerdo a su clasificación, cubriendo tanto activos físico como electrónicos.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios
CONTROL	**8.1.1 Funciones y responsabilidades**		
DESARROLLO			

Propósito: Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Definir y comunicar claramente los roles y responsabilidades de seguridad antes del empleo en las definiciones de trabajo adecuadas y en los términos y condiciones del empleo a los candidatos para el puesto de trabajo durante el proceso de preselección.

Recomendación:

- Se pueden utilizar las descripciones del puesto para documentar los roles y responsabilidades de seguridad.
- Se debiera definir y comunicar claramente a los candidatos, los roles y responsabilidades de la seguridad para el puesto durante el proceso de preselección.
- Se debe asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.
- Definir las sanciones que se aplicarán en caso de incumplimiento.

Actividades:

- Proteger los activos contra el acceso, divulgación, modificación, destrucción o interferencia no autorizada.
- Asegurar que se asigne a la persona la responsabilidad por las acciones tomadas.
- Reportar eventos de seguridad o eventos potenciales u otros riesgos de seguridad para la organización.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son

			considerados; y reducir el riesgo de robo, fraude y mal uso de los medios
CONTROL	**8.1.2 Investigación de antecedentes**		
DESARROLLO			

Propósito: Llevar a cabo controles de verificación del personal en el momento en que se solicita el puesto y debieran ser proporcionales a los requerimientos operativos, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Recomendación: Los chequeos de verificación de antecedentes de todos los candidatos para empleo, contratistas y terceros debieran llevarse a cabo en concordancia con las leyes, regulaciones y ética relevantes; y debieran ser proporcionales a los requerimientos productivos, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Cuando un puesto de trabajo, sea un nombramiento inicial o un ascenso, involucra que la persona tenga acceso a los medios de procesamiento de información, y en particular si las personas manejan información confidencial; por ejemplo, información financiera o información altamente confidencial; la organización también debiera considerar chequeos más detallados.

Se debiera llevar a cabo un proceso de investigación de antecedentes para los contratistas y terceras personas. Cuando éstos son provistos a través de una agencia, el contrato con la agencia debiera especificar claramente las responsabilidades de la agencia con relación a la investigación de antecedentes y los procedimientos de notificación que se necesitan seguir si no se ha completado la investigación de antecedentes.

Actividades: Realizarchequeos de verificación que incluyan:

- Disponibilidad de referencias de carácter satisfactorias tanto trabajadora como personal.
- Chequeo completo de la hoja de vida (currículum vital – CV) del postulante en cuanto integridad y exactitud.
- Confirmación de títulos académicos y profesionales mencionados por el postulante.
- Comprobación de su identidad.
- Solicitar certificados de antecedentes personales, disciplinarios y judiciales.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son

			considerados; y reducir el riesgo de robo, fraude y mal uso de los medios
CONTROL	**8.1.3 Términos y condiciones de contratación**		
DESARROLLO			

Propósito: Definir las funciones y responsabilidades de seguridad para cada uno de los usuarios de los sistemas de información; para ello es necesario establecer los mínimos privilegios necesarios para el desarrollo de dichas labores.

Recomendación: Todas las funciones y responsabilidades deben comunicarse a los usuarios involucrados en su ejecución, de una forma clara y asegurando su recepción y entendimiento.

El personal que dispone de acceso al sistema de información para el desarrollo de sus funciones, deben recibir información acerca de la obligación de mantener secreto profesional sobre los datos que conozca en el desarrollo de sus labores, aún después de finalizar la relación laboral que le une con la institución, para ello es necesario establecer dentro de la contratación, acuerdos de confidencialidad en el que se informe de sus funciones y obligaciones respecto a la información de la institución.

Actividades: Establecer acuerdos de confidencialidad para empleados y contratistas, antes de otorgarles acceso a los medios de procesamiento de la información.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano
CONTROL	**8.2.1 Responsabilidades de la dirección**		
DESARROLLO			

Propósito: Requerir que todos los empleados, contratistas y terceras personas apliquen la seguridad en concordancia con políticas y procedimientos establecidos por la institución.

Recomendación: La dirección debiera asegurar que todos los empleados, contratistas y terceras personas sean conscientes y estén apropiadamente informados sobre sus roles y responsabilidades de seguridad antes de otorgarles acceso a información confidencial o a los sistemas de información, para ello es necesario promover la divulgación y el conocimiento de la medidas de seguridad y de poner los medios formativos necesarios. Dicha formación debiera abarcar los requisitos de seguridad, responsabilidades legales, objetivos de control, así como el uso adecuado de los recursos de tecnologías de la información con el objetivo de cumplir con las normas, estándares y otras directrices definidas en la política de seguridad.

Actividades:

- Planificación de formación al personal en materia de seguridad de la información, antes de otorgarles accesos a los activos de información.
- Realizar campañas de motivación para cumplir con la política de seguridad, con el propósito de lograr un nivel de conciencia sobre seguridad de la información acorde a sus roles y responsabilidades. Ejemplo: Transmitir a través de píldoras institucionales y/o circuito cerrado de televisión.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano
CONTROL	**8.2.2 Concienciación, formación y capacitación en seguridad de la información**		
DESARROLLO			

Propósito: Capacitar a todos los funcionarios de la institución, contratistas y cuando sea relevante, los terceros en seguridad y actualizaciones regulares sobre las políticas y procedimientos institucionales conforme sea relevante para su labores.

Recomendación: Capacitar al personal de forma apropiada sobre seguridad y el uso correcto de los sistemas de información y sus recursos, así como sobre la importancia de la seguridad en el tratamiento de los datos. Este proceso debiera comenzar en una inducción formal para introducir las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios.

Se debe formar a todo el personal de la institución que vaya a tratar datos del sistema de información sobre las normas de utilización, medidas de seguridad definidas, las instrucciones para tratar los recursos, la respuesta ante incidencias de seguridad que debe contemplar en el tratamiento de los datos, es una forma de disminuir los errores y los malos usos de los recursos y correcto desempeño de sus funciones.

Actividades:

- Capacitación permanente a todo el personal en materia de seguridad de la información.
- Incluir en la inducción a los nuevos empleados a través de charlas, las políticas de seguridad antes de otorgar acceso a la información o servicios.
- Informar a todos los empleados y contratistas a fin de que cumplan con las medidas establecidas por la institución en el desempeño habitual de sus funciones.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano
CONTROL	**8.2.3 Proceso disciplinario**		
DESARROLLO			

Propósito: Implantar un proceso disciplinario para los funcionarios que cometan una violación a la seguridad.

Recomendación: Seguir el proceso disciplinario formal contemplado en las normas que rigen al personal de la Administración Pública, para los empleados que violen la política, normas y procedimientos de seguridad de la institución.

El proceso disciplinario contribuye como un elemento disuasivo para evitar que los empleados, contratistas y terceros violen las políticas y procedimientos de la seguridad institucional y cualquier otro incumplimiento de la seguridad.

Actividades: Establecer dentro del contrato una declaración de la obligación de dar cumplimiento sobre las políticas y procedimientos relativos a la seguridad de la información y que su incumplimiento deriva de las sanciones prescritas en la ley.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada
CONTROL	**8.3.1 Responsabilidad del cese o cambio**		
DESARROLLO			

Propósito: Definir y asignar claramente las responsabilidades de realizar la desvinculación o cambio en las funciones

Recomendación: La comunicación de las responsabilidades de terminación o cambio de puesto deben ser claramente definidas y asignadas, incluyendo requerimientos de seguridad y responsabilidades legales a posteriori y, cuando sea apropiado.

Informar de la obligación de mantener secreto profesional de los datos que conozca en desarrollo de sus funciones, a un después de finalizar la relación laboral que le une con la institución, dicha responsabilidad debiera estar contenida en acuerdos de confidencialidad y en los términos y condiciones del empleo.

Actividades: Incluir dentro de los contratos las responsabilidades de acuerdo al tipo de información manejada por el funcionario, y las contenidas dentro de un contrato de confidencialidad, aún por un tiempo luego de la desvinculación.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada
CONTROL	**8.3.2 Devolución de los activos**		
DESARROLLO			

Propósito: Devolver todos los activos de la institución que tengan en su posesión todos los usuarios empleados, contratistas y terceras personas al término de su empleo o contrato.

Recomendación: Todos los empleados, contratistas y terceros deben retornar todos los activos de la organización que estén en su posesión hasta la terminación de su empleo, contrato o acuerdo.

El proceso de finalización debe incluir la devolución de los siguientes activos (listado no exhaustivo):
a) Software
b) Documentos
c) Equipos
d) Tarjetas e identificaciones de acceso
e) Manuales
f) Información almacenada en diversos medios

En los casos en los que los empleados, contratistas o terceras partes hubieren utilizado equipos de su propiedad, debe documentarse y extremarse los medios para que toda información relevante sea transferida a institución y eliminada en forma segura de esos equipos.

El responsable del Área de Recursos Humanos, debiera incorporar los términos necesarios en los respectivos contratos para procurar el cumplimiento de los controles.

Actividades:

- Crear un procedimiento de devolución y reutilización de activos una vez se produzca la desvinculación o terminación del contrato. Este debe incluir el borrado efectivo de los datos y la estandarización del sistema al nuevo usuario.
- Generar un comunicado por parte de Recursos Humanos a Sistemas para que procedan a bloquear todos los accesos del usuario y pasarlo a estatus inactivo.
- Generar acta de entrega de cargo.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada
CONTROL	**8.3.3 Retirada de los derechos de acceso**		
DESARROLLO			

Propósito: Remover los derechos de acceso de todos los usuarios funcionarios, personal a honorarios y terceras personas a la información y los medios de procesamiento de información como consecuencia de su desvinculación, o deberían ser ajustados si sus funciones cambian.

Recomendación: En la terminación del contrato debiera retirarse los derechos del individuo los activos asociados con los sistemas y servicios de información tras la desvinculación.
En caso de cambio de un empleo deben removerse todos los derechos de acceso que no fueron aprobados para el nuevo empleo, tales como: accesos lógicos y físicos, llaves, tarjetas de identificación, instalaciones de procesamiento de la información, suscripciones, y remoción de cualquier documentación que lo identifique como un miembro corriente del Organismo.
Si un empleado, contratista o usuario de tercera parte que se está desvinculando tiene conocimiento de contraseñas para cuentas que permanecen activas, éstas deben ser cambiadas tras la finalización o cambio de empleo, contrato o acuerdo.

Actividades: Crear un procedimiento de baja de usuarios en los sistemas de información, que considere la revocación de sus cuentas de acceso dependiendo de los siguientes factores de riesgo:

- Cuando el termino o cambio de trabajo, es iniciado por el funcionario o contratista, o por razones administrativas.
- Las responsabilidades actuales del funcionario o contratista.
- Valor de los activos que actualmente maneja.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización
CONTROL	**9.1.1 Perímetro de seguridad física**		
DESARROLLO			

Propósito: Utilizar los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) para proteger las áreas que contengan información y recursos para su procesamiento.

Recomendación:

- Los perímetros de seguridad deben estar claramente definidos, y la ubicación y fuerza de cada uno de los perímetros dependerá de los requerimientos de seguridad de los activos dentro del perímetro y los resultados de la evaluación del riesgo.
- Los perímetros del área que contienen los medios de procesamiento de información deben ser físicamente sólidos (es decir, no debieran existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir un ingreso no autorizado).
- Las paredes externas del local deben ser una construcción sólida y todas las puertas externas deben estar adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control; por ejemplo, vallas, alarmas, relojes,etc.
- Las puertas y ventanas deben quedar aseguradas cuando están desatendidas y considerar una protección externa para las ventas.
- El área debe contar con una recepción o un(a) recepcionista u otros medios para controlar el acceso físico al área; el acceso al área debe ser restringida solamente al personal autorizado.
- Todas las puertas de emergencia en un perímetro de seguridad debieran contar con alarma, ser monitoreadas y probadas en conjunción con las paredes para establecer el nivel de resistencia requerido en concordancia con los adecuados estándares regionales, nacionales e internacionales.
- Se debe operar en concordancia con el código contra-incendios local de una manera totalmente segura.
- Instalar adecuados sistemas de detección de intrusos según estándares nacionales, regionales e internacionales, probados regularmente para abarcar todas las puertas externas y ventanas accesibles.
- Las áreas no ocupadas deben contar con alarma en todo momento.
- Proveer protección para otras áreas; por ejemplo, el cuarto de cómputo o cuarto de comunicaciones.
- Los medios de procesamiento de información manejados por la organización deben estar físicamente separados de aquellas manejadas por terceros.

Actividades:

- Definir y documentar claramente los perímetros de seguridad de acuerdo a la ubicación y requerimientos de seguridad de los activos.
- Ubicar las instalaciones de procesamiento de información dentro del perímetro del área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción).
- Instalar alarmas a las puertas de emergencia en un perímetro de seguridad
- Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área.

- Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.
- El Responsable de Seguridad de la Información debe llevar un registro actualizado de los sitios protegidos, indicando:

a) Identificación del Área.
b) Principales elementos a proteger.
c) Medidas de protección física

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización
CONTROL	**9.1.2Controles físicos de entrada**		
DESARROLLO			

Propósito: Proteger las áreas seguras mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.

Recomendación:

- La fecha y la hora de entrada y salida de los visitantes debe ser registrada y todos los visitantes deben ser supervisados a no ser que su acceso haya sido previamente aprobado.
- Sólo se le debe permitir acceso por propósitos específicos y autorizados a visitantes y se deben emitir las instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia.
- El acceso a áreas donde se procesa o almacena información sensible debe ser controlada y restringida sólo al personal autorizado.
- Se debe utilizar controles de autenticación; por ejemplo, tarjeta de control de acceso más PIN; para autorizar y validar todo los accesos; se debiera mantener un rastro de auditoría de todos los accesos.
- Para todos los usuarios empleados, contratistas y terceras personas y todos los visitantes deben usar como requisito alguna forma de identificación visible.
- Al personal de servicio de apoyo de terceros se le debe otorgar acceso restringido las áreas seguras o los medios de procesamiento de información confidencial, solo cuando sea necesario; este acceso debe ser autorizado y monitoreado.
- Los derechos de acceso a áreas seguras deben ser revisados y actualizados regularmente, y revocados cuando sea necesario.

Actividades:

- Establecer requerimientos de seguridad del área y los procedimientos de emergencia, para autorizar e instruir al visitante en el momento que se le permita el ingreso.
- Supervisar o inspeccionar a los visitantes a áreas protegidas.
- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.
- Diseñar controles de autenticación para autorizar y validar todos los accesos.
- Mantener un registro protegido que permita auditar todos los accesos.
- Implementar el uso de una identificación unívoca visible para todo el personal del área protegida.
- Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización
CONTROL	**9.1.3 Seguridad de oficinas, despachos e instalaciones**		

DESARROLLO

Propósito: Debiera diseñar y aplicar la seguridad física para las oficinas, despachos e instalaciones.

Recomendación:

- Se debe tener en cuenta los estándares y regulaciones de sanidad y seguridad relevantes;
- Se debe localizar los medios claves para evitar el acceso del público;
- El área de procesamiento de información relevante debe ser discreta y dar una indicación mínima de su propósito, sin carteles obvios dentro y fuera del área que indiquen la presencia de actividades de procesamiento de información;
- Los directorios y teléfonos internos que identifiquen la ubicación de los medios deprocesamiento de la información no debieran estar accesibles al público.
- Separar las instalaciones de procesamiento de información administradas por el Organismo de aquellas administradas por terceros.
- Las instalaciones críticas deben situarse evitando el acceso al público
- Debe existir un estándar para la elección de contraseñas robustas.

Actividades

- Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

- Establecer que el área donde se realicen actividades de procesamiento de información sean discretas y solo se muestre un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
- Establecer que las puertas y ventanas cerradas cuando no haya vigilancia tengan protección.
- Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
- Implementar una lista de lugares seguros para almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas del Organismo. Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.
- Ubicar un sitio seguro y distante del lugar de procesamiento para almacenar los equipos redundantes y la información de resguardo (back up), para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización
CONTROL	**9.1.4 Protección contra las amenazas externas y de origen ambiental**		
DESARROLLO			

Propósito: Asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Recomendación: Se deben considerar los siguientes lineamientos para evitar el daño por fuego, inundación,terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por elhombre:

- Los suministros a granel como papelería no debiera almacenarse en el área asegurada.
- El equipo de reemplazo y los medios de respaldo deben ubicarse a una distanciasegura para evitar el daño de un desastre que afecte el local principal.
- Proporcionar equipo contra-incendios ubicado adecuadamente.

Actividades

- Instalar a una distancia adecuada y en un área segura el equipamiento de contingencia, que permita evitar el daño frente a un desastre que afecte al sitio principal.
- Mantener en un lugar visible y de rápido acceso el equipamiento de extinción de incendios.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización
CONTROL	**9.1.5 Trabajo en áreas seguras**		
DESARROLLO			

Propósito: Diseñar y aplicar la protección física y los lineamientos para trabajar en áreas aseguradas.

Recomendación: Para incrementar la seguridad en las áreas protegidas se debe tener en cuenta:

- El personal debe estar al tanto de la existencia o las actividades dentro del área asegurada sólo conforme las necesite conocer.
- Evitar el trabajo no-supervisado en el área asegurada tanto por razones de seguridad como para evitar las oportunidades para actividades maliciosos.
- Las áreas aseguradas vacías deben ser cerradas físicamente bajo llave y revisadas periódicamente.
- No se debe permitir equipo fotográfico, de vídeo, audio y otro equipo de grabación; como cámaras en equipos móviles; a no ser que sea autorizado.

Actividades:

- Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
- Evitar la ejecución de trabajos por parte de terceros sin supervisión.
- Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
- Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado.
- Mantener un registro de todos los accesos de personas ajenas.

- Establecer barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
- Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho área o el Responsable del Área Informática y el Responsable de Seguridad de la Información.
- Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización
CONTROL	**9.1.6Áreas de acceso público y de carga y descarga**		
DESARROLLO			

Propósito: Controlar los puntos de acceso como las áreas de entrega y carga y otros puntos por donde personas no-autorizadas puedan ingresar al local y, si fuese posible, deben aislarse de los medios de procesamiento de información para evitar el acceso no autorizado.

Recomendación:

- El acceso al área de entrega y carga desde fuera de la institución se debe restringir al personal identificado y autorizado.
- Las puertas externas del área de entrega y carga deben estar aseguradas cuando se abren las puertas internas;
- Inspeccionar el material que ingresa para evitar amenazas potenciales antes que el material sea trasladado del área de entrega y carga al punto de uso.

Actividades:

- Controlar las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.
- Diseñar el área de entrega y carga de manera que se pueda descargar los suministros sin que el personal de entrega tenga acceso a otras partes del área de descargue.
- Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Organismo, sólo al personal previamente identificado y autorizado.
- Registrar el material que ingresa en concordancia con los procedimientos de gestión de activos a su ingreso al local.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
CONTROL	**9.2.1 Emplazamiento y protección de equipos**		
DESARROLLO			

Propósito: Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades del Organismo.

Proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no-autorizado.

Recomendación:

a) Ubicar el equipo de manera que se minimice el acceso innecesario a las áreas de trabajo.
b) Los medios de procesamiento de la información que manejan data confidencia deben ubicarse de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso.
c) Asegurar los medios de almacenaje para evitar el acceso no autorizado.
d) Aislar los ítems que requieren protección especial para reducir el nivel general de la protección requerida.
e) Adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.
f) Establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información.
g) Monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información.
h) Aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.
i) Proteger el equipo que procesa la información confidencial para minimizar el riesgo de escape de información debido a emanación.

Actividades:

- Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
- Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.

- Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará en un periodo no mayor a seis meses.
- Aplicar protección contra rayos a todos los edificios y se deben adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
CONTROL	**9.2.2 Instalaciones de suministro**		
DESARROLLO			

Propósito: Proteger los equipos de fallas de energía y otras interrupciones causadas por fallasen los servicios públicos de soporte.

Recomendación:

a) Todos los servicios públicos de soporte; como electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado; deben ser adecuados para los sistemas que soportan.
b) Los servicios públicos de soporte deben ser inspeccionados regularmente y conforme sea apropiado, probados para asegurar su adecuado funcionamiento y para reducir cualquier riesgo por un mal funcionamiento o falla.
c) proveer un suministro eléctrico adecuado que esté de acuerdo a las especificaciones del fabricante del equipo.
d) Se recomienda un dispositivo de suministro de energía ininterrumpido (UPS) para apagar o el funcionamiento continuo del equipo de soporta las operaciones comerciales críticas.
e) Los planes de contingencia para la energía debieran abarcar la acción a tomarse en el caso de una falla de energía prolongada.
f) considerar un generador de emergencia si se requiere que el procesamiento continué en el caso de una falla de energía prolongada.
g) Se debe tener disponible un adecuado suministro de combustible para asegurar que el generador pueda funcionar durante un período prolongado.
h) El equipo UPS y los generados se deben chequear regularmente para asegurar que tengan la capacidad adecuada y para probar su concordancia con las recomendaciones del fabricante.
i) se debe considerar al uso de múltiples fuentes de energía, si el área es grande, una subestación de energía separada.

j) Los interruptores de energía de emergencia se deben colocar cerca de las salidas de emergencia en las habitaciones donde se encuentra el equipo para facilitar el cierre del paso de corriente en caso de una emergencia.
k) proporcionar iluminación de emergencia en caso de una falla en la fuente de energía principal.
l) El suministro de energía debe ser estable y adecuado para suministrar aire acondicionado, equipo de humidificación y los sistemas contra-incendios (donde se utilicen).
m) Se debiera evaluar e instalar, si se requiere, un sistema de alarma para detectar mal funcionamiento en los servicios públicos de soporte.
n) El equipo de telecomunicaciones se debiera conectar al proveedor del servicio mediante por lo menos dos rutas para evitar que la falla en una conexión evite el desempeño de los servicios de voz.
o) Los servicios de voz deben ser adecuados para cumplir con los requerimientos legales de las comunicaciones de emergencia.

Actividades:

- Diseñar planes de contingencia que permitan contemplar las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS deberán ser inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
- Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía.
- Implementar protección contra descargas eléctricas en todas las áreas y líneas de comunicaciones externas de acuerdo a las normativas vigentes para cuando se presente una falla en el suministro principal de energía.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
CONTROL	**9.2.3 Seguridad del cableado**		
DESARROLLO			

Propósito: Proteger contra la intercepción o daño el cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información.

Recomendación:

- Cuando sea posible, las líneas de energía y telecomunicaciones que van a los medios de procesamiento de información deben ser subterráneas o estar sujetas a una alternativa de protección adecuada.
- Los cables de energía debieran estar separados de los cables de comunicaciones para evitar la interferencia
- Utilizar marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados
- Utilizar una lista de empalmes documentados para reducir la posibilidad de error.
- Para sistemas sensibles o críticos se debe considerar más controles como:
  - ✓ la instalación de un tubo blindado y espacios o cajas con llave en los puntos de inspección y terminación;
  - ✓ el uso de rutas alternativas y/o medios de transmisión proporcionan una seguridad adecuada;
  - ✓ el uso de cableado de fibra óptica;
  - ✓ el uso de un escudo electromagnético para proteger los cables;
  - ✓ la iniciación de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se adhieran a los claves;
  - ✓ acceso controlado para empalmar los paneles y los cuartos de cableado.

Actividades:

- Proteger contra intercepciones no autorizadas o daños el cableado de la red, por ejemplo, utilizando un tubo o evitando las rutas a través de áreas públicas.
- Rotular o marcar adecuadamente los cables para reducir al mínimo los errores de manejo.
- Separar los cables de energía de los cables de comunicación para evitar interferencia
- Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados
- Realizar un mapa de los patchpanels y un acceso controlado a la sala de cables.

- Realizar barridos técnicos e inspecciones físicas contra dispositivos no autorizados conectados a los cables.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
CONTROL	**9.2.4 Mantenimiento de los equipos**		
DESARROLLO			

Propósito: Mantener correctamente los equipos para asegurar su continua disponibilidad e integridad.

Recomendación:

a) El equipo se debe mantener en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor.
b) Sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo.
c) Mantener registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo.
d) Implementar los controles apropiados cuando se programa el equipo para mantenimiento, tomando en cuenta si su mantenimiento es realizado por el personal en el local o fuera de la organización; cuando sea necesario y revisar la información confidencial del equipo, o se debiera verificar al personal demantenimiento.
e) Cumplir con todos los requerimientos impuestos por las pólizas de seguros.

Actividades:

- Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área.
- Llevar un registro actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- Registrar el retiro de equipamiento de la sede del Organismo para su mantenimiento.
- Eliminar la información confidencial que contenga cualquier equipamiento, realizándose previamente las respectivas copias de resguardo antes de que se vallan a llevar el equipo para hacer mantenimiento.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
CONTROL	**9.2.5Seguridad de los Equipos Fuera de las Instalaciones**		
DESARROLLO			

Propósito: Aplicar seguridad al equipo fuera del área tomando en cuenta los diferentes riesgos de trabajar fuera de esta misma.

Recomendación

a) El equipo y medios sacados del área nunca deben ser dejados desatendidos en lugares públicos; durante un viaje, las computadoras portátiles deben ser llevadas como equipaje de mano y cuando sea posible, de manera disimulada.
b) Observar en todo momento las instrucciones de los fabricantes para proteger el equipo; por ejemplo, protección contra la exposición a fuertes campos electromagnéticos.
c) Determinar controles para el trabajo en casa a través de una evaluación del riesgo y los controles apropiados conforme sea apropiado; por ejemplo, archivos con llave, política de escritorio vacío, controles de acceso para las computadoras y una comunicación segura con la oficina.
d) Contar con un seguro adecuado para proteger el equipo fuera del local.
e) Los riesgos de seguridad; por ejemplo, daño, robo o intercepción; puede variar considerablemente entre los locales y se debe tomar esto en cuenta para determinar los controles más apropiados.

Actividades: Mantener una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Organismo, cuando sea conveniente.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
CONTROL	**9.2.6 Reutilización o retirada segura de equipos**		
DESARROLLO			

Propósito: Chequear los ítems del equipo que contiene medios de almacenaje para asegurar que se haya retirado o sobre-escrito cualquier data confidencial o licencia de software antes de su eliminación.

Recomendación: Los dispositivos que contienen información confidencial deben ser físicamente destruidos o se debieran destruir, borrar o sobre-escribir la información utilizando técnicas que hagan imposible recuperar la información original, en lugar de simplemente utilizar la función estándar de borrar o formatear.
Los dispositivos que contienen data confidencial pueden requerir una evaluación del riesgo para determinar si los ítems deben ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

Actividades: Diseñar e implementar procedimientos de borrado seguro de datos y de reutilización de equipos.

DOMINIO	Seguridad ligada a los recursos humano	**OBJETIVO**	Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
CONTROL	**9.2.7 Retirada de materiales propiedad de la empresa**		
DESARROLLO			

Propósito: El equipo, información o software no debe retirarse sin autorización previa.

Recomendación:
a) No se debe retirar equipo, información o software sin autorización previa.
b) Los usuarios empleados, contratistas y terceras personas que tienen la autoridad parapermitir el retiro de los activos fuera del área deben estar claramente identificados.
c) Establecer límites de tiempo para el retiro del equipo y se debe realizar un chequeo de la devolución.
d) Cuando sea necesario y apropiado, el equipo debe ser registrado como retirado del área y se debe registrar su retorno.

Actividades:
- Especificar un tiempo máximo para el equipamiento retirado y verificarse el cumplimiento de retorno.
- Llevar un registro de entrada y salida de los equipos de la dependencia.

DOMINIO	Gestión de Comunicaciones y Operaciones.	**OBJETIVO**	Asegurar la operación correcta y segura de los medios de procesamiento de la información
CONTROL	**10.1.1 Documentación de los procedimientos de operación**		
DESARROLLO			

Propósito: Documentar, mantener y poner a disposición los procedimientos de operación de todos los usuarios,a quien lo necesite.

Recomendación:

a) Preparar procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información y comunicación; tales como procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento del equipo, manejo de medios, cuarto de cómputo, manejo del correo y seguridad.
b) Los procedimientos de operación deben especificar las instrucciones para la ejecución detallada de cada trabajo incluyendo:
   - ✓ procesamiento y manejo de información;
   - ✓ copia de seguridad o respaldo;
   - ✓ requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y últimos trabajos;
   - ✓ instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema;
   - ✓ contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas;
   - ✓ instrucciones para el manejo de output especial y medios, tales como el uso de papelería especial o el manejo de output confidencial incluyendo los procedimientos para la eliminación segura del output de trabajo fallidos;
   - ✓ procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema;
   - ✓ la gestión de la información del rastro de auditoría y registro del sistema.

Los procedimientos de operación y los procedimientos documentados para las actividades del sistema deben ser tratados como documentos formales y cambios autorizados por la gerencia. Donde sea técnicamente factible, los sistemas de información deben ser manejados consistentemente, utilizando los mismos procedimientos, herramientas y utilidades.

Actividades:

- Documentar y mantener actualizados los procedimientos operativos identificados y sus cambios serán autorizados por el Responsable de Seguridad de la Información.
- Diseñar y establecer procedimientos para la operación de la infraestructura critica de las TIC'C que incluya:
  - manejo y procedimiento de la información
  - respaldos
  - requerimientos de tareas automatizadas, incluyendo las dependencias con otros sistemas. Alertas sobre tareas ejecutadas correcta e incorrectamente.
  - Instrucciones para manejar errores o condiciones excepcionales.
  - Contactos de soporte ante la eventualidad de dificultades técnicas.
  - Procedimientos de manejo de medios y de retención de datos.

- Reinicio de sistemas y procedimientos de recuperación ante fallas de los sistemas.
- Procedimientos de la administración de logs de auditoría.

- Preparar adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:
  - Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
  - Instalación y mantenimiento de las plataformas de procesamiento.
  - Monitoreo del procesamiento y las comunicaciones.
  - Inicio y finalización de la ejecución de los sistemas.
  - Programación y ejecución de procesos.
  - Gestión de servicios.
  - Resguardo de información.
  - Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
  - Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
  - Uso del correo electrónico.

DOMINIO	Gestión de Comunicaciones y Operaciones.	**OBJETIVO**	Asegurar la operación correcta y segura de los medios de procesamiento de la información
CONTROL	**10.1.2 Gestión de cambios**		
DESARROLLO			

Propósito: Controlar los cambios en los medios y sistemas de procesamiento de la información.

Recomendación:
Los sistemas operacionales y el software de aplicación deben estar sujetos a un estricto control gerencial del cambio.

El control inadecuado de los cambios en los medios de procesamiento de la información y los sistemas es una causa común de fallas en el sistema o en la seguridad.

Los cambios en el ambiente operacional, especialmente cuando se transfiere un sistema de la etapa de desarrollo a la etapa operacional, pueden influir en la confiabilidad de la aplicación.

Los cambios en los sistemas de operación sólo se deben realizar cuando existe una razón comercial válida para hacerlo, como un incremento en el riesgo para el sistema.

Actualizar los sistemas con la versión más moderna del sistema de operación o aplicación no es siempre lo mejor, ya que podría introducir más vulnerabilidades e inestabilidad que la versión actual.

Actividades

- Definir y establecer procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Estos procedimientos deben contemplar:
    a) identificación y registro de cambios significativos;
    b) planeación y prueba de cambios;
    c) evaluación de los impactos potenciales de los cambios, incluyendo los impactos de seguridad,
    d) procedimiento de aprobación formal para los cambios propuestos;
    e) comunicación de los detalles del cambio para todos las personas relevantes:
    f) procedimientos de emergencia y respaldo, incluyendo los procedimientos y responsabilidades para abortar y recuperarse de cambios fallidos y eventos inesperados.
- Establecer las responsabilidades y procedimientos formales para asegurar un control satisfactorio de todos los cambios en el equipo, software o procedimientos.
- Mantener un registro de auditoría que contenga toda la información relevante de cada cambio.
- El Responsable de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan, además debe evaluar el posible impacto operativo de los cambios previstos y verificar su correcta implementación.

DOMINIO	Gestión de Comunicaciones y Operaciones.	**OBJETIVO**	Asegurar la operación correcta y segura de los medios de procesamiento de la información
CONTROL	**10.1.3 Segregación de tareas**		
DESARROLLO			

Propósito: Reducir las oportunidades de una modificación no-autorizada o mal uso no-intencional o mal uso de los activos de la organización.

Recomendación:

a) Tener cuidado que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección.
b) Separar la iniciación de un evento de su autorización.
c) Considerar la posibilidad de colusión en el diseño de los controles.
d) Es importante que la auditoría de seguridad se mantenga independiente.

Actividades:

- Crear perfiles de usuario que sean consecuentes con las descripciones del cargo que desempeñen y que contengan los mínimos acceso a los sistemas de la información para llevar a cabo sus funciones.
- El encargado de seguridad debe validar estos perfiles y auditarlos al menos 2 veces al año.
- Separar la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.
- Implementar controles que incluya:
    - Monitoreo de las actividades.
    - Registros de auditoría y control periódico de los mismos.
    - Supervisión por parte de la Unidad de Auditoría Interna o en su defecto quien sea propuesto a tal efecto, siendo independiente al área que genera las actividades auditadas.

DOMINIO	Gestión de Comunicaciones y Operaciones.	**OBJETIVO**	Asegurar la operación correcta y segura de los medios de procesamiento de la información
CONTROL	**10.1.4 Separación de los recursos de desarrollo, prueba y operación**		
DESARROLLO			

Propósito: Separar los medios de desarrollo, prueba y operación para reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional.

Recomendación: Se debe identificar el nivel de separación necesario entre los ambientes de desarrollo, prueba y operación para evitar los problemas operacionales

Se debe considerar:

a) Definir y documentar las reglas para la transferencia de software del estado de desarrollo al operacional.
b) Los software de desarrollo y operacional deben correr en sistemas o procesadores de cómputo, y en diferentes dominios o directorios.
c) Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deben ser accesibles desde los sistemas operacionales cuando no se requieran.
d) El ambiente del sistema de prueba debe emular el ambiente del sistema operacional lo más estrechamente posible.
e) Los usuarios deben utilizar perfiles de usuario diferentes para los sistemas operacionales y de prueba, y los menús deben mostrar los mensajes de identificación apropiados para reducir el riesgo de error.
f) La data confidencial no debe ser copiada en el ambiente del sistema de prueba.

Las actividades de desarrollo y prueba pueden ser problemas serios; por ejemplo, una modificación no deseada de los archivos o el ambiente del sistema, o una falla en el sistema. En este caso, existe la necesidad de mantener un ambiente conocido y estable en el cual realizar una prueba significativa y evitar un inadecuado acceso del encargado del desarrollo.

Cuando el personal de desarrollo y prueba tiene acceso al sistema operacional y su información, ellos pueden introducir un código no-autorizado o no-probado o alterar la data de operación. En algunos sistemas esta capacidad puede ser mal utilizada para cometer fraude, o introducir un código no-probado o malicioso, el cual puede causar serios problemas operacionales.

Los encargados del desarrollo y las pruebas también podrían ser una amenaza para la confidencialidad de la información operacional. Las actividades de desarrollo y prueba pueden causar daños no-intencionados al software o la información si es que comparten el mismo ambiente de cómputo. Por lo tanto, es deseable separar los medios de desarrollo, prueba y operación para reducir el riesgo de un cambio accidental o acceso no-autorizado al software operacional y la data del negocio

Actividades

- Diseñar políticas y procedimientos para la transferencia del software desde ambientes de desarrollo a operaciones y registro de actividades.
- Establecer perfiles de usuario diferentes para los sistemas operacionales y de prueba.
- Separar las actividades de desarrollo y prueba, en entornos diferentes.
- Implementar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.
- Establecer una política que permita prohibir a los usuarios compartir contraseñas en estos sistemas.
- Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Implementary mantener el nivel apropiado de seguridad de la información y laentrega del servicio en línea con los acuerdos de entrega de servicios de terceros
CONTROL	**10.2.1 Provisión de servicios**		
DESARROLLO			

Propósito: Asegurar que los controles de seguridad, definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega del servicio de terceros se implementen, operen y mantengan.

Recomendación: La entrega del servicio por un tercero debe incluir los acuerdos de seguridad pactados, definiciones del servicio y aspectos de la gestión del servicio. En caso de los acuerdos de abastecimiento externo, la organización debe planear las transiciones necesarias (de información, medios de procesamiento de la información y cualquier otra cosa que necesite transferirse), y debe asegurar que se mantenga la seguridad a través del período de transición.

La organización debe asegurar que la tercera persona mantenga una capacidad de servicio suficiente junto con los planes de trabajo diseñados para asegurar que se mantengan el nivel de continuidad del servicio después de fallas importantes en el servicio o un desastre.

Actividades.

- Verificar que los servicios brindados por una tercera parte incluyan los acuerdos de seguridad arreglados, definiciones de servicio, y aspectos de la gestión del servicio.
- Establecer acuerdos de servicios para la recuperación ante desastres o fallas.
- En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio y se incluirán en el contrato, contemplando las siguientes cuestiones específicas:
  a) Identificar las aplicaciones sensibles o críticas que convenga retener en el Organismo.
  b) Obtener la aprobación de los propietarios de aplicaciones específicas.
  c) Identificar las implicancias para la continuidad de los planes de las actividades del Organismo.
  d) Especificar las normas de seguridad y el proceso de medición del cumplimiento.
  e) Asignar funciones específicas y procedimientos para monitorear todas las actividades de seguridad.
  f) Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Dichas consideraciones deben ser acordadas entre el Responsable de Seguridad de la Información, el Responsable del Área de Informática y el Responsable del Área Jurídica del Organismo.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Implementary mantener el nivel apropiado de seguridad de la información y laentrega del servicio en línea con los acuerdos de entrega de servicios de terceros
CONTROL	**10.2.2 Supervisión y revisión de los servicios prestados por terceros**		
DESARROLLO			

Propósito: Monitorear y revisar regularmente los servicios, reportes y registros provistos por terceros.

Recomendación: El monitoreo y revisión de los servicios de terceros deberá asegurar que se cumplan los términos y condiciones de seguridad de los acuerdos, y que se manejen apropiadamente los incidentes y problemas de seguridad de la información. Esto debiera involucrar una relación y proceso de gestión de servicio entre la organización y la tercera persona para:

- Monitorear los niveles de desempeño del servicio para chequear adherencia con los acuerdos.
- Revisar de los reportes de servicio producidos por terceros y acordar reuniones de avance regulares conforme lo requieran los acuerdos.
- Proporcionar información sobre incidentes de seguridad de la información y la revisión de esta información por terceros y la organización conforme lo requieran los acuerdos y cualquier lineamiento y procedimiento de soporte.
- Revisar los rastros de auditoría de terceros y los registros de eventos de seguridad, problemas operacionales, fallas, el monitoreo de fallas e interrupciones relacionadas con el servicio entregado.
- Resolver y manejar cualquier problema identificado.

La responsabilidad de manejar la relación con terceros se debiera asignar a una persona o equipo de gestión de servicios. Además, la organización debiera asegurar que los terceros asignen responsabilidad para el chequeo del cumplimiento de los requerimientos de los acuerdos. Se debieran poner a disposición las capacidades y recursos técnicos para monitorear los requerimientos del acuerdo, en particular si se cumplen los requerimientos de seguridad de la información. Se debiera tomar la acción apropiada cuando se observan deficiencias en la entrega del servicio.

La organización debiera mantener el control y la visibilidad general suficiente en todos los aspectos de seguridad con relación a la información confidencial o crítica o los medios de procesamiento de la información que la tercera persona ingresa, procesa o maneja. La organización debiera asegurarse de mantener visibilidad en las actividades de seguridad

como la gestión del cambio, identificación de vulnerabilidades y reporte/respuesta de un incidente desagradada través de un proceso, formato y estructura de reporte definidos.
En caso de abastecimiento externo, la organización necesita estar al tanto que la responsabilidad final de la información procesada por un proveedor externo se mantenga en la organización.

Actividades:

- Monitorear los niveles de servicio y chequear su adherencia a los acuerdos.
- Revisar los reportes generados por los terceros y acordar reuniones.
- Suministrar información ante incidentes de seguridad de manera de dar cumplimiento a la normativa de seguridad.
- Revisar los registros de auditoría de los terceros, frente a problemas de seguridad, operacionales, fallas y discontinuidad del servicio.
- Resolver los problemas identificados.

Estructura del documento:

Posibles formatos donde se puede mantener control y visibilidad general sobre:

Formato de registro la Gestión del Cambio

FECHA (D/M/AA)	DEPENDENCIA / ORIGEN DEL ERROR	CODIGO / TIPO DE ERROR	DESCRIPCION DEL ERROR	CAUSAS	PROCEDIMIENTO REALIZADO	RESPONSABLE
---	---	---	---	---	---	---
---	---	---	---	---	---	---

Matriz de Riesgos

ID	Riesgo	Posible resultado	Síntoma	Probabilidad	Impacto	Prioridad	Respuestas	Responsable
----	----	----	----	----	----	----	----	----
----	----	----						

- ID: Un código o número identificador del riesgo.

- Riesgo: Descripción detallada del riesgo.
- Posible resultado: Descripción específica sobre cuál sería el efecto del riesgo en caso de que este ocurra.
- Síntoma: Identifica y describe una señal de alarma o advertencia de que el riesgo puede ocurrir. Es importante mencionar que no todos los riesgos tienen síntomas.
- Probabilidad: Evalúa la probabilidad de que el riesgo suceda. Esta probabilidad puede ser alta, media o baja dependiendo del riesgo.
- Impacto: Evalúa el grado de impacto en caso de que el riesgo ocurra. Este impacto puede ser alto, medio o bajo dependiendo del riesgo en sí mismo.
- Prioridad: Prioriza los riesgos en una escala de 1 al 9, 1 indica el nivel máximo crítico y 9 el nivel mínimo.
- Respuestas: Especifica la acción (control) que el equipo llevará a cabo para eliminar, trasladar o mitigar el riesgo.
- Responsable: Nombre o rol del responsable de llevar a cabo la acción de respuesta al riesgo.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.
CONTROL	**10.2.3Manejo de cambios en los servicios de terceros**		
DESARROLLO			

Propósito: Manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad de la información existentes teniendo en cuenta el grado crítico de los sistemas y procesos del negocio involucrados y la re-evaluación de los riesgos.

Recomendación:

El proceso de manejar los cambios en el servicio de terceros necesita tomar en cuenta:

1. Los cambios realizados por la organización para implementar:

- Aumento los servicios ofrecidos actualmente.
- Desarrollo de cualquier aplicación y sistema nuevo.
- Modificaciones o actualizaciones de las políticas y procedimientos de la organización.
- Controles nuevos para solucionar incidentes de la seguridad de la información y para mejorar la seguridad.

2. Cambios en los servicios de terceros para implementar:

- Cambios y mejoras en las redes.
- Uso de tecnologías nuevas.
- Adopción de productos nuevos o versiones más modernas.

- Desarrollo de herramientas y ambientes nuevos.
- Cambios en la ubicación física de los medios del servicio.
- Cambio de vendedores.

Actividades:

El proceso de administración de cambios, necesita manejar:

Los cambios realizados por la institución para implementar mejoras a los servicios ofrecidos, desarrollo aplicaciones; modificaciones o actualizaciones de los procedimientos o políticas de la institución; nuevos controles que resuelvan incidentes de seguridad o mejoren el nivel.

Los cambios realizados por los terceros para mejorar las redes, el uso de nuevas tecnologías, adopción de nuevos productos o nuevas versiones, nuevas herramientas de desarrollo y ambientes, cambios a las locaciones físicas o facilidades de servicio, cambios en los fabricantes.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Minimizar el riesgo de fallas en el sistema.
CONTROL	**10.3.1 Gestión de la capacidad**		
DESARROLLO			

Propósito: Monitorear, afinar el uso de los recursos y realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido del sistema.

Recomendación: Se debe identificar los requerimientos de capacidad de cada actividad nueva y en proceso; además, se debe aplicar la afinación y monitoreo del sistema para asegurar y, cuando sea necesario, mejorar la disponibilidad y eficiencia de los sistemas.
Se deben establecer detectives de controles para indicar los problemas en el momento debido. Las proyecciones de requerimientos futuros deben tomar en cuenta los requerimientos de los negocios y sistemas nuevos y las tendencias actuales y proyectadas en las capacidades de procesamiento de la información de la organización.
Se debe prestar particular atención a cualquier recurso con tiempo de espera largos de abastecimiento o costos altos; por lo tanto, el Responsable del Área de Sistemas debe monitorear la utilización de los recursos claves del sistema.
El Responsable del Área de Sistemas debe utilizar esta información para identificar y evitar cuellos de botella potenciales y depender del personal clave que podría presentar una amenaza a la seguridad olos servicios del sistema, y se debe planear la acción apropiada.
Actividades: Llevar informes periódicos del uso de las capacidades de los sistemas, de tal forma que se pueda obtener un estimado de su rendimiento y capacidad máxima sin degradar los servicios.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Minimizar el riesgo de fallas en el sistema.
CONTROL	**10.3.2Aceptación del sistema**		
DESARROLLO			

Propósito: Establecer el criterio de aceptación de los sistemas de información nuevos, actualizaciones o versiones nuevas.

Realizar pruebas adecuadas del sistema(s) durante el desarrollo y antes de su aceptación.

Recomendación: El Responsable del Área de Sistemas y el Responsable de Seguridad de la Información deben asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados. Los sistemas de información nuevos, las actualizaciones y las versiones nuevas debieran migrar a la producción después de obtener la aceptación formal. Se debieran considerar los siguientes ítems antes de proporcionar la aceptación formal:

- El desempeño y los requerimientos de capacidad de la computadora.
- Procedimientos para la recuperación tras errores y reinicio, y planes de contingencia.
- Preparación y prueba de los procedimientos de operación rutinarios para estándares definidos.
- El conjunto de controles de seguridad acordados y aceptados.
- Procedimientos manuales efectivos.
- Arreglos para la continuidad del negocio.
- Evidencia que la instalación del sistema nuevo no afectará adversamente los sistemas existentes, particularmente en las horas picos del procesamiento.
- Evidencia que se está tomando en consideración el efecto que tiene el sistema nuevo en la seguridad general de la organización.
- Capacitación para la operación o uso de los sistemas nuevos.
- Facilidad de uso, ya que esto afecta el desempeño del usuario y evita el error humano.

Para los desarrollos nuevos importantes, la función de las operaciones y los usuarios debieran ser consultados en todas las etapas del proceso del desarrollo para asegurar la eficiencia operacional del diseño del sistema propuesto. Se debieran llevar a cabo las pruebas apropiadas para confirmar que se ha cumplido totalmente con el criterio de aceptación.
La aceptación puede incluir un proceso de certificación y acreditación formal para verificar que se hayan tratado apropiadamente los requerimientos de seguridad.

Actividades:

Establecer plataformas de pruebas para la aplicación de parches y actualizaciones de seguridad antes de ser puesto en ejecución, así también como el procedimiento asociado.

Considerar los siguientes ítems antes de la aceptación formal del sistema:

- Requerimientos de capacidad y desempeño.
- Procedimiento de recuperación ante errores y planes de contingencia.

- Preparación de rutinas de pruebas.
- Acuerdo de los controles de seguridad a implementar.
- Procedimientos de operación manual.
- Acuerdos de continuidad del negocio.
- Evidencia de que la instalación del nuevo sistema, no afectará a los actuales en producción, en particular en tiempos de utilización excesiva.
- Evidencia de que la instalación del nuevo sistema, no afectará el nivel de seguridad actual.
- Entrenamiento en la operación de los nuevos sistemas.
- Facilidad del uso, como afectan el desempeño de los usuarios y como proveen errores humanos.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Proteger la integridad del software y la integración.
CONTROL	**10.4.1Controles contra códigos maliciosos**		
DESARROLLO			

Propósito: Controles de detección, prevención y recuperación para proteger contra códigos maliciosos y se debieran implementar procedimientos para el apropiado conocimiento del usuario.

Recomendación: El Responsable de Seguridad de la Información debe definir controles de detección y prevención para la protección contra software malicioso y concientizar a los usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios. El Responsable del Área Informática, o el personal designado por éste, implementarán dichos controles. Se deberá considerar los siguientes lineamientos:

- Establecer una política formal prohibiendo el uso de software no-autorizado (ver15.1.2).
- Establecer una política formal para proteger contra riesgos asociados con la obtención de archivos, ya sea a través de redes externas o cualquier otro medio, indicando las medidas de protección a tomarse.
- Realizar revisiones regulares del software y contenido de data de los sistemas que sostienen los procesos críticos; se deberá investigar formalmente la presencia de cualquier activo no-aprobado o enmiendas no-autorizadas.
- La instalación y actualización regular de software para la detección o reparación de códigos maliciosos para revisar las computadoras y medios como un control preventivo o una medida rutinaria; los chequeos llevados a cabo debieran incluir:

  a) Chequeo de cualquier archivo en medios electrónico u ópticos, y los archivos recibidos a través de la red para detectar códigos maliciosos antes de utilizarlo.
  b) Chequear los adjuntos y descargas de los correos electrónicos para detectar códigos maliciosos antes de utilizarlos, este chequeo debiera llevarse a cabo en lugares diferentes; por ejemplo, servidores de correo electrónico, computadoras desktop y cuando se ingresa a la red de la organización.
  c) Definición, gestión, procedimientos y responsabilidades para lidiar con la protección de códigos maliciosos en los sistemas, capacitación en su uso, reporte y recuperación de ataques de códigos maliciosos.
  d) Preparar planes apropiados para la continuidad del negocio para recuperarse de ataques de códigos maliciosos, incluyendo toda la data y respaldo (back-up) de software y procesos de recuperación.
  e) Implementar procedimiento para la recolección regular de información, como suscribirse a listas de correos y/o chequear Web sites que dan información sobre códigos maliciosos nuevos.

f) Implementar procedimientos para verificar la información relacionada con el código malicioso y para asegurar que los boletines de advertencia sean exactos e informativos, El Responsable de Seguridad de la Información deberá asegurar que se utilicen fuentes calificadas; por ejemplo, periódicos acreditados, sitios de Internet confiables o proveedores que producen software para protegerse de códigos maliciosos; que diferencien entre bromas pesadas y códigos maliciosos reales; todos los usuarios debieran estar al tanto del problema de las bromas pesadas y qué hacer cuando se reciben.

El uso de dos o más productos de software para protegerse de códigos maliciosos a través del ambiente de procesamiento de la información de diferentes vendedores puede mejorar la efectividad de la protección contra códigos maliciosos.

Se puede instalar software para protegerse de códigos maliciosos para proporcionar actualizaciones automáticas de archivos de definición y motores de lectura para asegurarse que la protección esté actualizada. Además, este software se puede instalar en cada desktop para que realice chequeos automáticos.

Se debiera tener cuidado de protegerse contra la introducción de códigos maliciosos durante el mantenimiento y procedimientos de emergencia, los cuales pueden evadir los controles de protección contra códigos maliciosos normales.

Actividades:

- Establecer una política formal que prohíba el uso no autorizado de software.
- Establecer una política formal que proteja ante los riesgos asociados al obtener software y archivos a través de redes externas, o cualquier otro medio, indicando que medidas preventivas deber ser tomadas.
- Efectuar revisiones periódicas del software y los contenidos de los datos de los sistemas que soportan procesos de negocio críticos, y se debe investigar ante la presencia de cualquier archivo no autorizado.
- Se debe instalar software que detecte código malicioso que sea enviado a través de cualquier medio y este debe ser actualizado regularmente.
- Definir procedimientos y responsabilidades para tratar con código malicioso, entrenamiento en el uso, reporte recuperación ante ataques.
- Preparar apropiados planes de continuidad del negocio para recuperarse ante eventuales ataques.
- Implementar procedimientos para recopilar regularmente información como listas de correo o sitios informativos.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Proteger la integridad del software y la integración.
CONTROL	**10.4.2Controles contra códigos móviles**		
DESARROLLO			

Propósito: Donde se autorice el uso del código móvil, la configuración debiera asegurar que el código móvil autorizado opera de acuerdo con una política de seguridad claramente definida, y se debiera evitar la ejecución del código móvil no-autorizado.

Recomendación: Considerar las siguientes acciones para evitar que el código móvil realice acciones no-autorizadas:

- Ejecutar el código móvil en un ambiente aislado lógicamente.
- Bloquear cualquier uso del código móvil.
- Bloquear lo recibido del código móvil.
- Activar las medidas técnicas conforme estén disponibles en un sistema específico para asegurar el manejo del código móvil.
- Control de los recursos disponibles para el acceso del código móvil.
- Controles criptográficos para autenticar singularmente el código móvil.

Además de asegurar que el código móvil no contenga códigos maliciosos, el control de código móvil es esencial para evitar el uso no-autorizado o interrupción de un sistema o recursos de aplicación y otras fallas en la seguridad de la información.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Proteger la integridad del software y la integración.
CONTROL	**10.5.1 Copias de seguridad de la información**		
DESARROLLO			

Propósito: Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Recomendación: Se debiera proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de medios:

Se debieran considerar los siguientes ítems para el respaldo de la información:

- Se debiera definir el nivel necesario de respaldo de la información.
- Se debieran producir registros exactos y completos de las copias de respaldo y procedimientos documentados de la restauración.
- La extensión (por ejemplo: respaldo completo o diferencial) y la frecuencia de los respaldos debiera reflejar los requerimientos comerciales de la organización, los requerimientos de seguridad de la información involucrada, y el grado crítico de la información para la operación continua de la organización.
- Las copias de respaldo se debieran almacenar en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el local principal.
- A la información de respaldo se le debiera dar el nivel de protección física y ambiental apropiado consistente con los estándares aplicados en el local principal; los controles aplicados a los medios en el local principal se debiera extender para cubrir la ubicación de la copia de respaldo.
- Los medios de respaldo se debieran probar regularmente para asegurar que se puedan confiar en ellos para usarlos cuando sea necesaria en caso de emergencia.
- Los procedimientos de restauración se debieran chequear y probar regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación.
- En situaciones cuando la confidencialidad es de importancia, las copias de respaldo debieran ser protegidas por medios de una codificación.

Los procedimientos de respaldo para los sistemas individuales debieran ser probados regularmente para asegurar que cumplan con los requerimientos de los planes de continuidad del negocio. Para sistemas críticos, los procedimientos de respaldo debieran abarcar toda la información, aplicaciones y data de todos los sistemas, necesarios para recuperar el sistema completo en caso de un desastre.

Se debiera determinar el período de retención para la información comercial esencial, y también cualquier requerimiento para que las copias de archivo se mantengan permanentemente.

Los procedimientos de respaldo pueden ser automatizados para facilitar el proceso de respaldo y restauración. Estas soluciones automatizadas debieran ser probadas suficientemente antes de su implementación y también a intervalos regulares.

Actividades:

- Proveer registros completos y registros de la información que se respalda, así también como los procedimientos de recuperación.
- Probar regularmente los medios de recuperación para asegurar que puedan ser utilizados.
- Los procedimientos de restauración deben ser probados regularmente.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Asegurar la protección de la información en redes y la protección de lainfraestructura de soporte
CONTROL	**10.6.1 Controles de redes**		
DESARROLLO			

Propósito: Manejar y controlar las redes con el fin de proteger la información en las redes, y mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.

Recomendación: El Responsable de Seguridad de la Información debiera implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados. En particular, se debieran considerar los siguientes ítems:

- Cuando sea apropiado, la responsabilidad operacional para las redes se debiera separar de las operaciones de cómputo.
- Se debieran establecer las responsabilidades y procedimientos para la gestión del equipo remoto, incluyendo el equipo en las áreas del usuario.
- Se debieran establecer controles especiales para salvaguardar la confidencialidad y la integridad de la data que pasa a través de las redes públicas o a través de las redes inalámbricas; y proyectar los sistemas y aplicaciones conectados; también se pueden requerir controles especiales para mantener la disponibilidad de los servicios de la red y las computadoras conectadas.
- Se debiera aplicar registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes.
- Las actividades de gestión debieran estar estrechamente coordinadas para optimizar el servicio a la organización y para asegurar que los controles sean aplicados consistentemente a través de la infraestructura de procesamiento de la información.

Se puede encontrar información adicional sobre la seguridad de la red en ISO/IEC 18028, Tecnología de la Información – Técnicas de seguridad – Seguridad de Red TI.

Actividades:

- Separar la responsabilidad en la operación de las redes de las responsabilidades en el manejo de los servidores.
- Establecer responsabilidades y procedimientos de administración de equipamiento remoto.
- Establecer controles especiales para resguardar la confidencialidad e integridad de los datos que viajan sobre redes públicas o inalámbricas.
- Establecer los mecanismos apropiados de monitoreo y registro de las acciones relevantes para la seguridad.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Asegurar la protección de la información en redes y la protección de lainfraestructura de soporte
CONTROL	**10.6.2 Seguridad de los servicios de la red**		
DESARROLLO			

Propósito: Identificar e incluir las en el contrato de redes las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, ya sea que estos servicios sean provistos interna o externamente.

Recomendación: L**os** servicios de red incluyen la provisión de conexiones, servicios de redes privadas, redes de valor agregado y soluciones de seguridad de red manejadas como firewalls y sistemas de detección de intrusiones. Estos servicios pueden ir desde una simple banda ancha manejada ofertas complejas de valor agregado.

Las características de seguridad de los servicios de red pueden ser:

a) la tecnología aplicada para la seguridad de los servicios de red; como controles de autenticación, codificación y conexión de red.
b) parámetros técnicos requeridos para una conexión segura con los servicios de red en concordancia con las reglas de seguridad y conexión de red.
c) cuando sea necesario, procedimientos para la utilización del servicio de red para restringir el acceso a los servicios de red o aplicaciones.

De acuerdo a lo anterior, se debiera determinar y monitorear regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura, y se debiera acordar el derecho de auditoría.

Se debieran identificar los acuerdos de seguridad necesarios para servicios particulares; como las características de seguridad, niveles de servicio y requerimientos de gestión.

La organización se debiera asegurar que los proveedores de servicio de red implementen estas medidas.

Actividades:

- Aplicar tecnología para asegurar los servicios de red, tal como autenticación, encriptación y control de conexiones.
- Establecer conexiones seguras a través de reglas de accedo de acuerdo los requerimientos de la institución.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales
CONTROL	**10.7.1 Gestión de soportes extraíbles**		
DESARROLLO			

Propósito: Crear procedimientos para la gestión de los medios removibles.

Recomendación: Se debieran considerar los siguientes lineamientos para la gestión de medios removibles:

- Si ya no son requeridos, los contenidos de los medios re-usables que no son removidos de la organización no debieran ser recuperables.
- Se debieran establecer los procedimientos para identificar los ítems que podrían requerir de una eliminación segura.
- Podría ser más fácil arreglar que todos los ítems de medios se recolecten y eliminen de forma segura, en lugar de tratar de separar los ítems sensibles o confidenciales.
- Muchas organizaciones ofrecen servicios de recolección y eliminación de papeles, equipo y medios; se debiera tener cuidado al seleccionar el contratista adecuado con los controles y la experiencia adecuados.
- Cuando sea posible se debiera registrar la eliminación de ítems confidenciales para mantener un rastro de auditoría.

Cuando se acumula medios para ser eliminados, se debiera tener en consideración el efecto de agregación, el cual puede causar que una gran cantidad de información no-confidencial se convierta en confidencial.

Actividades:

- Los contenidos de cualquier medio reutilizable, deben ser removidos de la institución, haciéndolos irrecuperables.
- Todos los medios deben almacenarse en un ambiente seguro de acuerdo a las especificaciones del fabricante.
- La información almacenada en medios removibles que requiera estar disponible después del tiempo de vida del medio, debe ser almacenado en cualquier otro medio de tal manera que se garantice la permanencia de la información.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales
CONTROL	**10.7.2 Retirada de soportes**		

DESARROLLO
Propósito: Eliminar los medios de forma segura y sin riesgo cuando ya no sea requerido, utilizando procedimientos formales. **Recomendación:** El Responsable del Área Informática, junto con el Responsable de Seguridad de la Información deberá definir procedimientos para la eliminación segura de los medios de soporte de información respetando la normativa vigente. Los procedimientos deben considerar que los siguientes elementos requerirán almacenamiento y eliminación segura: • Documentos en papel. • Voces u otras grabaciones. • Papel carbónico. • Informes de salida. • Cintas de impresora de un solo uso. • Cintas magnéticas. • Discos u otros dispositivos removibles. • Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor). • Listados de programas. • Datos de prueba. • Documentación del sistema. La evaluación del mecanismo de eliminación debe contemplar el tipo de dispositivo y la criticidad de la información contenida.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales
CONTROL	**10.7.3 Procedimientos de manipulación de la información**		
DESARROLLO			
Propósito: Establecer los procedimientos para el manejo y almacenaje de información para proteger esta información de una divulgación no-autorizada o mal uso. **Recomendación:** Se debieran establecer los procedimientos para el manipuleo, procesamiento, almacenaje y comunicación de la información consistente con su clasificación (de acuerdo al 7.2). Se debieran considerar los siguientes ítems: • Manipuleo y etiquetado de todos los medios en su nivel de clasificación indicado. • Restricciones de acceso para evitar el acceso de personal no-autorizado. • Mantenimiento de un registro formal de destinatarios autorizados de la data.			

- Asegurar que el input de data esté completo, que el proceso se complete apropiadamente y que se aplique la validación del output.
- Protección de la data recolectada esperando el output en un nivel consistente con la confidencialidad.
- Almacenaje de medios en concordancia con las especificaciones de los fabricantes.
- Mantener la distribución de data en lo mínimo.
- Marcar claramente todas las copias de los medios con atención al destinatario autorizado.
- Revisión de las listas de distribución y las listas de los destinatarios autorizados a intervalos regulares.

Estos procedimientos se aplican a la información en documentos; sistemas de cómputo; redes; computación móvil; comunicaciones móviles; comunicaciones vía correo, correo de voz y voz en general; multimedia; servicios/medios postales, uso de máquinas de fax y cualquier otro ítem confidencial; por ejemplo cheques en blanco, facturas.

Actividades:

- Manejar y rotular todos los medios indicando su nivel de clasificación.
- Restringir el acceso solo al personal debidamente autorizado.
- Se debe mantener un registro formal.
- El almacenamiento de los medios debe estar acorde a las especificaciones del fabricante.
- Mantener la cadena de custodia al mínimo.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales
CONTROL	**10.7.4 Seguridad de la documentación del sistema**		
DESARROLLO			

Propósito: Proteger la documentación del sistema con accesos no-autorizados.

Recomendación: La documentación del sistema puede contener un rango de información confidencial; por ejemplo, una descripción de los procesos de aplicaciones, procedimientos, estructuras de data, procesos de autorización.

Para asegurar la documentación del sistema, se debieran considerar los siguientes ítems:

- La documentación del sistema se debiera almacenar de una manera segura.
- La lista de acceso para la documentación del sistema se debiera mantener en un nivel mínimo y autorizado por el propietario de la aplicación.
- La documentación del sistema mantenido en una red pública, o suministrada a través de una red pública, debiera estar adecuadamente protegida.

Actividades:

- Almacenar la documentación del sistema en forma segura.
- Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa
CONTROL	**10.8.1Políticas y procedimientos de intercambio de información**		
DESARROLLO			

Propósito: Establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.

Recomendación: Diseñar los procedimientos y controles cuando se utilizan medios de comunicación electrónicos para el intercambio de información. Se debieran considerar los siguientes ítems:

- Los procedimientos diseñados para proteger el intercambio de información de la intercepción, copiado, modificación, routing equivocado y destrucción.
- Los procedimientos para la detección y protección de contra códigos maliciosos que pueden ser transmitidos a través del uso de comunicaciones electrónicas (de acuerdo a la cláusula 10.4.1).
- Los procedimientos para proteger la información electrónica confidencial comunicada que está en la forma de un adjunto.
- Política o lineamientos delineando el uso aceptable de los medios de comunicación electrónicos.
- Los procedimientos para el uso de comunicación inalámbrica, tomando en cuenta los riesgos particulares involucrados.
- Las responsabilidades del usuario empleado, contratista y cualquier otro para que no comprometan a la organización; por ejemplo, a través de la difamación, hostigamiento, suplantación, reenvío de cadenas de cartas, compras no-autorizadas, etc.
- Uso de técnicas de codificación; por ejemplo, para proteger la confidencialidad, integridad y autenticidad de la información.
- Lineamientos de retención y eliminación de toda la correspondencia del negocio, incluyendo mensajes, en concordancia con la legislación y regulaciones nacionales y locales relevantes.

- No dejar la información confidencial o crítica en medios impresos; por ejemplo, copiadoras, impresoras y máquinas de fax; ya que personal no-autorizado puede tener acceso a ellas.
- Los controles y restricciones asociados con el reenvío de los medios de comunicación; por ejemplo, reenvío automático de correo electrónico a direcciones externas.
- Recordar al personal que debiera tomar las precauciones apropiadas; por ejemplo, no revelar información confidencial cuando realiza una llamada telefónica para evitar ser escuchado o interceptado por:

  a) Personas alrededor suyo, particularmente cuando se utilizan teléfonos Móviles.
  b) Intervención de teléfonos y otras formas de escucha no-autorizada a través del acceso físico al teléfono o la línea telefónica, o el uso de escáneres receptores.
  c) Personas en el otro lado de la línea, en el lado del receptor.
- No dejar mensajes conteniendo información confidencial en máquinas contestadoras dado que estos pueden ser escuchados por personas no-autorizadas, ni almacenados en sistemas comunitarios o almacenados incorrectamente como resultado de un equívoco al marcar.
- Recordar al personal el problema de utilizar máquinas de fax, principalmente por:

  a) Acceso no autorizado al almacén de mensaje incorporado para recuperar los mensajes.
  b) Programación deliberada o accidental de las máquinas para enviar mensajes a números específicos.
  c) Enviar documentos al número equivocado, ya sea por marcar un número equivocado o usando un número erróneamente almacenado.
- Recordar al personal no registrar data demográfica, como la dirección de correo electrónico u otra información personal, en ningún software para evitar que sea utilizada sin autorización.
- Recordar al personal que las máquinas de fax y fotocopiadoras modernas tienen páginas cache y almacenan páginas en caso de una falla en la transmisión o papel, las cuales se imprimirán una vez que la falla se aclare.
- Además, se debiera recordar al personal que no debieran mantener conversaciones confidenciales en lugares públicos, u oficinas o salas de reuniones abiertas, sin paredes a prueba de ruidos.

Los medios de intercambio de información debieran cumplir con cualquier requerimiento legal relevante.

Los intercambios de información pueden ocurrir a través del uso de un número de tipos de comunicación diferentes; incluyendo correo electrónico, de voz, fax y vídeo.El intercambio de software puede ocurrir a través de un número de medios diferentes; incluyendo la descarga de Internet y el adquirido en una tienda.

Se debieran considerar las implicancias comerciales, legales y de seguridad asociada con el intercambio electrónico de data, comercio electrónico y comunicaciones electrónicas, y los requerimientos de controles.

La información puede verse comprometida por la falta de conocimiento, política o procedimientos para el uso de los medios de intercambio de información; por ejemplo, ser escuchado al hablar de un teléfono móvil en un lugar público, dirección equivocada en un mensaje de correo electrónico, mensajes dejados en máquinas contestadores escuchados, acceso no-autorizado al sistema de correo de voz o accidentalmente enviar faxes al número equivocado.
Las operaciones comerciales pueden verse interrumpidas y la información puede verse comprometida si fallan los medios de comunicación, son escuchados o interrumpidos. La información puede verse comprometida si usuarios no-autorizados tienen acceso a ella.

Actividades:

- Diseñar los procedimientos para proteger el intercambio de información de la intercepción, copiado, modificación, ruting equivocado y destrucción.
- Diseñar el procedimiento para la detección y protección en contra de códigos maliciosos que puedan ser trasmitidos a través del uso de comunicaciones electrónicas.
- Diseñar el procedimiento para proteger la información electrónica confidencial.
- Crear una política o lineamiento para el uso aceptable de los medios de comunicación electrónicos.
- Crear el procedimiento para el uso de comunicación inalámbrica, tomando en cuenta los riesgos particulares involucrados.
- Uso de técnicas de codificación; para proteger la confidencialidad, integridad y autenticidad de la información.
- Creación de los lineamientos de retención, eliminación de toda la correspondencia de la universidad, incluyendo mensajes, en concordancia con la legislación y regulación local y nacional.
- No dejar la información confidencial o crítica en medios impresos; por ejemplo, copiadoras, impresoras y máquinas de fax; ya que el personal no-autorizado puede tener acceso a ella.
- Controles y restricciones asociados con el reenvío de información; por ejemplo, reenvío automático de correo electrónicos a direcciones externas.
- Instruir al personal para que tome medidas de precauciones apropiadas; por ejemplo, no revelar información confidencial cuando realiza una llamada telefónica para evitar ser escuchado o interceptado.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.
CONTROL	**10.8.2Acuerdos de intercambio**		
DESARROLLO			

Propósito: Establecer y mantener las políticas, procedimientos y estándares para proteger la información y medios físicos en tránsito, y se debiera hacer referencia en los acuerdos de intercambio.

Recomendación: Los acuerdos pueden ser electrónicos o manuales, y pueden tomar la forma de contratos formales o condiciones de empleo. Para la información sensible, los mecanismos específicos utilizados para el intercambio de dicha información debieran ser consistentes para todas las organizaciones y tipos de acuerdos.

Actividades:

- Estipular el manejo de las responsabilidades para el control y notificación de la transmisión, despacho y recepción.
- Crear los procedimientos para notificar al remitente de la transmisión, despacho y recepción.
- Diseñar los procedimientos para asegurar el rastreo y no-repudio.
- Estipular los estándares técnicos mínimos para el empaque y la transmisión.
- Describir los acuerdos de depósitos.
- Acordar los estándares de identificación del mensajero.
- Establecer las responsabilidades y obligaciones en el evento de incidentes de seguridad de la información, como la pérdida de data.
- uso de un sistema de etiquetado acordado para la información confidencial o crítica, asegurando que el significado de las etiquetas sea entendido inmediatamente y que la información sea adecuadamente protegida.
- Describir la propiedad y responsabilidades de la protección de data, derechos de autor, licencias de software y consideraciones similares.
- Diseñar los estándares técnicos para grabar y leer la información y software.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.
CONTROL	**10.8.3 Soportes físicos en tránsito**		
DESARROLLO			

Propósito: Proteger los medios que contienen información contra accesos no-autorizados, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.

Recomendación: Considerar los siguientes lineamientos para proteger los medios de información transportados entre diferentes ubicaciones:

- Se debieran utilizar transportes o mensajerías confiables.
- Se debiera acordar con la gerencia una lista de mensajerías autorizadas.
- Se debieran desarrollar procedimientos para chequear la identificación de los mensajeros.

- El empaque debiera ser suficiente para proteger los contenidos de cualquier daño que pudiera surgir durante el tránsito y en concordancia con las especificaciones de cualquier fabricante (por ejemplo, para software), por ejemplo protegiendo de cualquier factor ambiental que pudiera reducir la efectividad de la restauración de medios, tales como la exposición al calor, humedad o campos electromagnéticos.
- Donde sea necesario, se debieran adoptar controles para proteger la información confidencial de la divulgación o modificación no-autorizada, los ejemplos incluyen:
  a) Uso de contenedores cerrados con llave.
  b) Entrega en la mano.
  c) Empaque que haga evidente si ha sido manipulado (el cual revela cualquier intento por obtener acceso).
  d) En casos excepcionales, dividir el envío en más de una entrega y despacharlo por rutas diferentes.

La información puede ser vulnerable al acceso no-autorizado, mal uso o corrupción durante el transporte, por ejemplo cuando se envía medios por el servicio postal o servicio de mensajería.

Actividades:
- Utilizar transporte o mensajería confiable.
- Desarrollar procedimientos para chequear la identificación de los mensajeros.
- Proteger los contenidos de cualquier daño utilizando empaques rústicos.
- Adoptar controles para proteger la información confidencial de la divulgación o modificación no-autorizada.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.
CONTROL	**10.8.4 Mensajería electrónica**		
DESARROLLO			

Propósito: Proteger adecuadamente la información involucrada en mensajes electrónicos.

Recomendación: Los mensajes electrónicos como el correo electrónico, Intercambio Electrónico de Data (EDI), y los mensaje instantáneos representa un papel cada vez más importante en las comunicaciones comerciales. Los mensajes electrónicos tienen riesgos diferentes que las comunicaciones basadas en papel.

Las consideraciones de seguridad para los mensajes electrónicos debieran incluir lo siguiente:
- Proteger los mensajes del acceso no-autorizado, modificación o negación del servicio.
- Asegurar la correcta dirección y transporte del mensaje.

- Confiabilidad y disponibilidad general del servicio.
- Consideraciones legales, por ejemplo los requerimientos para firmas electrónicas.
- Obtener la aprobación antes de utilizar los servicios públicos externos como un mensaje instantáneo o intercambio de archivos.
- Niveles mayores de autenticación controlando el acceso de las redes de acceso público.

Actividades:

- Proteger los mensajes del acceso no-autorizado, modificación o negación del servicio.
- Asegurarla correcta asignación de la dirección y el transporte del mensaje.
- niveles altos de controles de autenticación para los accesos desde las redes públicamente accesibles.
- Obtención de aprobación previa al uso de los servicios públicos externos tales como mensajería instantánea o el compartir archivos.

DOMINIO	Gestión de las comunicaciones y operaciones	**OBJETIVO**	Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.
CONTROL	**10.8.5 Sistemas de información empresariales**		
DESARROLLO			

Propósito: Desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.

Recomendación: Los sistemas de información de oficina son oportunidades para una difusión e intercambio más rápidos de la información comercial utilizando una combinación de documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios/medios postales y máquinas de fax.

La consideración dada a las implicancias de seguridad y comerciales de interconectar dichos medios debiera incluir:

- vulnerabilidades conocidas en los sistemas administrativos y contables donde la información es compartida entre diferentes partes de la organización.
- Las vulnerabilidades de la información en los sistemas de comunicación comercial; por ejemplo, grabando llamadas o conferencias telefónicas, la confidencialidad de las llamadas, almacenaje de faxes, apertura de correo, distribución del correo.
- Política y los controles apropiados para manejar el intercambio de información.
- Excluir las categorías de información comercial confidencial y los documentos clasificados si el sistema no proporciona un nivel de protección apropiado.

- Restringir el acceso a la información diaria relacionada con personas seleccionadas; por ejemplo, el personal trabajando en proyectos confidenciales.
- Categorías del personal, contratistas o socios comerciales con autorización para utilizar el sistema y las ubicaciones desde las cuales pueden tener acceso.
- Restringir los medios seleccionados a categorías de usuarios específicas.
- Identificar el status de los usuarios; por ejemplo, los empleados de la organización o contratistas en directorios para beneficio de otros usuarios.
- Retención y respaldo de la información mantenida en el sistema.
- Requerimientos y acuerdos alternativos.

Actividades:
- Establecer una política y los controles apropiados para manejar el intercambio de información.

DOMINIO	Gestión de las Comunicaciones y Operaciones	**OBJETIVO**	Servicios de Comercio Electrónico
CONTROL	**10.9.1 Comercio Electrónico**		
DESARROLLO			

Propósito: Protegerse de la actividad fraudulenta, disputas de contratos, divulgación no autorizada y modificación, resguardando la seguridad de los servicios de comercio electrónico y su uso seguro.

Recomendación: El comercio electrónico es vulnerable a un gran número de amenazas de la red que pueden resultar en una actividad fraudulenta, divulgación o modificación de la información.
Se debieran considerar las implicaciones de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo las transacciones en-línea, y los requerimientos de controles. También se debiera considerar la integridad y la disponibilidad de la información publicada electrónicamente a través de los sistemas públicamente disponibles.
También se debe considerar los siguientes aspectos de seguridad para el comercio electrónico:
- La vulnerabilidad al acceso o modificación no autorizados o a la denegación de servicio.
- La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
- Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
- La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad en la estación receptora o de la red a la que se encuentra conectada.

- Las implicaciones de la publicación externa de información sensible o confidencial, accesibles al público.

Los acuerdos de comercio electrónico entre socios debieran ser respaldados por un contrato documentado el cual compromete a ambas partes a los términos acordados para la comercialización.

Actividades:

- Asegurar el nivel de confianza que cada parte requiere de la identidad de la otra; por ejemplo, a través de la autenticación.
- Determinar y garantizar los requerimientos para la confidencialidad, integridad, disponibilidad y el no-repudio de cualquier transacción.
- Evitar la pérdida o duplicación de la información de la transacción.

DOMINIO	Gestión de las Comunicaciones y Operaciones	**OBJETIVO**	Servicios de Comercio Electrónico
CONTROL	**10.9.2 Transacciones en línea**		
DESARROLLO			

Propósito: Asegurar la operación correcta y segura de los recursos de tratamiento de información, minimizando el riesgo de fallos en los sistemas para proteger la integridad de los sistemas y de la información; así como de la pérdida, modificación o mal uso de la información involucrada en las transacciones en-línea
Evitar una transmisión incompleta, ruta equivocada, alteración no-autorizada del mensaje, divulgación no-autorizada, duplicación o repetición no-autorizada del mensaje.

Recomendación: Las consideraciones de seguridad para las transacciones en-línea debieran incluir lo siguiente:
El uso de firmas electrónicas por cada una de las partes involucradas en la transacción.
Todos los aspectos de la transacción; es decir, asegurando que:

- Las credenciales de usuario de todas las partes sean válidas y verificadas.
- Que la transacción permanezca confidencial.
- Que se mantenga la privacidad asociada con todas las partes involucradas.

El camino de las comunicaciones entre las partes involucradas debiera ser codificado
Los protocolos utilizados para comunicarse entre todas las partes involucradas sean seguros

Cuando se utilice una autoridad confiables (por ejemplo, para propósitos de emitir ymantener firmas digitales y/o certificados digitales) la seguridad es integrada eintroducida durante todo el proceso de gestión de firma/certificado de principio a fin.

Actividades: Asegurar que el almacenaje de los detalles de la transacción se localice fuera decualquier ambiente público accesible; por ejemplo, en una plataforma de almacenajeexistente en el Intranet organizacional, y no se mantenga y exponga en un medio dealmacenaje directamente accesible desde el Internet.
Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.
Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.

Se deberían proteger los servicios y la información de registro de la actividad contra acciones forzosas o accesos no autorizados.

DOMINIO	Gestión de las Comunicaciones y Operaciones	**OBJETIVO**	Servicios de Comercio Electrónico
CONTROL	**10.9.3 Información Públicamente Disponible**		
DESARROLLO			

Propósito: Tomar medidas para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación.

Recomendación: El software, datos y otra información que requiere un alto nivel de integridad, puesta a disposición en un sistema públicamente disponible, se debiera proteger mediante los mecanismos apropiados. El sistema públicamente disponible debiera ser probado en busca de debilidades y fallas antes que la información esté disponible.
Se debiera implementar un procedimiento de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación.

Actividades: Se debieran controlar cuidadosamente los sistemas de publicación electrónica, especialmente aquellos que permiten retroalimentación y el ingreso directo de información de manera que:

- La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la Ley de Protección de Datos Personales.
- La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.
- La información sensible o confidencial sea protegida durante el proceso de recolección y su almacenamiento.

- El acceso al sistema de publicación no permita el acceso involuntario a las redes a las cuales se conecta el mismo.
- El responsable de la publicación de información en sistemas de acceso público sea claramente identificado.
- La información se publique teniendo en cuenta las normas establecidas al respecto.
- Se garantice la validez y vigencia de la información publicada

DOMINIO	Gestión de las Comunicaciones y Operaciones	**OBJETIVO**	Supervisión
CONTROL	**10.10.1 Registros de Auditoría**		
DESARROLLO			

Propósito: Producir y mantener registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un período acordado para permitir la detección e investigación de incidentes.

Recomendación: Se deben monitorear los sistemas y se deben reportar los eventos de seguridad de la información. Se deben utilizar bitácoras de operador y se deben registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información.

Actividades

- Utilizar identificadores IDs.
- Fechas, horas y detalles de eventos claves; por ejemplo, ingreso y salida.
- Identidad o ubicación de la identidad, direcciones IP
- Registros de intentos de acceso fallidos y rechazados al sistema.
- Registros de intentos de acceso fallidos y rechazados a la data y otros recursos.
- Cambios en la configuración del sistema.
- Uso de privilegios.
- Uso de las utilidades y aplicaciones del sistema.
- Archivos a los cuales se tuvo acceso y los tipos de acceso.
- Direcciones y protocolos de la red.
- Alarmas activadas por el sistema de control de acceso.
- Activación y desactivación de los sistemas de protección; como sistemas anti-virus y sistemas de detección de intrusiones.

DOMINIO	Gestión de las Comunicaciones y Operaciones	OBJETIVO	Supervisión
CONTROL	10.10.2 Supervisión del uso del sistema		
DESARROLLO			

Propósito: Determinar el nivel de monitoreo requerido para implementar controles para la protección de los registros de auditoría contra cambios no autorizados y problemas operacionales.

Recomendación: Cada sistema de registro implementado, debe ser monitoreado y protegido ante accesos no autorizados en las siguientes áreas

Acceso no autorizado

- ID del usuario.
- Fecha y hora de los eventos claves.
- Tipos de eventos.
- Archivo a los cuales se tuvo acceso.
- Programas/utilidades utilizados.

Operaciones privilegiadas

- Uso de las cuentas privilegiadas; por ejemplo, supervisor, raíz,, administrador,
- Inicio y apagado del sistema.
- Dispositivo I/O para adjuntar y eliminar lo adjuntado.

Intentos de acceso no autorizados

- Accesos del usuario fallidas o rechazadas.
- Acciones fallidas o rechazadas que involucran la data y otros recursos.
- Violaciones a la política de acceso y notificaciones para los ‘gateways’ y ‘firewalls’ de la red.
- Alertas de los sistemas de detección de intrusiones.

Alertas o fallas del sistema

- Alertas o mensajes en la consola.
- Excepciones del registro del sistema.
- Alarmas de la gestión de la red.
- Alarmas activadas por el sistema de control de acceso.

Actividades

- Cumplir con los requerimientos legales relevantes aplicables para sus actividades de monitoreo
- Utilizar de procedimientos de monitoreo para asegurar que los usuarios sólo estén realizando actividades para las cuales han sido explícitamente autorizados.

DOMINIO	Gestión de las Comunicaciones y Operaciones	**OBJETIVO**	Supervisión
CONTROL	**10.10.3 Protección de la Información de los registros**		
DESARROLLO			

Propósito: Registrar y revisar periódicamente en particular las actividades de los administradores y operadores de sistema.

Recomendación: Los controles debieran tener el objetivo de proteger contra cambios no autorizados y problemas operacionales, y el medio de registro debiera incluir:

- Las alteraciones registradas a los tipos de mensajes;
- Los archivos de registro que se editan o borran;
- Capacidad de almacenamiento del medio de archivos de registro que se está excediendo, resultando en una falla en el registro de eventos o la escritura encima de los eventos registrados en el pasado.

Actividades: Los registros de administrador y operador del sistema debieran ser revisados de manera regular.

DOMINIO	Gestión de las Comunicaciones y Operaciones	OBJETIVO	Supervisión
CONTROL	**10.10.4 Registros de administración y operación**		
DESARROLLO			

Propósito: Registrar las actividades del administrador del sistema y el operador del sistema

Recomendación: Revisión periódica las actividades de los administradores y operadores de los sistemas.

- Cuenta de administración u operación involucrada
- Momento en el cual ocurre un evento, hora del evento(éxito o falla);
- Información acerca del evento (por ejemplo, los archivos manipulados) o las fallas (por ejemplo, los errores ocurridos y las acciones correctivas tomadas);
- Procesos involucrados.

Actividades

- Los registros de administrador y operador del sistema debieran ser revisados de manera regular.
- Todas las cuentas con privilegios de usuario administrador o súper usuario deben ser continuamente registrados y monitoreados

DOMINIO	Gestión de las Comunicaciones y Operaciones	OBJETIVO	Supervisión
CONTROL	**10.10.5 Registro de fallos**		
DESARROLLO			

Propósito: Registrar y analizar las fallas, para tomar las acciones necesarias

Recomendación: Se debieran registrar todas las fallas reportadas por los usuarios o por los programas del sistema relacionadas con los problemas con el procesamiento de la información o los sistemas de comunicación. Debieran existir reglas claras para manejar las fallas reportadas incluyendo:

- Revisión de los registros de fallas para asegurar que las fallas se hayan resuelto satisfactoriamente;
- Revisión de las medidas correctivas para asegurar que los controles no se hayan visto comprometidos, y que la acción tomada haya sido completamente autorizada.

Actividades: Cada acción indebida realizada por una cuenta de acceso, debe ser oportunamente notificada al encargado de la seguridad de la información para tomar las acciones requeridas

DOMINIO	Gestión de las Comunicaciones y Operaciones	**OBJETIVO**	Supervisión
CONTROL	**10.10.6 Sincronización de relojes**		
DESARROLLO			

Propósito: Sincronizar con una fuente que proporcione la hora exacta los relojes de todos los sistemas de procesamiento de información relevantes.

Recomendación: El ajuste correcto de los relojes del computador es importante para asegurar la exactitud de los registros de auditoría, los cuales se pueden requerir para investigaciones o como evidencia en casos legales o disciplinarios. Se debiera utilizar un protocolo de hora de red para mantener todos los servidores sincronizados con el reloj maestro.

Cuando una computadora o dispositivo de comunicaciones tiene la capacidad para operar un reloj de tiempo-real, este reloj debiera ser puesto a la hora de acuerdo a un estándar acordado; por ejemplo, el Tiempo Universal Coordinado (UTC) o la hora estándar local. Ya que algunos relojes se atrasan o adelantan a lo largo del tiempo, debiera existir un procedimiento que los chequee y corrija cualquier variación significativa.

Actividades: Se deben sincronizar los relojes de todos los sistemas críticos contra un reloj central, y éste a su vez sincronizado con un reloj en internet

DOMINIO	Control de Acceso	**OBJETIVO**	Requisitos del negocio para el control de acceso
CONTROL	**11.1.1 Política de control de acceso**		
DESARROLLO			

Propósito: Controlar el acceso a la información. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos de negocio sobre la base de los requerimientos de negocio y de seguridad.

Recomendación: La política de seguridad debería tomar en cuenta lo siguiente:

- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones.
- Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes
- Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones y dispositivos disponibles.
- La revocación de los derechos de acceso.

Actividades

- Las reglas de control del acceso debieran tomar en cuenta las políticas para la divulgación y autorización de la información.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas

DOMINIO	Control de Acceso	**OBJETIVO**	Gestión de acceso de usuario
CONTROL	**11.2.1 Registro de usuario**		
DESARROLLO			

Propósito: Establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Recomendación: Un procedimiento formal de registro de usuarios para otorgar y revocar el acceso debiera tener en cuenta:

- Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
- Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad del Comité
- Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.

- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la Universidad o sufrieron la pérdida o robo de sus credenciales de acceso.
- Efectuar revisiones periódicas con el objeto de:
  - cancelar identificadores y cuentas de usuario redundantes
  - inhabilitar cuentas inactivas por un período de máximo de 60 días
  - eliminar cuentas inactivas por un período mayor a 120 días
- En el caso de existir excepciones, deben ser debidamente justificadas, aprobadas y documentadas.
- Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

Actividades: El Responsable de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información.

DOMINIO	Control de Acceso	**OBJETIVO**	Gestión de acceso de usuario
CONTROL	**11.2.2 Gestión de privilegios**		
DESARROLLO			

Propósito: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información. Se limitará y controlará la asignación y uso de privilegios.

- **Recomendación**
- Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

Actividades: Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad de la Información.

DOMINIO	Control de Acceso	**OBJETIVO**	Gestión de acceso de usuario
CONTROL	**11.2.3 Gestión de contraseña de usuario**		
DESARROLLO			

Propósito: Asignar contraseñas y se controlará a través de un proceso de administración formal

- **Recomendación**
- Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad
- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo deben suministrarse una vez acreditada la identidad del usuario.
- Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo formal cuando la reciban.
- Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la, verificación de firma, uso de autenticadores de hardware, etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad de la Información conjuntamente con el Responsable del Área de Informática y el Propietario de la Información lo determine necesario.
- Configurar los sistemas de tal manera que:
    - las contraseñas sean del tipo “password fuerte” y tengan mínimo 8 caracteres entre ellos alfanuméricos mayúsculas, minúsculas y especiales.
    - suspendan o bloqueen permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta. En caso de bloqueo debe pedir la rehabilitación ante quien corresponda.
    - solicitar el cambio de la contraseña cada 30 a 45 días.
    - impedir que las últimas 10 a 12 contraseñas sean reutilizadas,

Actividades

- Verificar la identidad del usuario antes de otorgar acceso a un sistema o servicio de información
- Monitorear periódicamente el cambio de contraseñas de usuario

DOMINIO	Control de Acceso	**OBJETIVO**	Gestión de acceso de usuario
CONTROL	**11.2.4 Revisión de los derechos de acceso de usuario**		
DESARROLLO			

Propósito: Inspeccionar los derechos de acceso de los usuarios a intervalos regulares utilizando un procedimiento formal.

Recomendación

- Revisar los derechos de acceso de los usuarios a intervalos de 4 a 6 meses y cuando haya cualquier cambio, asenso, cambio de puesto, terminación del contrato.
- Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 3 meses aproximadamente
- Revisar las asignaciones de privilegios a intervalos de en periodos no mayor a 6 meses, a fin de garantizar que no se obtengan privilegios no autorizados.
- Se debieran registrar los cambios en las cuentas privilegiadas para una revisión periódica.

Actividades: Revisar regularmente los derechos de acceso de los usuarios para mantener un control efectivo sobre el acceso a la data y los servicios de información.

DOMINIO	Control de Acceso	**OBJETIVO**	Responsabilidades de usuario
CONTROL	**11.3.1 Uso de contraseñas**		
DESARROLLO			

Propósito: Seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Recomendación

- Mantener las contraseñas en secreto.
- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad que:
    - Sean fáciles de recordar.
    - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.

- No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisorias en el primer inicio de sesión.
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

DOMINIO	Control de Acceso	**OBJETIVO**	Responsabilidades de usuario
CONTROL	**11.3.2 Equipo de usuario desatendido**		
DESARROLLO			

Propósito: Asegurar que los equipos desatendidos sean protegidos apropiadamente.

Recomendación

- Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
- Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

Actividades: Coordinar con el Área de Personal las tareas de concienciación a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos.

DOMINIO	Control de Acceso	**OBJETIVO**	Responsabilidades de usuario
CONTROL	**11.3.3 Política de puesto de trabajo despejado y pantalla limpia**		
DESARROLLO			

Propósito: La política de puesto de trabajo despejado y pantalla limpia reduce los riesgos de accesos no autorizados, perdida o daño de la información durante las horas normales de trabajo
Mantener el lugar de trabajo sin información que pueda causar futuros daños.

Recomendación

- La información confidencial o crítica; por ejemplo, en papel o medios de almacenamiento electrónicos; debiera ser guardada bajo llave (idealmente en una caja fuerte o archivador u otra forma de mueble seguro) cuando no está siendo utilizada, especialmente cuando la oficina está vacía.
- Cuando se dejan desatendidas, las computadoras y terminales debieran dejarse apagadas o protegidas con mecanismos para asegurar la pantalla y el teclado, controlados mediante una clave secreta, dispositivo o un mecanismo de autenticación de usuario similar y se debieran proteger con llave, claves secretas u otros controles cuando no están en uso.
- Se debieran proteger los puntos de ingreso y salida de correo y las máquinas de fax desatendidas.
- Se debiera evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (por ejemplo, escáneres, cámaras digitales)
- Los documentos que contienen información confidencial o clasificada debieran sacarse inmediatamente de la impresora.

Actividades: Mantener el escritorio lo más limpio y organizado posible, si está desordenado es muy probable que no nos demos cuenta que nos hace falta algo.

DOMINIO	Control de Acceso	**OBJETIVO**	Control de acceso a la red
CONTROL	**11.4.1 Política de uso de los servicios en red**		
DESARROLLO			

Propósito: Controlar el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

Recomendación

- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
- Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Actividades: El Responsable del Área Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a los servicios de la red
CONTROL	**11.4.2 Autenticación del usuario para las conexiones externas**		
DESARROLLO			

Propósito: Utilizar métodos de autenticación apropiados para controlar el acceso de usuarios remotos.

Recomendación: La autenticación de usuarios remotos se puede lograr usando, por ejemplo, una técnica con base criptográfica, *toquen*de hardware o protocolos de desafío / respuesta. La autenticación de usuarios remotos puede llevarse a cabo utilizando:

- Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:
  - Asignación de la herramienta de autenticación.
  - Registro de los poseedores de autenticadores.
  - Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
  - Método de revocación de acceso del autenticador, en caso de compromiso de seguridad. Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:
  - Establecimiento de las reglas con el usuario.
  - Establecimiento de un ciclo de vida de las reglas para su renovación.
  - También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Actividades: Implementar medidas de encriptación de datos para las comunicaciones remotas de usuarios

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a los servicios de la red
CONTROL	**11.4.3 Identificación del equipo en las redes**		
DESARROLLO			

Propósito: La identificación automática del equipo se debiera considerar como un medio para autenticar las conexiones de ubicaciones y equipos específicos.

Recomendación: Un identificador en el equipo o acoplado a este se puede usar para indicar si está permitido que este equipo se conecte a la red. Estos identificadores debería indicar con claridad a que red está permitido conectar el equipo, si existe más de una red y si estas redes tienen sensibilidad diferente. Puede ser necesario considerar la protección física del equipo para mantener la seguridad del identificador de este.

Actividades: Utilizar la identificar automáticamente los equipos como un medio para autenticar las conexiones de ubicaciones y equipos específicos.

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a los servicios de la red
CONTROL	**11.4.4 Protección de los puertos de diagnóstico y configuración remotos**		
DESARROLLO			

Propósito: Controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.

Recomendación: Los controles potenciales para el acceso a los puertos de diagnóstico y configuración incluyen el uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico Un ejemplo de un procedimiento de soporte es garantizar que los puertos de diagnóstico y configuración solo sean accesibles mediante acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware / software que requiere el acceso.

Actividades: Desactivar o remover los puertos, servicios y medios similares instalados en una computadora o red, que no son requeridos específicamente por funcionalidad.

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a los servicios de la red
CONTROL	**11.4.5 Segregación en redes**		
DESARROLLO			

Propósito: Segregar los grupos de servicios de información, usuarios y sistemas de información en redes.

Recomendación: Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "Gateway" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos.

Actividades. Crear "dominios de seguridad" en las redes de telecomunicaciones, que separen los tráficos de servicios productivos, usuarios, segmentos de desarrollo y desmilitarizados. Estos segmentos pueden ser lógicos o físicos dependiendo de la tecnología implementada.

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a los servicios de la red
CONTROL	**11.4.6 Control de conexión a la red**		
DESARROLLO			

Propósito: Restringir la capacidad de los usuarios para conectarse a la red, en línea con la política de control de acceso y los requerimientos de las aplicaciones de negocio.

Recomendación: Los derechos de acceso a la red de los usuarios se deberían mantener y actualizar según se requiera a través de la política de control de acceso.
La capacidad de conexión de los usuarios se puede restringir a través de puertas de enlace *(Gateway)* de red que filtren el tráfico por medio de tablas o reglas predefinidas.

Actividades: Restringir la capacidad de conexión de los usuarios a través de Gateway de la red que filtran el tráfico por medio de tablas o reglas predefinidas. Los ejemplos de aplicaciones a las cuales se pueden aplicar las restricciones son:

- Mensajes; por ejemplo, correo electrónico.
- Transferencia de archivos.
- Acceso interactivo.
- Acceso a una aplicación.

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a los servicios de la red
CONTROL	**11.4.7 Control de encaminamiento (routing) de red**		
DESARROLLO			

Propósito: Implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio.

Recomendación: Los controles de enrutamiento se deberían basar en mecanismos de verificación para las direcciones fuente / destino válidos.

Las puertas de enlace (Gateway) de seguridad se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes interna y externa, si se emplean tecnologías *proxy* y / o de traducción de dirección de red. Quienes desarrollan la implementación deberían ser conscientes de las fortalezas y deficiencias de los mecanismos desplegados. Los requisitos para el control del enrutamiento en la red se deberían basar en la política de control de acceso.

Actividades: Implementar controles de routing en las redes para asegurar que las conexiones de la computadora y los flujos de información no violen la política de control de acceso de las aplicaciones institucionales.

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a los sistemas operativos
CONTROL	**11.5.1 Procedimientos seguros de inicio de sesión**		
DESARROLLO			

Propósito: Controlar el acceso a los sistemas operativos mediante un procedimiento de registro seguro.

Recomendación: El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado.

Actividades: Diseñar un registro que cumpla con los siguientes aspectos:

- No debería mostrar identificadores del sistema o aplicación hasta que se haya completado satisfactoriamente el proceso de registro.
- Debería mostrar la advertencia general que a la computadora sólo pueden tener acceso los usuarios autorizados.
- No debería proporcionar mensajes de ayuda durante el procedimiento de registro que ayuden al usuario no-autorizado.
- Sólo debería validar la información del registro después de completar todo el input de data. Si surge una condición de error, el sistema debería indicar qué parte de la data es correcta o incorrecta.
- Debería limitar el número de intentos de registro infructuosos permitidos; por ejemplo, tres intentos.
- Debería limitar el tiempo máximo y mínimo permitido para el procedimiento de registro. Si se excede este tiempo, el sistema debería terminar el registro.
- Debería mostrar información al término de un registro satisfactorio
- No debería mostrar la clave secreta que se está ingresando o considerar esconder los caracteres de la clave secreta mediante símbolos.
- No debería transmitir claves secretas en un texto abierto a través de la red.

DOMINIO	Control de acceso	OBJETIVO	Evitar el acceso no autorizado a los sistemas operativos
CONTROL	**11.5.2 Identificación y autenticación del usuario**		
DESARROLLO			

Propósito: Escoger una técnica de autenticación adecuada para sustanciar la identidad de un usuario.

Recomendación: Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable, a fin de garantizar la trazabilidad de las transacciones. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

Actividades: Permitir el uso de IDs genéricos para una persona cuando las funciones accesibles no necesitan ser rastreadas (por ejemplo, sólo acceso de lectura), o cuando existen otros controles establecidos (por ejemplo, la clave secreta para un ID genérico sólo es emitido para una persona a la vez y se registra dicha instancia).

DOMINIO	Control de acceso	OBJETIVO	Evitar el acceso no autorizado a los sistemas operativos
CONTROL	**11.5.3 Sistema de gestión de contraseñas**		
DESARROLLO			

Propósito: Interactividad y calidad de contraseñas.

Recomendación: Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

Un sistema de gestión de contraseñas debería:

- Aplicar el uso de IDs de usuarios individuales y claves secretas para mantener la responsabilidad.
- Permitir a los usuarios seleccionar y cambiar sus propias claves secretas e incluir un procedimiento de confirmación para permitir errores de input.
- Aplicar la elección de claves secretas adecuadas.
- Aplicar los cambios de claves secretas.

- Obligar a los usuarios a cambiar las claves secretas temporales en su primer ingreso o registro.
- Mantener un registro de claves de usuario previas y evitar el re-uso.
- No mostrar las claves secretas en la pantalla en el momento de ingresarlas.

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a los sistemas operativos
CONTROL	**11.5.4 Uso de los recursos del sistema**		
DESARROLLO			

Propósito: Restringir y controlar estrechamente el uso de los programas de utilidad que podrían ser capaces de superar los controles del sistema y la aplicación.

Recomendación: Se debe tener en consideración:

- Uso de procedimientos de identificación, autenticación y autorización para las utilidades del sistema.
- Separación de las utilidades del sistema del software de aplicaciones.
- Limitación del uso de las utilidades del sistema a la cantidad mínima viable de usuarios de confianza autorizados.
- Autorización del uso ad hoc de las utilidades del sistema.
- Limitación de la disponibilidad de las utilidades del sistema, por ejemplo para la duración de un cambio autorizado.
- Registro de todo uso de las utilidades del sistema.
- Definición y documentación de los niveles de autorización para las utilidades del sistema.
- Retiro o inhabilitación de todas las utilidades o el software del sistema basado en software innecesario.
- No poner a disposición las utilidades del sistema a usuarios que tengan acceso a aplicaciones en sistemas en donde se requiere distribución de funciones.

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a los sistemas operativos
CONTROL	**11.5.5 Desconexión automática de sesión**		
DESARROLLO			

Propósito: Suspender las sesiones inactivas después de un periodo definido de inactividad.

Recomendación: Un dispositivo de cierre debiera borrar la pantalla de la sesión y también, posiblemente más adelante, cerrar la aplicación y las sesiones en red después de un período de inactividad definido. El tiempo de espera antes del cierre debiera reflejar los riesgos de seguridad del área, la clasificación de la información que está siendo manejada y la aplicación siendo utilizada, y los riesgos relacionados con los usuarios del equipo.

Actividades: Para las estaciones de trabajo, implementar la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a los sistemas operativos
CONTROL	**11.5.6 Limitación del tiempo de conexión**		
DESARROLLO			

Propósito: Utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional para las aplicaciones de alto riesgo.

Recomendación: Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se debiera implementar un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo áreas públicas o externas que estén fuera del alcance de la gestión de seguridad de la institución.

Actividades:
Se debiera considerar las siguientes restricciones:

- Uso de espacios de tiempo predeterminados
- Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.
- Documentar debidamente los agentes que no tienen restricciones horarios y las razones de su autorización.

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación
CONTROL	**11.6.1 Restricción del acceso a la información**		
DESARROLLO			

Propósito: Restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.

Recomendación:
Se debiera considerar controles para reforzar los requerimientos de restricción del acceso:

- Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones.
- Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder
- Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
- Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.

DOMINIO	Control de acceso	**OBJETIVO**	Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación
CONTROL	**11.6.2 Aislamiento de sistemas sensibles**		
DESARROLLO			

Propósito: Crear un entorno informático dedicado (aislados) a los sistemas sensibles.

Recomendación:
Se debe considerar:

- Que el propietario de la aplicación debería identificar y documentar explícitamente la sensibilidad o confidencialidad del sistema de aplicación.
- Cuando una aplicación confidencial va a correr en un ambiente compartido, el propietario de la aplicación confidencial debería identificar y aceptar los sistemas de aplicación con los cuales va a compartir recursos y los riesgos correspondientes.

DOMINIO	Control de acceso	**OBJETIVO**	Asegurar la seguridad de la información cuando se utiliza medios de computación ytele-trabajo móviles
CONTROL	**11.7.1 Ordenadores portátiles y comunicaciones móviles**		
DESARROLLO			

Propósito: Establecer una política y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil.

Recomendación: Cuando se utilizan dispositivos informáticos móviles (computadores portátiles livianos *(Notebooks)*, microcomputadores de bolsillo *(Palmtops)*, y computadores portátiles pesados *(Laptops)*, tarjetas inteligentes y teléfonos móviles) se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura de la institución.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto.

Se deberían desarrollar normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.

- No llamar la atención acerca de portar un equipo valioso.
- No poner identificaciones de la institución en el dispositivo, salvo los estrictamente necesarios.
- No poner datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada.

Actividades

- Se debiera establecer procedimientos para estos dispositivos, que abarquen los siguientes aspectos:
  - La protección física necesaria
  - El acceso seguro a los dispositivos
  - La utilización segura de los dispositivos en lugares públicos.
  - El acceso a los sistemas de información y servicios de la institución a través de dichos dispositivos.
  - Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
  - Los mecanismos de resguardo de la información contenida en los dispositivos.
  - La protección contra software malicioso.
- Entrenar al personal que los utiliza o utilizará.

DOMINIO	Adquisición,desarrolloymantenimientode sistemas deinformación	**OBJETIVO**	Garantizar que la seguridad sea una parte integral de los sistemas de información
CONTROL	**12.1.1 Análisis y especificación de los requerimientos de seguridad**		
DESARROLLO			

Propósito: Especificar los requisitos para los controles de seguridad en las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes.

Recomendación: Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Si se adquieren productos, se debería seguir un proceso formal de adquisición y prueba. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados. Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto. Cuando se proporciona funcionalidad adicional y ello causa un riesgo de seguridad, tal funcionalidad se debería inhabilitar o se debería revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

Actividades:

- Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados.
- Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.
- Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

DOMINIO	Adquisición,desarrollo ymantenimientode sistemas deinformación	**OBJETIVO**	Prevenir errores, pérdida, modificación no autorizada o mal uso de la informaciónen las aplicaciones
CONTROL	**12.2.2 Control del procesamiento interno**		
DESARROLLO			

Propósito: Incorporar en las aplicaciones los chequeos de validación para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.

Recomendación: El diseño e implementación de las aplicaciones debe asegurar que se minimicen los riesgos de fallas en el procesamiento que lleven a la pérdida de la integridad. Las áreas específicas a considerarse incluyen:

- El uso de funciones agregadas, modificadas y eliminadas para implementar cambios en la data.
- Los procedimientos para evitar que los programas corran en el orden equivocado o corran después de una falla en el procesamiento previo.
- El uso de programas apropiados para recuperarse de fallas para asegurar el correcto procesamiento de la data.
- Protección contra ataques utilizando excesos/desbordamientos de la memoria intermedia.

Actividades: Definir un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

- Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
- Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
- Procedimientos que establezcan la revisión periódica de los registros de auditoría o alertas de forma de detectar cualquier anomalía en la ejecución de las transacciones.
- Procedimientos que realicen la validación de los datos generados por el sistema.
- Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.
- Procedimientos que controlen la integridad de registros y archivos.
- Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.
- Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

DOMINIO	Adquisición,desarrollo ymantenimientode sistemas deinformación	**OBJETIVO**	Prevenir errores, pérdida, modificación no autorizada o mal uso de la

			informaciónen las aplicaciones
CONTROL	**12.2.3 Integridad de los mensajes**		
DESARROLLO			

Propósito: Identificar los requerimientos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, y se debieran identificar e implementar los controles apropiados.

Recomendación: Utilizar técnicas criptográficas como un medio apropiado para implementar la autenticación del mensaje.

Actividades:

- Diseñar e implementar controles criptográficos.
- Realizar una evaluación de los riesgos de seguridad para determinar si se requiera la integridad del mensaje y para identificar el método de implementación más apropiado.

DOMINIO	Adquisición,desarrollo ymantenimientode sistemas deinformación	**OBJETIVO**	Prevenir errores, pérdida, modificación no autorizada o mal uso de la informaciónen las aplicaciones
CONTROL	**12.2.4 Validación de los datos de salida**		
DESARROLLO			

Propósito: Validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada sea el correcto y el apropiado para las circunstancias.

Recomendación:

Se debe implementar:

- Chequeos de plausibilidad para comprobar si el output data es razonable.
- Conteo de control de conciliación para asegurar el procesamiento de toda la data.
- Proporcionar la información suficiente para un lector o el sistema de procesamiento subsiguiente para determinar la exactitud, integridad, precisión y clasificación de la información.
- Procedimientos para responder a las pruebas de validación de output; definir las responsabilidades de todo el personal involucrado en el proceso de outputde data.
- Crear un registro de las actividades en el proceso de validación del output de data.

DOMINIO	Adquisición,desarrollo ymantenimientode sistemas deinformación	**OBJETIVO**	Proteger la confidencialidad, autenticidad o integridad

			a través de medios criptográficos
CONTROL	**12.3.1 Política de uso de los controles criptográficas**		
DESARROLLO			

Propósito: Desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.

Recomendación:
Cuando se desarrolla una política criptográfica se debe considerar lo siguiente:

- El enfoque gerencial sobre el uso de los controles criptográficos a través de la organización, incluyendo los principios generales bajo los cuales se debe proteger la información comercial.
- En base a la evaluación del riesgo, se debe identificar el nivel de protección requerido tomando en cuenta el tipo, fuerza y calidad del algoritmo criptográfico requerido.
- El uso de codificación para la protección de la información confidencial transportada por los medios y dispositivos móviles o removibles o a través de las líneas de comunicación.
- El enfoque de la gestión de claves, incluyendo los métodos para lidiar con la protección de las claves criptográficas y la recuperación de la información codificada en el caso de claves pérdidas, comprometidas o dañadas.
- Roles y responsabilidades; por ejemplo, quién es responsable de:
    - la implementación de la política;
    - la gestión de claves, incluyendo la generación de claves;
- El impacto de utilizar información codificada sobre los controles que se basan en la inspección del contenido (por ejemplo, detección de virus).

Se pueden utilizar controles criptográficos para lograr diferentes objetivos de seguridad:

- confidencialidad: utilizando la codificación de la información para proteger la información confidencial o crítica, ya sea almacenada o transmitida;
- integridad/autenticidad: utilizando firmas digitales o códigos de autenticación del mensaje para proteger la autenticidad e integridad de la información confidencial o crítica almacenada o transmitida;
- no-repudiación: utilizando técnicas criptográficas para obtener prueba de ocurrencia o no-ocurrencia de un evento o acción.

Actividades:
Utilizar controles criptográficos en los siguientes casos:
1. Para la protección de claves de acceso a sistemas, datos y servicios.
2. Para la transmisión de información clasificada, fuera del ámbito del Organismo.
3. Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad de la Información.

Desarrollar procedimientos para la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

El Responsable del Área Informática propondrá la siguiente asignación de funciones:

FUNCIÓN	CARGO
Implementación de la Política de Controles Criptográficos	
Administración de Claves	

Utilizar los siguientes algoritmos de cifrado y tamaños de clave:

1. Cifrado Simétrico

Algoritmo	Longitud de Clave
AES	128/192/256
3DES	168 bits
IDEA	128 bits
RC4	128 bits
RC2	128 bits

2. Cifrado Asimétrico

Casos de Utilización	Algoritmo	Longitud de Clave
Para certificados utilizados en servicios relacionados a la firma digital (sellado de tiempo, almacenamiento seguro de documentos electrónicos, etc.)	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de sitio seguro	RSA	1024 bits
Para certificados de Certificador o de información de estado de certificados	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de usuario (personas físicas o jurídicas)	RSA	1024 bits
	DSA	1024 bits
Para digesto seguro	ECDSA SHA-1	160 bits 256 bits

Los algoritmos y longitudes de clave mencionados son los que a la fecha se consideran seguros. Se recomienda verificar esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes.

DOMINIO	Adquisición,desarrollo ymantenimientode sistemas deinformación	**OBJETIVO**	Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos
CONTROL	**12.3.2 Gestión de claves**		
DESARROLLO			

Propósito: Establecer la gestión de claves para dar soporte al uso de técnicas criptográficas en la organización.

Recomendación: Todas las claves criptográficas deben estar protegidas contra una modificación, pérdida y destrucción. Además, las claves secretas y privadas necesitan protección contra la divulgación no-autorizada.

Se debe proteger físicamente el equipo utilizado para generar, almacenar y archivar las claves.

El sistema de gestión de claves se debe basar en un conjunto de estándares, procedimientos y métodos seguros acordados para:

- Generar claves para los diferentes sistemas criptográficos y las diversas aplicaciones.
- Generar y obtener certificados de claves públicas.
- Distribuir claves a los usuarios planeados, incluyendo cómo se debieran activar las claves una vez recibidas.
- Almacenar claves, incluyendo cómo los usuarios autorizados obtienen acceso a las claves; cambiar o actualizar las claves incluyendo las reglas sobre cuándo se debe cambiar las claves y cómo se realiza esto.
- Lidiar con las claves comprometidas.
- Revocar las claves incluyendo cómo se debe retirar o desactivar las claves; por ejemplo, cuando las claves se han visto comprometidas o cuando el usuario deja la organización (en cuyos casos las claves también deben ser archivadas).
- Recuperar las claves cuando han sido pérdidas o corrompidas como parte de la continuidad y gestión del negocio; por ejemplo, para recuperar la información codificada.
- Archivar las claves; por ejemplo, para la información archivada o respaldada.
- Destruir las claves.
- Registrar y auditar las actividades relacionadas con la gestión de claves.

Para poder reducir la posibilidad de comprometer las claves, se debe definir las fechas de activación y desactivación para que las claves sólo se puedan utilizar durante un período de tiempo limitado. El período de tiempo dependerá de las circunstancias bajo las cuales se está utilizando el control criptográfico, y el riesgo percibido.

Además del manejo seguro de las claves secretas y privadas, también se debe considerar la autenticidad de las claves públicas. Este proceso de autenticación se puede realizar utilizando certificados de claves públicas, los cuales normalmente son emitidos por una autoridad de

certificación, la cual debe ser una organización reconocida con controles y procedimientos adecuados para proporcionar el grado de confianza requerido.

Los contenidos de los acuerdos o contratos de nivel de servicio con los proveedores externos de servicios de criptografía; por ejemplo, una autoridad de certificación; deben abarcar los temas de responsabilidad, confiabilidad de los servicios y tiempos de respuesta para la provisión de los servicios.

DOMINIO	Adquisición,desarrollo ymantenimientode sistemas deinformación	**OBJETIVO**	Garantizar la seguridad de los archivos del sistema
CONTROL	**12.4.1Control del software en explotación**		
DESARROLLO			

Propósito: Establecer procedimientos para el control de la instalación del software en los sistemas operacionales.

Recomendación:

Para minimizar el riesgo de corrupción de los sistemas operacionales, se deben considerar los siguientes lineamientos para controlar los cambios:

- La actualización del software operacional, aplicaciones y bibliotecas de programas sólo debe ser realizada por administradores capacitados con la apropiada autorización gerencial.
- Los sistemas operacionales sólo deben mantener códigos ejecutables aprobados, y no códigos de desarrollo o compiladores; el software de las aplicaciones y el sistema de operación sólo se implementa después de una prueba extensa y satisfactoria; las pruebas deben incluir pruebas de utilidad, seguridad, efectos sobre los sistemas y facilidad para el usuario; y se debe llevar a cabo en sistemas separados; se debe asegurar que se hayan actualizado todas las bibliotecas fuente correspondientes del programa.
- Utilizar un sistema de control de configuración para mantener el control de todo el software implementado, así como la documentación del sistema.
- Establecer una estrategia de "regreso a la situación original" (rollback) antes de implementar los cambios.
- Mantener un registro de auditoría de todas las actualizaciones a las bibliotecas del programa operacional.
- Mantener las versiones previas del software de aplicación como una medida de contingencia.
- Archivar las versiones antiguas del software, junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte durante todo el tiempo que se mantengan la data en archivo.

El software provisto por un vendedor y utilizado en el sistema operacional se debe mantener en el nivel donde recibe soporte del proveedor. A lo largo del tiempo, los proveedores dejarán de dar soporte a las versiones más antiguas del software.

La organización debe considerar los riesgos de trabajar con software que no cuenta con soporte.

Cualquier decisión para actualizar a una versión nueva debe tomar en cuenta los requerimientos comerciales para el cambio, y la seguridad de la versión; es decir, la introducción de la nueva funcionalidad de seguridad o el número y severidad de los problemas de seguridad que afectan esta versión.

Se pueden aplicar algunos parches de software cuando ayudan a remover o reducir las debilidades de seguridad.

Sólo se debe dar a los proveedores acceso físico o lógico para propósitos de soporte cuando sea necesario, y con aprobación de la gerencia.

Monitorear las actividades del proveedor.

El software de cómputo puede constar del software y módulos suministrados externamente, el cual se debe monitorear y controlar para evitar los cambios no-autorizados, los cuales introducen debilidades en la seguridad.

DOMINIO	Adquisición,desarrollo ymantenimientode sistemas deinformación	**OBJETIVO**	Garantizar la seguridad de los archivos del sistema
CONTROL	**12.4.2 Protección de los datos de prueba del sistema**		
DESARROLLO			

Propósito: Seleccionar, proteger y controlar cuidadosamente la data de prueba.

Recomendación: Evitar el uso de bases de datos operacionales conteniendo información personal o cualquier otra información confidencial para propósitos de pruebas.

Si la información personal o de otra manera confidencial se utiliza para propósitos de prueba, todos los detalles confidenciales deben ser removidos o modificados más allá de todo reconocimiento antes de utilizarlos.

Actividades

- Diseñar procedimientos de control de acceso, los cuales se aplican a los sistemas de aplicación operacional, y a los sistemas de aplicación de prueba.
- Establecer una autorización separada para cada vez que se copia información operacional en un sistema de aplicación de prueba, y llevar registro de tal autorización.
- Borrar la información operacional de los sistemas de aplicación de prueba inmediatamente después de haber completado la prueba.
- Registrar el copiado y uso de la información operacional para proporcionar un rastro de auditoría.
- Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.

DOMINIO	Adquisición,desarrollo ymantenimientode sistemas deinformación	**OBJETIVO**	Garantizar la seguridad de los archivos del sistema
CONTROL	**12.4.3 Control de acceso al código fuente de los programas**		
DESARROLLO			

Propósito: Restringir el acceso al código fuente del programa.

Recomendación:
El acceso al código fuente del programa y los ítems asociados (como diseños, especificaciones, planes de verificación y planes de validación) se deben controlar estrictamente para evitar la introducción de una funcionalidad no-autorizada y para evitar cambios no-intencionados.

Para el código fuente del programa, esto se puede lograr controlando el almacenaje central de dicho código, preferiblemente en las bibliotecas de fuentes del programa.

La actualización de las bibliotecas de fuentes del programa y los ítems asociados, y la emisión de las fuentes del programa para los programadores sólo se debe realizar después de haber recibido la apropiada autorización;

Actividades:

Controlar el acceso a dichas bibliotecas de las fuentes del programa para reducir elpotencial de corrupción de los programas de cómputo:

- Mantener las bibliotecas de fuentes del programa en los sistemas operacionales.
- Establecer procedimientos para el manejo del código fuente del programa y las bibliotecas de fuentes del programa.
- Establecer control de acceso a las bibliotecas de fuentes del programa para el personal de soporte.
- Mantener en un ambiente seguro los listados del programa.
- Mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa.
- Establecer procedimientos estrictos de control de cambios para el mantenimiento y copiado de las bibliotecas fuentes del programa.
- Generar una solicitud formal para la realización de la modificación, actualización o eliminación del dato.
- El Propietario de la Información afectada y del Responsable de Seguridad de la Información aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.
- generar cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento

de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.

- Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo.
- Registrar todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Responsable de Seguridad de la Información.

DOMINIO	Adquisición,desarrolloymantenimientode sistemas deinformación	**OBJETIVO**	Mantener la seguridad del software y la información del sistema de aplicación
CONTROL	**12.5.1Procedimientos del control del cambio**		
DESARROLLO			

Propósito: Controlar la implementación de los cambios mediante el uso de procedimientos formales para el control del cambio.

Recomendación: Se debieran documentar y hacer cumplir los procedimientos formales de control del cambio para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y los cambios importantes a los sistemas existentes debieran realizarse después de un proceso formal de documentación, especificación, prueba, control de calidad e implementación manejada.

Este proceso debiera incluir una evaluación del riesgo, análisis de los impactos del cambio y la especificación de los controles de seguridad necesarios. Este proceso también debiera asegurar que los procedimientos de seguridad y control existentes no se vean comprometidos, que a los programadores de soporte sólo se les proporcione acceso a aquellas partes del sistema necesarias para su trabajo, y que se obtenga el acuerdo y la aprobación formal de cualquier cambio.

La buena práctica incluye la prueba del software nuevo en un ambiente segregado de los ambientes de producción y desarrollo. Esto proporciona un medio para tener control sobre el software nuevo y permitir una protección adicional de la información operacional que se utiliza para propósitos de pruebas. Esto incluye parches, paquetes de servicio y otras actualizaciones. Las actualizaciones automatizadas no se debieran utilizar en los sistemas críticos ya que algunas actualizaciones pueden causar que fallen las aplicaciones críticas.

Actividades:

- Mantener un registro de los niveles de autorización acordados.
- Asegurar que los cambios sean presentados por los usuarios autorizados.
- Revisar los procedimientos de control e integridad para asegurar que no se vean comprometidos por los cambios.

- Identificar todo el software, información, entidades de base de datos y hardware que requieran enmiendas.
- Obtener la aprobación formal para propuestas detalladas antes de comenzar el trabajo.
- Asegurar que los usuarios autorizados acepten a los cambios antes de la implementación.
- Asegurar que el conjunto de documentación del sistema esté actualizado al completar cada cambio y que la documentación antigua se archive o se elimine.
- Mantener un control de la versión para todas las actualizaciones del software.
- Mantener un rastro de auditoría para todas las solicitudes de cambio.
- Asegurar que la documentación de operación (ver 10.1.1) y procedimientos de usuarios sean cambiados conforme sean necesarios para seguir siendo apropiados.
- Asegurar que la implementación de los cambios se realice en el momento adecuado y no disturbe los procesos comerciales involucrados.

DOMINIO	Adquisición, desarrollo y mantenimiento de los sistemas de información	**OBJETIVO**	Mantener la seguridad del software y la información del sistema de aplicación
CONTROL	**12.5.2Revisión técnica de las aplicaciones tras efectuar cambios en elsistema operativo**		

DESARROLLO

Propósito: Revisar y probar las aplicaciones institucionales críticas para asegurar que no exista un impacto adverso sobre las operaciones organizacionales o en la seguridad cuando se cambian los sistemas de operación.

Recomendación: Se le debiera asignar a un grupo o persona específica la responsabilidad de monitorear las vulnerabilidades y los parches y arreglos que lancen los vendedores.

- Revisar los procedimientos de control e integridad de la aplicación para asegurar que no se hayan visto comprometidos por los cambios en el sistema de operación.
- Asegurar que el plan y el presupuesto de soporte anual abarque las revisiones y pruebas del sistema resultantes de los cambios en el sistema de operación.
- Asegurar que la notificación de los cambios en el sistema de operación sea provista con tiempo para permitir realizar las pruebas y revisiones apropiadas antes de la implementación.
- Asegurar que se realicen los cambios apropiados en los planes de continuidad del negocio.

Actividades: Definir un procedimiento que incluya:

- Procedimientos de control e integridad de la aplicación.
- Asegurar que el plan y el presupuesto de soporte anual abarque las revisiones y pruebas del sistema resultantes de los cambios en el sistema de operación.
- Proveer y notificar con tiempo los cambios en el sistema de operación.
- Realizar los cambios apropiados en los planes de continuidad del negocio.

DOMINIO	Adquisición, desarrollo y mantenimiento de los sistemas de información	**OBJETIVO**	Mantener la seguridad del software y la información del sistema de aplicación
CONTROL	**12.5.3 Restricciones a los cambios en los paquetes de software**		
DESARROLLO			

Propósito: No fomentar modificaciones a los paquetes de software, se debieran limitar a los cambios necesarios y todos los cambios debieran ser estrictamente controlados.

Recomendación: Mientras sea posible y practicable, se debieran utilizar los paquetes de software suministrados por vendedores sin modificaciones. Cuando se necesita modificar un paquete de software se debieran considerar los siguientes puntos:

- El riesgo de comprometer los controles incorporados y los procesos de integridad.
- Si se debiera obtener el consentimiento del vendedor.
- La posibilidad de obtener del vendedor los cambios requeridos como actualizaciones del programa estándar.
- El impacto de si como resultado de los cambios, la organización se hace responsable del mantenimiento futuro del software.

Si son necesarios cambios, se debiera mantener el software original y se debieran aplicar los cambios en una copia claramente identificada. Se debiera implementar un proceso de gestión de actualizaciones del software para asegurar que la mayoría de los parches aprobados hasta la fecha y las actualizaciones de la aplicación se instalen para todo software autorizado. Todos los cambios debieran ser completamente probados y documentados, de manera que puedan ser replicados, si fuese necesario, a las futuras actualizaciones del software. Si fuese requerido, las modificaciones debieran probadas y validadas por un organismo de evaluación independiente.

DOMINIO	Adquisición, desarrollo y mantenimiento de los sistemas de información	OBJETIVO	Mantener la seguridad del software y la información del sistema de aplicación
CONTROL	**12.5.4 Fugas de información**		
DESARROLLO			

Propósito: Evitar las oportunidades para la fuga de información.

Recomendación: La filtración de la información se puede presentar a través del uso y explotación de los canales encubiertos (covertchannels).

Los Canales Encubiertos son caminos que no están destinadas a transportar flujos de información, pero que de cualquier manera pueden existir en un sistema o red. Por ejemplo, en el manipuleo de bits se pueden utilizar paquetes de protocolo de las comunicaciones como un método escondido de señalización. Por su naturaleza, es muy difícil, sino imposible, evitar la existencia de todos los canales encubiertos posibles. Sin embargo, la explotación de dichos canales casi siempre las realiza un código Troyano. Por lo tanto, tomar medidas para protegerse contra códigos Troyanos reduce el riesgo de la explotación de los canales encubiertos.

El evitar el acceso no-autorizado a la red, así como las políticas y procedimientos para no fomentar el mal uso de los servicios de información por parte del personal, ayudarán a protegerse de los canales encubiertos.

Actividades:

- Escanear el flujo de salida de los medios y las comunicaciones en busca de información escondida.
- Enmascarar y modular la conducta del sistema y las comunicaciones para reducir la probabilidad de que una tercera persona pueda deducir la información a partir de dicha conducta.
- Hacer uso de los sistemas y el software considerados de la más alta integridad; por ejemplo, utilizando productos evaluados (ver ISO/IEC 15408).
- Monitoreo regular de las actividades del personal y del sistema, cuando sea permitido bajo la legislación o regulación existente.
- Monitorear la utilización del recurso en los sistemas de cómputo.

DOMINIO	Adquisición, desarrollo y mantenimiento de los sistemas de información	OBJETIVO	Mantener la seguridad del software y la información del sistema de aplicación
CONTROL	**12.5.5 Externalización del desarrollo de software**		
DESARROLLO			

Propósito: Supervisar y monitorear el software de la organización abastecido externamente.

Recomendación: Cuando el software es abastecido externamente, se debieran considerar los siguientes puntos:

- Contratos de licencias, propiedad de códigos, derechos de propiedad intelectual (ver 15.1.2).
- Certificación de la calidad y exactitud del trabajo llevado a cabo.
- Contratos de depósito en custodia en el evento de la falla de una tercera persona.
- Derechos de acceso para la auditoría de la calidad y seguridad del trabajo realizado.
- Requerimientos contractuales para la funcionalidad de calidad y seguridad del código.
- Prueba antes de la instalación para detectar códigos maliciosos y Troyanos.

Actividades: Establecer normas y procedimientos que contemplen los siguientes puntos:

- Acuerdos de licencias, propiedad de código y derechos conferidos (Ver 15.1.2 Derechos de Propiedad Intelectual DPI).
- Requerimientos contractuales con respecto a la calidad y seguridad del código y la existencia de garantías.
- Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
- Verificación del cumplimiento de las condiciones de seguridad.
- Acuerdos de custodia de los fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

DOMINIO	Adquisición, desarrollo y mantenimiento de los sistemas de información	**OBJETIVO**	Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas
CONTROL	**12.6.1 Control de las vulnerabilidades técnicas**		
DESARROLLO			

Propósito: Obtener oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando, la exposición de la organización a dichas vulnerabilidades evaluadas, y las medidas apropiadas tomadas para tratar los riesgos asociados.

Recomendación: Un inventario actual y completo de los activos (ver 7.1) es un prerrequisito para la gestión efectiva de la vulnerabilidad técnica. La información específica necesaria para apoyar la gestión de la vulnerabilidad técnica incluye al vendedor del software, números de la versión, estado actual del empleo (por ejemplo, cuál software está instalado en cuál sistema), y la(s) persona(s) dentro de la organización responsable(s) del software.

Se debiera tomar la acción apropiada y oportuna en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se debiera seguir el siguiente lineamiento para establecer un proceso de gestión efectivo para las vulnerabilidades técnicas:

- La organización debiera definir y establecer los roles y responsabilidades asociadas con la gestión de la vulnerabilidad técnica; incluyendo el monitoreo de la vulnerabilidad, evaluación del riesgo de la vulnerabilidad, monitoreo de activos y cualquier responsabilidad de coordinación requerida.
- Se debieran identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas relevantes y mantener la conciencia sobre ellas para el software y otras tecnologías (en base a la lista de inventario de activos, ver 7.1.1), estos recursos de información debieran actualizarse en base a los cambios en el inventario, o cuando se encuentran recursos nuevo o útiles.
- Se debiera definir una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes.
- Una vez que se identifica la vulnerabilidad técnica potencial, la organización debiera identificar los riesgos asociados y las acciones a tomarse; dicha acción podría involucrar el parchado de los sistemas vulnerables y/o la aplicación de otros controles.
- Dependiendo de la urgencia con que se necesita tratar la vulnerabilidad técnica, la acción a tomarse debiera realizarse de acuerdo a los controles relacionados con la gestión de cambios (ver 12.5.1) o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información (ver 13.2).
- Si es posible el parche, se debieran evaluar los riesgos asociados con instalar el parche (los riesgos impuestos por la vulnerabilidad se debieran comparar con el riesgo de instalar el parche).

- Los parches de debieran probar y evaluar antes de instalarlos para asegurar que sean efectivos y no resulten efectos secundarios que no se puedan tolerar; si el parche no está disponible, se pueden considerar otros controles:
- 1) desconectar los servicios o capacidades relacionadas con la vulnerabilidad.
- 2) adaptar o agregar controles de acceso; por ejemplo, firewalls en los límites de la red.
- 3) mayor monitoreo para detectar o evitar ataques reales.
- 4) elevar la conciencia acerca de la vulnerabilidad.
- 5) mantener un registro de auditoría de todos los procedimientos realizados.
- 6) el proceso de gestión de vulnerabilidad técnica debiera ser monitoreado y evaluado regularmente para asegurar su efectividad y eficacia.
- 7) se debieran tratar primero los sistemas en alto riesgo.

El correcto funcionamiento del proceso de gestión de la vulnerabilidad técnica de la organización es crítico para muchas organizaciones y por lo tanto, debiera ser monitoreado regularmente. Un inventario exacto es esencial para asegurar que se identifiquen las vulnerabilidades técnicas potencialmente relevantes.

La gestión de la vulnerabilidad técnica puede ser vista como una sub-función de la gestión de cambios y como tal pueden beneficiarse de los procesos y procedimientos de la gestión del cambio.

Con frecuencia los vendedores se ven presionados a lanzar parches lo más pronto posible. Por lo tanto, un parche puede no tratar adecuadamente el problema y puede tener efectos secundarios negativos. También, en algunos casos, no es fácil desinstalar un parche una vez que este ha sido aplicado.

Si no es posible una prueba adecuada del parche; por ejemplo, debido a los costos o falta de recursos; se puede considerar una demora en el parchado para evaluar los riesgos asociados, basados en la experiencia reportada por otros usuarios.

Actividades:

- Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia.

DOMINIO	Gestión de incidentes en la seguridad de la información	**OBJETIVO**	Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna
CONTROL	**13.1.1 Notificación de los eventos de seguridad de la información**		
DESARROLLO			

Propósito: Reportar los eventos de seguridad de la información a través de los canales gerenciales apropiados lo más rápidamente posible.

Recomendación: Se debiera establecer un procedimiento formal para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de intensificación de incidentes, estableciendo la acción a tomarse al recibir un reporte de un evento en la seguridad de la información. Se debiera establecer un punto de contacto para el reporte de eventos en la seguridad de la información Se debiera asegurar que este punto de contacto sea conocido a través de toda la organización, que siempre esté disponible y sea capaz de proporcionar una respuesta adecuada y oportuna.

Todos los usuarios empleados, contratistas y terceros debieran estar al tanto de la responsabilidad de reportar cualquier evento en la seguridad de la información lo más rápidamente posible. También debieran estar al tanto del procedimiento para reportar eventos en la seguridad de la información y el punto de contacto. Los procedimientos de reporte debieran incluir:

- Procesos de retroalimentación adecuados para asegurar que aquellos que reportan eventos en la seguridad de la información sean notificados de los resultados después de haber tratado y terminado con el problema.
- Formatos donde se reporte los eventos en la seguridad de la información para respaldar la acción de reporte, y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento en la seguridad de la información.
- Se debiera tomar la conducta correcta en el caso de un evento en la seguridad de la información; es decir:
    1. Anotar todos los detalles importantes inmediatamente (por ejemplo, el tipo de no-cumplimiento o violación, mal funcionamiento actual, mensajes en la pantalla, conducta extraña).
    2. No llevar a cabo ninguna acción por cuenta propia, sino reportar inmediatamente al punto de contacto.
- Referencia a un proceso disciplinario formal establecido para tratar con los usuarios empleados, contratistas o terceros que cometen violaciones de seguridad.

En los ambientes de alto riesgo, se puede proporcionar una alarma de coacción mediante la cual una persona que actúa bajo coacción puede indicar dichos problemas. Los procedimientos para responder ante las alarmas de coacción debieran reflejar la situación de alto riesgo que estas alarmas indican.

Actividades:

- Establecer un procedimiento formal para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de notificación de incidentes, estableciendo la acción a tomarse al recibir un reposte de un evento en la seguridad de la información.

- Establecer un punto de contacto para el reporte de eventos en la seguridad de la información, dicho punto de contacto debe ser conocido por toda la Universidad; además, siempre deberá estar disponible.

DOMINIO	Gestión de incidentes en la seguridad de la información	**OBJETIVO**	Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.
CONTROL	**13.1.2Notificación de puntos débiles de seguridad**		
DESARROLLO			

Propósito: Requerir que todos los usuarios empleados, contratistas y terceros de los sistemas y servicios de información tomen nota de y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios.

Recomendación: Todos los usuarios empleados, contratistas y terceros debieran reportar estos temas al Responsable de Seguridad de la Información lo más rápidamente posible para evitar incidentes en la seguridad de la información. El mecanismo de reporte debiera ser fácil, accesible y estar disponible lo más posible.

Los usuarios empleados, contratistas y terceros debieran ser advertidos de no tratar de probar las debilidades de seguridad sospechadas. La prueba de las debilidades podría ser interpretada como un mal uso potencial del sistema y también podría causar daños al sistema o servicio de información y resultar en la responsabilidad legal para la persona que realiza la prueba.

Actividades:

- Dar a conocer a los empleados, contratistas y terceros el proceso de notificación de puntos débiles de seguridad.

DOMINIO	Gestión de incidentes en la seguridad de la información	OBJETIVO	Gestión de incidentes y mejoras en la seguridad de la información
CONTROL	13.2.1 Responsabilidades y procedimientos		
DESARROLLO			

Propósito: Establecer funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

Recomendación

- Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo como mínimo:

- Fallas operativas
- Código malicioso
- Intrusiones
- Fraude informático
- Error humano
- Catástrofes naturales

- Comunicar formalmente los incidentes a través de autoridades o canales apropiados tan pronto como sea posible.

- Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):

- Definición de las primeras medidas a implementar
- Análisis e identificación de la causa del incidente.
- Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
- Comunicación formal con las personas afectadas o involucradas con la recuperación, del incidente.
- Notificación de la acción a la autoridad y/u Organismos pertinentes.

- Registrar pistas de auditoría y evidencia similar para:

- Análisis de problemas internos.
- Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.
- Negociación de compensaciones por parte de los proveedores de software y de servicios.

- Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:

- Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
- Documentación de todas las acciones de emergencia emprendidas en forma detallada.
- Comunicación de las acciones de emergencia
- Constatación

Actividades: Establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados.

DOMINIO	Gestión de incidentes en la seguridad de la información	**OBJETIVO**	Gestión de incidentes y mejoras en la seguridad de la información
CONTROL	**13.2.2 Aprendizaje de los incidentes de seguridad de la información.**		
DESARROLLO			

Propósito: Definir un procedimiento que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías.

Recomendación: Se debiera utilizar la información obtenida de la evaluación de los incidentes en la seguridad de la información para identificar los incidentes recurrentes o de alto impacto.

Actividades: Evaluar la información obtenida a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

DOMINIO	Gestión de incidentes en la seguridad de la información	**OBJETIVO**	Gestión de incidentes y mejoras en la seguridad de la información
CONTROL	**13.2.3 Recopilación de evidencias**		
DESARROLLO			

Propósito: Recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en la(s) jurisdicción(es) relevante(s).

Recomendación: Se debieran desarrollar y seguir los procedimientos internos cuando se recolecta y presenta evidencia para propósitos de una acción disciplinaria manejada dentro de una organización.
En general, las reglas de evidencia debieran abarcar:

- admisibilidad de la evidencia: si la evidencia se puede o no se puede utilizar en la corte;

- peso de la evidencia: la calidad e integridad de la evidencia.

Actividades

- Para los documentos en papel: el original se debiera mantener de manera segura con un registro de la persona quien encontró el documento, el lugar donde se encontró el documento, cuándo se encontró el documento y quién presenció el descubrimiento; cualquier investigación debiera asegurar que no se alteren o manipulen los originales.
- Para la información en medios de cómputo: se debieran realizar imágenes dobles o copias de cualquier medio e información en discos duros o en memoria para asegurar su disponibilidad; se debiera mantener un registro de todas las acciones realizadas durante el proceso de copiado y el proceso debiera ser atestiguado; el medio original y el registro.

DOMINIO	Gestión de la continuidad del negocio	**OBJETIVO**	Aspectos de seguridad de la información en la gestión de lacontinuidad del negocio.
CONTROL	**14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.**		
DESARROLLO			

Propósito: Contraatacar las interrupciones a las actividades del organismo y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

Recomendación

- Identificar y priorizar los procesos críticos de las actividades de la división de sistemas.
- Asegurar que todos los integrantes de la división de sistemas comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
- Elaborar y documentar una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo.
- Proponer las modificaciones a los planes de contingencia.

Actividades: Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la división de sistemas frente a interrupciones imprevistas.

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la dependencia división de sistemas
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar

DOMINIO	Gestión de la continuidad del negocio	**OBJETIVO**	Aspectos de seguridad de la información en la gestión de lacontinuidad del negocio.
CONTROL	**14.1.2 Continuidad del negocio y evaluación de riesgos**		
DESARROLLO			

Propósito: Se debieran identificar los eventos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.

Recomendación

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor

Actividades: Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la máxima autoridad del Organismo para su aprobación.

DOMINIO	Gestión de la continuidad del negocio	**OBJETIVO**	Aspectos de seguridad de la información en la gestión de lacontinuidad del negocio.
CONTROL	**14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.**		
DESARROLLO			

Propósito: Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la división de sistemas. Estos procesos deben ser propuestos por el Comité de Seguridad de la Información

Recomendación

- Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
- Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
- Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
- Documentar los procedimientos y procesos acordados.
- Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
- Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:

- Objetivo del plan.
- Mecanismos de coordinación y comunicación entre equipos de personal involucrado.
- Procedimientos de divulgación.
- Requisitos de la seguridad.
- Procesos específicos para el personal involucrado.
- Responsabilidades individuales.

- Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

Actividades: Restaurar los servicios de comunicación específicos a los clientes en una cantidad de tiempo aceptable.
La gerencia debiera asegurarse que las copias de los planes de continuidad del negocio estén actualizadas y protegidas con el mismo nivel de seguridad aplicado en el local principal.

DOMINIO	Gestión de la continuidad del negocio	**OBJETIVO**	Aspectos de seguridad de la información en la gestión de lacontinuidad del negocio.
CONTROL	**14.1.4 Marco de referencia para la planificación de la continuidad del negocio.**		

DESARROLLO

Propósito: Se mantendrá un solo marco para los planes de continuidad de las actividades de la división de sistemas, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Recomendación

- Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.
- Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Organismo y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.
- Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de la dependencia o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.
- Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la dependencia división de sistemas.
- Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.
- Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.
- Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda.

Los administradores de los planes de contingencia son:

Plan de contingencia	Administrador

Actividades: Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

0DOMINIO	Gestión de la continuidad del negocio	**OBJETIVO**	Aspectos de seguridad de la información en la gestión de lacontinuidad del negocio.
CONTROL	**14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.**		

DESARROLLO

Propósito: Revisar y actualizar periódicamente los planes de continuidad de las actividades de la división de sistemas para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios del Organismo para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

Recomendación

- Se deben utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:
- Efectuar pruebas de discusión de diversos escenarios discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones.
- Realizar simulaciones especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis.
- Efectuar pruebas de recuperación técnica garantizando que los sistemas de información puedan ser restablecidos con eficacia.
- Realizar ensayos completos probando que el Organismo, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.
- Para las operaciones críticas del Organismo se tomarán en cuenta, además, los siguientes mecanismos:
- Efectuar pruebas de recuperación en un sitio alternativo ejecutando los procesos de las actividades del Organismo en paralelo, con operaciones de recuperación fuera del sitio principal.
- Realizar pruebas de instalaciones y servicios de proveedores garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos.

Todas las pruebas efectuadas deben ser documentadas, resguardándose la evidencia formal de la ejecución y de los resultados obtenidos.
La periodicidad de revisión de los planes de contingencia es la siguiente:

Plan de contingencia	**Revisar cada**	**Responsable de revisión**

Actividades: El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

DOMINIO	Cumplimiento	**OBJETIVO**	Cumplimiento de los requisitos legales
CONTROL	**15.1.1 Identificación de la legislación aplicable**		
DESARROLLO			

Propósito: Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la división de sistemas y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la institución.

Recomendación: Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

Actividades: Definir y documentar los controles y responsabilidades individuales específicos para satisfacer estos requerimientos.

DOMINIO	Cumplimiento	**OBJETIVO**	Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad
CONTROL	**15.1.2 Derechos de propiedad intelectual (DPI)**		
DESARROLLO			

Propósito: Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Recomendación

Se debe considerar lo siguiente:

- Una política de cumplimiento de los derechos de propiedad intelectual y publicación que defina el uso legal de los productos de software e información.
- Sólo adquirir software a través de fuentes conocidos y acreditados para asegurar que no sean violados los derechos de autor.
- Mantener el conocimiento de las políticas para proteger los derechos de propiedad intelectual y las medidas disciplinarias aplicables a su transgresión.
- Mantener un registro de los activos e identificar todos aquellos protegidos por el derecho de propiedad intelectual.
- Mantener prueba y evidencia de la propiedad de las licencias, discos originales, manuales, etc.
- Implementar controles para asegurar que no se exceda el número máximo de usuarios permitidos.
- Chequear que sólo se instalen softwares autorizados y productos con licencia.
- Proporcionar una política para mantener las condiciones de licencias en forma adecuada.
- Proporcionar una política para eliminar o transferir software a terceras partes.
- Utilizar las herramientas de auditoría apropiadas.

Actividades:

- Adquirir el software solamente a través de fuentes conocidas.
- Mantener los documentos que acrediten la propiedad de licencias.
- Comprobar que se instale solo software autorizado y productos bajo licencia.
- Establecer una política de mantenimiento y de eliminación de software no autorizado.

DOMINIO	Cumplimiento	**OBJETIVO**	Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad
CONTROL	**15.1.3 Protección de los documentos de la organización**		
DESARROLLO			
Propósito: Proteger los registros importantes contra perdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales.			

Recomendación: Los registros críticos de la institución se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la institución.

Los registros se clasificarán en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u ópticos.

Tipo de Registro	**Sistema deInformación**	**Período deRetención**	**Medio deAlmacenamiento**	**Responsable**

- Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante.
- Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.
- Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable, por ejemplo que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.
- El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal. Asimismo, permitir una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para la institución.

Actividades: Realizar un inventario de información clave y los controles para la protección de los registros y la información contra pérdida, destrucción o falsificación.

DOMINIO	Cumplimiento	**OBJETIVO**	Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad

CONTROL	15.1.4 Protección de datos y privacidad de la información de carácterpersonal
DESARROLLO	

Propósito: Asegurar la protección y privacidad de la data conforme lo requiera la legislación, regulaciones y, si fuesen aplicables, las cláusulas contractuales relevantes.

Recomendación: Todos los empleados deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

La institución debiera incluir un "Compromiso de Confidencialidad", el cual debe ser suscrito por todos los empleados y contratistas. La copia firmada del compromiso será retenida en forma segura por el por la institución.
Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer publicar información a ninguna persona, salvo autorización previa y escrita del Responsable del Activo.

Actividades: Desarrollar e implementar una política de protección y privacidad de los datos. Esta política debe ser comunicada a todas las personas involucradas en el procesamiento de información personal.

DOMINIO	Cumplimiento	OBJETIVO	Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad
CONTROL	**15.1.5 Prevención del uso indebido de recursos de tratamiento de la información**		
DESARROLLO			

Propósito: Disuadir a los usuarios de utilizar los medios de procesamiento de la información para propósitos no autorizados.

Recomendación: Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo. La utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos, debe ser considerada como uso indebido.

Actividades: La dirección debe aprobar la utilización de los medios de procesamiento de la información. Cualquier uso de estos medios para propósitos no-institucionales u otro no autorizado, será visto como un uso inapropiado de los recursos.

DOMINIO	Cumplimiento	**OBJETIVO**	Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad
CONTROL	**15.1.6 Regulación de los controles criptográficos**		
DESARROLLO			

Propósito: Utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.

Recomendación:

- Restricción de importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas.
- Restricción de importaciones y/o exportaciones de hardware y software de computadores diseñados para adicionarles funciones criptográficas.
- Restricciones sobre la utilización de la codificación.
- Métodos obligatorios o discrecionales para que las autoridades de los países tengan acceso a información codificada para garantizar su confidencialidad.

DOMINIO	Cumplimiento	**OBJETIVO**	Asegurar el cumplimiento de los sistemas con las políticas y estándares deseguridad organizacional
CONTROL	**15.2.1 Cumplimiento de las políticas y normas de seguridad**		
DESARROLLO			

Propósito: Los jefes de áreas debieran asegurar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para asegurar el cumplimiento de las políticas y estándares de seguridad.

Recomendación: Los jefes de áreas deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuadas, las normas y cualquier otro requisita de seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

- Determinar la causa del incumplimiento.
- Evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos.
- Determinar e implementar la acción correctiva apropiada.
- Revisar la acción correctiva que se ejecutó.

Actividades: Detectar algún incumplimiento y determinar las causas, evaluar la necesidad de acciones correctivas, implementarlas, revisar dicha acción mediante su registro e informarlo.

DOMINIO	Cumplimiento	**OBJETIVO**	Asegurar el cumplimiento de los sistemas con las políticas y estándares deseguridad organizacional
CONTROL	**15.2.2 Comprobación del cumplimiento técnico**		
DESARROLLO			

Propósito: Verificar periódicamente los sistemas de información para determinar el cumplimiento con las normas de implementación de la seguridad.

Recomendación: Verificar periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados.

La verificación del cumplimiento debiera comprender pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados.

Actividades

- Realizar manualmente (respaldado por las herramientas de software apropiadas, si fuese necesario) el chequeo del cumplimiento técnico por un especialista experimentado y/o con la asistencia de herramientas automatizadas que generen un reporte técnico.
- Planificar, documentar y repetir las pruebas de intrusión o evaluaciones de vulnerabilidad (ethical hacking).

- Realizar la verificación de cumplimiento técnico por personal competente y autorizado o bajo su supervisión.

DOMINIO	Cumplimiento	**OBJETIVO**	Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información
CONTROL	**15.3.1 Controles de auditoría de los sistemas de información**		
DESARROLLO			

Propósito: Planificar y acordar cuidadosamente los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos para minimizar el riesgo de interrupciones de los procesos del negocio.

Recomendación:

- Se deberían tener presente las siguientes lineamientos:
- Los requisitos de auditoría se deberían acordaron la dirección correspondiente.
- Se debería acordar y controlar el alcance de las verificaciones.
- Las verificaciones se deberían limitar al acceso de solo lectura del software y los datos.
- El acceso diferente al de solo lectura únicamente se debería permitir para copias aisladas de archivos del sistema que se puedan borrar al terminar la auditoría, o se debería dar protección adecuada, si existe la obligación de conservar dichos archivos según los requisitos de documentación de la auditoría.
- Los recursos para llevar a cabo las verificaciones se deberían identificar explícitamente estar disponibles.
- Se deberían identificar y acordar los requisitos para el procesamiento especial o adicional.
- Todo acceso se debería monitorear y registrar para crear un rastro para referencia; el uso de rastros de referencia de tiempo se debería considerar para dates o sistemas críticos.
- Se recomienda documentar todos los procedimientos, requisitos y responsabilidades.
- La persona que realiza la auditoría debería ser independiente de las actividades auditadas.

Actividades:

- Acordar los requerimientos de auditoría con la autoridad.
- Acordar y controlar el alcance de los chequeos.

- Los chequeos deben limitarse a un acceso de "sólo lectura" al software y los datos.
- Identificar explícitamente y disponer los recursos para realizar los chequeos.
- Monitorear y registrar todos los accesos para producir un histórico de referencia; considerar rastros de referencia con impresión horaria para los datos o sistemas críticos.
- Documentar todos los procedimientos, requerimientos y responsabilidades.

DOMINIO	Cumplimiento	**OBJETIVO**	Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información
CONTROL	**15.3.2 protección de las herramientas de auditoría de los sistemas de información**		
DESARROLLO			

Propósito: Proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

Recomendación: Las herramientas de auditoría de los sistemas de información, por ejemplo, software o archivos de datos, se deberían separar de los sistemas operativas y de desarrollo y no mantenerse en librerías de cinta, salvo que se les proporcione un nivel adecuado de protección adicional.

Actividades: Proteger el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso.

5. CONCLUSIONES

El estudio realizado se puede concluir que la División de Sistemas cuenta con mecanismos para la protección de la información y activos relacionados con ella, como son políticas, procedimientos, tecnologías y formatos; es de resaltar que la política institucional no se ajusta a los requerimientos de los estándares de la Gestión de la Seguridad, además se tienen establecidos controles internos que permiten mantener asegurada la información; sin embargo, dichos controles no se encuentran documentados en la política de seguridad.

Lo planteado en la política de seguridad institucional se encuentra desorganizada de acuerdo a los lineamientos estipulados por el estándar de buenas prácticas de la Gestión de la Seguridad.

La Guía de buenas prácticas basada en la ISO/IEC 27002 se convierte en un instrumento de fácil comprensión, en la cual se estableció unas sugerencias y actividades para cada uno de los controles a implementar.

Se concluye que la gestión de la seguridad de información no es un tema de mediana envergadura, sino que por el contrario es algo que debe estar incluido en la cultura organizacional, lo cual no se podrá lograr sin el apoyo de la alta gerencia como promotor activo de la seguridad.

6. RECOMENDACIONES

Implementar controles de una metodología de seguridad de la información (Sistema de Gestión de Seguridad de la Información) acorde a sus necesidades para garantizar la confidencialidad, integridad y disponibilidad de la información. Esto requiere de un alto compromiso de la dirección en conformar un marco de gobierno para la seguridad de la información institucional, al establecer políticas, procedimientos y controles en relación a los objetivos estratégicos de la institución, con objeto de mantener el riesgo en un nivel aceptable por la propia organización.

Como marco de referencia se puede utilizar la norma ISO/IEC 27002 Código de buenas prácticas en materia de seguridad de la información, que relaciona los posibles controles a elegir en base a diferentes conjuntos de objetivos planteados.

Es necesario crear un comité de seguridad de la información, el cual tiene la responsabilidad de supervisar la implementación de políticas y procedimientos, proponer estrategias y soluciones específicas para la implantación de los controles necesarios con el fin de llevar a cabo la materialización las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas.

Por otra parte, una vez creada la política se requiere la participación proactiva de todo el personal involucrado en el funcionamiento y mantenimiento de los activos de información de la institución.

Reubicar las instalaciones físicas donde se encuentra centralizada la información y los activos relacionados con ella; además, se deberá adquirir tecnología de punta que permita proteger contra accesos no autorizados y fenómenos naturales.

BIBLIOGRAFIA

ECHENIQUE GARCÍA, José Antonio. Auditoría en informática. 2da edición. Bogotá: McGraw Hill, 2004. 300p.

Norma ISO/IEC 27002:2005 Norma
Técnica Colombiana ISO 9001:2008, Cuarta edición, Bogotá, ICONTEC, 2008, 32p

REPÚBLICA DE COLOMBIA, Constitución Política De La República De Colombia De 1991, Actualizada hasta el Decreto 2576 del 27 de Julio de 2005

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). Bogotá D.C.:

ICONTEC, 2006. NTC ISO/IEC 27001. INSTITUTO COLOMBIANO DE NORMAS

TÉCNICAS Y CERTIFICACIÓN. Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. Bogotá D.C.: ICONTEC, 2007.NTC ISO/IEC 27002.

REFERENCIAS ELECTRONICAS

http://www.iso27000.es/download/doc_iso27000_all.pdf

http://www.iso27000.es/iso27000.html#section3a

AENOR ediciones, Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes). file:///D:/Downloads/PUB_DOC_Tabla_AEN_9551_1%20(1).pdf

AENOR ediciones, Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes). file:///D:/Downloads/PUB_DOC_Tabla_AEN_9551_1%20(1).pdf

Escuela Politécnica Nacional, plan de seguridad de la información basado en el estándar ISO 13335 aplicado a un caso de estudio. http://bibdigital.epn.edu.ec/bitstream/15000/5617/1/CD-4645.pdf

Ofiseg Consulting, S.L. ¿Qué es un SGSI http://www.ofisegconsulting.com/iso27000.html

Inteco. Normativa
http://www.inteco.es/Formacion_gl/SGSI_gl/Conceptos_Basicos_gl/Normativa_SGSI_gl

CONGRESO DE LA REPÚBLICA, Ley 1273 de 2009 (enero 5).
http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html

CONGRESO DE COLOMBIA. Ley 599 de 2000 (Julio 24).
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

CONGRESO DE COLOMBIA. Ley 43 de 1990 (Diciembre 13).
http://www.mineducacion.gov.co/1621/articles-104548_archivo_pdf.pdf

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

ANEXOS

Anexo A. Encuesta a empleados

Universidad Francisco de Paula Santander
Facultad de Ingenierías
Especialización en Auditoría de Sistemas

ENCUESTA DIRIGIDA A LOS EMPLEADOS DE LA DIVISION DE SISTEMAS DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

INSTRUCCIONES: A continuación usted encontrara una serie de preguntas de las cuales debe seleccionar la respuesta que considere marcando con una (X).

Esta información es muy importante para la investigación y será utilizada con toda reserva por los investigadores.

1. ¿Conoce y entiende la política de seguridad, su propósito e implicaciones?

   SI___ NO___

2. ¿Atreves de qué medios se le dieron a conocer la política?

Inducción___ Circulares informativas___ Correo electrónico___
Comunicación a través de charlas y reuniones___ Otro_____

3. ¿Conoce algún Plan de Emergencia que organice y defina las actuaciones, (quien debe actuar, con qué medios, que se debe hacer, qué no se debe hacer, como se debe hacer), frente a una catástrofe natural que pueda presentarse en la dependencia?

   SI___ NO___

4. ¿Atreves de qué medios se le dieron a conocer el Plan de Emergencia?

Inducción___ Circulares informativas___ Correo electrónico___
Comunicación a través de charlas y reuniones___ Otro___

5. ¿Cuándo fue la última vez que recibió una capacitación en el uso de equipos contra-incendios?

Hace dos años___ Hace un año___ Hace seis meses___
Nunca___ Otro_____

6. ¿Conoce la existencia de un Plan de Contingencia y su propósito?

   SI___ NO___

7. ¿Cuándo fue la última vez que recibió una capacitación en seguridad informática y/o seguridad de la información?

Hace dos años___ Hace un año___ Hace seis meses___
Nunca___ Otro_____

8. ¿Usted ha laborado en horarios fuera de su trabajo en el departamento de cómputo?
   SI___ NO___ ¿PORQUÉ?_____
9. ¿Ha recibido capacitación en el desempeño de sus funciones, para saber cómo actuar luego de presentarse incidentes o crisis?

   SI___ NO___

10. ¿Cada vez que se desatiende o se retira del puesto de trabajo utiliza un mecanismo de bloqueo adecuado?

    SI___ NO___

Gracias por su colaboración

Anexo B. Entrevista a Líder del Proceso

Universidad Francisco de Paula Santander
Facultad de Ingenierías
Especialización en Auditoría de Sistemas

ENTREVISTATA DIRIGIDA LIDER PROCESO DE LA DIVISION DE SISTEMAS DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

NOMBRE Y APELLIDOS _____
CÉDULA _____ LUGAR_____
TELEFONO_____ E-MAIL _____
CARGO_____ FECHA_____

POLITICA DE SEGURIDAD
1. ¿Cuenta el organismo con una Política de Seguridad de la Información formalmente establecida, aprobada y publicada?
2. La Política de Seguridad de la Información implementada ¿incluye normas y/o procedimientos para garantizar la continuidad de los sistemas de información, minimizando los riesgos de daño y asegurando el eficiente cumplimiento de los objetivos del organismo?
3. ¿Está sustentada la Política por una evaluación de riesgos?
4. En la elaboración de la Política ¿se tuvo en Cuenta la totalidad de los procesos de gestión llevados a cabo en el organismo? ¿Existen mecanismos formalmente establecidos que permitan verificar el cumplimiento de la Política de Seguridad de la Información? ¿Se encuentra el personal del organismo comprometido formalmente con la Seguridad de la información?
5. ¿Es conocida por la totalidad de la planta del organismo sea cual fuere su nivel jerárquico e incluyendo a funcionarios?
6. El personal del organismo ¿ha sido concientizado de la importancia de contar con dichas políticas?
7. ¿Celebra el organismo contratos de confidencialidad de la información con los encargados de administrar y resguardar la información del organismo?
8. ¿Existen políticas y procedimientos referentes a recuperación de información y continuidad de operaciones ante la ocurrencia de contingencias?
9. ¿Existen políticas y procedimientos para el desarrollo, adquisición y mantenimiento de software utilizado por el organismo?
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
10 ¿Se encuentra conformado el Comité de Seguridad de la Información?
11 ¿Se encuentran documentadas las responsabilidades que le corresponden a cada funcionario designado?
GESTION DE ACTIVOS
12 ¿Se encuentran completamente identificados y clasificados los activos importantes asociados a cada sistema de información en función de la administración de riesgos potenciales?

SEGURIDAD DEL PERSONAL
13 Quienes se incorporan a la organización ¿firman un acuerdo de confidencialidad o de no divulgación, respecto del tratamiento de la información del organismo?
POLÍTICA FÍSICA Y AMBIENTAL
14 ¿Considera adecuada la ubicación de las instalaciones físicas?
15 Para la selección y el diseño de las áreas protegidas, ¿se tuvieron en cuenta las posibilidades de daños producidos por incendio, inundación, explosión, tumulto, y otras formas de desastres naturales o provocados por el hombre?
16 ¿Se tomaron en Cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad?
17 ¿Existen controles para asegurar que el equipamiento, la información y el software no sean retirados de la sede del organismo sin autorización y de qué forma se lleva a cabo las comprobaciones?
GESTION DE COMUNICACIONES Y OPERACIONES
18 ¿Está documentado el procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la División de Sistemas? ¿Cada cuánto se realizan copias de seguridad?
CONTROL DE ACCESO
19 ¿Se mantiene un proceso de autorización y un registro de todos los privilegios asignados?
20 ¿Se cancelan inmediatamente los derechos de acceso de los usuarios que Cambiaron sus tareas, revocó su autorización o desvincularon del organismo?
21 ¿Existen procedimientos de gestión para proteger el acceso a las conexiones y servicios de red acordes a la política de control de acceso del organismo?
22 ¿Qué tipo de controles se efectúa para proteger el acceso a las conexiones y servicios de red?
23 ¿Cuáles son los procedimientos para la activación y desactivación de derechos de acceso a redes definidos por el organismo?
24¿Qué medidas/políticas de restricción del uso indebido de Internet existen en el organismo?
25 ¿Qué método de autenticación es utilizado para los usuarios especialmente autorizados para el ingreso desde el exterior?
26¿Existen controles sobre las claves de acceso a los aplicativos?
27¿Se establecieron controles sobre las áreas de base de datos y procesamiento?
28¿Se tiene en cuenta la seguridad en la administración de las copias de respaldo?
29¿Se realizan pruebas sobre los Planes de Resguardo (back-up), Planes de Contingencia, Planes de Recupero ante Desastres?
30 ¿Existe un procedimiento de registro y revisión de los registros de auditoría que produzcan informes de las amenazas detectadas contra los sistemas y los métodos utilizados?
31¿Se utilizan las técnicas criptográficas para la transmisión de la información clasificada?
ADQUISICION DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

32¿Existe un procedimiento que durante la etapa de análisis y diseño del sistema incorpore los controles de seguridad a los requerimientos del sistema?
33¿Se incluye una etapa de evaluación de riesgos previa al diseño?
34¿Se han definido y documentado los métodos de protección de la información crítica?
35¿Se desarrollan procedimientos respecto de la administración de claves, recuperación de información cifrada, en caso de pérdida, compromiso o daño?
36¿Qué algoritmos de cifrado simétrico y/o asimétrico se utilizan y cuál es su longitud de clave?
37 Toda vez que sea necesario realizar un cambio en el sistema operativo ¿Se revisan los sistemas de manera que no produzcan impactos en su funcionamiento o seguridad?
GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION
38 Cuándo ocurre un incidente, ¿Se recopilan las evidencias y se asignan responsabilidades para documentarlas a fin de aprender de dichos incidentes y monitorearlos?
39 Al detectar un evento de seguridad de la información, ¿Se registra, califica, prioriza y resuelve el incidente y se notifica a los usuarios afectados?
ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DEL ORGANISMO
40 ¿Se han identificado y priorizado los procesos críticos de las actividades del organismo?
41 ¿Se ha elaborado y documentado una estrategia de continuidad de las actividades del organismo consecuente con los objetivos y prioridades acordadas?
42 ¿Se ha considerado la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del organismo?
CUMPLIMIENTO
43 ¿Se verifica que los sistemas de información cumplan con las políticas, normas, y procedimientos de seguridad establecidas?
44 ¿Están definidos y documentados claramente todos los requisitos legales, normativos y contractuales presentes para cada sistema de información?
45 ¿Se realizan acciones para lograr la concienciación del personal respecto de las políticas de adquisición y derecho de propiedad intelectual sobre la adquisición del software?
46 ¿Se determinaron los procedimientos para la retención, almacenamiento, manipulación y eliminación de registros?
47 Que controles para proteger la información y los registros esenciales contra pérdida, destrucción o falsificación?

Anexo C. LISTA DE VERIFICACIÓN

División de Sistemas				**R/PT: 001**
CheckList				**C01**
Dominio	**5. Política de Seguridad**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Establece la Política, en forma clara y sencilla, sus objetivos y alcances generales?				
¿Incluye mínimamente los tópicos de organización de la seguridad, clasificación y control de activos, seguridad del personal, seguridad física y ambiental, gestión de comunicaciones y las operaciones, control de acceso, desarrollo y mantenimiento de los sistemas, administración de la continuidad de las actividades cumplimiento, entre otros?				
Al ser la información un activo para la organización ¿están definidos los recursos de información que deben ser protegidos?				
¿Incluye un esquema de clasificación que preserve los criterios de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad?				
¿La Política de Seguridad de la Información implementada incluye normas y/o procedimientos para garantizar la continuidad de los sistemas de información, minimizando los riesgos de daño y asegurando el eficiente cumplimiento de los objetivos del organismo?				
¿Está sustentada la Política por una evaluación de riesgos?				
¿Es la Política concordante con los objetivos del organismo?				
¿Contempla la Política las disposiciones legales vigentes?				
¿Define las responsabilidades de las personas, departamentos y organizaciones para los que aplica la política de seguridad?				
¿Define los roles objetivos para cada nivel de responsabilidad?				
¿Existe una adecuada segregación de funciones dentro del área de sistemas?				

¿Define las sanciones en caso de incumplimiento?				
¿Establece el resguardo adecuado de la información documentada? ¿Establece la existencia de controles de acceso a la información?				
¿Establece la existencia de procedimientos de copias de seguridad de la información?				
¿Se lleva a cabo la asignación de responsabilidades de la seguridad informática?				
¿Resguarda todos los procesos vinculados al organismo?				
¿Define la Política sanciones ante casos de incumplimientos?				
¿Cuenta el centro de cómputos con sistemas de control de acceso físico a sus instalaciones?				
¿Cumple el personal del Área de Sistemas con el perfil adecuado para el cargo que desempeña?				

División de Sistemas				**R/PT: 002**
CheckList				**C02**
Dominio	**6. Aspectos Organizativos de la Seguridad de la Información**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Existe un Responsable de Seguridad Informática designado por la máxima autoridad de la organización?				
¿Se encuentran definidos correctamente los procesos de seguridad de la información?				
¿Se ha realizado y documentado una evaluación de riesgo de la información del organismo?				

División de Sistemas				**R/PT: 003**
CheckList				**C03**
Dominio	**7. Gestión de Activos**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se encuentran completamente identificados y clasificados los activos importantes asociados a				

cada sistema de información en función de la administración de riesgos potenciales?				
¿Se elaboró un inventario con la información recabada sobre activos importantes? ¿Está actualizado?				
En la clasificación de los activos de información ¿se evalúan las tres (3) características sobre las que se basa la seguridad: confidencialidad, integridad y disponibilidad?				
¿Se realiza periódicamente un mantenimiento preventivo y prueba de los dispositivos de seguridad para la prevención, detección y extinción del fuego?				

División de Sistemas				**R/PT: 004**
CheckList				**C04**
Dominio	**8. Seguridad Ligada a los Recursos Humanos**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Existe una política de seguridad en la definición de puestos de trabajo y la asignación de recursos?				
¿Están incorporadas en la descripción de las responsabilidades de los puestos de trabajo, las funciones y responsabilidades en materia de Seguridad?				
¿Se llevan a cabo controles de verificación (investigación de antecedentes) del personal en el momento en que se solicita el puesto?				
Quienes se incorporan a la organización ¿firman un acuerdo de confidencialidad o de no divulgación, respecto del tratamiento de la información del organismo?				
¿Es retenida por el Área de Recursos Humanos otra área competente, en forma segura la copia del acuerdo de confidencialidad suscripto por el personal, cualquiera sea su situación de revista?				
¿Se comunican en forma detallada al empleado las actividades que van a ser monitoreadas por el acuerdo?				

¿Se planifica la revisión del contenido del acuerdo de confidencialidad o de no divulgación a un plazo inferior a un año?				
¿Se determinó la responsabilidad del empleado en materia de seguridad de la información, en los términos y condiciones del empleo?				
¿Se encuentran aclarados en los términos y condiciones de empleo, los derechos y obligaciones del empleado relativos a la seguridad de la información?				
¿Existen casos en los que las responsabilidades exceden la competencia del organismo el horario normal de trabajo?				
¿Reciben los empleados del organismo una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del organismo?				
¿Se tiene una política de inducción al personal antes de otorgar privilegios de acceso a los sistemas que corresponden?				
La Política de Seguridad ¿establece su aplicación en todo el ámbito del organismo?				
¿Existe un canal de comunicación formalmente establecido para informar y dar respuesta a incidentes indicando la acción que ha de emprenderse?				
¿Está definidas y asignadas claramente las responsabilidades de realizar la terminación del empleo o el cambio de empleo?				
¿se tiene un proceso formalizado para la terminación del contrato donde se incluya la devolución de todo el software, documentos corporativos y equipo entregado previamente ?				
¿Existen procedimientos para comunicar anomalías de software?				
¿Pueden los usuarios quitar el software que presenta una anomalía?				
¿Se cuenta con un proceso que documente, cuantifique y monitoree los tipos, volúmenes y costos de los incidentes y anomalías?				
¿Existen procesos disciplinarios contemplados en normas estatutarias o reglamentarias que rigen al personal de la Administración Pública?				

División de Sistemas				**R/PT: 005**
CheckList				**C05**
Dominio	**9. Seguridad Física y del Entorno**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Es la construcción del área físicamente sólida, contra daños producidos por incendio, inundación, explosión, tumulto, y otras formas de desastres naturales o provocados por el hombre?				
Las instalaciones donde se realiza el procesamiento de información crítica o sensible, ¿se encuentran ubicadas dentro del perímetro de un área protegida en el edificio?				
¿Están todas las aberturas que comunican las instalaciones de procesamiento de información con el exterior adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control?				
¿Existen sistemas de detección de intrusos (cámaras de seguridad, alarmas)?				
¿Existe un área de recepción atendida por personal?				
El acceso físico a las instalaciones donde se encuentra el equipamiento informático sensible, ¿está restringido sólo a los agentes que lo requieran para llevar a cabo sus tareas?				
¿Existen controles de autenticación; por ejemplo, tarjeta de control de acceso más PIN; para autorizar y validar todo los accesos. Para las áreas donde se procesa o almacena información sensible?				
¿Se mantiene un registro protegido de cada ingreso y egreso para permitir auditar todos los accesos?				
¿Existe un procedimiento definido para el acceso de visitas a las instalaciones del procesamiento de datos?				
¿Se acompaña a las personas ajenas al sector, en trabajos en áreas aseguradas?				
¿Se registra la fecha y horario de su ingreso y egreso, detallando propósitos específicos?				

¿Está previsto el requerimiento, que todos los usuarios empleados, contratistas y terceras personas y todos los visitantes usen alguna forma de identificación visible?				
¿Se restringe el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que el Responsable de Seguridad Informática, lo autorice formalmente?				
¿Se encuentran protegidos adecuadamente todos los equipos tecnológicos o dispositivos auxiliares de soporte sensitivos, como cableado, equipos generadores, dispositivos de red, almacenamiento de resguardos?				
¿Se lleva un registro actualizado de los sitios protegidos, indicando área, elementos a proteger y medidas implementadas?				
¿Se documentan adecuadamente todos los dispositivos de las instalaciones de procesamiento, los circuitos eléctricos, cableado telefónico, repuestos y elementos de reparación, dispositivos de seguridad como detectores de humo, etc.?				
¿Se han implementado medidas de seguridad para la prevención, detección y supresión de incendios en las instalaciones de procesamiento y en toda otra instalación que cuente con recursos informáticos, como por ejemplo cableado, UPS, caja de electricidad, etc.?				
¿Existe detectores de humo?				
¿El equipo contra-incendios está ubicado adecuadamente?				
¿Se ubicaron las instalaciones críticas en lugares discretos a los cuales no pueda acceder el público?				
Se encuentran separadas las instalaciones de procesamiento de información administradas por el organismo, de aquellas administradas por terceros?				
¿Se han identificado y documentado las amenazas potenciales, por ej., por robo o hurto, incendio, humo, inundaciones o filtraciones de				

agua (o falta de suministro), polvo, vibraciones, etc.?				
¿Se han adoptado controles para minimizar cada una de ellas?				
¿Se realiza periódicamente un mantenimiento preventivo y prueba de los dispositivos de seguridad para la prevención, detección y extinción del fuego?				
Los materiales peligrosos o combustibles ¿se almacenan en lugares seguros a una distancia prudencial de las áreas protegidas del organismo?				
¿Están claramente definidas las salidas de emergencia?				
Los equipos redundantes y la información de resguardo (back up), ¿se almacenan en un sitio seguro y distante del lugar de procesamiento, a fi n de evitar daños ante eventuales contingencias en el sitio principal?				
El sector donde se encuentra el equipamiento utilizado para el procesamiento de datos ¿Cuenta con adecuadas condiciones ambientales, temperatura, ventilación, agua potable, etc.?				
¿Se prohíbe comer, beber y fumar dentro de las instalaciones de procesamiento de la información?				
El suministro de energía ¿está de acuerdo con las especificaciones del fabricante o proveedor de los equipos?				
¿Se dispone de suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del organismo?				
¿Se cuenta con equipos de fuente no interrumpida (plantas eléctricas)?				
Los planes de contingencia ¿contemplan las acciones que han de emprenderse ante una falla de la UPS?				
Los generadores ¿son probados periódicamente de acuerdo con las instrucciones del fabricante o proveedor?				

¿Se dispone de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado?				
Los interruptores de emergencia ¿se encuentran ubicados cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, fi n de facilitar un corte rápido de la energía en caso de producirse una situación crítica?				
¿Se dispone de iluminación de emergencia para eventuales fallas en el suministro principal de energía?				
¿Se encuentra protegido el cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información?				
El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información ¿cumple con los requisitos técnicos vigentes?				
¿Se adoptaron medidas de protección para cableado de red contra intercepción no autorizada o daño?				
Los cables de energía de los cables de comunicaciones ¿se encuentran separados por conductos para evitar interferencias?				
¿Se instalaron recintos o cajas con cerraduras en los puntos terminales y de inspección?				
¿Se somete el equipamiento a tareas periódicas de mantenimiento preventivo?				
El Área de Informática ¿mantiene un listado actualizado del equipamiento con el detalle de la frecuencia en que se realiza el mantenimiento preventivo?				
¿Se ha establecido que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento?				
¿Se registran todas las fallas supuestas o reales y todo el mantenimiento preventivo correctivo realizado?				
¿Se definió un procedimiento para el ingreso y egreso de equipos o dispositivos informáticos a la sala de procesamiento del organismo?				

¿Existe un procedimiento para eliminar la información confidencial que contenga cualquier equipo que sea necesario retirar del organismo, realizándose previamente las respectivas copias de resguardo?				
¿Existen controles para asegurar que el equipamiento destinado al procesamiento de información fuera del ámbito del organismo, será autorizado por el propietario de la información almacenada en el mismo?				
¿Se respetan las instrucciones del fabricante respecto del cuidado del equipamiento?				
¿Se cuenta con un seguro para el equipamiento fuera del ámbito del organismo?				
Al momento de desafectar o reutilizar medios de almacenamiento ¿existen controles para proteger el material sensible que pudiera tener información sensitiva?				
¿Se destruyen o se sobrescriben en forma segura, los medios de almacenamiento que contienen material sensible, como por ejemplo, discos rígidos no removibles?				
¿Se utilizan las funciones de borrado estándar?				
¿En caso de ser documentos en papel, los mismos son físicamente destruidos?				
Los documentos en papel y los medios informáticos conteniendo información sensitiva ¿se almacenan bajo llave, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados?				
¿Se desconecta de la red / sistema / servicio o se protege mediante contraseñas al inicio y sobre protectores de pantalla a las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas?				
¿Se protegen los puntos de recepción y envío de correo postal y las máquinas de Fax no atendidas?				
¿Existen controles para asegurar que el equipamiento, la información y el software no sean retirados de la sede del organismo sin autorización?				

¿Se llevan a cabo comprobaciones periódicas destinadas a detectar el retiro no autorizado de activos del organismo?				
¿Existen medidas de prevención contra software malicioso, (por ej. virus, troyanos; entre otros) a fin de evitar la ocurrencia de tales amenazas?				
¿Se garantiza la confidencialidad, integridad, disponibilidad de la información que se emite o se recibe por los distintos canales?				
¿Están definidos los procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento?				
¿Se ha definido y documentado claramente por medio de una norma el uso de correo electrónico?				
¿Se han definido y documentado controles para la detección y prevención del acceso no autorizado?				
¿Se han desarrollado procedimientos vinculados a la concientización de los usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios?				

División de Sistemas				**R/PT: 006**
CheckList				**C06**
Dominio	**10. Gestión de Comunicaciones y Operaciones**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se documenta y se mantienen los procedimientos de operación y se ponen a disposición de todos los usuarios que lo necesiten?				
¿Se controlan los cambios en los sistemas y en los recursos de tratamiento de la información?				
¿Se tiene separadas las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la División?				
¿Tiene separado los recursos para el desarrollo, prueba y producción?				

¿La organización verifica la implementación de acuerdos con terceros?				
¿Los servicios, informes y registros suministrados por terceros son monitoreados y revisados regularmente?				
Se gestionan los cambios en la provisión del servicio y en los procedimientos y los controles se tiene en cuenta la importancia de los sistemas y procesos de la División de Sistemas				
¿Se realiza proyecciones de los requisitos de capacidad a futuro para reducir el riesgo de sobrecarga de los sistemas?				
¿Se documenta y se prueba, antes de su aceptación, los requisitos operacionales de los nuevos sistemas?				
Se desarrollan las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación?				
Se tiene implementado controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios?				
Se cuenta con ciertas precauciones para prevenir y detectar la introducción de código malicioso no autorizado?				
Los administradores introducen controles y medidas especiales para detectar o evitar la introducción de software malicioso o no autorizado?				
Se tiene establecido procedimientos de respaldo para realizar copias de seguridad y probar su puntual recuperación?				
Se realiza regularmente copias de seguridad de toda la información esencial del negocio y del software?				
Tiene establecido el tipo de almacenamiento, frecuencia de copia y prueba de soportes y lugar de respaldo?				
Se controla adecuadamente las redes para protegerlas de amenazas?				
Se mantiene la seguridad en los sistemas y aplicaciones que utilizan las redes?				

Tiene implantado estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red?				
Tiene establecido procedimientos para la gestión de los medios informáticos removibles?				
Se protege la documentación de los sistemas contra accesos no autorizados?				
Tiene establecido los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción?				
Se protegen los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la dependencia?				
Tiene establecido los procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito?				
Los sistemas se monitorean y los eventos de la seguridad de información son registrados?				
Se registran las actividades del administrador y de los operadores del sistema?				
Se registran, analizan y toman acciones apropiadas de las averías?				
Se produce y se mantiene durante un periodo establecido los registros de auditoría con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información, con el fin de facilitar las investigaciones futuras y el monitoreo?				

División de Sistemas				**R/PT: 007**
CheckList				**C07**
Dominio	**11. Control de Acceso**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Existen políticas, normas y procedimientos para Control de Acceso Seguridad Informática?				

¿Existen reglas de control de acceso obligatorias? Indicar en comentarios cuál es el criterio.				
¿Se revocan los privilegios al finalizar el periodo de vigencia establecido?				
¿Se promueve el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios?				
Las contraseñas provisorias asignadas cuando los usuarios olvidan su contraseña se suministran sólo una vez identificado el usuario?				
¿Los usuarios dan acuse de recibo de la recepción de la contraseña de carácter provisorio?				
Los sistemas operativos de red ¿están configurados de manera tal que las contraseñas tengan hasta ocho caracteres para cuentas administradoras y hasta seis caracteres para cuentas de usuarios comunes?				
¿Se suspende o bloque a permanentemente al usuario luego de tres (3) intentos de ingresar una contraseña incorrecta, siendo responsabilidad del usuario solicitar su rehabilitación al Responsable de Administración de Seguridad del organismo?				
¿Se solicita a los usuarios el cambio de la contraseña cada 30 días?				
¿Se impide el uso de las últimas doce 12 contraseñas utilizadas?				
¿Se toman los recaudos necesarios a fi n de garantizar que los usuarios cambien en su primer ingreso al sistema las contraseñas iníciales que les son asignadas?				
En dicho proceso ¿se revisan los derechos de acceso de los usuarios a intervalos no mayores de seis (6) meses o después de cualquier cambio?				
¿Se revisan las autorizaciones de privilegios especiales de derechos de acceso a intervalos no mayores de tres (3) meses?				
A fin de garantizar que no se obtengan privilegios no autorizados ¿se revisan las asignaciones de privilegios de todos los				

usuarios a intervalos no mayores de seis (6) meses?				
¿Garantizan los usuarios que los equipos desatendidos sean protegidos adecuadamente contra accesos no autorizados?				
¿Concluyen los usuarios las sesiones activas al finalizar las tareas o bien se protegen mediante un mecanismo de bloqueo adecuado?				
¿Existen procedimientos para la activación y desactivación del derecho de acceso a redes?				
¿Están identificadas las redes y servicios de red a los cuales se permite el acceso mediante normas y procedimientos?-¿Existen gateways/firewalls en el organismo que direccionen los puertos específicos a su correspondiente aplicación y a la vez descarten los paquetes con puertos de destino que no estén específicamente direccionados?				
¿Están divididos los grupos de usuarios del organismo en redes privadas virtuales o dominios lógicos?				
¿Se restringe el acceso a redes estableciendo dominios lógicos separados en redes virtuales separadas?				
¿Existen procedimientos que los usuarios deben seguir para solicitar el acceso a Internet en el caso de existir políticas de restricción para su utilización?				
¿Existen dispositivos de hardware o software utilizados para el monitoreo del uso de Internet?				
¿Existe en el organismo, documentación en la que figuren las pautas de propiedades de seguridad de los servicios de red?				
¿Se limitan los horarios de conexión al horario normal de oficina?				
¿Se ha definido un usuario que realice controles sobre el uso y las actividades de los aplicativos?				
¿Se realizan informes sobre las actividades y el uso de los aplicativos?¿Con qué frecuencia?				
Sobre las sesiones usuario ¿se establecieron controles de caducidad, tiempos de espera, etc.?				
¿Se han contemplado los sistemas críticos en las políticas de seguridad?				

¿Incluye intentos exitosos fallidos de acceso al sistema?				
¿Incluyen intentos exitosos y fallidos de acceso a datos y otros recursos?				
¿Existe un cronograma de depuración de registros en línea?				
¿Cumple el cronograma de depuración de registros en línea con las normas vigentes y las necesidades propias del organismo?				
¿Se monitorean accesos no autorizados?				
¿Se incluyen los detalles de identificación de usuario?				
¿Se registran fecha hora de eventos clave?				
¿Se distinguen tipos de eventos?				
¿Se registran los archivos a los que se accede?				
¿Se registran los utilitarios y programas utilizados?				
¿Se monitorean todas las operaciones que requieren privilegios especiales (como la utilización de cuenta de supervisor)?				
¿Se monitorea el inicio cierre del sistema?				
¿Se monitorea la conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos?				
¿Se monitorea el cambio de fecha/hora?				
¿Se monitorean los cambios en la configuración de la seguridad?				
¿Se monitorean intentos de accesos no autorizados como intentos fallidos?				
¿Se monitorean violaciones de la Política de Accesos y notificaciones para Gateway de red y firewalls?				
¿Existen alertas de sistema de detección de intrusiones?				
¿Existen alertas o mensajes de consola?				
¿Existen alarmas del sistema de administración de redes?				
¿Existen alarmas de accesos remotos al sistema?				
¿Los equipos que generan registros tienen correctamente configurados los relojes?				
¿Existen procedimientos de ajuste de relojes que comparen los mismos con una fuente				

externa confiable y efectúen correcciones en caso de desviaciones?				
¿Se dispone de protección contra software malicioso?				

División de Sistemas				**R/PT: 008**
CheckList				**C08**
Dominio	**12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Se han planificado, documentado y ejecutado los requerimientos de seguridad de las etapas de Desarrollo, Implementación y Mantenimiento del sistema?				
¿Existen registros de auditoría que controlen la validación de los datos de entrada, salida y procesamiento interno?				
¿Se han incorporado reglas de validación de campos en los programas o formularios de entrada de datos o en la definición de las tablas de la base de datos?				
¿Se ha implementado un sistema de administración de claves criptográficas?				
¿Utiliza el organismo técnicas criptográficas de clave pública y clave privada? ¿Se protegen las claves contra la modificación y/o destrucción, copia o divulgación?				
¿Se protege el equipamiento destinado a generar, almacenar y archivar claves?				
¿Se han redactado normas, procedimientos y métodos de administración de claves para generar, almacenar, actualizar, revocar, recuperar, archivar y destruir las mismas?				
¿Tienen las claves fechas de entrada caducidad de vigencia?				
¿Se cuenta con certificados de clave pública?				
¿Existen normas o procedimientos para proteger los datos de prueba del sistema?				
¿Se ha implementado un formulario de solicitud de modificación de programas una hoja de seguimiento de los casos de la modificación?				

¿Se impide que el administrador tenga permisos de modificación sobre los programas fuentes bajo su custodia?				
¿Existe un responsable único para cada aplicación desarrollada internamente o adquirida a un proveedor externo? ¿Fue designado formalmente?				
¿Los cambios propuestos tienen la autorización de los usuarios y/o del propietario de la información? ¿Pueden los cambios comprometer la integridad de los controles y procedimientos?				
¿Se mantiene un control de versiones para todas las actualizaciones de software?				
¿Se garantiza que la implementación se llevará a cabo minimizando la discontinuidad de las actividades?				
¿Se dispone de herramientas preventivas para evitar la infección del software con código malicioso?				

División de Sistemas				**R/PT: 009**
CheckList				**C09**
Dominio	**13. Gestión de Incidentes en la Seguridad de la Información**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
¿Están definidos los procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento?				
¿Se documenta la gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones?				
¿Se han desarrollado procedimientos vinculados a la concienciación de los usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios?				
¿Se establecen responsabilidades y procedimientos de manejo de incidentes?				
¿Existen procedimientos para los planes de contingencia normales ante eventuales incidentes?				

¿Se documentan en forma detallada todas las acciones de emergencia adoptadas?				
¿Se notificó de la medida adoptada ante la contingencia a la autoridad y/o organismos pertinentes?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por fallas operativas?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por código malicioso?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por intrusiones?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por fraude informático?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por error humano?				
¿Se contemplan los incidentes relativos a la seguridad ocasionados por catástrofes naturales?				
¿Se analizó el incidente y se identificó su causa?				
¿Se planificaron e implementaron las soluciones a efectos de evitar la repetición del incidente?				
¿Se comunican las acciones de emergencia al jefe inmediato? ¿Se revisa su cumplimiento?				

División de Sistemas				**R/PT: 010**
CheckList				**C10**
Dominio	**14. Gestión de la Continuidad del Negocio**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**
Existe un Comité de Seguridad de la Información el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de la actividad del organismo?				
¿Se han definido objetivos organizacionales de las herramientas de procesamiento de información?				
¿Está la administración de la continuidad de las actividades del organismo incorporada a los procesos y estructura del mismo?				

¿Se han identificado y priorizado los procesos críticos de las actividades del organismo?				
¿Comprenden los integrantes del organismo los riesgos que el mismo enfrenta, en términos de probabilidades de ocurrencia e impacto de las posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del organismo?				
¿Se ha elaborado y documentado una estrategia de continuidad de las actividades del organismo consecuente con los objetivos y prioridades acordadas?				
¿Se han aprobado planes de continuidad de las actividades del organismo de conformidad con la estrategia de continuidad acordada?				
¿Se han coordinado pruebas y actualizaciones periódicas de los planes y procesos implementados?				
¿Se ha considerado la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del organismo?				
¿Se han identificado los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades como por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio?				
¿Se han evaluado los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación?				
¿Se identificaron los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y se especificaron las prioridades de recuperación?				
¿Se han identificado los controles preventivos (sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de *backup, los* registros no electrónicos vitales, etc)?				
¿Han participado los propietarios de los procesos y recursos de información y el Responsable de Seguridad Informática en el				

proceso de identificación y evaluación de riesgos?				
¿Se consideraron todos los procesos de las actividades del organismo sin Imitarse a las instalaciones de procesamiento de la información?				
Como resultado de la evaluación de riesgos ¿se ha desarrollado un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del organismo?				
Como resultado de la evaluación de riesgos ¿se ha desarrollado un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del organismo?				
¿El plan estratégico ha sido aprobado por el Comité de Seguridad de la Información?				
Dicho Comité ¿ha elevado el Plan Estratégico a la máxima autoridad de la organización para su aprobación?				
¿Se documentaron los procedimientos y procesos de emergencia acordados?				
¿Se llevó a cabo la capacitación adecuada del personal en materia de procedimientos procesos de emergencia incluyendo el maneo de crisis?				
¿Se desarrolló el proceso de capacitación del personal involucrado en los procedimientos de reanudación y recuperación?				
¿Se trataron mecanismos de coordinación y comunicación entre equipos (personal involucrado)?				
¿Se incluyeron procedimientos de divulgación en el plan de contingencia?				
¿Se contemplaron requisitos en materia de seguridad?				
¿Se adecuaron procesos específicos para el personal involucrado?				
¿Cuenta el personal involucrado con documentación específica que indique cuál es su participación en el proceso de contingencia?				
¿Se designó a los responsables de ejecutar cada componente del mismo?				

¿Se encuentran definidos los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del organismo y/o la vida humana?				
¿Existen procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del organismo o de servicios de soporte a ubicaciones transitorias alternativas?				
¿Se redactaron los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del organismo?				
¿Se definió un cronograma de mantenimiento que especifique cómo y cuándo se probará el plan, y el proceso para el mantenimiento del mismo?				
¿Se realizaron actividades de concientización y capacitación diseñadas para propiciar la comprensión de los procesos de continuidad del negocio y garantizar que los procesos sigan siendo eficaces?				
¿Se realizaron simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión luego de incidentes o crisis)?				
¿Se revisan y actualizan periódicamente los planes de continuidad de las actividades del organismo para garantizar su eficacia permanente?				
¿Existe un programa de administración de cambios del organismo que incluya procedimientos para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades?				

División de Sistemas				**R/PT: 011**
CheckList				**C11**
Dominio	**15. Cumplimiento**			
Cuestionario				
Pregunta	**SI**	**NO**	**NA**	**Comentarios**

¿Incluyen estas normas de procedimiento controles específicos y responsabilidades individuales que garanticen el cumplimiento de los recursos de tecnología informática?				
¿Se verifica que los sistemas de información cumplan con las políticas, normas, y procedimientos de seguridad establecidas?				
¿Se solícita, en caso de ser necesario, la participación de especialistas externos?				
El funcionario a cargo del Área Legal con la asistencia del Responsable de la Seguridad Informática ¿definieron y documentaron todos los requisitos legales, normativos y contractuales que debe cumplir cada uno de los sistemas de información?				
El funcionario a cargo del Área Legal con la asistencia del Responsable de la Seguridad Informática ¿redactaron un Acuerdo de Confidencialidad para ser suscripto por todos los integrantes de la organización?				
¿Existe una fi gura sobre la cual recae la responsabilidad de hacer cumplir las normas y procedimientos de seguridad?				
¿Se han implementado procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por las normas de propiedad intelectual?				
¿Utilizan los empleados únicamente material autorizado por el organismo?				
¿Se respetan las normas que fijan los derechos de propiedad intelectual de los sistemas de información, procedimientos, documenta?				