Pontificia Universidad Católica del Ecuador

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA PUCE

USO INTERNO

Octubre 2022

Versión 1.0

REGISTRO DE EMISIÓN Y REVISIÓN

NOMBRES	CARGO	FIRMA
APROBADO POR:		
Dr. Fernando Ponce León S.J.	Rector de la PUCE	
REVISADO POR:		
Mtr. Charles Escobar	Presidente del Comité de Seguridad de la Información	
Mtr. Javier España	Director General Financiero	
Mtr. Javier España	Director General Administrativo (e)	
Mtr. Gina Valdivieso	Directora General de Talento Humano	
Ing. Orlando Acosta	Director de Informática	
Mtr. Nancy Crespo	Directora del Centro de Educación Virtual	
Dr. Andrés Mideros	Director General Académico	
Mtr. Lorena Araujo	Directora General de Estudiantes	
Dr. Julio Michelena	Asesor Jurídico General	
ELABORADO POR:		
Eco. Mónica Mancheno	Directora de Aseguramiento de la Calidad	
Mst. Karina Molina	Oficial de Seguridad de la Información	

CONTENIDO

La Pontificia Universidad Católica del Ecuador identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la institución, razón por la cual se establece un marco de gestión que asegure que la información es protegida de una manera adecuada salvaguardando dicha información contra el uso, revelación y modificación no autorizada, así como daños y pérdidas independientemente de la forma en la que ésta sea administrada, procesada, transportada o almacenada.

1. DECLARACIÓN DE LA POLÍTICA

La Pontificia Universidad Católica del Ecuador se compromete a velar por el cumplimiento de la legislación en materia de protección de datos y seguridad de la información aplicable a todos los procesos de la universidad, precautelando la confidencialidad, integridad y disponibilidad de la información, para lo cual fortalecerá la cultura organizacional en relación a la seguridad de la información y a la mejora continua del Sistema de Seguridad de la Información.

La alta dirección de la universidad promueve el cumplimiento de las políticas de seguridad de la información para lo cual se compromete a:

- Cumplir la normativa vigente aplicable a la seguridad de la información.
- Promocionar de la cultura de seguridad.
- Asegurar los recursos requeridos para implementar y mantener las políticas de seguridad de la información.
- Apalancar la mejora continua del Sistema de Seguridad de la Información.

Las políticas incluidas en este documento se constituyen como parte fundamental del Sistema de Gestión de Seguridad de la Información de la Pontificia Universidad Católica del Ecuador y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La administración de la Seguridad de la Información de la Pontificia Universidad Católica del Ecuador está basada en las Normas ISO 27000, su operación es competencia de todos los colaboradores, contratistas o proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios, recursos de procesamiento y cualquier otro activo de información de la universidad.

Las políticas de seguridad de la información definen el campo de acción en el cual debe ser protegido los activos de información, es decir los QUÉ (qué debe ser protegido, qué es importante, qué es prioritario), mientras que el CÓMO hacerlo lo deben definir las áreas implementando controles, procedimientos y demás que estarán sujetos a verificación sobre su eficacia y cumplimiento.

2. OBJETIVOS DE LA POLÍTICA

- Proteger y mantener la disponibilidad, integridad, confidencialidad de los activos de información y tecnologías para su procesamiento.
- Identificar, clasificar y mantener actualizados los activos de información.
- Identificar, clasificar y tratar los riesgos de seguridad de la información.
- Minimizar los riesgos de seguridad de la información.
- Definir los roles, responsabilidades y competencias de los colaboradores.
- Establecer lineamientos, normativas y procedimientos relacionados con la seguridad de la información.
- Monitorear la implementación del Sistema de Gestión de la Información.
- Socializar la política de seguridad de la información con todos los miembros de la comunidad universitaria.

3. REFERENCIAS NORMATIVAS

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

Por su parte, el artículo 92 en su parte pertinente *dice "... En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados".*

La Ley Orgánica de Transparencia y Acceso a la Información Pública en el literal d) del artículo 2 determina: *"Garantizar la protección de la información personal en poder del sector público y/o privado".*

Código de Ética de la PUCE en su capítulo III Comportamientos éticos a seguir, en la sección 3 indica: Comportamientos de los miembros de la comunidad universitaria en sus literales; 41 - 49 y 52 - 59.

Código de Ética de la PUCE en el capítulo III Comportamientos éticos a seguir en la sección 4: Comportamientos de los miembros de la comunidad universitaria en sus

relaciones mutuas, con otros beneficiarlos y con la sociedad en general., en sus literales: 64 – 67.

4. DEFINICIONES

Activos. - son bienes y derechos propiedad de la empresas o instituciones, tales como: edificios, equipo de oficina, dinero, entre otros y que pueden convertirse en dinero u otros medios líquidos equivalentes.

Activo de Información. – son los recursos del sistema de información o relacionado con éste, necesarios para que la Institución funcione correctamente y alcance los objetivos propuesto, en general algo que tiene valor para la institución, por ejemplo: los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios, así como el hardware y el software utilizado para el procesamiento, transporte o almacenamiento de información.

Activo tecnológico. – computadores, laptops, tablets, celulares, o cualquier otro dispositivo de propiedad institucional.

Administración de la información. - proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes.

Análisis de riesgos. - proceso continuo de identificación de fuentes, estimación de probabilidades e impactos y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Área segura: se denomina a aquel sitio donde se maneja información sensible o valiosa que puede ser equipos informáticos, información, entre otros y que reúne todas las condiciones físicas (ambientales, de seguridad, etc.).

Comité de Seguridad de la Información. - comisión especializada encargada de evaluar, orientar y supervisar los aspectos relacionados con la seguridad de la información.

Confidencialidad. - atributo de la información que define la accesibilidad o divulgación de aquellos que están autorizados.

Continuidad. - proceso permanente que garantiza la continuidad de los procesos clave de la universidad a través de la efectividad del mantenimiento del plan de continuidad.

Control. - toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter académico, administrativo, tecnológico, físico o legal.

Controles criptográficos: utilizan el cifrado de información para proteger información sensible o crítica y poderla almacenar o transmitir de forma segura.

Criptografía: es la técnica que protege documentos y datos, la cual funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet

Cumplimiento. - se refiere a el acatamiento de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las universidades están sujetos.

Custodio de la información: es el colaborador designado por parte de la universidad, para administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Disponibilidad. - atributo de la información que indica que debe estar siempre accesible para aquellos que estén autorizados.

Escritorios limpios: esta política implica no dejar expuesta, desatendida en el escritorio la información institucional sensible, esto incluye memorias USB, cuadernos, tarjetas de acceso, documentos impresos, entre otros, Esto con el propósito de prevenir la pérdida de información sensible en los puestos de trabajo.

Gestión de incidentes. - acciones para atender las incidencias que se presenten. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de seguridad de la información. - parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Gestión de riesgos. - actividades coordinadas para identificar, evaluar, y definir planes de tratamiento para disminuir o controlar los riesgos, así como también el efecto que podrían tener estos en la institución (posible pérdidas o daños).

Incidente de seguridad. - es el evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad de comprometer las operaciones institucionales y amenazar la seguridad de la información.

Información. - cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de un servicio.

Información desatendida: se considera a cualquier activo de información que se encuentre expuesto sin la protección necesario con base a su clasificación (pública, uso interno, restringida, confidencial).

Integridad. - atributo de la información que indica que debe permanecer correcta (integridad de datos) y tal como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.

IP (protocolo de internet): es una dirección única que identifica a un dispositivo en internet o en una red local.

Log: es un registro en archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado y que ayudan a ver la trazabilidad de un evento, detectar y analizar errores, problemas relativos a eventos de red y de sistemas, de bd.

Lugar seguro: espacio dispuesto para el resguardo del activo de información que tengan las condiciones físicas y ambientales necesarias.

Novedades de personal: son los formatos que se originan a partir de un cambio notificado en un acto administrativo, tal como traslados de dependencia, encargos de puestos, promociones, cambios de categoría, licencias, vinculaciones, desvinculaciones, entre otros de los colaboradores en la universidad.

Oficial de Seguridad de la Información.- es el responsable de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.

Permanencia mínima: es el tiempo mínimo por el cual se acuerda mantener hardware, software, suministros, para garantizar durante ese tiempo soporte, repuestos, actualizaciones, garantía según corresponda.

PETI: es el Plan Estratégico de las Tecnologías de la Información y Comunicaciones, es el instrumento que se utiliza para expresar la estrategia de tecnología.

Política. - definición de principios generales que se deben cumplir, serie de reglas y directrices básicas acerca del comportamiento que se espera de los colaboradores, servidores y terceros relacionados.

Propietarios de la información. - persona encargada de cuidar la integridad, confidencialidad y disponibilidad de la información; debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidades.

Proyecto: esfuerzo temporal que se lleva a cabo para crear un producto o servicio, que tiene con una duración determinada y un fin concreto

Relación Jurídica: es el vínculo jurídico entre dos o más sujetos de derecho, en virtud del cual, al menos uno de ellos tiene la facultad de exigir al otro el cumplimiento de una obligación de dar, hacer o no hacer, de conformidad con los términos que hubieren acordado o prestablecidos en la Ley.

Riesgo. - posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información. - son los mecanismos implantados para garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.

Sistema de Gestión de Seguridad de la Información. - conjunto ordenado de normas y procedimientos, interdependientes, interactuantes e interrelacionados entre sí que sirven para la gestión de seguridad de la Información.

Software malicioso. _ es cualquier software o aplicación móvil diseñada para dañar a los ordenadores, dispositivos móviles o el software que se ejecute en ellos.

Terceros. - personas ajenas a la institución, ejemplo: auditores, consultores, proveedores, etc.

VPN (red privada virtual): es una tecnología de red que sirve para conectar una o más computadoras a una red privada utilizando como medio una red pública como internet.

Vulnerabilidad. - debilidad de un activo o grupo de activos de información que puede ser aprovechada por una o más amenazas.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Introducción

- Este dominio define el ámbito de aplicación de la presente política y su periodicidad de actualización.

5.1. DIRECCIÓN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Objetivo

- Proporcionar orientación y soporte a la gestión de seguridad de la información, de acuerdo con los requisitos de la universidad, las leyes y demás normativa vigente.

5.1.1. POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

El presente documento y las políticas definidas en él son aplicables para la Pontificia Universidad Católica del Ecuador en todas sus sedes y su cumplimiento es mandatorio para toda la comunidad universitaria y terceros debidamente autorizados (auditores, consultores, proveedores, entre otros) que hagan uso de los activos de información de la institución para el desarrollo de sus funciones y actividades o para el cumplimiento de obligaciones.

5.1.2. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para garantizar la vigencia de la política, ésta deberá ser revisada cada año o cada vez que se presente un cambio o requerimiento significativo en los distintos ámbitos que regula, por ejemplo: tecnológicos, legales, contractuales, de seguridad, entre otros.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Introducción

- Este dominio permite definir requisitos o controles para que la organización establezca las funciones y responsabilidades de todos los actores de la universidad para gestionar la seguridad de la información incluida las terceras partes. También define la necesidad de manejar la separación de funciones para evitar usos o accesos indebidos a la información. Adicionalmente, precisa la necesidad de incluir en la definición de los proyectos la sección de riesgos para precautelar la seguridad de la información en la ejecución de estos.
- Finalmente resalta la importancia de mantener contacto con grupos de interés para estar actualizados en cuanto a la seguridad de la información.

Objetivo

- Establecer el marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la universidad.

6.1. ORGANIZACIÓN INTERNA

6.1.1. FUNCIONES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

La Pontificia Universidad Católica del Ecuador establece el siguiente esquema para la administración de la seguridad de la información, en dónde se especifican actividades de supervisión, administración y operación a través de la definición de los siguientes roles y responsabilidades:

RECTOR Y PRORRECTORES DE LA PUCE

a) Definir la dirección del uso de los activos de información de la Pontificia Universidad Católica del Ecuador.
b) Autorizar la asignación y optimización de los recursos financieros, de personal y demás para el cumplimiento de las estrategias de seguridad de la información con base en la planificación operativa.
c) Aprobar y apoyar las iniciativas para la protección de los activos de información propuestos por el Comité SI.
d) Conocer los resultados de los programas de formación y toma de conciencia relacionados con el Sistema de Gestión de Seguridad de la Información.
e) Conocer los resultados de las revisiones de las valoraciones de los riesgos, así como los niveles de riesgo aceptable identificado.
f) Conocer los incidentes de severidad ALTA relativos a la seguridad de la información y dar seguimiento a su solución.
g) Facilitar y promover el desarrollo de iniciativas sobre seguridad de la Información.
h) Aprobar las normas, políticas, manuales, procesos y procedimientos que apalanquen la implementación del Sistema de Gestión de Seguridad de la Información con base en lo definido en la *"NORMATIVA PROCEDIMENTAL INTERNA PARA LA APROBACION DE INSTRUMENTOS NORMATIVOS EN LA PUCE"*

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN. - el cual estará conformado por:

- Rector, prorrector o su delegado, quién lo presidirá.
- Director General Académico o su delegado.
- Director General de Estudiantes o su delegado.

- Director General Administrativo o su delegado.
- Director General Financiero o su delegado.
- Director General de Talento Humano o su delegado.
- Director de Informática o su delegado.
- Director del Centro de Educación Virtual o su delegado.
- Responsable de Asesoría Jurídica o su delegado.
- Oficial de Seguridad de la Información, quién actuará como secretario de la comisión.

Para la aplicación en las sedes serán los representantes de las distintas áreas enunciadas correspondientes o equivalentes en estas, lo cual deberá ser informado al Oficial de Seguridad de la Información de la sede matriz.

El Comité de Seguridad de la Información de la PUCE, sesionará cuatrimestralmente de forma ordinaria y extraordinariamente cuando sea convocado por el Oficial de Seguridad de la Información a través del correo institucional al menos con veinte y cuatro horas de anticipación, y en la cual deberán constar los temas a ser tratados.

El quorum para las sesiones se establecerá con la mitad más uno de sus integrantes y las decisiones la tomarán con la mayoría absoluta de los votos, sin embargo, siempre deberán al menos estar presentes el Director de Informática o su delegado, el Rector o su delegado, así como el Oficial de Seguridad de la Información o su delegado.

El presidente del comité tendrá voto dirimente.

En cada sesión el secretario elaborará el acta borrador la cual es objeto de aprobación por cada uno de los asistentes, quienes deberán enviar sus observaciones y/o aceptación dentro de un plazo máximo de dos días laborables a partir de la recepción de la misma.

El mencionado comité tendrá dentro de sus responsabilidades:

a) Asesorar y proponer al rector o su equivalente en las sedes la creación, modificación y/o implementación de políticas, planes, programas o proyectos relacionados con la SI.
b) Evaluar y priorizar la ejecución de las iniciativas y/o planes de acción relacionados con la seguridad de la información.
c) Conocer y participar en la formulación y evaluación de planes de acción para evitar, mitigar, transferir y/o aceptar los riesgos de seguridad de la información.
d) Orientar y tomar decisiones ante amenazas al programa de seguridad de la información.

e) Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes y realizar las recomendaciones que fuere el caso.
f) Verificar el cumplimiento de las obligaciones legales y regulatorias relacionadas con la seguridad de la información.
g) Recomendar y monitorear los planes, iniciativas y proyectos relacionados con la mejora de la seguridad de la información.
h) Promover la difusión y sensibilización de la seguridad de la información dentro de la institución y velar por su cumplimiento.
i) Dar seguimiento al cierre de los incidentes de seguridad de la información y aplicación de sanciones si fuera el caso.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (OSI)

a) Proponer al Comité de SI directrices y lineamientos sobre seguridad de la información.
b) Implementar, actualizar y vigilar el cumplimiento de las políticas de seguridad de la información establecidas en la institución, las normativas, procedimientos y estándares que la soportan.
c) Apoyar en la definición e implementación de procesos, procedimientos, controles y políticas para gestionar la seguridad de la información institucional.
d) Difundir las políticas y directrices de seguridad de la información
e) Coordinar el mantenimiento y actualización periódica del inventario de activos de Información que se utilizará para identificar los activos que hacen parte del Sistema de Gestión de Seguridad de la Información.
f) Coordinar y hacer seguimiento a la ejecución de evaluaciones de riesgo e impacto a las actividades institucionales de los activos de información, así como de los planes de tratamiento planteados para la administración de los mismos.
g) Apoyar e implementar proyectos de seguridad de la información, así como definir el ámbito de competencia y dirección de los proyectos que correspondan a las áreas de Seguridad Informática, Seguridad Física y Seguridad de Personas.
h) Coordinar el apoyo interinstitucional para dar respuesta oportuna a los incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los procesos o sistemas afectados.

PROPIETARIO DE LA INFORMACIÓN

Los niveles organizacionales de los propietarios de la información son: Rector, o su equivalente en las sedes, Vicerrector, Decanos, Directores y demás autoridades administrativas y académicas de la universidad. Sus responsabilidades en relación con la administración de la seguridad de la información son:

a) Generar, verificar y validar periódicamente la información producto de los procesos de su área, asegurando la confidencialidad, la integridad y la disponibilidad de la información.
b) Levantar y mantener actualizado el inventario de los activos de información de los procesos a su cargo.
c) Clasificar cada uno de los activos de información de los cuales es responsable, así como actualizarla según se requiera.
d) Definir permisos, lineamientos, protocolos y responsabilidades a los estudiantes que realizan prácticas o pasantías para que accedan solo a activos de información no considerados como críticos – confidenciales.
e) Definir permisos, lineamientos, protocolos y responsabilidades con las personas que la universidad establezca una relación civil, en estos casos al menos deberá suscribirse el acuerdo de confidencialidad.
f) Definir y reportar a la autoridad competente los permisos y tipos de acceso a la información de acuerdo al cargo, funciones, competencias y colaboradores.
g) Cumplir y hacer cumplir las políticas y procedimientos de seguridad de la información para salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información definidos por la Oficina de Seguridad de la Información y por la Dirección Informática.
h) Identificar los riesgos a los cuáles se encuentran expuestos los activos de información a su cargo.
i) Definir los requerimientos de control necesarios, planes de tratamiento para sus activos de información de acuerdo con los niveles de clasificación establecidos y el nivel de seguridad requerido, validar la operación y efectividad de los controles definidos
j) Asegurar la implementación de los controles que sean requeridos por los acuerdos legales con terceras partes o por la regulación vigente.
k) Comunicar las novedades de personal (altas, movimientos internos y bajas) a la Dirección General de Talento Humano con el fin de que se definan los permisos y tipos de acceso a la información con base en el cargo, funciones y competencias del colaborador.
l) Comunicar al Oficial de Seguridad de la Información sus requerimientos en capacitación sobre seguridad de la información.
m) Participar y colaborar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.
n) Reportar los incidentes de SI al jefe inmediato y al oficial de Seguridad de la Información.
o) Velar por el cierre de las brechas y hallazgos identificados en auditorias y pruebas de seguridad.

CUSTODIO DE LA INFORMACIÓN

Se constituyen los docentes, personal administrativo, de servicios, proveedores, contratistas, estudiantes becarios o personas a los cuales el propietario de la información le otorga el acceso y la custodia respecto de la información que maneja. Sus responsabilidades en relación con la administración de la seguridad de la información son:

a) Proveer información consistente, validarla y resguardarla de accesos indebidos o no autorizados.
b) Garantizar los parámetros de integridad, disponibilidad y confidencialidad sobre los activos de información de los cuales sea custodio.
c) Velar por el respaldo de la información.
d) Mantener registros respecto del acceso a la información bajo su custodia cuando aplique de acuerdo a su nivel de clasificación.
e) Coordinar con el propietario de la información y demás instancias que sean necesarias en caso de requerirse medidas de seguridad adicional para resguardar la información con base en su nivel de clasificación.
f) Aceptar, comprender y aplicar las políticas, normativas, procedimientos y estándares de seguridad de la información de la institución en el cumplimiento de sus funciones diarias.

USUARIOS FINALES

Los niveles organizacionales de los colaboradores finales son: docentes, personal administrativo y de servicios, estudiantes, proveedores, contratistas, entidades gubernamentales, terceras partes, u otras personas autorizadas para utilizar la información de la Pontificia Universidad Católica del Ecuador, quienes en cumplimiento de sus funciones y/o la ejecución de sus actividades, en materia de seguridad de la información tienen la responsabilidad de:

a) Mantener la confidencialidad y reserva de la información sensible provista por la Pontificia Universidad Católica del Ecuador para llevar a cabo sus actividades.
b) Reportar eventos o incidentes de seguridad a las autoridades competentes para su tratamiento y gestión
c) Aceptar, comprender y aplicar las políticas, normativas, procedimientos y estándares de seguridad de la información de la institución en el cumplimiento de sus actividades.
d) Utilizar la información y los recursos informáticos institucionales de forma ética, responsable y exclusivamente para los propósitos autorizados.

6.1.2. SEPARACIÓN DE FUNCIONES

Se requiere disponer de procesos definidos y documentados; así como del manual de funciones que debe ser conocido por los colaboradores, en función de los cuales se deberá realizar la asignación de responsabilidades al personal.

Los colaboradores deben conocer la estructura organizacional y los procesos de su dirección o unidad, de modo que conozcan en dónde y cuándo intervienen sus funciones y responsabilidades dentro de cada proceso.

La documentación formal debe tener responsables de su elaboración, revisión y aprobación, en este sentido ningún colaborador está facultado para realizar por sí mismo todas las etapas.

6.1.3. CONTACTO CON LAS AUTORIDADES

El Oficial de Seguridad de la Información reportará a las autoridades de la institución los incidentes de seguridad de la información considerado como nivel de severidad ALTO (con base en lo definido en la Normativa Procedimental para la Gestión de Incidentes de Seguridad de la Información de la PUCE).

6.1.4. CONTACTO CON GRUPOS DE INTERÉS

Con el propósito de intercambiar experiencias, obtener asesoramiento sobre la aplicación de las mejores prácticas y controles de seguridad, el Oficial de Seguridad de la Información y/o su delegado podrán mantener contacto con cualquier institución pública, privada o grupos de interés con las que se pueda mantener relaciones de cooperación para efectos del cumplimiento de la presente política.

6.1.5. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

Independiente de la naturaleza del proyecto ya sean procesos clave de la universidad, procesos internos, investigación, vinculación, servicios o productos, procesos de tecnología de la información, entre otros, se deberá considerar la seguridad de la información dentro de todas las fases del proyecto para incluirla dentro de los objetivos del proyecto, riesgos, identificación e implementación de controles, entre otros.

6.2. DISPOSITIVOS MÓVILES Y TELETRABAJO

Objetivo

Garantizar la seguridad de la información contenida en dispositivos móviles y establecer lineamientos para el teletrabajo.

6.2.1. DISPOSITIVOS MÓVILES Y TELETRABAJO

La Dirección de Informática debe:

a) Elaborar, socializar e implementar la política para el uso de dispositivos móviles y computadoras externas a la institución no deberán conectarse a la red cableada, salvo excepciones a ser aprobadas por el director o responsable del área o unidad a la que pertenece el colaborador y contar con la validación de la Dirección Informática, quienes evaluarán que la misma no constituye una vulneración para la PUCE.
b) Restringir la utilización de las computadoras de escritorio, portátiles o cualquier otro activo de la PUCE de modo que sean utilizados exclusivamente dentro del campus universitario, salvo autorización expresa del jefe inmediato y las direcciones que correspondan.

Los propietarios de la información tienen la responsabilidad de:

c) Proteger los equipos que se les haya asignado para el desempeño de sus funciones para lo cual deberán considerar al menos:

   - No exponer el equipo a condiciones de inseguridad física y/o ambiental.
   - Generar y proteger las claves de acceso con base en las políticas definidas en el presente documento, así como por la Dirección Informática.
   - Proteger la información que se almacene en el dispositivo.

d) Solicitar los permisos correspondientes de su Dirección o Unidad y la Dirección de Seguros y Control de Activos, en caso de que se requiera usar los equipos fuera de las instalaciones de la institución.

6.2.2. TELETRABAJO

La Dirección de Informática será responsable de:

a) Garantizar el acceso remoto a los sistemas internos de la universidad a través de tecnologías seguras.

b) Definir procedimientos para solicitar el acceso remoto, en el cual al menos se debe especificar: el equipo, nombre del colaborador, autorizador, fecha inicio – fin y justificación.
c) Mantener un registro actualizado de los accesos / retiros autorizados para uso de acceso remoto.
d) Enviar al Oficial der Seguridad de la Información (OSI) de forma mensual el listado de usuarios con conexiones remotas activas.
e) Enviar al OSI de forma mensual listado de solicitudes de acceso a conexiones remotas procesadas (con al menos los siguientes campos: nombre de usuario, fecha de inicio y fin autorizado, departamento)
f) Facilitar al OSI cuando requiera soporte de solicitud de acceso remoto realizada por el usuario.
g) Definir políticas para la protección contra software malicioso o cualquier otro indicio de vulneración a los sistemas de la PUCE.

Los propietarios de la información tienen la responsabilidad de:

h) Limitar el uso de wifi gratuito (restaurantes, centros comerciales, o cualquier otra zona pública) para acceder a los sistemas internos de la universidad.
i) Cuidar y custodiar las herramientas, equipos y /o dispositivos asignados por la Pontificia Universidad Católica del Ecuador para el desarrollo normal de las actividades propias del cargo que desempeña y que deberán ser utilizadas exclusivamente para las actividades de teletrabajo.
j) Asumir la responsabilidad respecto del cuidado y custodia de la confidencialidad de la información a la que tiene acceso por las actividades propias que desempeña con relación al cargo.

7. SEGURIDAD EN RECURSOS HUMANOS

Introducción

- El presente dominio aborda los controles para la seguridad de información que se deben considerar en la fase de contratación, durante el empleo y en la fase de finalización del empleo, esto debido a que las personas normalmente se constituyen en uno de los principales riesgos para la seguridad de la información por lo que se debe asegurar que los colaboradores entiendan sus responsabilidades y roles relativas a la SI.

Objetivos

- Concientizar e informar a los colaboradores desde su ingreso y en forma continua acerca del rol que desempeñan en la universidad, así como su responsabilidad sobre la información que manejaran en el desarrollo de sus funciones.
- Proteger los intereses de la universidad como parte del cumplimiento de las responsabilidades de seguridad de la información que tienen los colaboradores en la universidad durante todo el ciclo (vinculación, cambios, permanencia, desvinculación).

7.1. ANTES – DURANTE Y AL FINALIZAR EL EMPLEO

La Dirección General de Talento Humano será responsable de:

a) Definir dentro de las responsabilidades del colaborador las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información.
b) Comprobar los antecedentes de los candidatos.
c) Regular dentro de las relaciones jurídicas con la universidad la protección de la propiedad intelectual.
d) Entregar formalmente al personal, las funciones y responsabilidades que tendrá a su cargo, tanto en su contratación inicial como en la modificación de funciones durante su desempeño laboral conforme el rol de puesto y la unidad administrativa o académica a desempeñar.
e) Definir con base en el literal d) los accesos asociados con los que debe contar el colaborador.
f) Gestionar la suscripción del acuerdo de confidencialidad y no-divulgación, antes de que los colaboradores tengan acceso a la información, el mencionado acuerdo debe establecer como mínimo: parámetros de vigencia del acuerdo, información confidencial referida, responsabilidades y sanciones. La copia firmada del acuerdo deberá ser guardada de forma segura por la Dirección General de Talento Humano.
g) Comunicar las responsabilidades legales subsistentes con respecto al manejo de la información una vez terminada la relación laboral con la universidad.
h) Verificar que el colaborador desvinculado haya realizado la transferencia de la documentación e información de la que fue responsable al nuevo colaborador a cargo, y en caso de ausencia, al jerárquico superior o su delegado. De igual forma deberá incluir el punto de verificación mediante el cual el colaborador desvinculado realice la entrega formal de los bienes y activos de información que hayan estado a su cargo.
i) Dentro del proceso de desvinculación del colaborador se deberá incluir el documento de descargo mediante el cual el ex colaborador faculta a la universidad para poder acceder y hacer uso de la información tanto del correo electrónico, computador

asignado y demás recursos institucionales que se le hayan asignado dentro del ejercicio de su cargo para realización de actividades institucionales.

j) Informar de ser necesario, a los colaboradores, o terceros, de los cambios de personal y los acuerdos de funcionamiento con el fin de precautelar accesos no autorizados.

k) Enviar a la Dirección de Informática y al Oficial de Seguridad de la Información o quien haga sus veces la notificación de la finalización de la relación laboral de los colaboradores (esta no debe ser posterior al día de salida del colaborador), de modo que la Dirección de Informática proceda a retirar oportunamente los privilegios de acceso a los activos de información y a los servicios de procesamiento de la información.

l) Enviar a la Dirección de Informática la notificación de ingreso de personal, así como de cambios/ promociones de los colaboradores para que se proceda con la asignación de accesos o actualizaciones de los mismos sobre los activos de información y a los servicios de procesamiento de la información.

m) Enviar mensualmente al Oficial de Seguridad de la Información el reporte de los colaboradores en estado activo.

n) Enviar mensualmente al Oficial de Seguridad de la Información el reporte de colaboradores desvinculados a el Oficial de Seguridad de la Información.

o) Incluir como parte de la inducción al personal nuevo y a las personas naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con la universidad, el material informativo necesario sobre seguridad de la información, que debe considerar (compromiso con la seguridad de la información, importancia del conocimiento y el cumplimiento de las obligaciones aplicables de seguridad de la información, responsabilidad de sus propias acciones u omisiones en la protección de la información, conocimiento procedimientos de notificación de incidentes de seguridad, uso de contraseñas seguras, control sobre software malicioso, limpieza de escritorios, protección pantallas desatendidas).

p) Definir y comunicar el proceso disciplinario a ser aplicado a los colaboradores en caso de provocar o participar en alguna infracción a los lineamientos de seguridad de la información.

q) Incluir dentro del proceso de desvinculación la entrega formal de toda la información contenida dentro del correo institucional, equipo y medios de almacenamiento asignados por la universidad.

El Oficial de Seguridad de la Información será responsable de:

r) Establecer programas orientados a fortalecer la cultura de seguridad de la información.

8. GESTIÓN DE ACTIVOS DE INFORMACIÓN

Introducción

- Este dominio tiene el propósito de identificar, mantener un registro actualizado de los activos de información (etiquetar, clasificar), definir los propietarios, el uso aceptable de los activos y evaluar las medidas de protección adecuadas para cada activo con base a la evaluación de riesgos.

Objetivos

- Identificar, clasificar los activos de información de la universidad y definir los niveles de protección requerida para cada activo de información.
- Controlar la difusión, modificación, eliminación o destrucción no autorizadas de la información almacenada en los medios.

8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS DE INFORMACIÓN

Los propietarios de la información tienen la responsabilidad de:

a) Identificar e inventariar los activos de información asociados al proceso de su competencia con base en la Metodología para la Gestión de Riesgos de Seguridad de la Información de la PUCE.
b) Documentar y actualizar el inventario de activos de información conforme se realicen las adquisiciones, movimientos o eliminaciones de los activos de información.
c) Definir los colaboradores que deben acceder a la información y el tipo de permisos que tendrán de acuerdo a sus funciones y competencias.
d) Autorizar y justificar los cambios funcionales a las aplicaciones y modificaciones a la información a través de accesos directos a la base de datos (de manera excepcional siempre y cuando no se pueda solventar por aplicativo).
e) Participar en el proceso de levantamiento y clasificación de activos de información, análisis de riesgos y plan de tratamiento de los mismos.
f) Hacer uso del activo de información (correo electrónico, internet, computadores, entre otros) únicamente para la ejecución de las actividades inherentes a las funciones que se desarrollan en la universidad y no para otro propósito, dado que la información y documentos generados en la institución, almacenados y enviados por cualquier medio o herramienta electrónica son propiedad de la universidad.
g) Prescindir del acceso a cualquier página web que ponga en riesgo a la universidad.
h) Utilizar la identidad gráfica institucional (logos – formatos institucionales) en todos los documentos generados como parte de las funciones inherentes (exclusivamente) al cargo que desempeña dentro de la universidad.

i) Entregar formalmente toda la información contenida dentro del correo institucional, equipo y medios de almacenamiento asignados por la universidad una vez concluida la relación con la universidad.
j) Comunicar las responsabilidades legales subsistentes con respecto al manejo de la información una vez terminada cualquier tipo de relación con la universidad.

Los custodios de la información tienen la responsabilidad de:

k) Identificar e inventariar los activos de información asociados al proceso de su competencia con base en la Metodología para la Gestión de Riesgos de Seguridad de la Información de la PUCE.
l) Documentar y actualizar el inventario de activos de información conforme se realicen las adquisiciones, movimientos o eliminaciones de los activos de información.
m) Participar en el proceso de levantamiento y clasificación de activos de información, análisis de riesgos y plan de tratamiento de los mismos.
n) Hacer uso del activo de información (correo electrónico, internet, computadores, entre otros) únicamente para la ejecución de las actividades inherentes a las funciones que se desarrollan en la universidad y no para otro propósito, dado que la información y documentos generados en la institución, almacenados y enviados por cualquier medio o herramienta electrónica son propiedad de la universidad.
o) Prescindir del acceso a cualquier página web que ponga en riesgo a la universidad.
p) Utilizar la identidad gráfica institucional (logos – formatos institucionales) en todos los documentos generados como parte de las funciones inherentes (exclusivamente) al cargo que desempeña dentro de la universidad.
q) Entregar formalmente toda la información contenida dentro del correo institucional, equipo y medios de almacenamiento asignados por la universidad una vez concluida la relación con la universidad.

Los usuarios finales de la información tienen la responsabilidad de:

r) Hacer uso del activo de información (correo electrónico, internet, computadores, entre otros) únicamente para la ejecución de las actividades inherentes a las funciones que se desarrollan en la universidad y no para otro propósito, dado que la información y documentos generados en la institución, almacenados y enviados por cualquier medio o herramienta electrónica son propiedad de la universidad. abstener
s) Prescindir del acceso a cualquier página web que ponga en riesgo a la universidad.

A más de las responsabilidades descritas que son propias de todos los propietarios de la información, la Dirección General de Talento Humano debe:

t) Asegurar que en el proceso de desvinculación de los colaboradores se incluya la devolución de todo activo físico y/o digital que sea propiedad de la universidad o esté bajo su custodia.

A más de las responsabilidades descritas que son propias de todos los propietarios de la información, la Dirección Financiera debe:

u) Garantizar que el inventario de activos de la universidad (medios tecnológicos tales como computadores, servidores, fuentes de almacenamiento externo, entre otros) se encuentre actualizado, considerando los ingresos de personal, desvinculaciones, cambios o promociones de puesto, con el objetivo de que los datos de cada custodio/responsable de activos de información se encuentren actualizados.

v) Asegurar que el proceso de control de activos este articulado con los procesos de desvinculación de personal de la Dirección General de Talento Humano para que se realice un proceso efectivo de entrega de bienes por parte del personal que se desvincule de la universidad y/o terceros.

A más de las responsabilidades descritas que son propias de todos los propietarios de la información, la Dirección de Informática debe:

w) Inventariar los activos de información tecnológicos o digitales incluyendo información adicional según corresponda: número de licencia, vigencia, tipo de tecnología, equipo donde se encuentra instalado, versión, ubicación geográfica, etc.

x) Asegurar que dentro de sus procesos cuando un colaborador se desvincule de la universidad se realice la devolución de todo activo tecnológico que esté bajo la administración de la Dirección de Informática y que sean de propiedad de la universidad o estén bajo su custodia.

y) Elaborar, socializar, documentar e implementar las políticas de acceso y/o uso remoto, internet, intranet, wifi, correo electrónico, y sus aplicaciones/servicios, solicitudes de respaldos, almacenamiento; para lo cual se deberán considerar las responsabilidades y roles de los colaboradores, dentro de las cuales al menos se debe restringir el uso del dominio del correo electrónico de modo que el mismo solo este habilitado para las personas de la comunidad universitaria (estudiantes activos, personal docente y administrativo activo), para cualquier excepción el área requirente deberá presentar el análisis costo beneficio el cual deberá ser analizado y aprobado por el Comité de Seguridad de la Información.

z) Limitar el acceso de los colaboradores a páginas de internet, aplicaciones o servicios que pudieren perjudicar los intereses y la reputación de la institución, entre ellas que atenten a la ética y moral, que no estén relacionadas con el desempeño de las funciones institucionales o que puedan provocar incidentes de seguridad en la información.

El Oficial de Seguridad de la Información tiene la responsabilidad de:

aa) Emitir la Metodología para la Gestión de Riesgos de Seguridad de la Información de la PUCE.
bb) Coordinar, apoyar y realizar el seguimiento en todo el proceso de gestión de los activos de información.

8.2 CLASIFICACIÓN DE LA INFORMACIÓN

Los propietarios de la información tienen la responsabilidad de:

a) Clasificar la información en relación con su valor, normativa legal vigente, sensibilidad y criticidad para la universidad, ante revelación o modificación no autorizada, con base en la Metodología para la Gestión de Riesgos de Seguridad de la Información de la PUCE.
b) Categorizar y etiquetar los activos de información (pública, uso interno, restringida, confidencial) de acuerdo a la clasificación de la información con base en "Normativa procedimental interna para la Gestión de la Información Institucional de la Pontificia Universidad Católica del Ecuador".
c) Notificar al OSI la necesidad de protección o mejora, en los controles para los activos de información del cual es responsable y asegurar el cumplimiento de las medidas de seguridad necesarias para resguardar los activos de información a su cargo considerando el grado de sensibilidad y criticidad de los mismos.

8.3 MANEJO DE LOS MEDIOS

Los propietarios de la información tienen la responsabilidad de:

a) Identificar los activos de información que requieran eliminación segura.
b) Definir, documentar e implementar el manejo adecuado para el borrado o destrucción de los activos de información con base en su valor, normativa legal vigente, sensibilidad, criticidad y tipo de información (pública, uso interno, restringida, confidencial).
c) Mantener el activo de información almacenado únicamente dentro de la infraestructura institucional.

La Dirección de Informática tiene la responsabilidad de:

d) Definir e implementar procedimientos para la transferencia de medios físicos (proveedores, etc.) de modo que durante el transporte fuera de los límites físicos de la universidad los medios que contengan información estén protegidos contra accesos no autorizados, usos indebidos o deterioro, considerando la criticidad de la información.

e) Mantener registros e identificar el contenido de los medios, la protección aplicada, así como reflejar los momentos de transferencia a los custodios y la recepción en el destino.

9 CONTROL DE ACCESOS

Introducción

- Establecer medidas de control de accesos orientadas a controlar y monitorizar los accesos a los medios de información y a las aplicaciones, así como responsabilizar al usuario respecto del uso de las credenciales de acceso.

Objetivos

- Definir procedimientos para todas las etapas del ciclo de los accesos de los colaboradores de todos los niveles, desde el registro inicial de nuevos colaboradores hasta la privación final de derechos de los colaboradores que ya no requieren el acceso.
- Asegurar el acceso de usuarios autorizados a los sistemas y servicios.
- Controlar la asignación de accesos a los sistemas de información, bases de datos y servicios de información.
- Responsabilizar a los usuarios respecto de la administración de su información de autenticación.
- Impedir accesos no autorizado a los sistemas de información, así como a las instalaciones de procesamiento de la información.

9.1 REQUISITOS INSTITUCIONALES PARA EL CONTROL DE ACCESO

Los propietarios de la información tienen la responsabilidad de:

a) Definir qué usuarios y qué niveles de acceso deben tener a los diferentes activos de información salvo el alta y baja de usuarios que es responsabilidad de la DGTH.
b) Garantizar que el control de accesos a los diferentes activos de información esté acorde con la separación de las funciones y con las responsabilidades de acuerdo al cargo de los colaboradores.
c) Revisar periódicamente y notificar cualquier cambio en los derechos de acceso definidos y autorizados.

Con base en el cumplimiento obligatorio de los puntos descritos anteriormente, **la Dirección de Informática tiene la responsabilidad de:**

d) Definir y mantener el inventario actualizado de las redes (lan, wan, inalámbricas, entre otras) y los servicios de red a los que se tiene acceso,

e) Definir y mantener el inventario actualizado de todos los servicios (directorio activo, correo, archivos, entre otros).
f) Definir, documentar, implementar y revisar periódicamente el cumplimiento de los procedimientos para la gestión de accesos y/o uso a todos los sistemas, bases de datos, servicios de información, uso de accesos remotos, redes y servicios de red, en los cuales como mínimo se deberá definir cómo se autoriza la asignación, modificación, revocación de cuentas y/o privilegios.
g) Establecer los controles necesarios y/o la configuración para el ingreso a la red y los procedimientos respectivos para proteger el acceso a las conexiones de red y a los servicios de la red.
h) Controlar que todo computador o dispositivo electrónico que intente conectarse a cualquier red de datos de la universidad, cuente al menos con sus parches de seguridad actualizados, mantenga un sistema de antivirus y se encuentre debidamente autorizado antes de permitir el acceso a la red.
i) Configurar que toda cuenta se bloquee luego del tercer intento fallido de acceso.
j) Controlar el tiempo de inactividad de los sistemas.
k) Desactivar o inhabilitar según corresponda toda cuenta de usuario que no se encuentre activo por más de 90 días.
l) Controlar que la creación de cualquier cuenta genérica (proveedores, terceros u otros) sea solicitada por el área requirente quienes a su vez definirán el colaborador de la universidad que actuará como custodio de la misma.
m) Monitorear el uso de las instalaciones de procesamiento de la información, uso de los servicios de red.
n) Controlar que el acceso remoto solo se lo pueda realizar a través de herramientas autorizadas.
o) Mantener el registro que permita identificar los usuarios autorizados para acceder a las redes y servicios de red a través de conexiones remotas (autorización, tiempo de vigencia, justificación).
p) Determinar a qué aplicativos e información se puede acceder mediante el uso del wifi, los procedimientos de autorización, los controles de gestión para la protección de las redes, los requisitos de autenticación y la supervisión del uso.
q) Restringir el uso de los servicios de la red cuando no se cumpla con labores propias de la universidad.
r) Cancelar la cuenta o desconectar temporal o permanentemente al usuario de la red, cuando se detecte un uso no aceptable del activo de información.
s) Mantener la premisa de "Todo acceso se encuentra prohibido, a no ser que se permita expresamente".

9.2 GESTIÓN DE ACCESO DE LOS USUARIOS

Los propietarios de la información tienen la responsabilidad de:

a) Cumplir con los procedimientos definidos por la Dirección de Informática para solicitar el acceso a los diferentes servicios y aplicaciones de la universidad.
b) Notificar a la DGTH en casos excepcionales la necesidad de mantener los accesos de los usuarios en caso, comisiones, licencias, u otras situaciones que lo ameriten.

La Dirección General de Talento Humano tiene la responsabilidad de:

c) Garantizar que previo a solicitar a la Dirección de Informática la creación de las credenciales de acceso de cualquier colaborador, éste haya firmado el acuerdo de confidencialidad.
d) Notificar a la Dirección de Informática la necesidad de suspender temporalmente los accesos de los usuarios en caso, comisiones, licencias, u otras situaciones que lo ameriten. Esta suspensión temporal de los accesos será para los sistemas en los cuales se maneje información sensible.

Con base en el cumplimiento obligatorio de los puntos descritos anteriormente, la **Dirección de Informática tiene la responsabilidad de:**

e) Definir los procedimientos y/o políticas para la creación (al menos generación aleatoria, robusta y qué fuerce el cambio de la clave al colaborador en su primer ingreso) y entrega de claves de acceso a los sistemas.
f) Establecer lineamientos en dónde consten las características mínimas que los colaboradores deberán considerar al momento de cambiar sus claves, tales como complejidad, tiempo de caducidad, histórico de claves, entre otros.
g) Crear, cambiar o retirar los accesos para los usuarios, verificando que exista la solicitud por parte del colaborador autorizado, así como que se cumpla con los procedimientos definidos.
h) Desactivar de forma inmediata las credenciales de acceso a los diferentes sistemas y/o servicios cuando el colaborador se encuentra desvinculado de la universidad con base en la notificación recibidas por DI de las salidas de personal realizado por DGTH; para cualquier excepción DGTH deberá notificar con la correspondiente justificación.
i) Suspender temporalmente los accesos de los colaboradores (en caso de vacaciones, permisos temporales) con base en la solicitud de Dirección General de Talento Humano.
j) Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso otorgado a los colaboradores.

k) Controlar los derechos de acceso privilegiados mediante un proceso específico, en el cual se deben identificar:
   - Las políticas de acceso privilegiado definidas.
   - Los colaboradores que tienen accesos privilegiados a cada servicio o aplicativo.
   - Fecha de vigencia del acceso privilegiado.
   - Verificación periódica de las competencias de los usuarios

l) Controlar y restringir el uso de cuentas privilegiadas, con base en la siguiente categorización:

   - **Cuentas de usuario de fábrica:** son las cuentas genéricas incorporadas en los sistemas o aplicaciones (root, administrador, sa, admin, entre otras), el custodio de las mismas es el colaborador que administra el sistema o aplicación. Estas cuentas solamente deberán ser usadas en la configuración inicial o en caso de una emergencia que requiera acceso privilegiado el cual deberá ser temporal, estas cuentas no deben ser usadas en la administración diaria o regular.
   - **Cuentas de administración personal:** están asociadas a un usuario que tienen accesos privilegiados para administrar los sistemas o aplicaciones.
   - **Cuentas compartidas – genéricas - institucionales:** usuarios genéricos, estas cuentas no se crean para el uso exclusivo de un usuario en particular, sin embargo, deben tener un custodio – responsable asignado, generalmente se usan por imagen o por prestación de un servicio, redes sociales, etc. Adicionalmente, al emplear este tipo de cuentas se deberá definir el colaborador responsable del envío (en caso de cuenta de correo) y en caso de usuarios y claves de acceso genéricos el colaborador que será el responsable de la administración de la mencionada cuenta.

m) Asegurar la **confidencialidad** de la entrega de contraseñas en todos sus procesos (forzando el cambio de clave después del primer uso, identificar al usuario antes de la entregar, uso de contraseñas seguras, no compartidas, etc.)

n) Forzar el cambio de clave a los colaboradores en caso de presunción respecto del mal uso.

El Oficial de Seguridad de la Información tiene la responsabilidad de:

o) Verificar el cumplimiento de lo establecido para el control de accesos (registro de colaboradores, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de colaboradores, uso controlado de utilitarios del sistema, registro de eventos) con base en la información de monitoreo proporcionada por la Dirección Informática.

p) Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso con base en la información de monitoreo proporcionada por la Dirección Informática.

q) Concientizar a los colaboradores sobre las políticas de seguridad.

r) Realizar visitas sorpresa a los puestos de los colaboradores para verificar cumplimiento del mantenimiento de "escritorios limpios", "pantallas (monitores) sin información desatendida", "impresiones desatendidas" y demás políticas relacionadas con la seguridad de la información.

9.3 RESPONSABILIDADES DEL USUARIO

Los propietarios de la información deben:

a) Implementar las políticas de seguridad respecto del cuidado y uso de las credenciales de acceso. En ese sentido, las credenciales de acceso son de uso **PERSONAL E INTRANSFERIBLE**, no se las puede compartir con otros colaboradores, se prohíbe: almacenar la clave en registros físicos (papel, archivos) o electrónicos, así como ingresar sus credenciales en formularios de dudosa procedencia, y demás lineamientos de la Dirección Informática.
b) Bloquear la pantalla del equipo, computador cuando abandone su puesto de trabajo, así sea por unos instantes.
c) Retirar inmediatamente la información sensible una vez impresa.
d) Cambiar las contraseñas cuando haya indicios de posible divulgación o vulneración de la misma.
e) Mantener los escritorios, pantallas (monitores) sin información desatendida, para reducir el riesgo de daño o accesos no autorizados.
f) Almacenar bajo llave según la categorización de la información, los documentos en papel y en medios informáticos cuando no estén siendo utilizados.
g) Comunicar al Oficial de Seguridad de la Información cuando haya presunción de divulgación, vulneración o mal uso de las credenciales de acceso.
h) Solicitar a la máxima autoridad de la Unidad Académica reporte respecto del uso de las plataformas que tenga información sensible en caso de requerirlo.

Los custodios de la información pueden:

i) Solicitar a la máxima autoridad de la Unidad Académica el reporte respecto del uso de las plataformas que tengan información sensible del solicitante en caso de requerirlo.

Los usuarios finales de la información pueden:

j) Solicitar a la máxima autoridad de la Unidad Académica el reporte respecto del uso de las plataformas que tengan información sensible del solicitante en caso de requerirlo.

9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

A más de las responsabilidades antes descritas, la Dirección de Informática tiene que:

a) Garantizar que el acceso a los sistemas y a las aplicaciones sea a través de un procedimiento seguro de inicio de sesión, el cual deberá revelar el mínimo de información sobre el sistema o aplicación, no proporcionar mensajes o indicios de ayuda durante el proceso de autenticación que pudiera ayudar a un usuario no autorizado, registrar intentos acceso con y sin éxito.
b) Mantener registro de log de auditoría en los sistemas críticos que permitan identificar la actividad de los colaboradores (identificación del usuario, fecha y hora de inicio y terminación de la acción (transacción), identidad y/o ubicación del origen y destino, registros de intentos exitosos y fallidos.
c) Velar para que los desarrolladores tanto internos como externos acojan buenas prácticas de desarrollo seguro en los productos generados, para controlar el acceso lógico y evitar accesos no autorizados a los sistemas de información.
d) Velar por la seguridad de la información para lo cual controlar que no se instale ni use programas utilitarios diferentes a los permitidos dentro del catálogo de aplicaciones institucionales definido por la Dirección Informática.
e) Garantizar el acceso únicamente a las personas que por su función requieren acceder a los programas fuente, librerías y demás repositorios, a fin de prevenir la introducción de funcionalidades no autorizadas y evitar cambios no intencionados.
f) Resguardar en entornos seguros los programas fuente, librerías y mantener el registro de auditoria respectivo.
g) Mantener un registro actualizado de todos los programas fuentes en uso, en el cual se especifique como mínimo: nombre del programa, programador, autorizador, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación o en producción).

10 CRIPTOGRAFÍA

Introducción

- Dependiendo de la clasificación de la información y la evaluación del riesgo, este dominio define a la criptografía como el mecanismo de protección de la información para proteger la confidencialidad e integridad de la información.

Objetivo

- Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.

10.1 CONTROLES CRIPTOGRÁFICOS

Los propietarios de la información tienen la responsabilidad de:

a) Definir y reportar a la Dirección de Informática y a la Oficina de Seguridad de la información sensible que requiere ser encriptada.

La Dirección de Informática tiene la responsabilidad de:

b) Utilizar controles criptográficos para la protección de claves de acceso a: sistemas, datos y servicios. Las claves deberán ser almacenadas de manera codificada, cifrada (encriptada) en la base de datos y/o en archivos de parámetros.
c) Utilizar controles de cifrado (criptográficos) para la transmisión y almacenamiento de información clasificada, fuera del ámbito de la universidad.
d) Resguardar la información sensible con base en la solicitud del propietario de la información.

11 SEGURIDAD FISICA Y DEL ENTORNO

Introducción

Este dominio se centra en la necesidad de identificar y establecer medidas de control físicas para proteger adecuadamente los activos de información con el propósito de evitar incidentes que afecten a la integridad física de la información.

Objetivos

- Prevenir el acceso físico no autorizado, los daños e interferencia a la información y a las instalaciones de procesamiento de la información.
- Proteger los activos de información críticos ubicándolos en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas y controles de acceso apropiados.
- Proporcionar protección proporcional a los riesgos identificados.

11.1 ÁREAS SEGURAS

Los propietarios de la información tienen la responsabilidad de:

a) Definir la necesidad de disponer de áreas seguras, así como los activos de información a resguardar.

b) Resguardar en un lugar seguro la información catalogada como sensible – confidencial de acuerdo con lo definido por la Normativa procedimental interna para la Gestión de la Información Institucional de la PUCE.
c) Portar en un lugar visible la credencial de acceso a la universidad tanto para colaboradores como visitantes.
d) Definir y revisar periódicamente el listado de quienes dispondrán de derechos de accesos en las áreas catalogadas como seguras.
e) Coordinar con la Dirección General Administrativa la implementación de las medidas de seguridad física y de monitoreo, en las cuales al menos se deberá contemplar: seguridad perimetral (muros, alarmas, suelo, protección ventanas, segmentación de espacios, cerraduras, accesos, cámaras, salidas de aire, demarcaciones de las áreas, sistemas antiincendios, entre otros), áreas de atención – recepción.
f) Mantener control del acceso y registrar los accesos a aquellas áreas definidas como seguras (el registro debe tener como mínimo (nombre, fecha y hora de ingreso – salida – área a la que ingresa – motivo)
g) Supervisar el trabajo de terceros.
h) Prohibir el uso de móviles / cámaras y similares en caso de requerirse en zonas catalogadas como seguras.

Los custodios y usuarios finales de la información tienen la responsabilidad de:

i) Portar en un lugar visible la credencial de acceso a la universidad tanto para colaboradores como visitantes.

11.2 EQUIPOS

Los propietarios de la información tienen la responsabilidad de:

a) Adoptar controles para minimizar el riesgo de amenazas físicas potenciales como: robo, incendio, explosión, humo, inundación, polvo, vibración, interferencia del suministro eléctrico e interferencia a las comunicaciones.
b) Coordinar con la dirección competente, la ejecución de mantenimientos programados y emergentes de las instalaciones eléctricas, UPS, sistemas de climatización, ductos de ventilación, equipos tecnológicos y dispositivos, de acuerdo a las especificaciones y recomendaciones del proveedor a través de personal calificado y autorizado.
c) Conservar los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas.

A más de lo descrito, la Dirección General Administrativa deberá:

d) Establecer controles para la protección de los equipos de modo de minimizar el riesgo ante posibles amenazas físicas, ambientales o de accesos no autorizado.

e) Definir el procedimiento para la asignación, retiro y control de equipos móviles de la universidad.
f) Definir procedimientos para la asignación y control para que los colaboradores pueda sacar temporalmente los equipos fuera de la universidad.

A más de las responsabilidades descritas que son propias de todos los propietarios de la información, la Dirección de Informática debe:

g) Definir e implementar medidas de seguridad física y ambiental para el resguardo de los activos tecnológicos críticos, en función a un análisis de riesgos.
h) Definir, socializar, implementar, evaluar y mantener registros del plan de mantenimiento que garantice la disponibilidad e integridad de los equipos y de la infraestructura tecnológica.
i) Configurar de modo que todo equipo tecnológico desatendido se bloquee de forma automática con base en el lineamiento de la Dirección Informática.
j) Disponer de un protocolo para la destrucción, borrado o sobre escritura en los dispositivos que contienen información sensible, de modo que no se permita la recuperación de la información.

12 SEGURIDAD DE LAS OPERACIONES

Introducción

El presente dominio define políticas para asegurar la operación correcta y segura de las instalaciones de procesamiento de información entre ellas contar con procedimientos y definiciones para la operación, protección malware, manejo de copias de seguridad, registro y monitoreo de actividad, control software, vulnerabilidades técnicas, auditoría, entre otras.

Objetivos

- Garantizar el funcionamiento correcto y seguro de la infraestructura tecnológica.
- Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

La Dirección de Informática tiene la responsabilidad de:

a) Definir, ejecutar y documentar los procedimientos instalación, configuración y operación de los sistemas y/o aplicaciones, dentro de los cuales al menos se deberá considerar los siguientes procesos:

- Procesamiento y manejo de la información automatizada y manual, incluyendo la interrelación con otros sistemas.
- Respaldo y restauración de la información (pruebas periódicas de restauración).
- Servicios de procesamiento de datos.
- Monitoreo de los sistemas y/o aplicaciones.
- Reinicio y recuperación de los sistemas en caso de fallas.
- Corrección de errores, excepciones y restricciones en los sistemas durante la ejecución de las tareas.
- En todos los equipos institucionales deberán administrar medidas de seguridad de la información, restringir la instalación de software no autorizado, desinfección de virus, instalación y actualización periódica el software de antivirus a la última versión liberada por el fabricante, actualización de parches de seguridad autorizados por el fabricante.

b) Restringir la incorporación de equipos tecnológicos que no pertenezcan a la universidad, así como el uso de aplicaciones y/o servicios de la red institucional,
c) Asignar a todos los colaboradores (según corresponda con base en las funciones que desempeña) el computador (de escritorio o portátil) para el desempeño normal de su trabajo, en el cual deberá ingresar con el usuario y claves de acceso personales asignadas.
d) Limitar las tareas de soporte o mantenimiento a equipamiento que pertenezca a la institución.
e) Definir, ejecutar y documentar procedimientos para el control de cambios tanto en la infraestructura tecnológica, en las aplicaciones y bases de datos.
f) Monitorear la capacidad de la infraestructura tecnológica ante la necesidad actual, gestionar las futuras demandas de capacidad.
g) Actualizar los equipos considerando la fecha fin de venta asociado a los mismos y su fecha de fin de soporte.
h) Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, entre otros, así como para la eliminación segura de los mismos.
i) Participar en el tratamiento de los incidentes de seguridad, de acuerdo a la normativa establecida.
j) Administrar y garantizar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento (desarrollo, prueba y producción).
k) Documentar los registros de auditoría y de la información de registro del sistema.
l) Documentar los contactos de soporte, necesarios en caso de incidentes.
m) Disponer del estándar de redundancia y seguridad del centro de datos para garantizar la disponibilidad de la información, con base al PETI vigente,
n) Planificar y ejecutar el plan anual de mantenimiento del centro de datos.
o) Todos los servidores de información deben estar alojados en el centro de datos (físico o en la nube) definido por la Dirección Informática.

12.2 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

La Dirección de Informática tiene la responsabilidad de:

a) Elaborar y socializar la política para prohibir el uso de software no autorizado en el cual se incluya el listado del software – aplicativos autorizados.
b) Asegurar que todos los equipos institucionales ya sean de escritorio, portátiles y servidores tengan instalados y actualizados el software antivirus y sistemas de detección de código malicioso.
c) Instalar y/o mantener actualizados los parches de seguridad en todos los equipos de la universidad.
d) Establecer el procedimiento dirigido a los colaboradores respecto de sus obligaciones con la seguridad de la información tales como: no abrir archivos adjuntos sin asegurarse de que no sean maliciosos, no abrir enlaces dudosos en correos electrónicos, no visitar sitios web que puedan cargar virus, reportar sitios o contactos para que sean agregados en lista negra y/o restringidos en su uso, entre otros.
e) Elaborar políticas para minimizar el uso de medios extraíbles u otros dispositivos a las redes para evitar la introducción de virus.

12.3 COPIAS DE SEGURIDAD

Los propietarios de la información tienen la responsabilidad de:

a) Identificar la información que sea sensible en su área de acuerdo con su criticidad y coordinar con la Dirección de Informática la gestión de su respaldo periódico y su permanencia.

La Dirección de Informática tiene la responsabilidad de:

b) Elaborar y/o actualizar periódicamente, implementar y socializar la política de respaldos de la información.
c) Verificar la validez de las copias de seguridad a través de la ejecución de proceso de restauración simulados.
d) Asegurar que las copias de seguridad se encuentren en ubicaciones alternativas a las instalaciones donde se encuentren dispuestas, este sitio alternativo debe disponer de los controles de seguridad adecuados, así como las medidas de protección y seguridad física apropiadas.
e) Mantener registros de las copias de seguridad, así como de la comprobación de la validez de las mismas con base en la permanencia definida por el propietario de la información.

12.4 REGISTRO Y MONITOREO

La Dirección de Informática tiene la responsabilidad de:

a) Elaborar e implementar los procedimientos para que en caso de manejo de excepciones, fallos, eventos de seguridad de la información y actividad atípica en las bases de datos, dispositivos de red, servidores, aplicativos y cualquier componente de la infraestructura tecnológica con los que opera la universidad, se pueda disponer de un registro de la información reportada por los dispositivos, sistemas operativos o aplicaciones que permitan identificar al menos (usuario, intentos de acceso exitosos y fallidos, desconexiones del sistema, acciones ejecutadas, alertas por fallos en el sistema, fecha y hora en que se producen los eventos, tiempos de detención).
b) Monitorear el comportamiento de la red, base de datos, dispositivos de red, servidores y demás infraestructura con el objetivo de detectar oportunamente anomalías, mal uso de recursos y/o validar configuraciones.
c) Controlar que los administradores de sistema y/o aplicaciones no puedan borrar o desactivar el registro de sus propias actividades.
d) Sincronizar con una fuente común y exacta de tiempo todos los equipos de cómputo, sistemas, servidores, bases de datos y de comunicaciones que se encuentren en la red de la universidad.

12.5 CONTROL DEL SOFTWARE OPERACIONAL

La Dirección de Informática tiene la responsabilidad de:

a) Restringir la instalación de software, de modo que solo lo puedan realizar los colaboradores autorizados,
b) Valorar la necesidad de actualización o instalación del software institucional.
c) Comprobar la compatibilidad con el entorno antes de instalar software nuevo y/o actualizado.
d) Probar las nuevas aplicaciones y/o software en ambientes de pruebas.
e) Disponer la forma de volver a versiones anteriores en caso de requerirse.
f) Separar los entornos de desarrollo del ambiente operativo.
g) Establecer procedimientos y/o herramientas de monitoreo del software para detectar cambios no autorizados.
h) Monitorear la red posterior a la implementación de una instalación y/o cambio para identificar cualquier tráfico inesperado o cambio en el comportamiento habitual en la red.
i) Actualizar el catálogo de software institucional autorizado después de cualquier cambio y/o instalación.

12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

La Dirección de Informática tiene la responsabilidad de:

a) Elaborar, implementar y socializar una política de monitoreo continuo sobre los sistemas y/o aplicaciones en producción con el ánimo de detectar vulnerabilidades técnicas y adoptar las medidas necesarias para solucionarlas.
b) Realizar pruebas de ataques simulados.
c) Realizar escaneos periódicos de vulnerabilidades.

12.7 CONSIDERACIONES SOBRE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

La Dirección de Informática en conjunto con el área de Auditoría tiene la responsabilidad de:

a) Planificar y acordar las actividades de auditoría que impliquen comprobaciones en los sistemas para prevenir, evitar interrupciones en los procesos, así como facilitar la investigación respecto a posibles incidentes de seguridad de la información.
b) Asegurar que la persona que realiza la auditoría sea independiente de las actividades auditadas, solo otorgarle acceso de lectura.

13 SEGURIDAD EN LAS COMUNICACIONES

Introducción

- Establecer los controles adecuados para proteger el intercambio de información dentro y fuera de la organización a través de la protección de la información de las redes e infraestructura, monitoreo y registro de las actividades, restricción de permisos, definición de niveles de servicio.

Objetivos

- Asegurar la protección de la información en las redes de comunicaciones y sus instalaciones de soporte en el procesamiento de información.
- Mantener la seguridad de la información transferida a cualquier institución y/o entidad externa.

13.1 GESTIÓN DE LA SEGURIDAD DE REDES

Los propietarios de la información tienen la responsabilidad de:

a) Validar con la Dirección de Informática los controles requeridos para realizar transferencia de información a terceros.

La Dirección de Informática tiene la responsabilidad de:

b) Establecer las responsabilidades y los procedimientos para la administración de los equipos en la infraestructura de la red.
c) Evaluar y/o implementar la segregación de redes en distintos dominios para una mayor seguridad.
d) Definir la calidad de servicio - niveles de servicio (SLA) tanto para la prestación de servicios internos o con el apoyo de terceros.
e) Evaluar y/o implementar la autenticación de inicio de sesión para el uso de la red a través de múltiples factores.

13.2 TRANSFERENCIA DE INFORMACIÓN

Los propietarios de la información cuando realicen acuerdos entre instituciones para el intercambio de información y software, tiene la responsabilidad de:

a) Gestionar la firma de los acuerdos de confidencialidad y de no revelación de información cuando se requiera.
b) Especificar el grado de sensibilidad de la información involucrada y las consideraciones de seguridad sobre la misma, dentro de las cuales se deberá considerar al menos:
    - Procedimientos de notificación de emisión, transmisión, envío y recepción.
    - Trazabilidad de los datos.
    - Cumplimiento de normas técnicas y legales.
    - Responsabilidades y obligaciones en caso de pérdida de datos.
    - Controles especiales en caso de requerir protección (cifrado).
    - Términos y condiciones de la licencia bajo la cual se suministra el software.
    - Información sobre la propiedad de la información suministrada y las condiciones de su uso, y protección y custodia de la información.

La Asesoría Jurídica General es la responsable de:

c) Establecer y mantener actualizado el contenido de los acuerdos de confidencialidad y de no revelación de información para la firma de todos los colaboradores internos y externos, de acuerdo con las necesidades de la institución y las leyes vigentes.

El rector, su equivalente en las sedes o su delegado es el responsable de

d) Suscribir y custodiar los acuerdos de confidencialidad firmados.

14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA

Introducción

Este dominio define la aplicación de controles para la seguridad de la información al ciclo de vida completo de los sistemas de información (definición de requisitos, manejo de políticas de desarrollo seguro, protección uso datos de prueba, adecuada gestión de cambios tanto para sistemas propios como subcontratados, así como el establecimiento de controles que faciliten la integración, operación y mantenimiento de los nuevos sistemas con los actuales a través de una validación previa de cumplimiento de los estándares y compatibilidad con la infraestructura existente por parte de DI.

Objetivos

- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura base en la cual se apoyan.
- Asegurar la protección de los datos utilizados para las pruebas.

14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Para la adquisición, desarrollo y mantenimiento de hardware, software (propietario o libre) o soluciones tecnológicas, los propietarios de la información tienen la responsabilidad de:

a) Incluir el software o solución tecnológica requerido en el portafolio de proyectos y servicios del plan estratégico y operativo.
b) Solicitar el aval a la Dirección de Informática en función de los estándares definidos.
c) Identificar y priorizar los requerimientos funcionales y técnicos con la participación y aprobación formal de las áreas usuarias con base en las políticas institucionales. Esto incluye, tipos de colaboradores/perfiles, requerimientos de: entrada, definición de interfaces, almacenamiento, procesamiento, salida, controles, seguridades, plan de pruebas y pistas de auditoría de las transacciones en donde se aplique el registro de información.
d) Considerar mecanismos de autorización, integridad de la información, control de acceso, respaldos, auditoría y requerimientos de seguridad.

Además de lo descrito la Dirección de Informática las siguientes actividades:

e) Verificar que el software o solución tecnológica requerido por el propietario de la información conste dentro del portafolio de proyectos y servicios del plan estratégico y operativo aprobado.
f) Validar que los sistemas operativos, bases de datos, lenguajes, herramientas de programación, arquitectura, que contemplen la solución tecnológica requerida por el propietario de la información estén dentro de los estándares definidos por la Dirección de Informática de la universidad, los cuales deben tener una permanencia mínima y obsolescencia tanto de software como hardware con base en las garantías y soporte de los fabricantes.
g) Definir y controlar la permanencia mínima y obsolescencia tanto de software como hardware con base en las garantías y soporte de los fabricantes.
h) Diseñar e implementar los mecanismos de autorización, integridad de la información, control de acceso, respaldos, auditoría y requerimientos de seguridad requeridos por el propietario de la información y/o delegado.
i) Controlar que los derechos de autor del software desarrollado a la medida pertenecerán a la universidad, que el software adquirido cuenta con las licencias de uso, de igual para todos software o solución tecnológica adquirida por donación se deberá validar el licenciamiento. En todo caso, se estará a lo que dispone la normativa en propiedad intelectual, en materia de derecho de autor.
j) En caso de la participación de un tercero, debe existir la firma de acuerdo de confidencialidad.
k) Realizar el análisis previo a la compra, dentro del cual como mínimo se deberá considerar los siguientes aspectos:
    - **Análisis precio**: considerar costo inicial, de mantenimiento y consumibles por el período estimado de uso de los equipos.
    - **Análisis calidad**: considerar parámetros cualitativos que especifiquen las características técnicas de los recursos informáticos.
    - **Análisis experiencia**: presencia en el mercado, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.
    - **Análisis desarrollo tecnológico**: analizar grado de obsolescencia, nivel tecnológico con respecto a la oferta existente y la permanencia en el mercado.
    - **Análisis capacidad**: deberá satisfacer la demanda actual con un margen de holgura y capacidad de crecimiento.

En el caso de tratarse de adquisición de hardware se deberá considerar adicionalmente:

h) Consten en las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo.
i) Sean equipos integrados de fábrica o ensamblados con componentes previamente evaluados por la Dirección Informática, exclusivamente relacionado con equipos tecnológicos de su competencia.

j) Que la marca de los equipos o componentes cuenten con presencia y permanencia demostrada en el mercado nacional, así como con asistencia técnica y de repuestos local.
k) Para servidores, equipos de comunicaciones, concentradores, switches y otros equipos de operación crítica y/o de alto costo, deberán contar con un cronograma de mantenimiento preventivo y correctivo.
l) Para los computadores institucionales al finalizar su garantía de compra, deberán al menos tener servicio de mantenimiento preventivo.
m) En la adquisición de equipo de cómputo se deberá incluir el sistema operativo vigente precargado con su licencia correspondiente.

En la implementación, adquisición, desarrollo y/o instalación de hardware, software (propietario o libre) o soluciones tecnológicas, la Dirección de Informática tiene la responsabilidad de:

n) Incluir los procedimientos de configuración, aceptación y prueba (estándar o personalizadas). Los aspectos a considerar incluyen la validación frente a los términos contractuales, la arquitectura de información, interoperabilidad con las aplicaciones existentes y las bases de datos, eficiencia en el desempeño del sistema, documentación y manuales de usuario, integración y planes de prueba del sistema.
o) Formalizar en actas la aceptación por parte de los colaboradores, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.
p) Elaborar y/o entregar manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente.
q) Mantener registros adecuados de los activos de información "licencias" para proteger los derechos de propiedad intelectual.
r) Elaborar y/o actualizar periódicamente el catálogo (inventario) de software – aplicativos (desarrollo interno o por un tercero), con licencias, sistemas, infraestructura y estándares técnicos de la universidad.
s) Garantizar que las versiones de los aplicativos en producción correspondan al menos a las dos últimas versiones liberadas por el fabricante y que dispongan de soporte.

14.2 SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE

La Dirección de Informática tiene la responsabilidad de:

a) Garantizar el control de software en producción de modo que ningún programador acceda a realizar modificaciones en los ambientes de producción.
b) Asignar al personal competente para la correcta implementación o despliegue de aplicaciones en ambientes de producción. Así como también la implementación de modificaciones o nuevos programas en el ambiente de producción.

c) Validar que la solución tecnológica considere estándares internacionales para: desarrollo seguro, codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.
d) Vigilar la correcta aplicación del procedimiento de control de cambios.
e) Velar y garantizar el manejo y segregación adecuada de los ambientes de: desarrollo (configuración orientada al desarrollo de software, en el cual se puede crear y modificar los objetos), **pruebas** (configuración orientada a la generación de pruebas, replica del ambiente de producción en donde se realizarán todas las pruebas necesarias para garantizar el buen funcionamiento de los aplicativos) y **producción** (configuración orientada al usuario final donde se realiza el procesamiento real de la información utilizada para la toma de decisiones de la universidad).
f) Garantizar que en cada ambiente exista una configuración independiente (sistema operativo, base de datos y aplicación), así como que en cada ambiente se maneje credenciales de acceso diferentes.
g) Ejecutar procedimientos de copias de seguridad de la información con versiones anteriores del software instalado como medida de contingencia.

14.3 DATOS DE PRUEBA

La Dirección de Informática tiene la responsabilidad de:

a) Establecer controles y registros de auditoría, verificando:
   - La validación de datos de entrada: ejemplo asegurar la validez de los datos ingresados en el punto de entrada de los mismos, controlar parámetros de los sistemas, verificar negación de ingreso de datos (duales, fuera de rango, caracteres no válidos, datos incompletos o ausentes, formatos incorrectos, entre otros.), definición de estándar de respuesta ante errores de validación.
   - El procesamiento interno: ejemplo controles para protección contra ataques por desbordamiento/exceso en el buffer
   - La autenticación de mensajes (interfaces entre sistemas)
   - La validación de datos de salida.

b) Realizar pruebas de datos del sistema en coordinación con el propietario de la información, para lo cual como mínimo se considerará:
   - Realizar las pruebas sobre datos extraídos del ambiente de producción.
   - Prohibir el uso de bases de datos en producción.
   - Mantener registro de las copias de base de datos de producción a ambientes de prueba justificando para que se realiza la copia.
   - Eliminar inmediatamente las copias una vez completadas las pruebas.
   - La data de ambientes de pruebas y desarrollo deberá ser similar a la de producción.

15 RELACIONES CON PROVEEDORES

Introducción

- Este dominio da pautas para el manejo de relaciones con proveedores en los casos que impliquen acceso a los sistemas de información y/o activos de información.

Objetivos

- Asegurar la protección de los activos de la universidad que sean accesibles a los proveedores.
- Mantener un nivel acordado de seguridad de la información y la provisión de servicios en línea con los acuerdos con proveedores.

15.1 SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON LOS PROVEEDORES

Los propietarios de la información tienen la responsabilidad de:

a) Definir y coordinar en conjunto con la Dirección de Informática al menos los siguientes puntos:
   - El tipo de acceso requerido (físico/lógico y a qué recurso).
   - Los motivos para los cuales se solicita el acceso.
   - Los controles empleados por la tercera parte.
   - La incidencia de este acceso en la seguridad de la información.

b) Suscribir acuerdos de confidencialidad y controles aplicables al caso, restringiendo al mínimo necesario los permisos a otorgar a los contratistas o proveedores, lo mencionado para todo contrato que implique la prestación de servicios o adquisición de bienes.

c) Impedir el acceso a terceros a la información institucional, ni a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta que se suscriba el contrato o acuerdo en donde se defina las condiciones para la conexión o el acceso.

d) Incluir en los contratos con los proveedores o terceros los requisitos para enfrentar los riesgos de seguridad de la información relacionados con la tecnología, asociados con la cadena de suministros de los servicios y productos.

15.2 GESTIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR

La Dirección de Informática tiene la responsabilidad de:

a) Controlar, revisar y auditar regularmente con los administradores de contrato la provisión de servicios de índole tecnológico.
b) Mantener registros del monitoreo y revisión.
c) Reportar al administrador del contrato en caso de incidentes de seguridad de la información incurridos por parte del proveedor.
d) Incluir en las cláusulas de los contratos con los proveedores que cualquier equipo que se conecte a la red de la universidad previa autorización como mínimo disponga de software autorizado, uso de software con licencia.

16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Introducción

- En este dominio se define políticas para la gestión de incidentes de seguridad.

Objetivo

- Definir la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

16.1 GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS

Los propietarios, los custodios y los usuarios finales de la información tienen la responsabilidad de:

a) Reportar al jefe inmediato, así como al Oficial de Seguridad de la Información al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, o presunción de un incidente de seguridad de la información.
b) Omitir la realización de pruebas por sí mismo para detectar y/o utilizar una supuesta debilidad o falla de seguridad.
c) Implementar y cumplir la Normativa Procedimental para la Gestión de Incidentes de Seguridad de la Información de la PUCE dentro de su área de responsabilidad, así como participar en el tratamiento de los incidentes de seguridad de la información con el propósito de investigarlos y dar solución a los mismos.

El Oficial de Seguridad de la Información, será el responsable de:

d) Definir, socializar la Normativa Procedimental para la Gestión de Incidentes de Seguridad de la Información de la PUCE.

e) Actuar en la gestión de incidentes de seguridad con base en lo definido en la Normativa Procedimental para la Gestión de Incidentes de Seguridad de la Información de la PUCE.

La Dirección de Informática tiene la responsabilidad de:

f) Participar en la gestión de incidentes de seguridad con base en lo definido en la Normativa Procedimental para la Gestión de Incidentes de Seguridad de la Información de la PUCE.

g) Comunicar al Oficial de Seguridad de la información y actualizar periódicamente cualquier cambio en los insumos detallados en la Normativa Procedimental para la Gestión de Incidentes de Seguridad de la Información de la PUCE tales como: tabla tipo de incidentes y respuesta, listado de puertos, diagrama de red, listado de aplicativos, entre otros.

La Dirección General de Talento Humano tiene la responsabilidad de:

h) Aplicar procesos disciplinarios formales a los colaboradores en caso de participación directa o indirecta en incidentes de seguridad de la información.

17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DE LOS PROCESOS CLAVE DE LA UNIVERSIDAD.

Introducción

Este dominio define la importancia de disponer de un plan de continuidad como una herramienta para dar respuesta a la materialización de amenazas, de modo de implantar medidas de protección y de recuperación ante posibles desastres.

Objetivos

- Determinar las necesidades de seguridad de la información y de continuidad de la gestión de la misma en situaciones adversas.
- Asegurar la disponibilidad de las instalaciones de procesamiento de la información

17.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

El Oficial de Seguridad de la Información tiene la responsabilidad de:

a) Coordinar con las diferentes direcciones la identificación y priorización de los procesos críticos de la universidad.
b) Revisar y/o actualizar en coordinación con las demás unidades académicas y administrativas los documentos y aplicaciones relacionadas con la continuidad de los procesos clave de la universidad.
c) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad.

La Dirección de Informática tiene la responsabilidad de:

d) Contemplar dentro del PETI la gestión de la continuidad, en el cual se deberá al menos incluir:
    - Identificar los activos y actividades involucrados en los procesos críticos de la universidad en los cuales están implicados los servicios informáticos.
    - Objetivos y alcance del plan.
    - Condiciones para su puesta en marcha,
    - Funciones y responsabilidades.
    - Definir los planes y procedimientos de respuesta y recuperación que se activarán.
    - Procedimientos de cambios.
    - Evaluar la capacidad de respuesta ante desastres verificando los tiempos de respuesta, validez de los procedimientos y capacidad de los responsables.

e) Elaborar, implementar, socializar y disponibilizar el plan de continuidad de los servicios informáticos.
f) Revisar y actualizar periódicamente los planes de continuidad y procesos relacionados.
g) Revisar, identificar y actualizar eventos (amenazas) que puedan ocasionar interrupciones en los procesos de continuidad de los procesos clave de la universidad.
h) Revisar, identificar y actualizar controles preventivos.
i) Evaluar la capacidad de respuesta.
j) Ejecutar y probar la funcionalidad de los procesos, procedimientos y controles para la continuidad de los procesos clave de la universidad.

La Dirección de Talento Humano y la Dirección Administrativa son los responsables de:

k) Identificar, definir y actualizar los protocolos de manejo de personal y la seguridad del mismo en eventos que afecten la continuidad del negocio.

17.2 REDUNDANCIAS

La Dirección de Informática tiene la responsabilidad de:

a) Identificar los sistemas de información en los que se requiera garantizar la disponibilidad exigida por los procesos clave de la universidad sin un sistema de respaldo.
b) Asegurar la disponibilidad de las instalaciones de procesamiento de la información, el centro de datos debe cumplir un estándar de redundancia y seguridad que garantice la disponibilidad de la información y/o sistemas.
c) Realizar pruebas tanto de buen funcionamiento de los sistemas redundantes como de transición sin interrupciones de un sistema principal a un sistema redundante.

18 CUMPLIMIENTO

Introducción

Este dominio tiene la finalidad de enfatizar en la importancia de implementar controles para cumplir con la legislación respecto de la protección de datos personales, así como el valor de desarrollar los insumos legales para respaldar a la institución respecto del cumplimiento de la protección de la confidencialidad, integridad y disponibilidad de la información.

Objetivos

- Velar por el cumplimiento de las obligaciones legales, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad
- Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos de la universidad.

18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES

Los propietarios de la información tienen la responsabilidad de:

a) Asegurar la protección y privacidad de los datos personales de sus estudiantes, docentes, personal administrativo y de servicios, su almacenamiento, procesamiento y transmisión, con el fin de evitar posibles adulteraciones, pérdidas, consultas, usos o accesos no autorizados.
b) Asegurar que ninguna información que contenga datos personales sea transmitida sin la debida autorización expresa del responsable; y en caso de que se facilite

información a terceros se garantice el buen uso y tratamiento de acuerdo a la finalidad autorizada por parte el titular de los datos.

A más de las responsabilidades antes descritas, la Dirección de Informática debe:

c) Asegurar la no violación de derechos de copia.
d) Actualizar y/o mantener las licencias del software comprado.
e) Controlar e implementar controles para evitar sobrepasar el número máximo permitido de usuarios en los sistemas.
f) Velar y verificar periódicamente que sólo se instalen productos con licencia y software autorizado.
g) Asegurar el registro (constancia electrónica) de cada operación o actividad realizada por los colaboradores en los diferentes aplicativos institucionales o sistemas.

A más de las responsabilidades antes descritas, la Asesoría Jurídica General debe:

h) Definir, documentar, socializar y velar por el cumplimiento de los requisitos obligatorios en relación con leyes laborales, requisitos de seguridad relacionados con la seguridad de la información, derechos de propiedad intelectual y leyes de derechos de autor, privacidad, cifrado de datos y leyes de protección, pertinentes para cada sistema de información.
i) Velar por el cumplimiento de los sistemas de almacenamiento de datos y períodos de retención legal o normativo requeridos de acuerdo al tipo de información, entre ellos registros contables, registros de base de datos, registros de auditoría, entre otros, de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable dentro del ámbito legal y de justicia.
j) Crear y/o actualizar periódicamente los documentos de "Acuerdos de Confidencialidad", que deberán suscribir todos quienes tengan acceso a información institucional en especial la clasificada como confidencial – secreta de modo que se la use específicamente para lo cual está destinada, así como deberá especificar que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del subscriptor.
k) Desarrollar, implementar y socializar la política de protección y privacidad de la información, según dispone la normativa legal vigente.
l) Crear y/o actualizar los instrumentos legales de su competencia tales como contratos, acuerdos de confidencialidad y demás que permitan afianzan y apalancar el cumplimiento de los controles de seguridad de la información, así como proteger a la institución respecto de las acciones y/o sanciones que pueda realizar con el propósito de velar por sus activos de información.

A más de las responsabilidades antes descritas, la Secretaría General debe:

m) Crear y/o actualizar los instrumentos legales de su competencia tales como: reglamento interno de trabajo, de estudiantes, código de ética, y demás que permitan afianzan y apalancar el cumplimiento de los controles de seguridad de la información, así como proteger a la institución respecto de las acciones y/o sanciones que pueda realizar con el propósito de velar por sus activos de información.
n) Armonizar la normativa interna vigente de la universidad con relación a la seguridad de la información.

A más de las responsabilidades antes descritas, la Dirección de Talento Humano:

o) Definir, implementar y actualizar las funciones y responsabilidades de los colaboradores de la PUCE, de modo que en las mismas se incluya las atribuciones para poder dar cumplimiento con las actividades relacionadas con la seguridad de la información.

18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de seguridad de la información debe ser revisada al menos una vez al año, o cuando se produzcan cambios significativos en la institución, las revisiones deben ser realizadas por personal independiente al personal que es auditado.

Los propietarios de la información tienen la responsabilidad de:

a) Cumplir las regulaciones en materia de seguridad de la información, que sea aplicable a la universidad.
b) Mantener un adecuado registro de activos de información.
c) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, entre otros.
d) Determinar cómo revisar los requisitos de seguridad de la información definidos en las regulaciones en materia de seguridad de la información, que sea aplicable a la universidad.
e) Revisar periódicamente el cumplimiento del procesamiento de la información y que los procedimientos dentro de su área se realicen correctamente.
f) Facilitar los insumos acordados y requeridos para revisar el cumplimiento dentro del campo normativo de la seguridad de la información, y en caso de incumplimiento identificar las causas, definir e implementar las acciones necesarias para cumplir.

La Dirección de Talento Humano tiene la responsabilidad de:

g) Definir, socializar y aplicar las sanciones por incumplimiento de la Política de Seguridad de la Información de la PUCE, o por participar directa o indirectamente en eventos que comprometan la seguridad de la información de la PUCE.

h) Proceder con la firma y custodia de los acuerdos de confidencialidad de los colaboradores.

Finalmente, todo colaborador que no cumpla lo dispuesto en la presente Política de Seguridad de la Información de la PUCE será sancionado a través de la Dirección de Talento Humano conforme lo descrito en la normativa institucional y leyes vigentes sin perjuicio de las demás acciones de carácter legal que haya lugar.

19 DISPOSICIONES GENERALES

PRIMERA. - la presente política entrará en vigencia una vez que el Rector de la Pontificia Universidad Católica del Ecuador la apruebe y derogará cualquier disposición de igual o menor jerarquía que se hayan emitido con anterioridad en la matriz o sedes, para su posterior difusión conforme lo prevé la normativa vigente y aplicable de la institución.

SEGUNDA. - encargar la codificación y difusión de la presente política a la Secretaría General de la PUCE.

TERCERA. - la Pontificia Universidad Católica del Ecuador a través de las distintas unidades académicas y/o administrativas dentro de su ámbito de competencia y en coordinación con la Dirección de Aseguramiento de la Calidad a través de la Oficina de Seguridad de la Información, instrumentarán la **normativa secundaria necesaria para el cumplimiento de la presente norma**, con el propósito de asegurar su correcta implementación y despliegue.

CUARTA: La Dirección General de Talento Humano será responsable de: gestionar la suscripción del acuerdo de confidencialidad y no-divulgación de todos los colaboradores vinculados actualmente a la universidad de modo de garantizar que todos cuenten en su expediente con la copia firmada del mencionado acuerdo en un plazo no mayor a ciento ochenta días.