Pontificia Universidad Católica del Ecuador

Seréis mis testigos

Política General de Seguridad de la Información de la PUCE

31 de enero de 2025

Versión 02.01

CONTENIDO

EL CONSEJO SUPERIOR DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

CONSIDERANDO

Que la Constitución de la República del Ecuador, en su artículo 18, numeral 1 señala que*: "Todas las personas, en forma individual o colectiva, tienen derecho a*:

1. *Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior"*

Que en el artículo 66 de la Constitución de la República se reconoce y garantiza a las personas, entre otros derechos: "(…) 19. *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 (…)"*.

Que en el artículo 92 de la Constitución de la República, en su parte pertinente contempla*: "… 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".*

Que 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 privado".*

Que el artículo 16 literal b) del Estatuto de la PUCE confiere al Consejo Superior la atribución de aprobar las políticas generales de la universidad, reformarlas e interpretarlas de manera auténtica;

Que el literal b) del artículo 4 del Reglamento Específico para la Administración de la Documentación Normativa Interna de la PUCE establece que una política general constituye un "*Conjunto de orientaciones que brindan coherencia a la acción de la universidad para la consecución de su misión, visión y funciones sustantivas. El Consejo Superior es el órgano competente para su aprobación, reforma e interpretación."*

Que el Código de Ética de la PUCE en su capítulo III Comportamientos éticos a seguir, en la sección 3, en los artículos 41 al 49 y del 52 al 59 contempla los Comportamientos de los miembros de la comunidad universitaria.

Que el Código de Ética de la PUCE en el capítulo III Comportamientos éticos a seguir en la sección 4: en los artículos 64 al 67 menciona los Comportamientos de los miembros de la comunidad universitaria en sus relaciones mutuas, con otros beneficiarios y con la sociedad en general.

En ejercicio de sus deberes y atribuciones establecidos en el Estatuto de la PUCE, emite la siguiente:

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA PUCE

CAPÍTULO I. PROPÓSITO

Artículo 1.- Propósito de la Política General de Seguridad de la Información:

La Pontificia Universidad Católica del Ecuador identifica 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 salvaguardándola del 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.

CAPÍTULO II. OBJETIVOS

Artículo 2.- Objetivos de Seguridad de la Información

- Proteger y mantener la disponibilidad, integridad, confidencialidad de los activos de información y las tecnologías asociadas a 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 miembros de la comunidad universitaria.
- Establecer lineamientos, normativas y procedimientos relacionados con la seguridad de la información.
- Monitorear la implementación del Sistema de Gestión de Seguridad de la Información y promover la mejora continua para adaptarse a los nuevos riesgos y cambios tecnológicos.
- Socializar la política de seguridad de la información con todos los miembros de la comunidad universitaria.

CAPÍTULO III. COMPROMISO

Artículo 3.- Compromiso de la alta dirección

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 con 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 la cultura de seguridad de la información.
- Asegurar los recursos requeridos para implementar y mantener la política 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 que se definan.

La administración de la Seguridad de la Información de la Pontificia Universidad Católica del Ecuador está basada en los estándares de la Norma 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.

La política de seguridad de la información define 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.

CAPÍTULO IV. MEJORA CONTINUA

Artículo 4.- Mejora continua de la Política General 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.

CAPÍTULO V. ORGANIZACIÓN

Artículo 5.- Controles Organizacionales

5.1 Políticas para la seguridad de la información

La presente Política General de Seguridad de la Información deberá ser aprobada por el Consejo Superior de la PUCE, posterior tiene que ser publicada en la intranet para conocimiento y cumplimiento de todo el personal y las partes interesadas.

5.2 Roles y responsabilidades en 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, para lo cual se tiene:

COMITÉ NACIONAL DE SEGURIDAD DE LA INFORMACIÓN. – este comité estará conformado por:

- Rector o su delegado, quién lo presidirá.
- Responsable nacional de la unidad encargada de la docencia y estudiantes o su delegado.
- Responsable nacional de la unidad encargada de la investigación, vinculación e innovación o su delegado.
- Responsable nacional de la unidad encargada de la educación en línea.
- Responsables nacionales de las unidades encargadas del desarrollo organizacional y finanzas o sus delegados.
- Responsable nacional de la unidad encargada de tecnología o su delegado.
- Responsable nacional de la unidad encargada de la asesoría jurídica o su delegado.
- Responsable nacional de la Secretaría General o su delegado.
- Responsable nacional de la unidad encargada de la comunicación o su delegado.
- Responsable nacional de la unidad encargada de la seguridad de la información, quién actuará como secretario de la comisión.

Los comités locales en las sedes deberán ser conformados por los representantes de las distintas áreas enunciadas o equivalentes en estas, lo cual deberá ser informado al responsable nacional de la unidad encargada de seguridad de la información.

En aras de la eficiencia administrativa el Comité Nacional de Seguridad de la Información de la PUCE funcionará a la vez como el Comité Local de la Sede Quito.

Tanto el Comité Nacional de Seguridad de la Información de la PUCE, como los comités locales, sesionarán semestralmente de forma ordinaria y extraordinaria cuando sea convocado por el responsable nacional o local de la unidad encargada de la seguridad de la información en las sedes, según corresponda, para lo cual serán convocados a través del correo institucional con 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 presentes, sin embargo, siempre deberán al menos estar presentes el responsable encargado del área de tecnología o su delegado, el Rector/Prorrector o su delegado, así como el responsable nacional encargado de la seguridad de la información o los responsables locales encargados de la seguridad de la información o su delegado según corresponda.

El presidente del comité tendrá voto dirimente. En cada sesión el secretario elaborará el acta respectiva la cual es objeto de aprobación por cada uno de los asistentes, quienes deberán enviar sus observaciones y aceptación dentro de un plazo máximo de dos días laborables a partir de la recepción de esta.

El Comité Nacional de Seguridad de la Información tiene las siguientes responsabilidades:

a) Garantizar que la normativa y estrategias estén alineadas con las necesidades y objetivos de la institución.
b) Proponer, evaluar y priorizar la ejecución de planes de acción relacionados con la seguridad de la información a nivel nacional.
c) Proponer, analizar y validar ajustes requeridos en la PGSI.
d) Evaluar el impacto y definir el nivel de riesgo que se asume y la estrategia a adoptar ante riesgos institucionales.
e) Recomendar, orientar y tomar decisiones ante amenazas al sistema de gestión de seguridad de la información.
f) Promover la mejora de seguridad de la información en la institución.
g) Verificar el cumplimiento de las obligaciones legales, regulatorias y normativas relacionadas con 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.

Los comités locales de Seguridad de la Información tienen las siguientes responsabilidades:

a) Supervisar el Sistema de Gestión de Seguridad de la Información.
b) Evaluar y proponer al rector o su equivalente en las sedes, la implementación de planes, programas o proyectos locales relacionados con la SI.
c) Orientar y tomar decisiones ante amenazas al programa de seguridad de la información.
d) Verificar el cumplimiento de las obligaciones legales, regulatorias y normativas relacionadas con la seguridad de la información.
e) Promover la difusión y sensibilización de la seguridad de la información dentro de la institución y velar por su cumplimiento.
f) Analizar, evaluar el impacto y definir la estrategia a adoptar ante riesgos locales.
g) Promover la mejora de seguridad de la información en la institución.
h) Dar seguimiento al cierre de los incidentes de seguridad de la información y aplicación de sanciones si fuera el caso.

RESPONSABLE NACIONAL DEL ÁREA DE SEGURIDAD DE LA INFORMACIÓN.

El responsable nacional de la unidad encargada de la seguridad de la información tiene las siguientes responsabilidades:

a) Analizar y proponer al Comité Nacional de Seguridad de la Información la creación, modificación y eliminación de políticas, planes, programas, proyectos, procesos, procedimientos, controles relacionados con la SI.
b) Implementar y mantener el Sistema de Gestión de Seguridad de la Información, el cumplimiento de las políticas de seguridad de la información establecidas en la institución, las normativas, procedimientos y estándares que la soportan.
c) Establecer las estrategias para difundir las políticas y directrices de seguridad de la información.
d) 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.
e) 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 estos.
f) 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.
g) 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.

h) Definir y articular las estrategias de capacitación para el personal, en materia de seguridad de la información, en coordinación con el área responsable del talento humano, así como coordinar las acciones requeridas impulsar la implementación y cumplimiento de la PGSI.
i) Monitorear y reportar los avances a nivel nacional respecto de la Implementación Sistema de Gestión de Seguridad de la Información.

RESPONSABLE LOCAL DEL ÁREA DE SEGURIDAD DE LA INFORMACIÓN

El responsable local de la unidad encargada de la seguridad de la información tiene las siguientes responsabilidades:

a) Proponer al responsable nacional de la unidad encargada de la seguridad de la información la creación, modificación y eliminación de políticas, planes, programas, lineamientos o proyectos relacionados con la SI.
b) Apoyar en la implementación local de procesos, procedimientos, controles y políticas para gestionar la seguridad de la información institucional.
c) Socializar las políticas y directrices de seguridad de la información.
d) Actualizar periódicamente el inventario de activos de Información local.
e) Dar seguimiento a la evaluación de riesgos y ejecución de los planes de tratamiento planteados para la administración de estos.
f) Articular la respuesta oportuna a los incidentes de seguridad de la información.
g) Reportar el avance local respecto de la Implementación Sistema de Gestión de Seguridad de la Información

RESPONSABLE NACIONAL DEL ÁREA DE TECNOLOGÍA

El responsable nacional del área de tecnología en el ámbito de seguridad de la información tiene las siguientes responsabilidades:

a) Establecer, mantener y difundir políticas, procedimientos de los servicios de tecnología en concordancia con el cumplimiento de la normativa de seguridad de la información.
b) Mantener la custodia de la información que reposa en los diferentes sistemas, bases de datos y aplicativos de la institución que son administrados desde la sede Quito.
c) Definir y documentar controles nacionales para la detección y prevención de accesos no autorizados, protección contra software malicioso, seguridad de los datos institucionales y servicios conectados a la red.
d) Evaluar el impacto operativo a nivel de seguridad, respecto de la implementación de cambios en sistemas, servicios y equipamiento implementado a nivel nacional.
e) Gestionar los incidentes de seguridad de la información, dentro de sus competencias, en articulación con el responsable de seguridad de la información.

f) Proporcionar las medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la institución.
g) Analizar, comunicar e implementar o fortalecer los controles de seguridad identificados y aprobados a partir de la ocurrencia de un evento o incidentes ya sea por brechas, fallos de funcionamiento o por una inadecuada gestión de cambios.
h) Supervisar el cumplimiento de normativas de seguridad de la información incluyendo la protección de datos, especialmente en entornos que se comparte o gestiona información entre sedes.
i) Realizar monitoreo permanente de la red y responder oportunamente a incidentes de ciberseguridad que puedan comprometer la información digital de la institución.
j) Evaluar y supervisar los servicios y proveedores externos (como servicios en la nube, servicios on premise, entre otros) para asegurar que cumplan con los estándares de seguridad de la institución.
k) Asegurar que los acuerdos (SLAs) con terceros incluyan compromisos específicos de seguridad de la información incluidos la protección de datos personales.
l) Realizar auditorías periódicas en plataformas y sistemas críticos para evaluar el nivel de seguridad y asegurar el cumplimiento de las políticas.

RESPONSABLE LOCAL DEL ÁREA DE TECNOLOGÍA

El responsable local del área de tecnología en el ámbito de seguridad de la información tiene las siguientes responsabilidades:

a) Aplicar, mantener y difundir políticas, procedimientos y manuales de operación y mantenimiento de los servicios de tecnología en concordancia con el cumplimiento de la presente política.
b) Mantener la custodia de la información que reposa en los diferentes sistemas, bases de datos y aplicativos de la institución.
c) Informar de los eventos o incidentes al responsable local de seguridad de la información.
d) Definir y documentar controles locales para la detección y prevención de accesos no autorizados, protección contra software malicioso, seguridad de los datos institucionales y servicios conectados a la red.
m) Identificar los incidentes de seguridad de la información a nivel local en articulación con el responsable de seguridad de la información.
e) Evaluar el impacto operativo a nivel de seguridad respecto de la implementación de cambios en sistemas/servicios y equipamiento.
f) Proveer de los recursos necesarios para permitir la segregación de los ambientes de procesamiento.
g) Monitorear las capacidades de la infraestructura y sistemas en operación para proyectar futuras demandas y soportar amenazas de seguridad de la información.
h) Mantener y supervisar los procesos de respaldo de la información institucional.
i) Gestionar los incidentes de seguridad de la información en articulación con el responsable local de seguridad de la información.

j) Proporcionar las medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la institución.
k) Definir procedimientos para solicitar el acceso remoto bajo las justificaciones pertinentes.
l) Mantener un registro actualizado de los accesos / retiros autorizados para uso de acceso remoto.
m) Garantizar el acceso remoto a los sistemas internos de la universidad a través de tecnologías seguras.
n) Enviar al responsable local de seguridad de la información de forma mensual el listado de usuarios con conexiones remotas activas.
o) Enviar al responsable local de seguridad de la información de forma mensual, el 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).
p) Facilitar al responsable local de seguridad de la información cuando requiera soporte de solicitud de acceso remoto realizada por el usuario.
q) Auditar y supervisar cuando haya sospecha de actividades no autorizadas que impliquen el tratamiento de información confidencial o restringida en condiciones habilitadas para ejecución de teletrabajo.
r) Coordinar con el responsable nacional de tecnología y con el responsable nacional de SI para activar el protocolo de respuesta ante incidentes cuando sea necesario.
s) Analizar, comunicar e implementar o fortalecer los controles de seguridad y sus protocolos a partir de la ocurrencia de un evento o incidentes ya sea por brechas, fallos de funcionamiento o por una inadecuada gestión de cambios.
t) Realizar simulaciones controladas de seguridad en acompañamiento con el responsable local de seguridad de la información.
u) Enviar al responsable local de seguridad de la información de forma mensual, el listado de usuarios activos de los diferentes aplicativos y servicios, incluyendo cuentas genéricas y administradores.
v) Asegurar la disponibilidad de un plan de recuperación ante desastres que permita restablecer la operatividad de los sistemas locales en caso de pérdida de datos o fallo de sistema/servicio.
w) Evaluar los riesgos de seguridad asociados a los servicios de terceros y proveedores utilizados en la sede, asegurando que cumplan con los estándares de seguridad de la institución.
x) Asegurar que los acuerdos de confidencialidad y privacidad estén en vigor y que los proveedores externos tengan controles de seguridad adecuados.
y) Reportar de forma periódica al responsable nacional de seguridad de la información sobre el estado de la seguridad en el campus, incluyendo avances y necesidades de mejora.

RESPONSABLE DEL ÁREA DE TALENTO HUMANO:

El responsable local del área de talento humano en el ámbito de seguridad de la información tiene las siguientes responsabilidades:

a) Establecer controles en sus procesos de selección del personal para verificar los antecedentes, los mismos que deberán considerar la sensibilidad de la información a la que tendrá acceso, así como a los riesgos asociados al desempeño del cargo.
b) Incluir dentro de los acuerdos contractuales de empleo las responsabilidades del personal con relación a la seguridad de la información.
c) 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 la que pertenece el colaborador.
d) Enviar a las áreas responsables de Tecnología y Educación Virtual, la notificación de ingreso de personal, así como de cambios o promociones de los colaboradores para que se proceda con la asignación de accesos o actualizaciones de estos sobre los activos de información y a los servicios de procesamiento de la información.
e) Validar la información insumo para cualquier sistema/servicio que esté relacionado con nómina.
f) Enviar mensualmente al responsable de seguridad de la información, el reporte de los colaboradores en estado activo.
g) Incluir como parte de la inducción al personal nuevo, 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).
h) Incluir en el plan de capacitación anual programas orientados a fortalecer la cultura de seguridad de la información en coordinación con el responsable del área de seguridad de la información.
i) 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.
j) Comunicar las responsabilidades legales subsistentes con respecto al manejo de la información una vez terminada la relación laboral con la universidad.
k) Incluir dentro de los instrumentos empleados para la aplicación de la normativa de talento humano, el que se realice la transferencia de la documentación e información de la persona a cargo o responsable de la misma, en caso de cese de funciones o cambio de puesto o unidad, al nuevo colaborador a cargo; o 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.

l) Informar, de ser necesario, a los colaboradores sobre los cambios de personal y los acuerdos de funcionamiento con el fin de precautelar accesos no autorizados.
m) Enviar a las áreas responsables de Tecnología y de Educación Virtual o quienes 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 se proceda a retirar oportunamente los privilegios de acceso a los activos de información y a los servicios de procesamiento de la información.
n) Enviar mensualmente al responsable local de seguridad de la información el reporte de colaboradores desvinculados.
o) 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.
p) Custodiar el documento firmado donde el colaborador se compromete a cumplir las cláusulas de confidencialidad para proteger la información institucional.

RESPONSABLE DEL ÁREA ENCARGADA DE LA GESTIÓN ADMINISTRATIVA

El responsable local del área encargada de la gestión administrativa en el ámbito de seguridad de la información tiene las siguientes responsabilidades:

a) Definir y actualizar periódicamente las áreas seguras en la institución.
b) Definir e implementar controles de acceso, vigilancia, monitoreo y protección contra amenazas físicas y ambientales en las áreas seguras en la institución.
c) Revisar periódicamente el funcionamiento de los controles de acceso, vigilancia, monitoreo y de protección contra amenazas físicas y ambientales implementados para confirmar su funcionamiento normal.
d) Corregir en caso de mal funcionamiento de los controles de acceso, vigilancia, monitoreo y de protección contra amenazas físicas y ambientales implementados.
e) Establecer y realizar mantenimientos periódicos a los distintos controles de acceso, vigilancia, monitoreo y de protección contra amenazas físicas y ambientales implementados.
f) Establecer controles en sus procesos de selección de proveedores para verificar los antecedentes, los mismos que deberán considerar la sensibilidad de la información a la que tendrá acceso, así como los riesgos asociados al producto o servicio que prestará.

PROPIETARIOS DE LA INFORMACIÓN

Los niveles organizacionales de los propietarios de la información son: Rector, los Prorrectores de las Sedes, Vicerrectores, 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:

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.

a) Asegurar que el inventario de los activos de información de los procesos a su cargo sea actualizado.
b) Valorar, clasificar y proteger por la información que está bajo su administración.
c) Definir el tiempo de retención de la información bajo su administración.
d) Definir, autorizar, restringir los permisos a los usuarios a la información que está bajo su administración con base en los roles y responsabilidades.
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) 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 los responsables de las unidades encargadas de: seguridad de la información, tecnología.
g) Promover la capacitación y concienciación sobre la importancia de la seguridad de la información.
h) Velar por la identificación y evaluación periódica de los riesgos a los cuáles se encuentran expuestos los activos de información bajo su administración y comunicar al responsable de seguridad de la información cualquier cambio o mejora requerida.
i) Definir y asegurar la implementación de los controles necesarios para proteger los activos de información de acuerdo con los niveles de clasificación establecidos y el nivel de seguridad requerido, así como, validar la operación y efectividad de los controles definidos.
j) Comunicar las novedades de personal (ingresos, movimientos internos y salidas) a la unidad encargada del 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.
k) Participar en evaluaciones y auditorías de seguridad para identificar áreas de mejora.
l) Velar por el cierre de las brechas y hallazgos identificados en auditorias y pruebas de seguridad de la información.
m) Comunicar al responsable de seguridad de la información, la necesidad de asesoramiento sobre seguridad de la información del personal a su cargo.

CUSTODIOS DE LA INFORMACIÓN

Se constituyen los docentes, personal administrativo, de servicios, becarios, proveedores, contratistas, o personas a los cuales el propietario de la información le otorga el acceso y la custodia sobre una activo de información que usa para el desempeño de su rol o funciones. Sus responsabilidades con relación a 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.

USUARIOS FINALES

Los niveles organizacionales de los usuarios finales son: estudiantes, entidades gubernamentales, terceras partes, u otras personas autorizadas para utilizar la información de la universidad.

RESPONSABILIDADES EN COMÚN DE LOS DIFERENTES ROLES DE SEGURIDAD DE LA INFORMACIÓN

A continuación, constan las responsabilidades que cualquier miembro de la comunidad universitaria tiene dentro del ámbito de seguridad de la información, lo mencionado independiente del rol de seguridad de la información que desempeñe en la universidad, estas son:

a) Aceptar, comprender y aplicar las políticas, normativas, procedimientos, controles y estándares relacionados con la seguridad de la información establecidos en la institución.
b) Utilizar la información y los recursos informáticos institucionales de forma ética, responsable y exclusivamente para los propósitos autorizados.
c) Mantener la confidencialidad y reserva de la información sensible de la universidad.
d) No compartir credenciales, contraseñas, tarjetas de acceso u otras credenciales que permitan el acceso a la información o a los sistemas/servicios de la universidad.
e) No divulgar la información confidencial o sensible a terceros no autorizados.
f) No utilizar la información para fines personales, comerciales o en actividades ajenas a las de la universidad.
g) Identificar y comunicar los riesgos a los cuáles se encuentran expuestos los activos de información a su cargo y gestionar la implementación de los controles necesarios para protegerlos.
h) 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.
i) Mantener registros respecto del acceso a la información bajo su custodia cuando aplique de acuerdo con su nivel de clasificación.
j) Reportar los incidentes de SI al jefe inmediato y al responsable de seguridad de la información.
k) Participar y colaborar en la resolución de incidentes de seguridad cuando se lo requiera.

5.3 Segregación de tareas

El área responsable del talento humano tiene que:

Definir y socializar el manual de funciones, con base en el cual se deberá realizar la asignación de responsabilidades al personal, estableciendo diferentes responsables para las funciones de elaboración, revisión y aprobación, en este sentido ningún colaborador deberá estar facultado para realizar por sí mismo todas las etapas.

El área responsable de seguridad de la información

Velar porque en la institución estén definidas las responsabilidades en lo que corresponde a seguridad de la información de todos los involucrados con la institución.

5.4 Responsabilidades de la dirección

CONSEJO SUPERIOR DE LA PUCE

Conforme lo establecido en el estatuto de la PUCE, el Consejo Superior será el encargado de aprobar las políticas generales, reformarlas e interpretarlas de manera auténtica.

RECTOR Y PRORRECTORES DE LA PUCE

El rector y prorrectores tienen las siguientes responsabilidades:

a) Definir la dirección del uso de los activos de información de la universidad a nivel nacional o en las sedes según corresponda.
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 los Comités nacional y locales de SI correspondientes.
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 incidentes de severidad ALTA relativos a la seguridad de la información y dar seguimiento a su solución.
f) Facilitar y promover el desarrollo de iniciativas sobre seguridad de la Información.
g) 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 *"Lineamiento de Estructuración de la Documentación Normativa Interna".*
h) Impulsar y fomentar una cultura de concienciación sobre la seguridad de la información en toda la institución.

5.5 Contacto con las autoridades

El responsable de seguridad de la información reportará a las autoridades de la institución, los incidentes de seguridad de la información considerados de severidad ALTA, con base en lo definido en la normativa institucional correspondiente.

5.6 Contactos con grupos de interés especial

Con el propósito de intercambiar experiencias, obtener asesoramiento sobre la aplicación de las mejores prácticas y controles de seguridad, el responsable de seguridad de la información podrá 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.

5.7 Inteligencia de amenazas

El área responsable de seguridad de la información tiene que:

a) Definir mecanismos que faciliten las acciones informadas, para evitar que las amenazas causen daño a la entidad y reducir su impacto.
b) Evaluar y verificar la información sobre inteligencia de amenazas para aplicarla en la institución, con el fin de prevenir y mitigar posibles amenazas.

5.8 Seguridad de la información en la gestión de proyectos

El área responsable de seguridad de la información tiene que:

Realizar el seguimiento a las áreas que gestionan proyectos para que incluyan en el perfil, la sección de gestión de riesgos de seguridad de la información.

5.9 Inventario de información y otros activos asociados

El área responsable de la gestión administrativa tiene que:

a) Documentar y actualizar el inventario de activos conforme se realicen las adquisiciones, movimientos y dadas de baja de los activos, lo mencionado correspondiente a los activos tecnológicos (tales como: computadores, servidores, equipo de infraestructura tecnológica, entre otros), equipo eléctrico, de comunicaciones, de seguridad física, entre otros que permitan la operación de la institución.
b) Documentar y actualizar el inventario de activos en congruencia con las vinculaciones, movimientos y desvinculaciones de personal, para lo cual deberá articular con el área responsable del talento humano.

El área responsable de tecnología tiene que:

Inventariar y mantener actualizado 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.

El área responsable de seguridad de la información tiene que:

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

5.10 Uso aceptable de la información y activos asociados

El área responsable de comunicación tiene que:

Definir la identidad gráfica institucional (logos – formatos institucionales) para el uso en los documentos oficiales de la institución.

El área responsable de tecnología tiene que:

a) Limitar el acceso a los miembros de la comunidad universitaria 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, o en atención a solicitud del Comité Nacional o Local de Seguridad de la Información según corresponda.
b) Mantener la premisa de *"Todo acceso se encuentra prohibido, a no ser que se permita expresamente"*.

5.11 Devolución de activos

El área responsable del talento humano tiene que:

Incluir dentro de los instrumentos empleados en el proceso de desvinculación del personal, la devolución de todo activo físico o digital que sea propiedad de la universidad o esté bajo su custodia, incluido el carnet de acceso a las instalaciones.

El área responsable de tecnología tiene que:

Asegurar que dentro de sus procesos cuando un colaborador se desvincule de la universidad, realice la devolución de todo bien tecnológico que sea de propiedad de la universidad.

El área responsable de la gestión administrativa tiene que:

a) Controlar que los miembros de la comunidad universitaria que hayan tenido bajo su custodia algún bien, realicen la devolución de este.
b) Actualizar el inventario de bienes con base en el cumplimiento del literal a).

5.12 Clasificación de la información

El área responsable de seguridad de la información tiene que:

Definir y controlar que la información institucional tanto digital como física sea clasificada en relación con su valor, normativa legal vigente, sensibilidad y criticidad para la universidad, con base en la Metodología para la Gestión de Riesgos de Seguridad de la Información de la PUCE.

5.13 Etiquetado de la información

El área responsable de seguridad de la información tiene que:

a) Definir con el área responsable de tecnología, la herramienta tecnológica para aplicar el etiquetamiento de la información digital.
b) Definir los mecanismos para aplicar el etiquetamiento de la información física.
c) Definir y controlar que la información institucional tanto digital como física sea etiquetada con base en la clasificación del numeral 5.12.

5.14 Transferencia de la Información

El área responsable de asesoría jurídica tiene que:

a) Establecer y mantener actualizado el contenido de los acuerdos de confidencialidad y de no revelación de información para la firma de todos los miembros de la comunidad universitaria (internos y externos) de acuerdo con las necesidades de la institución y las leyes vigentes.
b) Definir, actualizar y socializar los instrumentos a través de los cuales se debe realizar la transferencia de información en cumplimiento con las leyes aplicables.

El rector, prorrector o su delegado tiene que:

a) Suscribir los acuerdos de confidencialidad firmados.
b) Designar la autoridad para la firma los instrumentos definidos por la institución a través de los cuales se deba realizar la transferencia de información, en el caso de requerirse.

5.15 Control de acceso

El área responsable de la gestión administrativa tiene que:

a) Definir los procedimientos para la gestión de acceso físico de los usuarios a las instalaciones y áreas seguras definidas.
b) Mantener actualizado el reporte de accesos a instalaciones y áreas seguras.
c) Mantener actualizado el reporte de usuarios con acceso autorizado a las áreas seguras.
d) Revisar periódicamente el cumplimiento de los procedimientos para la gestión acceso físico de los usuarios a las instalaciones y áreas seguras definidas.

El área responsable del talento humano tiene que:

a) Garantizar que, previo a solicitar al área responsable de tecnología la creación de las credenciales de acceso de cualquier miembro de la comunidad universitaria, éste haya firmado las cláusulas de confidencialidad.
b) Notificar al área responsable de tecnología 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.

El área responsable de tecnología tiene que:

a) Definir los procedimientos para la gestión de acceso de los usuarios a aplicaciones, servicios, sistemas, bases de datos, servicios de información, accesos remotos, redes y servicios de red.
b) Mantener actualizado el reporte de computadores o dispositivos electrónicos que tengan accesos a la red de datos de la universidad.
c) Mantener actualizado el reporte de usuarios con acceso autorizado.
d) Mantener registro de la gestión de acceso de los usuarios a aplicaciones, servicios, redes, sistemas, bases de datos, servicios de información, accesos remotos, redes y servicios de red, de modo que se evidencie: fecha de creación, eliminación, suspensión, activación, cambios o eliminación según corresponda.
e) Revisar periódicamente el cumplimiento de los procedimientos para la gestión de accesos y uso de los sistemas, bases de datos, servicios de información, accesos remotos, redes y servicios de red, así como el acceso físico a instalaciones críticas a su cargo.
f) Controlar que la creación de cualquier cuenta genérica (proveedores, terceros u otros) sea solicitada y autorizada por el responsable del área requirente, quien a su vez definirá el colaborador de la universidad que actuará como custodio de esta.
g) Controlar el acceso físico a las instalaciones de procesamiento de la información e infraestructura tecnológica.

El área responsable de seguridad de la información tiene que:

a) Verificar el cumplimiento de lo establecido para el control de accesos (registro de colaboradores, administración de contraseñas, utilización de servicios de red, autenticación de colaboradores) con base en la información de monitoreo proporcionada por el área responsable de tecnología.
b) Revisar periódicamente los derechos de acceso.
c) Concientizar a los miembros de la comunidad universitaria sobre las políticas de gestión de accesos.

5.16 Gestión de identidad

El área responsable de la gestión administrativa tiene que:

a) Definir, implementar y controlar los mecanismos para asignar una identificación única a las personas que accedan a las instalaciones de la universidad, garantizando que los accesos sean asignados según las funciones y necesidades de cada usuario.
b) Desactivar o eliminar oportunamente las identidades que ya no son necesarias (ejemplo: colaboradores desvinculados).

El área responsable de tecnología tiene que:

a) Establecer los controles necesarios, la configuración para el ingreso a la red y definir los procedimientos respectivos para proteger el acceso a las conexiones de red y a los servicios de la red, en los cuales como mínimo se considerará la forma de 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.
b) Incluir en los procedimientos de gestión de accesos la creación de cuentas genéricas para el uso de proveedores, terceros u otros, en el cual como mínimo se deberá establecer que la creación sea solicitada por el responsable del área requirente, quien deberá definir que colaborador de la universidad actuará como custodio de esta.
c) Restringir el uso de los servicios de la red cuando no se cumpla con labores propias de la universidad.

5.17 Información de autenticación

El área responsable de tecnología tiene que:

Definir, documentar, implementar y revisar periódicamente el cumplimiento de los procedimientos para la gestión de accesos y 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 privilegios.

El área responsable de seguridad de la información tiene que:

Revisar el cumplimiento de las políticas y lineamientos emitidos por las áreas responsables de seguridad de la información y de tecnología, respecto del uso de la información de autenticación.

5.18 Derechos de acceso

El área responsable del talento humano tiene que:

Notificar a las áreas encargadas de tecnología, educación virtual y seguridad de la información, el ingreso de personal, cambios de unidad, de puesto de trabajo, encargos de puestos, promociones, cambios de categoría, licencias, y desvinculaciones para que procedan con la asignación de accesos, actualizaciones o retiro de estos a los activos de información y a los servicios de procesamiento de la información, lo mencionado se debe realizar el mismo día en el que ocurra el evento con base en la solicitud y autorización del responsable correspondiente.

El área responsable de tecnología tiene que:

a) Definir los procedimientos para la creación y entrega de claves de acceso a los sistemas, en el cual, al menos incluir la generación de claves de forma aleatoria, robusta y qué fuerce el cambio de esta en su primer ingreso.
b) Establecer lineamientos en dónde consten las características mínimas que los miembros de la comunidad universitaria deberán considerar al momento de cambiar sus claves, tales como complejidad, tiempo de caducidad, histórico de claves, entre otros
c) Crear, cambiar o retirar los accesos para los usuarios, verificando que exista la solicitud por parte del propietario del activo de información autorizando la ejecución.
d) Desactivar de forma inmediata las credenciales de acceso a los diferentes sistemas y servicios del miembro de la comunidad universitaria cuando este ya no sea parte de la institución.
e) Suspender temporalmente los accesos de los colaboradores (en caso de vacaciones, permisos y licencias temporales) con base en el reporte del área responsable del Talento Humano.
f) 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.)

El área responsable de la atención de solicitudes administrativas de los estudiantes tiene que:

Enviar periódicamente a las áreas responsables de: tecnología, de seguridad de la información, el listado de estudiantes graduados para que procedan con la desactivación del usuario del dominio correspondiente a la universidad.

5.19 Seguridad de la información en las relaciones con los proveedores

El área responsable de la gestión administrativa tiene que:

Velar juntamente con las áreas administrativas o académicas a cargo del manejo de relaciones contractuales, para que se incluya y suscriba cláusulas de confidencialidad cuando corresponda.

5.20 Abordar la seguridad de la información dentro de los acuerdos de proveedores

El área responsable de la gestión administrativa tiene que:

Velar conjuntamente con las áreas administrativas o académicas a cargo del manejo de relaciones contractuales en los que se manejen activos de información con proveedores, se cuente con planes de contingencias y continuidad que garantice la operación, así como el cumplimiento de controles de seguridad de la información.

5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

El área responsable de la gestión administrativa tiene que:

Velar porque los responsables de las áreas administrativas o académicas a cargo del manejo de relaciones contractuales, en los que se manejen activos de información con proveedores, monitoreen y evalúen a los proveedores para asegurar que cumplan con los requisitos de seguridad de la información establecidos, para hacer frente a los riesgos relacionados con la cadena de suministros de los servicios y productos que proveen.

5.22 Seguimiento, revisión y gestión del cambio de los servicios de proveedores

El área responsable de la gestión administrativa tiene que:

Velar porque los responsables de las áreas administrativas o académicas que estén a cargo de manejar relaciones con proveedores en los cuales estén involucrados activos de información, formalicen el manejo de la gestión de cambios.

5.23 Seguridad de la información para el uso de servicios en la nube

El área responsable de tecnología tiene que:

a) Definir los riesgos de seguridad de la información asociados con el uso de servicios en la nube, incluidos los servicios suministrados por terceros.
b) Solicitar y verificar la conformidad de los controles de seguridad de la información con los que cuenta el proveedor de servicios en la nube.
c) Establecer criterios técnicos para evaluar o adquirir los servicios de cómputo en la nube.
d) Disponer de una herramienta para monitorear las capacidades de la nube, optimizando de manera periódica los recursos desplegados.
e) Establecer con los proveedores de nube, los niveles de servicio correspondientes a los tiempos de atención para fallas, nuevos requerimientos y demás que se requieran para la operación.
f) Definir criterios de seguridad y privacidad para el aprovisionamiento y configuración de los recursos de nube.
g) Manejen ambientes de pruebas, desarrollo y producción al igual que se usan en la infraestructura tecnológica en sitio (On-premise) en los casos que apliquen.
h) Utilicen controles de seguridad de la información según corresponda, tales como:
   - Segmentos de redes por roles de servidores a nivel de aplicaciones, bases de datos y web hacia internet.
   - Gestión de identidades y acceso a los servicios.
   - Grupos de seguridad de red o reglas de firewall para restringir el tráfico de red entrante y saliente a los recursos de la nube.
   - Monitoreo uso de los recursos en la nube.
   - Alertas sobre eventos de seguridad en los elementos de la nube.
   - Otros controles pertinentes.
i) Validar que el país en donde se aloja la información disponga de seguridad jurídica para la transferencia o transmisión de estos.
j) Incluir cláusulas en los contratos con los proveedores de servicios en la nube en donde al menos:
   - Se establezca que la institución tiene la propiedad de cualquier información agregada, creada, generada, modificada, almacenada o en cualquier otra forma asociada con la propiedad intelectual, la cual no podrá ser reclamada por el proveedor.
   - Se exija al proveedor la eliminación segura de la información de la entidad al finalizar el contrato.
   - Se otorgue a la institución acceso a los reportes del proveedor asociados a: auditorías de seguridad de la información, continuidad y riesgos de seguridad y privacidad de la información, siempre que la institución lo requiera.

5.24 Planificación y preparación gestión de incidentes de seguridad de la información

El área responsable del talento humano tiene que:

Definir y actualizar según corresponda los procesos disciplinarios formales para sancionar a los colaboradores en caso de participación directa o indirecta en incidentes de seguridad de la información.

El área responsable de regular el comportamiento de los docentes tiene que:

Definir los procedimientos disciplinarios, faltas y sanciones a aplicar sobre los docentes en caso de participación directa o indirecta en incidentes de seguridad de la información.

El área responsable de regular el comportamiento de los estudiantes tiene que:

Definir los procesos disciplinarios formales para sancionar a los estudiantes en caso de participación directa o indirecta en incidentes de seguridad de la información.

El área responsable de tecnología tiene que:

a) Mantener actualizado el inventario de activos de información tecnológicos, identificando y monitoreando continuamente los insumos que podrían verse comprometidos en caso de un evento o incidente de seguridad de la información.
b) 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 y comunicar al responsable de seguridad de la información.
c) Monitorear permanentemente los sistemas, alertas, logs y comportamientos de la red institucional y sus componentes para detectar oportunamente cualquier indicio de incidentes de seguridad.
d) Definir planes de respuesta y contingencia a incidentes que incluya la identificación, contención, erradicación y recuperación ante incidentes de seguridad, así como medidas para prevenir su recurrencia.
e) Comunicar al responsable de seguridad de la información al tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, o presunción de un incidente de seguridad de la información
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) Registrar el incidente de seguridad de la información en la bitácora correspondiente.

El área responsable de seguridad de la información tiene que:

a) Revisar y 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.
b) Efectuar actividades de concientización e instrucción a los miembros de la comunidad universitaria, diseñadas para propiciar la comprensión de los incidentes de seguridad de la información.

5.25 Evaluación y decisión sobre los eventos de seguridad de la información

El área responsable de seguridad de la información tiene que:

a) Analizar los incidentes de seguridad de la información reportados.
b) Convocar al equipo de atención de incidentes de seguridad de la información cuando corresponda para evaluar y dar respuesta al incidente.
c) Comunicar a la autoridad correspondiente, acerca de la ocurrencia de incidentes de seguridad de la información evaluados con severidad alta.
d) 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.

El equipo de atención de incidentes de seguridad de la información tiene que:

a) Atender el llamado del responsable de seguridad de la información cuando se presente un incidente de seguridad de la información.
b) Participar en la evaluación, definición de estrategias y atención al incidente de seguridad de la información según corresponda.

5.26 Respuesta a incidentes de seguridad de la información

El área responsable de tecnología tiene que:

a) Implementar la estrategia para dar atención al incidente de seguridad de la información.
b) Implementar las acciones correctivas resultantes de la atención del incidente de seguridad de la información.
c) Ejecutar las actividades post incidentes con base en lo definido en la Normativa correspondiente para la Gestión de Incidentes de Seguridad de la Información de la PUCE.

El equipo de atención de incidentes de seguridad de la información tiene que:

a) Actuar en la gestión de incidentes de seguridad con base en lo definido en la Norma de Gestión Interna de Incidentes de Seguridad de la Información.
b) Dar seguimiento a la implementación de la estrategia de atención seleccionada y al cierre del incidente de seguridad de la información.

Las áreas responsables de aplicar sanciones al personal administrativo, de servicios, docentes y estudiantes

Aplicar procesos disciplinarios formales a los miembros de la comunidad universitaria en caso de participación directa o indirecta en incidentes de seguridad de la información.

El área responsable de asesoría jurídica tiene que:

Velar por la correcta actuación de la institución ante incidentes de seguridad de la información, en lo que respecta a aspectos y sanciones legales aplicables.

5.27 Aprender de los incidentes de seguridad de la información

El equipo de atención de incidentes de seguridad de la información tiene que:

a) Participar en la actualización de lecciones aprendidas (base de conocimientos) según corresponda.
b) Socializar las mejores prácticas resultantes de las lecciones aprendidas.

El área responsable de tecnología tiene que:

Fortalecer los controles con base en: los resultados de las lecciones aprendidas y en lo definido por el equipo de atención de incidentes de seguridad de la información.

El área responsable de seguridad de la información tiene que:

a) Fortalecer los controles de seguridad de la información con base en los resultados de las lecciones aprendidas.
b) Actualizar la normativa de seguridad de la información cuando corresponda con base en los resultados de las lecciones aprendidas.
c) Definir la formación y concienciación para los miembros de la comunidad universitaria con base en las lecciones aprendidas.
d) Documentar la base de conocimiento con nuevas amenazas, vulnerabilidades y oportunidades de mejora con base en las lecciones aprendidas.
e) Mantener el registro de lecciones aprendidas.

5.28 Recopilación de evidencias

Cuando en el incidente de seguridad de la información esté involucrado activos de información de índole tecnológico, el área responsable de tecnología debe:

a) Aislar la escena.
b) Identificar las fuentes de información.
c) Recoger y examinar las fuentes de evidencia digital
d) Análisis de la información.
e) Elaborar el reporte del incidente de seguridad de la información.
f) Disponer de los medios requeridos para manejo de respaldos
g) Tomar las medidas necesarias para minimizar la pérdida o alteración de datos de evidencia.

5.29 Seguridad de la información durante la interrupción

El área responsable de tecnología tiene que:

Ejecutar los protocolos de contingencia y continuidad que correspondan, considerando la criticidad de los servicios, procesos y procedimientos afectados cuando corresponda.

El área responsable de seguridad de la información tiene que:

a) Coordinar con las diferentes direcciones la priorización de la atención de los procesos críticos de la universidad.
b) Activar los protocolos de contingencia y continuidad.
c) Comunicar a la comunidad universitaria afectada la priorización de restauración de servicios y la contingencia adoptada.

5.30 Preparación de las TIC para la continuidad del negocio

El área responsable de tecnología tiene que:

a) Contemplar dentro del PETI la gestión de la continuidad, en el cual se deberá al menos incluir:
   - Objetivos y alcance del plan.
   - Funciones y responsabilidades.
   - Identificar los activos y actividades involucrados en los procesos críticos de la universidad en los cuales están implicados los activos de información tecnológicos.
   - Las estrategias de continuidad de las TIC considerando el antes, durante y después del evento para las aplicaciones y sistemas de información con sus correspondientes procedimientos de operación.

- Definir los planes y procedimientos de contingencia y continuidad que se activarán.
- Definir planes de respaldos y estrategias de recuperación ante desastres para proteger la continuidad de la operación.
- Definir el tiempo de recuperación de la disponibilidad de los activos de información tecnológicos afectados.
- Condiciones para su puesta en marcha.
- Procedimientos de cambios.
- Ejecutar los planes y procedimientos de contingencia y continuidad para evaluar la efectividad y validez de estos.

5.31 Identificación de requisitos legales, reglamentarios y contractuales

El área responsable de la asesoría jurídica tiene que:

a) Identificar, definir, documentar, socializar y velar por el cumplimiento de los requisitos obligatorios en relación con la normativa vigente aplicable, requisitos relacionados con la seguridad de la información, pertinentes para cada sistema de información.
b) Identificar los documentos en los cuales corresponda incluir o actualizar periódicamente cláusulas de confidencialidad entre otras, para la suscripción de quienes tengan acceso a información institucional en especial la clasificada como confidencial – restringida.
c) Crear y actualizar los instrumentos legales de su competencia tales como contratos, acuerdos de confidencialidad y demás, que permitan afianzar y apalancar el cumplimiento de los controles de seguridad de la información, así como proteger a la institución respecto de las acciones y sanciones que pueda realizar con el propósito de velar por sus activos de información.
d) Comunicar periódicamente las actualizaciones a los documentos legales a las partes interesadas relevantes.
e) Asesorar la pertinencia de la aplicación de sanción a los colaboradores requerida por el área competente, ante la participación de este en incidentes de seguridad de la información.

El área responsable de la normativa interna tiene que:

a) Armonizar la normativa interna vigente de la universidad con relación a la seguridad de la información.
b) Comunicar periódicamente las actualizaciones a las partes interesadas relevantes.

El área responsable del talento humano tiene que:

Definir, implementar y actualizar en los instrumentos normativos y jurídicos del área de Talento Humano respecto a la responsabilidad que tienen los colaboradores de cumplir las obligaciones en el ámbito de seguridad de la información.

El área responsable de tecnología tiene que:

a) Implementar los instrumentos técnicos para proteger la información institucional en sus parámetros de confidencialidad, disponibilidad e integridad precautelando el cumplimiento de las relaciones legales y contractuales.
b) Actualizar y mantener las licencias del software comprado.
c) Controlar e implementar controles para evitar sobrepasar el número máximo permitido de usuarios en los sistemas.
d) Velar y verificar periódicamente que sólo se instalen productos con licencia y software autorizado.

5.32 Derechos de propiedad intelectual (DPI)

El área responsable de la asesoría jurídica tiene que:

a) Definir, documentar, socializar y velar por el cumplimiento de los requisitos obligatorios en relación con los derechos de propiedad intelectual y leyes de derechos de autor, privacidad, cifrado de datos y leyes de protección de datos, pertinentes para cada sistema de información.
b) Identificar los documentos en los cuales corresponda incluir o actualizar periódicamente cláusulas de propiedad intelectual, confidencialidad y protección de datos personales para la suscripción de quienes hayan desarrollado contenido para la institución.
c) Desarrollar, implementar y socializar la política de propiedad intelectual y privacidad de la información, según dispone la normativa legal vigente.
d) Comunicar periódicamente las actualizaciones a las partes interesadas relevantes.

5.33 Protección de los documentos

El área responsable de tecnología tiene que:

Asegurar el registro (constancia electrónica) de operación o actividad realizada por los miembros de la comunidad universitaria en los aplicativos institucionales o sistemas misionales.

El área responsable de la gestión documental tiene que:

a) Definir, socializar y velar por la actualización del contenido de la tabla de retención documental respecto de la información legal que se requiera mantener, de acuerdo

con el tipo de información, de modo tal que los datos puedan estar disponibles de acuerdo a lo definido en el ámbito legal y de justicia.

b) Custodiar los instrumentos legales de su competencia 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 sanciones que pueda realizar con el propósito de velar por sus activos de información.

El área responsable de la normativa interna tiene que:

a) Definir, socializar y velar por la actualización del contenido de la tabla de retención documental, respecto de la información normativa que se requiera mantener de acuerdo con el tipo de información, de modo tal que los datos puedan estar disponibles de acuerdo a lo definido por la normativa interna.
b) Registrar y custodiar los instrumentos normativos 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 sanciones que pueda realizar con el propósito de velar por sus activos de información.

5.34 Privacidad y protección de datos de carácter personal (DCP)

El área responsable de asesoría jurídica tiene que:

a) Actualizar y socializar la normativa de Protección de Datos Personales de la institución según dispone la normativa legal vigente.
b) Implementar la normativa de Protección de Datos Personales de la institución.
c) Comunicar periódicamente las actualizaciones a las partes interesadas relevantes.

5.35 Revisión independiente de la seguridad de la información

El área responsable de seguridad de la información tiene que:

Articular con el área responsable de auditoría, para que se realice la revisión respecto del cumplimiento de las regulaciones en materia de seguridad de la información, que sea aplicable a la universidad.

5.36 Cumplimiento de las políticas y normas de seguridad de la información

El área responsable de talento humano tiene que:

a) Dar seguimiento y proceder con la recepción de la firma o constancia de estar en conocimiento de la política y normas internas de seguridad de la información; así como custodiar los mencionados documentos.

b) Definir con el responsable local de seguridad de la información, las estrategias para fortalecer la cultura organizacional en el ámbito de seguridad de la información.

Las áreas responsables de aplicar sanciones al personal administrativo, de servicios, docentes, estudiantes, según corresponda tienen que:

Definir y aplicar las sanciones a los miembros de la comunidad universitaria, según corresponda, por incumplimiento de la Política General 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.

La aplicación de las sanciones la ejecutará el área correspondiente determinada según los cuerpos normativos internos.

El área responsable de seguridad de la información tiene que:

a) Dar seguimiento a las diferentes áreas respecto al cumplimiento de esta política.
b) Informar sobre el incumplimiento de esta política a las partes interesadas, para su gestión.

5.37 Documentación de procedimientos operacionales

El área responsable de tecnología tiene que:

a) Definir, documentar e implementar los procedimientos de operación de los sistemas y aplicaciones, dentro de los cuales al menos se deberá considerar el procedimiento para procesamiento y manejo de la información automatizada y manual, incluyendo la interrelación con otros sistemas.
b) Socializar con los usuarios los procedimientos de operación de los sistemas y aplicaciones cuando corresponda.

El área responsable de seguridad de la información tiene que:

Revisar la consonancia de los procedimientos de operación de los sistemas y aplicaciones definidos por el área responsable de tecnología con el cumplimiento de la normativa de seguridad de la información.

CAPÍTULO VI. PERSONAS

Artículo 6.- Controles de personas

6.1 Comprobación

Todo colaborador tiene que:

a) Especificar en su hoja de vida al menos:
   - Grado académico
   - Experiencia laboral
   - Referencias laborales
   - Demás detalles solicitados por el área responsable del talento humano que permita validar su formación académica, experiencia y competencias, acorde a la función a la que postula.

6.2 Términos y condiciones de contratación

Todo colaborador, proveedor o terceras partes (pasante) tiene que:

a) Conocer el manual de funciones, estructura organizacional, procesos y entender las funciones y responsabilidades a cargo.
b) Conocer y cumplir con las disposiciones, lineamientos y demás normativa institucional, definida en el ámbito de seguridad de la información.
c) Comprometerse a proteger la confidencialidad, integridad y disponibilidad de la información bajo su responsabilidad.
d) No divulgar información institucional confidencial o restringida.
e) Conocer, suscribir y dar cumplimiento a los documentos definidos por la institución en los cuales se definan las cláusulas para proteger la confidencialidad de los activos de información, así como precautelar los derechos de autor de la universidad sobre el contenido desarrollado cuando corresponda.
f) Hacer uso y acceder únicamente a los activos de información, con base en la definición del rol y funciones para las cuales fue contratado.
g) Portar todo el tiempo y de manera visible el carné de acceso a las instalaciones de la universidad.

6.3 Concienciación, educación y formación en seguridad de la información

Todo miembro de la comunidad universitaria tiene que:

Participar y cumplir de forma obligatoria con todas las capacitaciones, inducciones y eventos organizados por la institución para fortalecer el ámbito de seguridad de la información.

6.4 Proceso disciplinario

Todo miembro de la comunidad universitaria tiene que:

Dar cumplimiento a la sanción impuesta, en caso de participación directa o indirecta en incidentes de seguridad de la información o por incumplimiento de las disposiciones dadas por la institución para precautelar la seguridad de la información.

6.5 Responsabilidades ante la finalización o cambio de la relación laboral

Todo propietario de activos de información tiene que:

Notificar a las áreas responsables: del talento humano y de seguridad de la información cuando cualquier usuario, bajo su cargo, haya producido un cambio de puesto o rol que conlleve cambios de responsabilidades en el ámbito de seguridad de la información.

Todo miembro de la comunidad universitaria tiene que:

a) Una vez concluida la relación con la universidad o al ser parte de un proceso de promoción o cambio de responsabilidades, realizar la transferencia formal de la documentación e información (física y digital) contenida en cualquier medio de almacenamiento, equipos, archivos, entre otros de la que fue responsable al nuevo colaborador a cargo, y en caso de ausencia, al jerárquico superior o su delegado.
b) Cumplir con las responsabilidades legales subsistentes con respecto al manejo de la información una vez terminada la relación laboral con la universidad.
a) Realizar la entrega formal de los bienes y activos de información que hayan estado a su cargo, incluido el carné de acceso a las instalaciones de la universidad.

6.6 Acuerdos de confidencialidad o no divulgación

Todo miembro de la comunidad universitaria tiene que:

a) Firmar y dar cumplimiento a lo estipulado en los acuerdos de confidencialidad y de no revelación de información.
b) Dar a conocer y velar por el cumplimiento de la suscripción de los documentos definidos por la institución en aras de proteger la confidencialidad de la información cuando sea responsable de manejar relaciones con terceros por contratación de bienes o servicios.

6.7 Teletrabajo

Todo miembro de la comunidad universitaria tiene que:

a) Solicitar los permisos correspondientes al área responsable de activos fijos para hacer uso del equipo institucional fuera de las instalaciones de la universidad.
b) Cumplir con el proceso formal definido por el área responsable de tecnología para acceder al uso de conexión remota.
c) Usar la herramienta definida por la institución para conectarse remotamente a la red institucional.
d) Dar cumplimiento a los mecanismos definidos por la institución para autenticarse de forma segura.
e) 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.
f) Cuidar y custodiar las herramientas, equipos y /o dispositivos asignados por la universidad para el desarrollo normal de las actividades propias del cargo que desempeña y que deberán ser utilizadas exclusivamente para las actividades de teletrabajo.
g) Restringirse de usar de wifi gratuito (restaurantes, centros comerciales, o cualquier otra zona pública) para acceder a los sistemas internos de la universidad.
h) Notificar a las áreas responsables de: tecnología y de seguridad de la información cuando haya existido una revelación no autorizada o fuga de información confidencial o restringida.
i) Tomar las precauciones correspondientes para restringir el acceso y uso a los equipos y la información por parte de familiares o visitantes.
j) Abstenerse de realizar copia de información institucional clasificada como restringida o confidencial en equipos personales o que no sean propiedad de la institución.
k) Dar las facilidades al área responsable de tecnología cuando esta requiera auditar y supervisar las actividades que impliquen información confidencial en circunstancias altamente sensibles.
l) Gestionar con el área responsable de tecnología la revocación de acceso remoto cuando finalicen las actividades de teletrabajo.

6.8 Notificación de los eventos de seguridad de la información

Todo miembro de la comunidad universitaria en caso de identificar o tener presunción de evento de seguridad de la información tiene que:

a) Reportar al jefe inmediato, así como al responsable de seguridad de la información al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, presunción de ocurrencia de un evento o incidente de seguridad de la información. A continuación, se detalla por sede el medio por el cual reportar:

#	Sede	Medio para reportar	Correo electrónico
1	Ambato	Correo electrónico	incidentesinformación@pucesa.edu.ec
2	Esmeraldas	Correo electrónico	incidentesinformacion@pucese.edu.ec
3	Ibarra	Correo electrónico	incidentesinformacion@pucesi.edu.ec
4	Manabí	Correo electrónico	incidentesinformacion@pucesm.edu.ec
5	Santo Domingo	Correo electrónico	incidentesinformacion@pucesd.edu.ec
6	Quito	Correo electrónico	incidentesinformacion@puce.edu.ec

b) Abstenerse de realizar pruebas por cuenta propia para detectar o explotar una posible debilidad o falla de seguridad.
c) Participar en el tratamiento de los eventos o incidentes de seguridad de la información con el propósito de investigarlos y dar solución a los mismos.
d) Reportar al área responsable de tecnología cuando detecte o sospeche que el equipo se encuentra contaminado por software malicioso, virus o tiene una falla física.
e) Reportar al responsable de seguridad de la información los eventos o incidentes de seguridad que hayan involucrado daño, robo o compromiso de activos de información.
f) Comunicar y solicitar a la máxima autoridad de la unidad académica, el reporte respecto del uso de las plataformas que tenga información sensible en caso de requerirlo.

6.9 Operación institucional ámbito seguridad de la información

ADMINISTRACIÓN DE LA INFORMACIÓN

Los propietarios de activos de información deben:

a) Cumplir con la implementación de los controles de seguridad de la información para proteger los activos de información, con base en lo dispuesto por las áreas responsables de tecnología y de seguridad de la información.
b) Definir, revisar periódicamente y actualizar, según corresponda en la tabla de retención de la información bajo su cargo, los parámetros de frecuencia de respaldo y tiempo de permanencia de la información.
c) Coordinar con el área responsable de tecnología la gestión de respaldo periódico y permanencia de la información institucional bajo su cargo.
d) Documentar los procedimientos operativos relacionados con el procesamiento y tratamiento de activos de información dentro del ámbito de competencia.

Todo miembro de la comunidad universitaria tiene las siguientes responsabilidades:

a) Clasificar y etiquetar la información institucional física y digital con base en su nivel de sensibilidad en: pública, uso interno, restringida o confidencial.

b) Utilizar las herramientas dispuestas por la institución para clasificar y etiquetar la información institucional.
c) Definir y articular con las áreas responsables de tecnología y de seguridad de la información cuando requiera encriptar información sensible.

ACCESOS A LAS INSTALACIONES

Los propietarios de activos de información deben:

a) Definir y actualizar periódicamente según corresponda, las áreas seguras que requieren acceso restringido.
b) Definir y actualizar periódicamente según corresponda, las personas autorizadas para acceder a las áreas seguras.
c) Reportar al área responsable de la gestión administrativa en caso de detectar accesos no autorizados a las áreas seguras.

ACCESOS A LAS APLICACIONES

Los propietarios de activos de información deben:

a) Definir los accesos y revisar periódicamente el tipo de acceso a los servicios y aplicaciones de los usuarios a su cargo con base en el rol y función que desempeña, incluidos los accesos privilegiados.
b) Notificar al área encargada del talento humano la creación, modificación o retiro de accesos al colaborador con base en lo definido en el literal anterior, así como los casos **excepcionales** en los que se requiere mantener los accesos de los usuarios tales como comisiones, licencias, u otras situaciones que lo ameriten.
c) Aprobar y gestionar el otorgamiento de accesos privilegiados a los diferentes activos de información acorde con la separación de las funciones y con las responsabilidades según al cargo de los miembros de la comunidad universitaria a ser asignados.
d) Acoger de forma obligatoria las medidas o controles implementadas por la institución para fortalecer la seguridad de la información, tales como doble factor de autenticación.

Todo miembro de la comunidad universitaria tiene las siguientes responsabilidades:

a) Cumplir con las políticas y lineamientos emitidos por las áreas de: seguridad de la información y de tecnología respecto del cuidado y uso de las credenciales de acceso. Considerando que estas son de uso **PERSONAL E INTRANSFERIBLE.**
b) No compartir las credenciales de acceso con ninguna persona.
c) No almacenar las credenciales de acceso en ningún registro físicos o electrónico

d) Abstenerse de ingresar las credenciales de acceso en sitios web, aplicaciones o formularios de origen no verificado o que presenten signos de actividad sospechosa, previniendo así posibles ataques de suplantación o robo de identidad.

USO ADECUADO DE LOS ACTIVOS DE INFORMACIÓN

Todo miembro de la comunidad universitaria tiene las siguientes responsabilidades:

a) Usar los activos de información tales como: correo electrónico, credenciales de acceso, sistemas, información física o digital, internet, computadores, entre otros únicamente para la ejecución de las actividades inherentes a las funciones laborales 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.
b) Proteger la información institucional incluyendo su integridad, almacenamiento, procesamiento, transmisión, difusión, con el fin de evitar posibles adulteraciones, pérdidas, hurto, usos o accesos no autorizados
c) No exponer los activos de información asignados, a condiciones de inseguridad física, ambiental, de acceso o cualquier otra.
d) No alterar la integridad de la información contenida en los distintos activos de información institucional.
e) Evitar abrir, ejecutar, descargar archivos de fuentes desconocidas.
f) No instalar por sí mismo, software en los equipos institucionales bajo su cargo.
g) Prescindir del acceso a cualquier página web que ponga en riesgo a la universidad.
h) Bloquear la pantalla del equipo, computador cuando deje su puesto de trabajo, así sea por unos instantes.
i) Retirar inmediatamente de la impresora la información sensible una vez impresa.
j) Asegurarse de almacenar bajo llave los documentos y los medios informáticos cuando estos no estén siendo utilizados.
k) Responsabilizarse por las llaves asignadas para el almacenamiento y cuidado de los dispositivos de punto final de los cuales es custodio.
l) Utilizar la información institucional, incluida la identidad gráfica (logos y formatos institucionales), únicamente para actividades relacionadas con el desempeño de sus funciones.
m) Facilitar al responsable de seguridad de la información los soportes que permitan evidenciar el cumplimento de los requisitos de seguridad de la información establecidos por la institución.

TRANSFERENCIA DE INFORMACIÓN

Todo miembro de la comunidad universitaria tiene las siguientes responsabilidades:

a) 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.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS – SOFTWARE

Todo miembro de la comunidad universitaria encargado de gestionar la adquisición, desarrollo o mantenimiento de sistemas tecnológicos, software o aplicativos debe:

a) Identificar y priorizar los requerimientos funcionales y técnicos con la participación y aprobación formal de las áreas usuarias, esto incluye, tipo de perfiles, mecanismos de autorización, control de acceso, definición de interfaces, almacenamiento, respaldos, procesamiento, entradas, salidas, controles, seguridades, plan de pruebas y pistas de auditoría de las transacciones en donde se aplique el registro de información.
b) Solicitar la validación y aval del software, hardware o solución tecnológica que se desee adquirir.

GESTIÓN DE PROYECTOS

Todo miembro de la comunidad universitaria encargado de gestionar proyectos de cualquier índole, sin importar su naturaleza (procesos clave de la universidad, procesos internos, investigación, vinculación, servicios o productos, tecnología, entre otros), deberán:

a) Definir dentro del perfil del proyecto según corresponda, los siguientes aspectos:
   - La criticidad de la información que se utilizará en el proyecto.
   - El tiempo que la información será utilizada.
   - Periodos de conservación de la información.
   - Forma de accesibilidad a la información por parte de los involucrados.
   - El análisis de riesgos en el cual se incluya aspectos de la privacidad de la información y los datos personales.
   - Firma de acuerdos de confidencialidad y de entrega de información según corresponda.

b) Entregar periódicamente al responsable del área de seguridad de la información el listado de proyectos en ejecución, así como los perfiles de proyectos que sean solicitados para verificar el cumplimiento del literal a).
c) Asegurar que todos los interesados estén informados y capacitados, respecto de la gestión de los riesgos de seguridad de la información asociados al proyecto.

GESTIÓN CON PROVEEDORES O TERCEROS:

Todo miembro de la comunidad universitaria encargado de gestionar relaciones contractuales con proveedores o terceros tiene las siguientes responsabilidades:

a) Definir y coordinar con el área responsable de tecnología y el proveedor 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.
   - Entrega de manuales de operación y usuario correspondientes a los productos o servicios objeto de la relación con el proveedor cuando corresponda.
b) Controlar que en los contratos con los proveedores o terceros se incluyan cláusulas a través de las cuales la universidad:
   - Tenga el derecho de verificar y evaluar el Sistema de Gestión de Seguridad de la Información del proveedor.
   - Exija al proveedor informar sobre cualquier incidente de seguridad, aunque sea leve.
   - Se asegure que el proveedor tenga un plan de respuesta a incidentes, infracciones y ataques a la seguridad de la información.
   - Exija el cumplimiento de requisitos de seguridad de la información en la cadena de suministros de servicios y productos contratado.
   - Vele porque el proveedor cuente con un plan de contingencias y continuidad que garantice la prestación del servicio contratado.
   - Se asegure que el proveedor maneje procedimiento de gestión de cambios.
   - Incluya y suscriba acuerdos de confidencialidad para proteger la confidencialidad de la información institucional.
   - Proteja el derecho de propiedad de la universidad sobre lo contratado, cuando aplique.
   - Obligue una vez finalizada la relación contractual con el proveedor o tercero ser realice la eliminación de la información institucional de forma segura, cuando corresponda.

GLOSARIO

Accesos privilegiados: se refiere a los permisos especiales otorgados a ciertos usuarios que les permiten realizar acciones que los usuarios normales no pueden. Los usuarios con acceso privilegiado suelen ser administradores de sistemas, personal de TI, y otros roles críticos dentro de una organización.

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 propuestos, 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.

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.

Áreas seguras: son zonas dentro de una organización diseñadas para proteger los activos de información y equipos críticos contra accesos no autorizados y amenazas físicas.

Comité Nacional 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.

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

Evento de seguridad de la información: es cualquier incidente o actividad que afecta la confidencialidad, integridad o disponibilidad de los datos y sistemas de una organización. Estos eventos pueden incluir accesos no autorizados, ataques cibernéticos, pérdida de datos, o fallos en los sistemas de seguridad.

Gestión administrativa: área encargada en la institución de planificar, dirigir y controlar los procesos administrativos para el desarrollo Institucional.

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. - proceso 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 de la información: es un evento que compromete la confidencialidad, integridad o disponibilidad de los datos y sistemas de una organización. Esto puede incluir accesos no autorizados, violaciones de datos, ataques de malware, o cualquier otra actividad que ponga en riesgo la seguridad de la información.

Incidentes de severidad ALTA. – cuando un evento afecta a los activos de información que influyen directamente en la consecución de los objetivos misionales de la institución, afectan la reputación institucional o involucran el incumplimiento de aspectos legales.

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.

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.

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 bases de datos.

Novedades de personal. - son los registros en formatos institucionales 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.

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, y terceros relacionados.
Procedimiento. - acciones que se realizan, con una serie común de pasos claramente definidos, que permiten realizar correctamente una tarea o alcanzar un objetivo. Se distinguen dos clases de procedimientos: obligatorios y recomendados. Estos últimos representan "buenas prácticas", que son aconsejables, pero no requeridas. Si en un procedimiento no se utiliza la palabra "recomendado" se asume que es obligatorio.
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.
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 (SI). - son los controles definidos para proteger 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.
Tiempo de permanencia: se refiere al período durante el cual los datos, documentos o registros deben ser conservados antes de ser eliminados o archivados. Este tiempo puede estar determinado por normativas legales, políticas internas de la organización o necesidades operativas específicas.
Vulnerabilidad. - debilidad de un activo o grupo de activos de información que puede ser aprovechada por una o más amenazas.

DISPOSICIONES GENERALES

PRIMERA. - la presente política entrará en vigencia una vez que el Consejo Superior 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 de la presente política a la Secretaría General de la PUCE., así como la difusión del extracto de la misma en la cual no se incluirá los capítulos 5, 7 y 8, por considerarlos información técnica inherente al funcionamiento de las áreas involucradas.

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

CUARTA. - la Pontificia Universidad Católica del Ecuador a través de las distintas unidades académicas o administrativas dentro de su ámbito de competencia, instrumentarán o actualizarán los procesos, procedimientos y lineamientos que se requieran para la implementación y cumplimiento de la presente política.

CERTIFICACIÓN. - En mi calidad de secretario del Consejo Superior, certifico que la presente Política General de Seguridad de la Información de la PUCE fue analizada y aprobada en sesión de 21 de enero de 2025

Esta Política General de Seguridad de la Información de la PUCE entrará en vigencia desde su publicación en la Gaceta de la PUCE.

ALEX FABRICIO JARAMILLO ALVAREZ

Firmado digitalmente por ALEX FABRICIO JARAMILLO ALVAREZ
Fecha: 2025.01.30 16:48:48 -05'00'

Dr. Alex Fabricio Jaramillo
SECRETARIO DEL CONSEJO SUPERIOR DE LA PUCE

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación	Aprobado por
02.01	Enero/2025	Adaptación a la nueva definición de la ISO 27001 y 27002 Actualización nombres de áreas responsables Adaptación estructura nacional y local Extracto de la Política General de Seguridad de la Información Supresión Capítulo 7 y 8 Ajustes de forma	**Consejo Superior**