Pontificia Universidad Católica del Ecuador

Seréis mis testigos

Lineamientos de Seguridad de la Información

Enero| 2024

Versión 01.01

CONTENIDO

1. INTRODUCCIÓN

La Pontificia Universidad Católica del Ecuador en su afán de proteger la información institucional en todos sus procesos y precautelar la confidencialidad, integridad y disponibilidad de la información aprobó la Política de Seguridad de la Información de la PUCE, en la cual se contempla que como parte de la implementación y articulación de la misma se "instrumentarán la **normativa secundaria necesaria para el cumplimiento de la presente política**, con el propósito de asegurar su correcta implementación y despliegue"

2. MARCO LEGAL

Que en la Política de Seguridad de la Información de la PUCE dentro de sus disposiciones generales señala ***"la Pontificia Universidad Católica del Ecuador a través de las distintas unidades académicas y/o administrativas dentro de su ámbito de competencia y en coordinación con la unidad encargada de la Planificación y 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."***

3. OBJETIVOS

General:

Especificar un conjunto de lineamientos con base en lo contemplado en la Política de Seguridad de la Información de la PUCE de modo que se permita articular el cumplimiento de la misma al definir las actividades que los usuarios deben cumplir para administrar de forma segura la información física y digital a la cual accede a través de los diferentes activos de información tales como: sistemas, herramientas, aplicativos, fuentes, servicios, infraestructura y de este modo proteger la confidencialidad, integridad y disponibilidad de los activos de información.

Específicos:

- Regular la gestión de los activos de información con base en su nivel de confidencialidad y riesgos asociados de modo que se pueda aplicar los niveles de protección adecuados.
- Disponer de lineamientos para almacenar y destruir la información institucional tanto física como digital, con el propósito de reducir los impactos de los riesgos generados por fallas, robos, inadecuado almacenamiento y/o destrucción que podrían generar pérdida total o parcial de información.
- Definir lineamientos respecto del aprovisionamiento de usuarios con base en el ciclo de vida de las credenciales desde creación, modificaciones y revocación de accesos.
- Definir los lineamientos para la conexión de dispositivos móviles a la red institucional y/o equipos institucionales según corresponda.
- Definir la forma en que los usuarios se deben conectar de forma remota a la red institucional.

- Definir las reglas para el uso adecuado del correo electrónico institucional tanto para el envío o recepción de mensajes de correo electrónico y archivos adjuntos, de modo que los usuarios tengan claridad de lo que se considera uso aceptable e inaceptable.
- Definir las reglas para el uso adecuado – aceptable del internet con la finalidad de minimizar los riesgos asociados a su uso.

4. ALCANCE

Aplica a todo el personal de la PUCE en todas sus sedes que administren y/o custodien información institucional en formato físico y/o digital considerando dentro de estas las acciones de creación, envío, impresión, recepción y almacenamiento a través del uso de medios, servicios y/o sistemas que sean de propiedad, arrendados, administrados o autorizados por la PUCE.

5. DESARROLLO DEL CONTENIDO

5.1. Lineamiento para la clasificación y etiquetamiento de la información

- La información institucional independientemente del medio en donde sea almacenada, por ejemplo: ordenadores, archivadores, escritorio, papelera, correo, servidores, entre otros debe ser protegida del acceso, alteración, divulgación y/o destrucciones no autorizadas.
- La información y los sistemas institucionales proporcionados a los colaboradores, contratistas, socios comerciales y representantes son propiedad de la PUCE, quién determina las reglas de uso y acceso adecuado.
- Se ha definido cuatro niveles de confidencialidad de la información, que son:

Nivel de Confidencialidad	Etiquetado a incluir en el documento	Criterios de Clasificación	Restricción de Acceso
Pública	PÚBLICA	Cuando la información a ser publicada no cause perjuicio o dañe a la Universidad. Y esta es de interés público.	La información está disponible para todo público
Uso Interno	USO INTERNO	Cuando el acceso no autorizado a la información podría ocasionar daños y/o inconvenientes menores a la Universidad.	La información está disponible para toda la comunidad universitaria (administrativos, docentes y estudiantes) y terceros debidamente autorizados.
Restringida	RESTRINGIDA	Cuando el acceso no autorizado a la información podría causar un daño considerable a la Universidad o a su reputación.	La información está disponible solamente para grupos específicos de la comunidad universitaria, grupos definidos por las respectivas autoridades.
Confidencial	CONFIDENCIAL	Cuando el acceso no autorizado a la información podría dañar de forma catastrófica (irreparable) a la Universidad o a su reputación.	La información está disponible solamente para personas específicas y autorizadas por las autoridades respectivas de la PUCE.

Tabla 1: Clasificación de la información

- Para resguardar la información, la PUCE ha definido tres roles que son: propietarios, custodios y usuarios finales.

Rol	Quiénes	Definición
Propietario	Rector, o su equivalente en las sedes, Vicerrector, Decanos, directores y demás autoridades administrativas y académicas de la universidad.	El término "propietario de la información" en el ámbito de seguridad de la información se refiere a la persona que posee la responsabilidad del activo de información.
Custodio	Docentes, personal administrativo, de servicios, proveedores, contratistas, estudiantes becarios o personas a los cuales el propietario de la información le otorga el acceso y la custodia respecto de la información que maneja.	Son aquellos que tienen información a su cargo a través del uso de sistemas, aplicaciones o procesos, también aquellos que operan bases de datos, y/o en sus actividades laborales manejan copias físicas de documentos.
Usuario final	Docentes, personal administrativo y de servicios, estudiantes, proveedores, contratistas, entidades gubernamentales, terceras partes, u otras personas autorizadas para utilizar la información de la PUCE.	Son todos los usuarios que consumen la información institucional.

Tabla 2: Roles de seguridad de la información

- Los "propietarios de la información" son los responsables de que la información del área de la cual es encargado sea clasificada y etiquetada con base en los niveles de confidencialidad definidos en la tabla 1.
- El propietario de la información es el responsable de validar y/o actualizar el inventario de los activos de información al menos cada dos años.
- El propietario de la información es el responsable de aprobar el acceso, uso, copia, modificación, divulgación y eliminación del activo de información físicos y/o digitales.
- Los administradores de los sistemas involucrados son responsables de supervisar las actividades de las personas, el funcionamiento de los sistemas y las redes, para que los controles se cumplan adecuadamente.
- El propietario de la información es el responsable de que se reporte cualquier cambio (nombre del activo, custodio, ubicación, nivel de criticidad) en el inventario de los activos de información significativos que pertenezcan o sean utilizados por la universidad al responsable de la unidad encargada de la seguridad de la información.
- El propietario de la información es el responsable de autorizar a un tercero el acceso a la información física, digital y/o sistemas de información con los tipos de permisos que correspondan, la asignación de credenciales de acceso directamente a un tercero aplica únicamente cuando estas son imprescindible para ejecutar la actividad tales como revisar el funcionamiento del sistema, auditorías a los sistemas de información, hacer pruebas de rendimiento u otros relacionados que impliquen necesariamente acceso directo a los sistemas de información en cuyo caso el custodio de información siempre deberá realizar el acompañamiento . Caso contrario el acceso a la información la realizará el custodio de información quien facilitará la misma al tercero según corresponda.
- Todo miembro de la PUCE tiene la responsabilidad de identificar y procurar la implementación de controles de seguridad según corresponda para resguardar los activos de información de los cuales es responsable.

- Todo miembro de la PUCE que es responsable de un activo de información físico clasificado como confidencial, restringida o de uso interno tiene la responsabilidad de resguardarla con protección física tales como almacenamiento bajo llave, en caso de traslado embalaje, entre otros.
- Todo miembro de la PUCE que es responsable de un activo de información digital clasificado como confidencial, restringida o de uso interno tiene la responsabilidad de resguardarlo según corresponda con cifrado, claves de acceso, limitación de tipo de permisos de acceso, etc.
- Todo miembro de la PUCE que es responsable de un activo de información deberá considerar la siguiente definición de controles aplicables con base en la clasificación y etiquetado de la información.

Clasificación de la información	**Controles**
Pública	• Es información de alta difusión por lo cual es necesario protegerla para que no sea modificada y el contenido sea el correcto cuando el público acceda a ella. • El almacenamiento es importante de modo que se pueda garantizar que la información esté habilitada cuando sea requerida. • La información debe ser almacenada en recursos institucionales con los controles de seguridad generales de la institución. • Al compartir información se debe considerar que las herramientas permiten configurar a quien se le da acceso y qué tipo acceso (lectura y escritura)
Uso Interno	• El acceso a este tipo de información debe corresponder a la necesidad de conocer la misma, y la debe autorizar el administrador del activo de información. • Esta información no se la debe divulgar a nadie ajeno a la institución a excepción de cuando es específicamente requerida con fines propios al cumplimiento de la misión de la institución, en cuyos casos debe ser protegida a través de la firma de un acuerdo de confidencialidad. • El almacenamiento y manipulación debe darse de forma segura. • La impresión de esta información se la debe realizar en una impresora conocida y segura, y las mismas deben estar resguardadas, para lo cual no se requiere de la aprobación del propietario de la información. • La información puede transmitirse sin cifrar siempre y cuando no contenga información sensible, de modo que en caso de pérdida no pueda representar una amenaza para la institución. • Al compartir información se debe considerar que las herramientas permiten configurar a quien se le da acceso y qué tipo acceso (lectura y escritura)
Restringida	• Los controles de seguridad deben incluir control de acceso a grupos específicos, auditoría del acceso de escritura a los activos, implementación de hash y firmas digitales, controles de integridad con base en las atribuciones del área o grupo al cual pertenece el colaborador en la institución, el cual debe ser aprobado por el propietario del activo de información. • La divulgación a un tercero de este tipo de información debe ser aprobado por el propietario del activo de información y debe estar soportada por la firma de un acuerdo de confidencialidad. • La transmisión de este tipo de información debe realizarse con los controles adecuados, entre ellos cifrado, doble factor de autenticación, embalaje seguro entre otros. • Se debe mantener respaldo de este tipo de información dentro de la infraestructura institucional con las seguridades correspondientes. • La copia de este tipo de información debe ser controlada y aprobada por el propietario del activo de información.

	• Se debe disponer de un sistema alternativo para restaurar la información en caso de requerirlo. • La opción para compartir, así como descargarse la información debe estar restringida, para el manejo de excepciones el propietario de la información deberá autorizarlos. • Al compartir información se debe considerar que las herramientas permiten configurar a quien se le da acceso, qué tipo acceso (lectura y escritura) y la opción de permitir descarga o no.
Confidencial	• El acceso y control a la información se la debe otorgar a usuarios específicos con base en los roles que desempeña. • Aplicar según corresponda controles de acceso de escritura monitorizado, implementación de algoritmos hash, firmas digitales, control dual, autenticación de dos factores. • Debido a que son activos de información de alta disponibilidad es necesario disponer de una solución alternativa para almacenamiento y restauración oportuna de la información. • Se requiere disponer redundancia para garantizar el funcionamiento de los activos de información que requieren alta disponibilidad. • Este tipo de activos de información deben estar considerados en el Plan de Continuidad y Planes de Recuperación. • La copia de este tipo de información debe ser controlada y aprobada por el propietario del activo de información. • Los respaldos deben someterse a pruebas de restauración periódica. • La opción para compartir, así como descargarse la información debe estar restringida, para el manejo de excepciones el propietario de la información deberá autorizarlos. • Al compartir información se debe considerar que las herramientas permiten configurar a quien se le da acceso, qué tipo acceso (lectura y escritura) y la opción de permitir descarga o no.

Tabla 3: Clasificación de la información y controles aplicables

- Todos los usuarios tienen la responsabilidad de mantener la confidencialidad de la información de la cual son custodios para el desempeño laboral.
- Todo colaborador debe firmar el acuerdo de confidencialidad y/o cláusulas contractuales diseñadas por la universidad para proteger aspectos de confidencialidad, integridad y propiedad de los activos de información. Adicionalmente, el área de Talento Humano es la responsable de gestionar su firma y custodiar los mencionados instrumentos.
- Adicionalmente, cuando se requiera que un tercero acceda a la información confidencial, restringida o de uso interno, el propietario de la información deberá gestionar la firma del acuerdo de confidencialidad, el cual debe ser revisado y enviado para custodia de la asesoría jurídica.
- La unidad encargada de las tecnologías de la información es responsable de implementar los controles para proteger los activos de información digital a solicitud del propietario de la información con base en la aplicabilidad del mismo de acuerdo a lo definido en el presente lineamiento.
- La unidad encargada de la parte administrativa es responsable de implementar los controles físicos para proteger los activos de información a solicitud del propietario de la información con base en la aplicabilidad de los mismos de acuerdo a lo definido en el presente lineamiento.

5.2. Lineamiento para el almacenamiento y eliminación de la información

- El propietario de la información es el responsable que la información tanto física como digital del área de la cual es responsable sea clasificada y etiquetada con base en lo definido en el lineamiento **para la clasificación de la información.** Así como que la misma cuenta con la definición del **tiempo de retención documental (Anexo 1).**
- El medio de almacenamiento institucional es la nube (sharepoint).
- El propietario de la información es el responsable de garantizar que la información del área de la cual esté a cargo sea almacenada en los servidores de la institución que son administrados en el centro de datos por la unidad encargada de las tecnologías de la información.
- Para el almacenamiento de la información la unidad encargada de las tecnologías de la información se encargará de crear y otorgar accesos a la estructura de carpetas requerida por el área.
- La unidad encargada de las tecnologías de la información es responsable del almacenamiento y respaldo de la información digital con base en lo definido en la tabla d**e tiempo de retención documental (Anexo 1)** por el propietario de la información.
- Los custodios de la información física son responsables del almacenamiento y protección de los mismos con base en lo definido en la tabla d**e tiempo de retención documental (Anexo 1)**.
- Al compartir información se debe considerar que las herramientas permiten configurar a quien se le da acceso, qué tipo acceso (lectura y escritura) y la opción de permitir descarga o no. En el caso que se requiera resguardar la disponibilidad del contenido de correos electrónicos incluidos sus adjuntos como parte de la información institucional, el custodio de los mismos deberá almacenarlo en la estructura de carpetas destinado para su área con base en lo definido en la tabla d**e tiempo de retención documental (Anexo 1).**
- El propietario de la información es el responsable de adoptar los controles físicos-técnicos adecuados en coordinación con las unidades encargadas de las tecnologías de la información, de la parte administrativa y de la seguridad de la información para garantizar que los datos personales no puedan utilizarse indebidamente.
- El propietario de la información es el responsable de que se realice la eliminación segura de la información digital en coordinación con la unidad encargada de las tecnologías de la información según corresponda, lo mencionado cuando ya no se requiera conservar la misma con base en lo definido en la tabla de tiempo de retención documental (Anexo 1).
- El propietario de la información es responsable de que se ejecute de forma segura la destrucción de los documentos físicos a través del uso de trituradoras de papel con base en la clasificación de confidencialidad de los documentos físicos, así como lo definido en la **tabla de tiempo de retención documental (Anexo 1).**
- Considerando que suele existir varias copias de un mismo documento se recomienda evitar la mencionada práctica, en aquellos casos que sea estrictamente necesaria mantener la duplicidad de los documentos en atención a la ejecución de un algún proceso institucional se recomienda eliminar la mencionada copia creada tan pronto como sea posible. Para la copia y eliminación de información se debe contar la autorización del propietario del activo de información.
- El almacenamiento de bases de datos fuera de los sistemas de información digitales se encuentra restringido, la forma adecuada para acceder a la misma es solicitando las credenciales de acceso con los correspondientes permisos al propietario de la información, las excepciones deberán ser aprobadas por el propietario de la información y se deberá cumplir con los demás puntos de este lineamiento para salvaguardarla.

- Se prohíbe almacenar en los servidores institucionales información de carácter personal tales como música, videos y demás que no tengan relación con el cumplimiento de los objetivos de la PUCE.
- Los propietarios de la información son quienes deben autorizar las solicitudes de recuperación de información a través del procedimiento definido por la unidad encargada de las tecnologías de la información.
- Se prohíbe a los usuarios almacenar la información institucional clasificada como de uso interno, confidencial y/o restringida en herramientas como Dropbox o Google Drive.
- La unidad encargada de las tecnologías de la información es el responsable de la custodia y respaldos de la información almacenada en SharePoint institucional con base en la definición del tiempo de retención documental definido por los propietarios de la información.
- El proceso de recuperación de información deberá ser atendido por la unidad encargada de las tecnologías de la información de acuerdo al formato de solicitud recibido, el tiempo de restauración de la información se lo realizará con base en lo definido en el proceso establecido acorde al nivel de clasificación de la información.

5.3. Lineamiento para la gestión de accesos.

- Para cada red, sistema, medio de almacenamiento u otro tipo de activo de información institucional se debe disponer de la definición de quién es el propietario del activo de información.
- Las unidades encargadas de las tecnologías de la información y de la seguridad de la información deberán custodiar y mantener actualizado el inventario de red, sistema, medio de almacenamiento u otro tipo de activo de información institucional con la correspondiente definición del propietario del activo de información.
- Las áreas dónde se encuentre el centro de datos y en sí lo sistemas informáticos y de comunicaciones deberán estar protegidos con la infraestructura física adecuada de manera que se controle y restringa el acceso según corresponda.
- Cualquier externo autorizado que requiera acceder a las áreas restringidas debe estar siempre acompañado del personal de la unidad encargada de las tecnologías de la información.
- La asignación de accesos a cualquier red, sistema, medio de almacenamiento u otro tipo de activo de información institucional deberán corresponder a la autorización del propietario del activo de información.
- Los accesos otorgados a las redes, sistemas y medios de almacenamiento institucional deberán cumplir la regla de privilegios mínimos con base en las funciones y rol que desempeñan.
- El propietario de los activos de información debe validar periódicamente los accesos otorgados, considerando siempre la regla de privilegios mínimos con base en las funciones y rol que desempeñan.
- Toda red, sistema, medio de almacenamiento u otro tipo de activo de información institucional deben contar con mecanismos de autenticación, con periodo de caducidad, y su acceso debe ser controlado en función de la identidad del usuario.
- Eliminar y/o limitar en los computadores institucionales los servicios, aplicaciones y protocolos de red no requeridos con base en el rol y funciones del usuario.
- Cambiar en las cuentas de administración las credenciales que vienen predeterminadas
- Los administradores técnicos de los diferentes sistemas deben realizar una continua depuración y control de las cuentas, incluidas las no utilizadas, creadas temporalmente, etc.
- Configurar el bloqueo de pantalla y/o accesos a aplicativos luego de 5 minutos de inactividad.

- Controlar la red inalámbrica de modo que esté segmentada de tal forma que no pongan en riesgo los aplicativos misionales limitando su acceso según el rol que corresponda.
- Todo activo de información con base en su clasificación de confidencialidad deberá usar según corresponda mecanismos de control de accesos por capas, tales como: doble factor de autenticación, cifrado, configuraciones de inicio de sesión personales en los dispositivos, configuraciones para usos compartidos de carpetas y archivos, listas de control de acceso (ACL) entre otros.
- Es responsabilidad de cada usuario comprender la clasificación de confidencialidad los datos del cual es custodio y en concordancia con lo mencionado tratarlos con el cuidado que corresponda aun cuando no existan controles técnicos y/o estos fallen.
- La asignación, revocación o modificación de los accesos tanto físicos como virtuales a la red, sistema, medio de almacenamiento u otro tipo de activo de información institucional según corresponda se los deberá realizar de forma oportuna, es decir con base en la fecha de inicio y/o finalización de la relación laboral, comercial y/o de servicio con proveedores y/o terceros, el manejo de excepciones deberá ser analizado por las unidades encargadas de talento humano así como de las tecnologías de la información y de seguridad de la información y el propietario del activo de información deberá enviar a las tres áreas antes mencionadas la constancia por escrito la excepción solicitada, el conocimiento del riesgo que asume con la justificación correspondiente.
- El uso de las cuentas privilegiadas está autorizado únicamente para la instalación y/o reconfiguración de programas y/o sistemas, se prohíbe el uso de las mismas para actividades propias de la administración - operación y su asignación debe estar restringida, controlada y autorizada por el propietario del activo de información.
- El uso de accesos compartidos y genéricos está prohibido cuando implique acceso a información clasificada como confidencial.
- El uso de accesos compartidos y genéricos está restringido y solo se autorizará bajo circunstancias excepcionales siempre y cuando se cuente con controles equiparables al cual se exceptúe.
- Se debe segregar y restringir el acceso a las herramientas de auditoría, logs de registro de datos y/o sistemas que registran la interacción entre el usuario y los activos de información.
- Restringir a los usuarios el acceso y/o uso de programas utilitarios que puedan comprometer o poner en riesgo a las redes, sistemas, medios de almacenamiento u otro tipo de activo de información institucional.
- Cada usuario debe comprender la sensibilidad de sus datos y tratarlos en consecuencia. Aun cuando los controles técnicos fallen o estén ausentes, cada usuario debe mantener la seguridad de la información con base en su clasificación de confidencialidad.
- Ningún usuario debe hacer uso de las credenciales de acceso de otro usuario aun cuando este lo haya autorizado.
- Cada usuario es responsable del uso de las credenciales de acceso asignadas, esto incluye el uso de la misma de forma personal e intransferible, evitar el uso de las utilidades de “guardar contraseña” disponible en los aplicativos y/o navegadores de internet, no escribirla y/o almacenarla en ningún medio físico y/o digital, cambiarla con periodicidad y emplear las características definidas por la unidad encargada de las tecnologías de la información para su creación.
- Cada usuario es responsable de validar periódicamente sus recursos compartidos y eliminarlos cuando el acceso ya no es requerido.
- Los usuarios siempre que sea posible deben priorizar la conexión a la red y recursos institucionales a través de la red cableada.

5.4. Lineamiento para el uso de dispositivos móviles

- Los dispositivos móviles institucionales deben tener actualizados y/o habilitados los parches del sistema operativo, software antivirus, antimalware actualizado, y de ser el caso funciones para el cifrado de datos.
- Los usuarios son responsables de la protección del dispositivo móvil del cual es custodio, así como de la información almacenada en el mismo.
- En caso de pérdida y/o robo de un dispositivo móvil institucional, el usuario debe reportarlo a incidentesinformacion@puce.edu.ec con copia a su jefe inmediato superior.
- Los dispositivos móviles externos (que no son de propiedad de la institución) únicamente podrán conectarse a las redes wifi, la misma que debe estar segmentada de tal forma que no pongan en riesgo los aplicativos misionales limitando su acceso según el rol que corresponda, la conexión a la red cableada institucional está restringida, cualquier excepción a este punto debe ser justificada y aprobada por escrito por el jefe inmediato superior del solicitante.
- Cualquier dispositivo móvil externo autorizado como excepción a conectarse a la red cableada debe cumplir los siguientes requisitos: tener los parches del sistema operativo, software antivirus y antimalware actualizado.
- Los datos institucionales clasificados como restringidos y confidenciales de los cuales un usuario es custodio no deben ser almacenados en ningún dispositivo móvil.
- Una vez que se cuente con la autorización y justificación del jefe inmediato, la unidad encargada de las tecnologías de la información revisará y aprobará si el dispositivo móvil externo cumple los requisitos para permitir la conexión a la red cableada y en caso de ser necesario instalará, con la aceptación del usuario, un agente para monitorear que este actualizado el SO y antivirus.
- La unidad encargada de las tecnologías de la información mantendrá un registro actualizado de todos los dispositivos móviles no institucionales conectados a la red cableada, el cual debe permitir identificar el cumplimiento de los requisitos definidos para la autorización de su conexión.
- La unidad encargada de las tecnologías de la información cada año actualizará los requisitos a ser considerados para autorizar la conexión a la red cableada institucional de dispositivos móviles externos.

5.5. Lineamiento para el acceso remoto

- El acceso remoto está permitido únicamente para los casos autorizados por la unidad encargada de talento humano en los que aplica teletrabajo.
- Cualquier usuario que requieran acceder a la red institucional de forma remota lo deben realizar a través una conexión de red cifrada (cliente VPN).
- Los usuarios no deben tener conexiones persistentes.
- Los usuarios deben cerrar las sesiones remotas una vez finalizado el trabajo.
- Las sesiones de acceso remoto se finalizarán automáticamente cuando no se detecte actividad luego de 20 minutos.
- La autenticación se permitirá únicamente a cuentas del directorio activo.
- Los usuarios de acceso remoto no deben almacenar información institucional en dispositivos personales.
- Es obligatorio el uso de doble factor de autenticación para el acceso remoto.
- Los usuarios deben utilizar su cuenta de directorio activo institucional para el acceso remoto.

- La unidad encargada de las tecnologías de la información habilitará el acceso y deberá llevar un registro actualizado de todos los accesos remotos otorgados.
- Los usuarios nunca deben acceder a los recursos institucionales haciendo uso de conexiones no seguras tales como puntos de acceso inalámbrico desprotegidos (wifi gratis).

5.6. Lineamiento para el uso del correo electrónico institucional

- Todos los correos electrónicos institucionales procesados por los sistemas informáticos y la red de la PUCE se consideran de propiedad institucional.
- Los usuarios deben limitar el uso del correo electrónico institucional para el desempeño de activades de índole laboral y/o académico relacionados con la institución, por lo que deben abstenerse de usar el correo electrónico institucional para la realización de trabajos de índole privado, reenvío de cadenas o de caridad no relacionados con el ejercicio legítimo de la institución, así como para crear, enviar, reenviar o almacenar correos electrónicos con mensajes, archivos adjuntos, hipervínculos o con referencias a otros sitios web que puedan ser ilegales, ofensivo, perturbador, poco ético o inapropiado con contenido sexualmente explícito, racista, difamatorios, abusivos, obscenos, despectivos, discriminatorios, amenazantes, acosadores, virus u otro software malicioso, de igual forma para recibir información de carácter personal como facturas, resultados médicos, entre otros.
- Una vez dada la baja del usuario, luego de treinta (90) días calendario se deberá borrar la cuenta de usuario y buzón de correo electrónico.
- Queda prohibido el uso del correo electrónico institucional para registrarse en plataformas externas de redes sociales, de música, juegos, streaming, video, mensajería y demás para uso personal, en caso que cualquiera de los mencionados recursos sea requerido para uso de la institución deben ser solicitados por el jefe inmediato y estar asociados a una cuenta genérica, la cuenta debe tener definido un responsable para su administración.
- La solicitud de creación y uso de grupos de correos está limitada solo para aquellas personas que con base en su responsabilidad requieren enviar comunicaciones a grandes grupos de usuarios y su creación deberá ser aprobada por el responsable de área cuando corresponda a una necesidad institucional.
- La solicitud de creación y uso de cuentas genéricas está limitada solo para el desempeño de aquellas funciones que tengan atención masiva de clientes, para lo cual el responsable del área debe aprobar la creación de cuentas genéricas y definir el responsable de la administración de la mencionada cuenta.
- El responsable del área a la que le corresponda la administración de cuentas genéricas y grupos de correo es responsable de comunicar cualquier cambio en el responsable asociado a la cuenta genérica, así como de reportar periódicamente cambios en los integrantes de los grupos.
- Los usuarios deben limitarse de enviar información sensible a través del correo electrónico institucional, en caso de requerirlo deben hacerlo protegiendo el archivo con contraseña y/o usando un sistema de encriptación.
- Los usuarios no deben manipular las cabeceras de los mensajes electrónicos para intentar ocultar o falsear la identidad del usuario remitente del mensaje.
- Los usuarios del correo electrónico institucional en caso de recibir spam deben marcarlo como tal y reportarlo a los siguientes correos electrónicos incidentesinformacion@puce.edu.ec, SOPORTEREMOTO@puce.edu.ec; infrati@puce.edu.ec;

- Los usuarios al usar el correo electrónico institucional deben aplicar criterio profesional como por ejemplo seguir las reglas de etiqueta generalmente aceptadas, revisar cuidadosamente el contenido antes de enviarlo, no relevar innecesariamente información confidencial.
- Los usuarios no deben usar el correo electrónico institucional para enviar declaraciones a nivel personal que podrían ser interpretadas como una declaración pública oficial sobre la PUCE, a menos que sea un portavoz explícitamente autorizado por la universidad.
- Los usuarios no deben hacer uso de servicios de correo electrónico externos o de terceros similares para enviar información institucional.
- Los usuarios no deben usar el correo electrónico institucional para enviar mensaje desde la cuenta de otra persona o en su nombre, las/los asistentes autorizados pueden enviar un correo electrónico en nombre de un tercero a través de la opción 'enviar en nombre de'.
- El uso del correo electrónico institucional únicamente está permitido para estudiantes vigentes, personal administrativo y/o docente que mantiene una relación laboral con la PUCE, en caso de que la necesidad institucional requiera el uso para otro segmento se lo deberá gestionar a través de la creación de un subdominio bajo análisis de pertinencia por parte del Comité Nacional de Seguridad de la Información.
- Los usuarios no deben almacenar información personal en su cuenta de correo institucional.
- Los usuarios deben limpiar periódicamente su buzón por ejemplo eliminar correos electrónicos antiguos que ya no son necesarios.
- Los usuarios deben incluir al final del correo electrónico el texto de descargo de responsabilidad.

5.7. Lineamiento para el uso del servicio de internet institucional

- El uso del servicio de internet institucional debe enfocarse en el desarrollo de actividades académicas y/o laborales con base en el rol que desempeña.
- Se limita el uso del internet para publicar, distribuir o transferir información clasificada como de uso interno, confidencial y/o restringida sin disponer de la autorización del propietario del activo de información y/o que no corresponda a las funciones que desempeña en la institución.
- Se limita el uso del internet para distribuir información que vulnere la Política de Protección de Datos Personales de la PUCE.
- Se limita el uso de internet para realizar conexiones remotas a dispositivos y/o infraestructura de terceros sin autorización y/o no correspondencia al rol que desempeña en la institución.
- Se limita el uso del internet para realizar descargas de software o contenido protegido por derechos de autor sin disponer de la licencia y/o aprobación legitimo para su uso.
- Se limita el uso de internet para visitar sitios, realizar o distribuir actividades ilegales, con contendido obsceno, ofensivo, difamatorio, de acoso, racista, juegos de azar, fraude, spam o piratería de software/medios, de hackeo, o de gran tamaño que pueda poner en riesgo la seguridad y/o el rendimiento de la infraestructura de la institución.
- Se limita el uso de internet para el cometimiento de actividades deliberadas tales como introducir malware o que impliquen desperdicio de recursos.
- Cualquier archivo descargado del internet deberá ser analizado por el antivirus.

6. GLOSARIO

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.

Aprovisionamiento de usuarios. - proceso de gestión de acceso y cuentas de usuario, a través del cual se garantiza que la creación, modificación o revocación de derechos de acceso de usuarios esté actualizado.

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

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.

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

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.

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

Servidor. - es un computador que forma parte de una red informática y provee de servicios específicos al resto de dispositivos que son parte de la red. Es un equipo que se encarga de procesar y almacenar información que será compartida con otros dispositivos que son parte de la red.

Sharepoint. - es una plataforma de colaboración y gestión de contenido de Microsoft, en la cual se puede crear sitios web, almacenar, organizar y compartir información.

Tiempo de retención documental. - instrumento donde se especifica el tiempo de retención o conservación de los documentos, para cuya definición se consideran los tiempos en términos de reserva legal, caducidad, prescripción de las acciones legales que recaen sobre los mismos.

DISPOSICIONES GENERALES

PRIMERA. - los presentes lineamientos entrarán en vigencia una vez que sea aprobada y derogará cualquier disposición de igual o menor jerarquía que se hayan emitido con anterioridad en la matriz

o sedes, para su posterior difusión conforme lo prevé la normativa vigente y aplicable de la institución.

SEGUNDA. - encargar la codificación y difusión de los presentes lineamientos a la Secretaría General de la PUCE.

TERCERA. - el responsable de la unidad encargada de la seguridad de la información o su delegado realizará revisiones periódicas aleatorias respecto del cumplimiento de los lineamientos, a través de cualquier método visitas recorridos periódicos, monitoreo automatizado, informes de herramientas comerciales, auditorías internas y externas.

CUARTA. - cualquier excepción a los presentes lineamientos deberán ser revisados por los responsables de las unidades encargadas de seguridad de la información, así como de las tecnologías de la información.

QUINTA. - la unidad encargada de las tecnologías de la información deberá verificar periódicamente según corresponda el cumplimiento de los presentes lineamientos a través de los procedimientos establecidos.

SEXTA. - el colaborador que haya infringido los presentes lineamientos estará sujeto a medidas disciplinarias definidas por la unidad encargada de talento humano y el marco normativo vigente.

DISPOSICIONES TRANSITORIAS

PRIMERA. -el cumplimiento de los presentes lineamientos están supeditados a la asignación de recursos y priorización de la ejecución de iniciativas para la implementación de controles de seguridad de la información conforme a las políticas institucionales. El responsable de la unidad encargada de la seguridad de la información validará aquellos controles que están en ejecución, implementación o a ser implementados para lo cual, las máximas autoridades de la PUCE procurarán la asignación de recursos y priorización de la ejecución de iniciativas para la implementación de controles de seguridad de la información.

SEGUNDA. – Las denominaciones de los actores, así como las áreas responsables de articular el cumplimiento de los presentes lineamientos se ajustarán una vez que se expida la nueva estructura organizacional de la universidad.

7. FORMULARIOS

7.1. Formulario de definición del tiempo de retención documental

A más de las leyes y/o reglamentos aplicables para la retención de la información, los propietarios de la información deberán considerar que si dentro de la misma consta información de carácter personal se deberá dar cumplimento a lo estipulado en la Ley Orgánica de Protección de Datos.

Nombre carpeta nivel 1	Nombre carpeta nivel 2	Nombre carpeta nivel 3	Propietario de la Información	Nombre de área o unidad académica y/o administrativa propietaria	Nombre de subárea académica y/o administrativa propietaria	Descripción de la información almacenada en la carpeta nivel 3	Tipo archivo (pdf, word, excel, imagen, audio, video)	Especificar si la información es un insumo	Confidencialidad	Integridad	Disponibilidad	Tamaño	Tiempo de almacenamiento conservación activo	Frecuencia de respaldo almacenamiento activo	Tiempo de almacenamiento conservación pasivo	Ubicación

ACTA DE APROBACIÓN

Aprobación	Firma	Sumilla	Fecha
Mónica Mancheno **Directora de Aseguramiento de la Calidad**			Enero 2024
Revisión			
Charles Escobar **Presidente del Comité de Seguridad de la Información**			Enero 2024
Elaboración			
Karina Molina **Oficial de Seguridad de la Información**			Enero 2024

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación	Aprobado por
V 01.01	Enero 2024	Versión inicial	Directora de Aseguramiento de la Calidad