NORMAS INSTITUCIONALES PARA EL USO DE TECNOLOGÍAS DE INFORMACIÓN

REVISADO POR	APROBADO POR
Coordinador de Seguridad TI Jefe de Infraestructura de TI Director del Centro de Servicios Informáticos Director de la Oficina Jurídica Secretario General de la Seccional	Vicerrector Administrativo

Tabla de contenido

1. OBJETIVO

La Pontificia Universidad Javeriana Cali establece normas y lineamientos para el uso adecuado de los recursos tecnológicos de información y comunicación, con el objetivo de garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información. Estas normas aplican a todos los miembros de la comunidad universitaria y deben ser cumplidas de manera responsable y ética. El acceso a los recursos será otorgado según el principio de mínimo privilegio, y los usuarios deberán proteger la información confidencial, asegurando su correcta gestión y evitando su divulgación no autorizada. Además, la Universidad se compromete a garantizar la integridad y disponibilidad de la información, y el incumplimiento de estas normas podrá conllevar sanciones, conforme a los procedimientos disciplinarios establecidos.

2. GENERALIDADES

El cumplimiento de las normas institucionales establecidas en el presente documento es obligatorio para todos los usuarios de las Tecnologías de Información y Comunicación de la Pontificia Universidad Javeriana Cali.

Cualquier infracción a estas normas podrá dar lugar a medidas correctivas, que incluyen, pero no se limitan a, la suspensión o cancelación de cuentas de usuario, la suspensión indefinida de los servicios tecnológicos y la aplicación de sanciones conforme a los reglamentos internos de la Universidad o a los contratos firmados entre las partes, así como aquellas de naturaleza legal que correspondan.

El Centro de Servicios Informáticos (CSI), a través de su Coordinación de Seguridad TI, es la entidad encargada de supervisar y garantizar el cumplimiento de estas disposiciones.

3. DEFINICIONES

- **Activo de Información:** Cualquier elemento relacionado con el tratamiento de información que tiene valor para la organización, incluyendo procesos de negocio, datos, aplicaciones, equipos informáticos, soportes de información, redes y/o instalaciones.
- **Alta Disponibilidad:** Característica de un sistema o servicio que minimiza el tiempo de inactividad en caso de fallo, garantizando que el servicio esté accesible con la menor interrupción posible.

- **Análisis de Riesgos:** Proceso sistemático de identificación de activos de información, evaluación de sus vulnerabilidades y amenazas, y determinación de la probabilidad e impacto de estas amenazas, con el objetivo de implementar controles apropiados para mitigar los riesgos.

- **Análisis de Vulnerabilidades:** Proceso de identificación y documentación de fallos o debilidades en sistemas informáticos, tanto físicas (ej. inundaciones, incendios) como lógicas (ej. configuraciones incorrectas, desactualización), que podrían ser explotadas maliciosamente, representando un riesgo para la seguridad de la organización.

- **Antivirus:** Software diseñado para detectar, prevenir y eliminar programas maliciosos (malware) que intenten dañar un sistema informático o comprometer su integridad.

- **Auditoría de Seguridad:** Evaluación exhaustiva realizada por profesionales en tecnologías de la información (TI), destinada a identificar vulnerabilidades en sistemas, redes, servidores y aplicaciones, asegurando que se cumplan las políticas y estándares de seguridad.

- **Autenticación:** Proceso mediante el cual un sistema verifica la identidad de un usuario a través de la presentación de credenciales, como contraseñas, documentos o biometría.

- **Backup (Copia de Seguridad):** Copia de datos o aplicaciones de un sistema informático que permite su recuperación en caso de daño o pérdida de los datos originales.

- **BIA (Business Impact Analysis):** Análisis que evalúa el impacto potencial de la interrupción de procesos críticos de negocio, ayudando a priorizar recursos y definir objetivos de recuperación en un escenario de crisis.

- **Borrado Seguro:** Método de eliminación de archivos que asegura que los datos no puedan ser recuperados, sobrescribiendo múltiples veces el espacio ocupado por la información original, tanto en soportes físicos como digitales.

- **BYOD (Bring Your Own Device):** Política que permite a los empleados utilizar sus dispositivos personales (smartphones, laptops, tablets) para acceder a los recursos tecnológicos y redes corporativas, integrando actividades profesionales y personales en un único dispositivo.

- **Centro de Servicios Informáticos (CSI):** Dependencia encargada de proporcionar y mantener los servicios tecnológicos y sistemas de información necesarios para el funcionamiento de la Universidad, apoyando las necesidades operativas y tecnológicas de la institución.

- **Cifrado:** Proceso de codificación de información para prevenir su acceso no autorizado, de modo que solo aquellos con la clave correspondiente puedan leerla

- **Confidencialidad:** Propiedad que asegura que la información solo sea accesible a las personas autorizadas, protegiendo los datos sensibles de divulgaciones no autorizadas.

- **Contraseña:** Clave secreta utilizada como método de autenticación para acceder a sistemas y recursos informáticos, garantizando que solo usuarios autorizados puedan acceder a la información.

- **Control de Acceso:** Sistema que regula el acceso a los recursos de información, permitiendo su uso solo por aquellos usuarios o entidades con los derechos y privilegios adecuados.

- **Copia de Seguridad:** Proceso que implica duplicar información de un sistema a otro medio de almacenamiento, con el fin de recuperarla en caso de falla del sistema original.

- **Correo Spam:** Correo electrónico no solicitado, generalmente enviado en grandes cantidades con fines publicitarios o maliciosos, como en ataques de phishing.

- **Criticidad:** Medida que evalúa el impacto potencial de un error o incidente en un proceso, sistema o equipo, determinando la importancia de la información y las operaciones afectadas.

- **Cuarentena:** Acción de aislar archivos sospechosos o infectados, previniendo que propague daños al resto del sistema hasta su limpieza o eliminación.

- **Datos Personales:** Información que identifica o puede identificar a una persona física, incluyendo datos de contacto, identificación personal, historial profesional o académico, entre otros.

- **Denegación de Servicio (DoS):** Ataque dirigido a interrumpir el servicio de un sistema, aplicación o dispositivo, saturándolo con solicitudes que lo sobrecargan y lo dejan fuera de servicio.

- **Disponibilidad:** Propiedad de un sistema o servicio que asegura su accesibilidad y uso por parte de los usuarios autorizados cuando lo necesiten.

- **Doble Factor de Autenticación (2FA):** Sistema de autenticación que agrega una capa adicional de seguridad mediante la verificación de un segundo factor, como un código enviado al móvil o una huella dactilar, además de la contraseña.

- **Fuga de Información:** Evento en el que información sensible se filtra o es divulgada sin autorización, afectando la confidencialidad de los datos.

- **Gestión de Incidentes:** Conjunto de actividades planificadas para detectar, responder y mitigar incidentes de seguridad, garantizando la continuidad de los servicios y protegiendo los activos de información.

- **Impacto:** Medición de los efectos causados por un incidente, desastre o riesgo, y cómo estos afectan los procesos, operaciones y niveles de servicio de la organización.

- **Incidente de Seguridad:** Cualquier suceso que compromete la confidencialidad, integridad o disponibilidad de los activos de información de la organización, requiriendo una respuesta para mitigar sus efectos.

- **Integridad:** Propiedad que asegura que la información no ha sido alterada de manera no autorizada, manteniendo su exactitud y fiabilidad a lo largo del tiempo.

- **Ingeniería Social:** Técnicas utilizadas por atacantes para manipular a los usuarios y obtener información confidencial, como credenciales o datos de acceso, aprovechando la confianza humana.

- **Malware:** Software diseñado para infiltrarse y dañar un sistema informático sin el consentimiento del propietario, comprometiendo su seguridad y funcionamiento.

- **Parche de Seguridad:** Actualización de software destinada a corregir vulnerabilidades y fallos de seguridad en programas o sistemas operativos, protegiendo contra posibles ataques.

- **Pasarela de Pagos:** Servicio que facilita la transmisión segura de datos financieros entre compradores y vendedores en plataformas de comercio electrónico, garantizando la seguridad en las transacciones.

- **Phishing:** Técnica de ataque en la que los delincuentes se hacen pasar por entidades legítimas para engañar a los usuarios y obtener información sensible, como contraseñas o datos bancarios.

- **Plan de Contingencia:** Estrategia diseñada para garantizar la continuidad de los servicios críticos en caso de incidentes graves, incluyendo recursos, organización y procedimientos para restaurar la operación de los sistemas afectados.

- **Plan de Continuidad de Negocio (BCP):** Conjunto de planes de emergencia, comunicaciones, recursos y contingencias que permiten a la organización seguir operando frente a situaciones de crisis, asegurando la protección de la información y los procesos esenciales.

- **Recursos Tecnológicos:** Conjunto de infraestructuras y herramientas tecnológicas, tanto de hardware como de software, utilizadas para facilitar las actividades y operaciones dentro de la organización.

- **Redundancia:** Estrategia de duplicación de componentes, sistemas o servicios que permite mantener la operación en caso de fallo o fallo parcial de los recursos primarios.

- **Resiliencia:** Capacidad de una organización para adaptarse y recuperarse rápidamente ante incidentes o adversidades, manteniendo la continuidad operativa.

- **Respuesta de Incidentes:** Procedimientos documentados y herramientas diseñadas para enfrentar y mitigar los efectos de un incidente de ciberseguridad, minimizando su impacto en los activos y servicios críticos.

- **Riesgo:** Probabilidad de que una amenaza explote una vulnerabilidad en el sistema, causando un daño o pérdida de información o accesibilidad.

- **SLA (Acuerdo de Nivel de Servicio):** Contrato que define el nivel de calidad y servicio que un proveedor de servicios se compromete a ofrecer a su cliente, estableciendo indicadores de desempeño y responsabilidades.

- **Suplantación de Identidad:** Acto de un atacante que se hace pasar por una persona o entidad legítima para cometer fraudes, acceder a sistemas o robar información sensible.

- **Tecnologías de Información y Comunicación (TIC):** Conjunto de herramientas y recursos tecnológicos que facilitan el procesamiento, almacenamiento, transmisión y acceso a la información, incluyendo hardware, software y redes de comunicación.

- **Usuario:** Persona autorizada para utilizar los recursos y servicios de Tecnologías de Información y Comunicación proporcionados por la Universidad, ya sea de forma permanente o temporal.

- **Vulnerabilidad:** Debilidad o defecto en un sistema que puede ser explotado por una amenaza para causar daño o comprometer la seguridad de los activos de información.

4. NORMAS INSTITUCIONALES PARA EL USO DE RECURSOS TECNOLÓGICOS

4.1. Gestión de Activos de Información.

La gestión adecuada de los activos de información es fundamental para proteger la confidencialidad, integridad y disponibilidad de los datos dentro de la Universidad.

Esto implica no solo la correcta clasificación y manejo de la información, sino también garantizar su resguardo, respaldo y, en su caso, eliminación segura. A continuación, se detallan las directrices que todos los usuarios deben seguir para asegurar una gestión efectiva de los activos de información.

- Los usuarios deben seguir el procedimiento establecido para la devolución de los activos de información, asegurando que estos sean entregados en condiciones adecuadas y sin comprometer la seguridad de la información almacenada

- Cualquier incidente o actividad no autorizada relacionada con los activos de información debe ser reportada de inmediato tanto al responsable del activo como al CSI, para que se tomen las acciones correctivas y preventivas correspondientes.

- La información debe ser clasificada y etiquetada de acuerdo con su nivel de

criticidad, siguiendo el procedimiento de clasificación y etiquetado definido por la Universidad. Este proceso es esencial para determinar las medidas de seguridad a aplicar, según la sensibilidad de la información.

- El líder de cada proceso es responsable de mantener actualizado el inventario de los activos de información bajo su cargo. Este inventario debe ser revisado y actualizado al menos una vez al año. Cualquier cambio o actualización en el inventario debe ser reportado al CSI, garantizando la correcta gestión y seguimiento de los activos.

- Además, el usuario debe implementar los mecanismos de respaldo necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información almacenada en los equipos asignados. Esto implica realizar copias de seguridad periódicas y seguir los procedimientos definidos para la restauración de los datos.

- La información institucional debe ser almacenada exclusivamente en las plataformas oficiales autorizadas por la Universidad, utilizando Onbase como sitio de custodia y repositorio institucional, SharePoint como sitio de trabajo colaborativo y de gestión de los documentos de las dependencias. Es responsabilidad de los usuarios hacer un uso adecuado de estas plataformas, garantizando la correcta protección y disponibilidad de la información.

- Los activos que contengan información confidencial o sensible deben ser protegidos adecuadamente contra el acceso no autorizado, el uso indebido o la corrupción. Se deben adoptar todas las medidas de seguridad necesarias, como cifrado de datos, control de accesos y monitoreo constante, para asegurar la protección de estos activos.

- Todos los procedimientos establecidos para el almacenamiento, eliminación o destrucción de los activos de información deben ser seguidos de manera rigurosa. Esto incluye el manejo adecuado de los dispositivos de almacenamiento, la destrucción segura de la información y la eliminación permanente de los datos que ya no sean necesarios, cumpliendo con las mejores prácticas de seguridad de la información

4.2. Gestión de Cuentas de Usuario.

La gestión adecuada de las cuentas de usuario es esencial para garantizar la seguridad, privacidad y eficiencia en el uso de los recursos digitales de la Universidad. Este proceso debe seguir estrictamente las políticas definidas, que

aseguren el uso exclusivo de las cuentas para fines laborales, académicos y legales, protegiendo tanto la información institucional como la de los usuarios.

A continuación, se detallan las normas y directrices relacionadas con la gestión de las cuentas de usuario en diferentes contextos dentro de la Universidad:

- Las cuentas de usuario son propiedad exclusiva de la Universidad, al igual que la información que en ellas se almacena. Estas cuentas deben ser utilizadas exclusivamente para fines académicos, laborales o legales, evitando cualquier uso personal.

- La Universidad se reserva el derecho de gestionar y disponer de las cuentas de usuario en cualquier momento, según lo considere necesario.

- Si se sospecha que una cuenta de usuario ha sido comprometida, el incidente debe ser reportado inmediatamente al correo seguridad.ti@javerianacali.edu.co para activar las medidas correctivas correspondientes.

- El acceso a las cuentas debe realizarse únicamente a través de redes seguras. Se debe evitar el uso de redes públicas, ya que son más vulnerables a ataques que comprometan la seguridad de la información o la identidad del usuario.

- Al acceder a las cuentas desde dispositivos externos, se recomienda asegurar que el equipo esté protegido con antivirus actualizado y que el sistema operativo cuente con las últimas actualizaciones. Además, es fundamental cerrar sesión correctamente al finalizar cualquier actividad.

- En caso de que el CSI detecte una posible vulnerabilidad o compromiso en una cuenta de usuario, notificará al usuario mediante correo electrónico y tomará las medidas adecuadas, como el cambio de contraseñas, para mitigar cualquier riesgo.

- Las cuentas genéricas o de servicio deberán contar con un responsable asignado. Los usuarios de estas cuentas solo podrán ser designados y autorizados por el CSI. Además, se evaluará anualmente la continuidad de estas cuentas, tomando en cuenta las necesidades y responsabilidades asociadas.

- Las cuentas de usuario de personas reportadas como fallecidas serán inactivadas de inmediato.

Consideraciones para estudiantes:

- Los estudiantes tienen derecho a crear una cuenta de usuario a través del autoservicio en línea, una vez completado el proceso de matrícula.
- Si un estudiante finaliza sus estudios y se convierte en egresado, su cuenta se mantendrá activa bajo su nueva categoría. La cuenta será vitalicia, pero se desactivará si no se utiliza durante un período de dos años.
- En caso de que el estudiante realice un retiro temporal o definitivo, su cuenta permanecerá activa por un plazo máximo de dos años. Si no se registra actividad dentro de ese período, la cuenta será desactivada.
- En situaciones de expulsión o exclusión, la cuenta será desactivada inmediatamente.
- Los estudiantes que además sean colaboradores o profesores de la Universidad recibirán una nueva cuenta exclusiva para su rol de estudiante, separada de la cuenta vinculada a su actividad laboral o docente.
- Los egresados que no cuenten con cuenta institucional podrán solicitarla mediante una solicitud formal al CSI.

Consideraciones para colaboradores y profesores:

- La cuenta de usuario de los colaboradores y profesores será asignada por la Oficina de Gestión Humana al momento de su vinculación laboral.
- La cuenta estará conformada por la combinación del nombre y apellido del usuario, salvo excepciones derivadas de situaciones previas a la implementación de esta directriz.
- La cuenta de usuario de los colaboradores y profesores se desactivará al finalizar su contrato.
- Si un colaborador o profesor ya posee una cuenta como estudiante, se le asignará una cuenta adicional para su actividad laboral o docente.
- En caso de un cambio de cargo dentro de la Universidad, no se generará una nueva cuenta, sino que la cuenta existente será modificada según corresponda.

Consideraciones para proveedores y contratistas:

- Los proveedores y contratistas deberán solicitar una cuenta de usuario a través del CSI, gestionada por el líder del proceso o la persona responsable de la relación con el proveedor.

- La solicitud debe incluir los datos personales del titular, la justificación para la creación de la cuenta y la duración de la relación contractual.

- Cada cuenta de proveedor o contratista deberá contar con un responsable dentro de la Universidad, que garantice el uso adecuado de la cuenta.

- Al concluir la relación contractual, la cuenta de usuario será desactivada. En caso de requerir una extensión, el responsable debe solicitarlo formalmente al CSI.

4.3. Gestión de Contraseñas.

La gestión de contraseñas es un componente crucial para la seguridad de los sistemas de información de la Universidad. Una contraseña robusta y bien gestionada asegura la protección de los datos y el acceso a los recursos digitales. A continuación, se presentan las directrices y procedimientos para una adecuada gestión de contraseñas, enfocados en garantizar la confidencialidad y la integridad de los accesos.

- Las contraseñas deben tener al menos 10 caracteres e incluir una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Además, deben ser fáciles de recordar, pero no deben basarse en información personal o identificable por terceros o personas cercanas.

- Cada usuario es responsable de mantener su contraseña confidencial e intransferible. En ningún caso debe compartirla con otros usuarios, ni revelarla por medios telefónicos, por correo electrónico u otros canales de comunicación.

- Los usuarios deberán actualizar sus contraseñas dentro de los plazos establecidos por la Universidad. En caso de sospecha de que otra persona ha conocido su contraseña, el usuario debe cambiarla inmediatamente para evitar posibles compromisos de seguridad.

- La gestión del cambio de contraseña es responsabilidad del propio usuario. Para garantizar que el cambio se realice de forma segura, los usuarios deben seguir

los procedimientos establecidos por la Universidad.

- La Universidad permite y fomenta el uso de gestores de contraseñas para facilitar la creación y gestión de contraseñas fuertes y seguras. Esta herramienta ayuda a los usuarios a almacenar y acceder a sus contraseñas de forma segura y eficiente

- Al crear un nuevo usuario en cualquier sistema de la Universidad, el administrador podrá asignar una contraseña inicial. El sistema solicitará automáticamente el cambio de contraseña al realizar el primer acceso, asegurando que el usuario configure una clave personalizada y segura.

- Los sistemas de información críticos de la Universidad implementan mecanismos de seguridad adicionales, como la autenticación de doble o múltiple factor (2FA o MFA), para reforzar la protección de los accesos.

- Las contraseñas de usuarios privilegiados deben ser actualizadas o bloqueadas de inmediato tras la desvinculación de un colaborador, profesor, proveedor o contratista que haya tenido acceso a cuentas con privilegios. Asimismo, se deben modificar las contraseñas de los servicios a los que dicho usuario haya tenido acceso, para evitar cualquier riesgo de intrusión.

- Las credenciales por defecto proporcionadas por los fabricantes de hardware o software deben ser cambiadas inmediatamente después de la instalación de cualquier equipo o software adquirido por la Universidad. Esto es fundamental para evitar vulnerabilidades en los sistemas.

4.4. Gestión de la Ciberseguridad.

La ciberseguridad es una prioridad fundamental para proteger la infraestructura tecnológica de la Universidad y asegurar la integridad, confidencialidad y disponibilidad de la información institucional. El Centro de Servicios Informáticos (CSI) es el responsable principal de gestionar la ciberseguridad, implementando estrategias y herramientas para salvaguardar los sistemas y los datos frente a amenazas y riesgos cibernéticos. A continuación, se detallan las funciones y responsabilidades clave en la gestión de la ciberseguridad:

- El CSI es responsable de proteger la red institucional, los servidores y las bases de datos mediante la implementación de medidas de seguridad avanzadas, tales como firewalls, sistemas de detección de intrusiones (IDS) y controles de acceso. Estas medidas garantizan la integridad, disponibilidad y confidencialidad

de la información, previniendo accesos no autorizados o ataques cibernéticos.

- Todos los equipos de cómputo y servidores deben contar con protección antimalware (antivirus) actualizada y con los sistemas operativos en su última versión para prevenir y detectar posibles amenazas de software malicioso. El CSI asegura que estos sistemas estén debidamente configurados y actualizados

- Los dispositivos de acceso a la red, los equipos de red, los servidores y las bases de datos no deben ser instalados con configuraciones, credenciales o claves predeterminadas. Además, se debe asegurar que existan copias de respaldo de las configuraciones de estos dispositivos, lo que garantiza su recuperación rápida en caso de fallas técnicas y minimiza riesgos operativos.

- El CSI implementara una segmentación adecuada de las redes de datos a través de dominios, grupos de servicios, áreas o ubicaciones. El uso de VLANs (Redes de Área Local Virtual) permite separar lógicamente las redes, lo que reduce el acceso no autorizado y protege los activos más críticos y la información sensible.

- El CSI debe monitorear continuamente la capacidad del proveedor de servicios de red para asegurarse de que se gestionen los servicios contratados de manera segura, conforme a los lineamientos establecidos por la gestión de TI, y se cumpla con los estándares de ciberseguridad definidos por la Universidad.

- El CSI debe integrar medidas específicas de ciberseguridad en todas las etapas del ciclo de vida del desarrollo de software. Esto incluye la realización de análisis de vulnerabilidades, pruebas de penetración y la implementación de controles de acceso. De esta manera, se garantiza que las aplicaciones creadas sigan los estándares y mejores prácticas para la seguridad de la información.

- Para proteger las aplicaciones contra ataques de denegación de servicio (DoS), el CSI implementará tecnologías como WAF (Firewall de Aplicaciones Web) y CAPTCHA. Estas medidas ayudan a mitigar las amenazas y a garantizar la disponibilidad y seguridad de las aplicaciones de la Universidad.

- En las interfaces de carga de archivos, el CSI debe restringir el tamaño y tipo de archivos permitidos para evitar la ejecución de archivos potencialmente maliciosos, como programas o scripts. Esta medida ayuda a proteger la seguridad de las aplicaciones y la infraestructura tecnológica.

- El CSI diseñara y aplicara procedimientos y mecanismos específicos para prevenir la fuga de información sensible, utilizando tecnologías de cifrado y control de acceso para evitar que los datos críticos sean divulgados de manera

no autorizada.

- Toda la información sensible que circule por las redes de la Universidad debe ser cifrada mediante protocolos seguros, como HTTPS, para protegerla durante su transmisión y evitar accesos no autorizados.

- El CSI desarrollará y mantendrá procedimientos para la identificación, análisis y gestión de incidentes de ciberseguridad, con el fin de proteger la infraestructura tecnológica frente a amenazas. Este enfoque incluye la respuesta rápida ante posibles incidentes y la restauración de los servicios afectados.

- Se debe llevar a cabo una evaluación continua de los riesgos cibernéticos que puedan afectar a la Universidad. Las estrategias de respuesta, recuperación y restauración deben estar integradas en el plan de continuidad del negocio para enfrentar posibles ataques cibernéticos.

- Se implementarán programas de concientización en ciberseguridad dirigidos a toda la comunidad universitaria, con el objetivo de fortalecer la cultura de seguridad y reducir los riesgos asociados al manejo de la información y los sistemas tecnológicos.

- El CSI llevará a cabo auditorías periódicas y un monitoreo proactivo de la infraestructura tecnológica, que incluirá redes, servidores y aplicaciones, para detectar vulnerabilidades y posibles brechas de seguridad. Estas acciones son fundamentales para garantizar la resiliencia de los sistemas frente a amenazas cibernéticas.

4.5. Seguridad en los Recursos Humanos.

La seguridad de la información no solo depende de la infraestructura tecnológica, sino también de la gestión de los recursos humanos, quienes juegan un papel crucial en el cumplimiento de las políticas y en la protección de los datos sensibles de la Universidad. La siguiente normativa establece las directrices que deben seguir todos los colaboradores, profesores y contratistas para asegurar que la información se maneje de manera adecuada y que los recursos tecnológicos sean utilizados de forma responsable y conforme a las políticas de seguridad de la Universidad.

- Todos los contratos laborales, de aprendizaje y de contratistas deberán incluir cláusulas de confidencialidad y responsabilidad sobre el uso adecuado de las herramientas tecnológicas y la información. Estas cláusulas deben garantizar el cumplimiento de las políticas de seguridad de la información, la protección de

datos personales, la propiedad intelectual y la aceptación del monitoreo de herramientas tecnológicas corporativas.

- En caso de incumplimiento de las políticas de seguridad de la información, se aplicarán las sanciones contempladas en el reglamento interno de trabajo. La investigación y la sanción de la conducta se llevarán a cabo conforme a las normativas vigentes en la Universidad.

- Si el incumplimiento proviene de un tercero contratado, se aplicarán las sanciones contractuales previamente establecidas. En situaciones graves, se podrán activar las sanciones civiles y penales correspondientes para proteger los intereses de la Universidad.

- Si se confirma que una violación a las políticas de seguridad de la información ha causado un incidente que compromete la Universidad, se procederá de inmediato a revocar los derechos de acceso del responsable. Esto iniciará un proceso disciplinario conforme a los términos contractuales y a las responsabilidades relacionadas con la seguridad de la información.

- La Oficina de Gestión Humana notificará oportunamente los cambios de cargo, rol o retiro de colaboradores y profesores. Esta notificación iniciará el proceso de inactivación de usuarios y perfiles asociados durante su permanencia en la Universidad, asegurando que no queden accesos activos que puedan comprometer la seguridad.

- El proceso de terminación de contrato para colaboradores, profesores y terceros incluirá la devolución de todos los activos relacionados con la información bajo su responsabilidad, tales como software, documentos corporativos, equipos tecnológicos (dispositivos móviles, tarjetas de acceso, credenciales de administración, entre otros) y la información almacenada en medios electrónicos. Este procedimiento es clave para asegurar que no se pierda el control sobre los activos institucionales.

- El CSI definirá y comunicará un procedimiento formal para la eliminación de datos biométricos, cuentas de usuario, roles y perfiles en los sistemas de información de aquellos que ya no pertenezcan a la Universidad. Este proceso de depuración se realizará de forma periódica o bajo solicitud, garantizando que los datos y accesos sean gestionados de manera adecuada.

- Se implementarán programas periódicos de inducción, capacitación y sensibilización para asegurar que toda la comunidad Javeriana reciba información actualizada sobre las políticas, lineamientos y procedimientos de seguridad de la información. Esta formación es esencial para fortalecer la cultura de seguridad en todos los miembros de la Universidad.

- Los colaboradores y profesores son responsables de la custodia, el cuidado y el uso adecuado de los equipos de cómputo y periféricos asignados. Esto incluye la obligación de reportar inmediatamente cualquier daño, pérdida o incidente relacionado con dichos equipos, para minimizar riesgos y garantizar la operatividad de los sistemas.

- Los equipos de cómputo y periféricos asignados a los colaboradores y profesores son exclusivamente para el desempeño de funciones relacionadas con sus cargos. Se debe priorizar el uso de los recursos y los datos de la Universidad, evitando almacenar información personal en dichos dispositivos, para proteger la confidencialidad de la información institucional.

- En la finalización del contrato de colaboradores, profesores o terceros, se llevará a cabo una revisión exhaustiva de los accesos a los sistemas de información de la Universidad. Esto garantizará que todos los permisos y accesos sean eliminados o revocados de inmediato, asegurando que no queden accesos sin control tras la desvinculación.

- Los colaboradores, profesores y contratistas deberán hacer un uso responsable de las herramientas de inteligencia artificial generativa, absteniéndose de ingresar, procesar o compartir información confidencial, sensible o protegida de la Universidad a través de estas plataformas. Su utilización debe alinearse en todo momento con las directrices de seguridad de la información y preservar la confidencialidad de los datos institucionales.

4.6. Escritorio y Pantalla limpia.

La protección de la información sensible y confidencial es responsabilidad de todos los usuarios, no solo dentro de los sistemas informáticos, sino también en el entorno físico de trabajo. Para evitar la exposición no autorizada y minimizar los riesgos de acceso a datos críticos, es fundamental implementar buenas prácticas en la gestión de la información, tanto digital como en papel, en los espacios de trabajo. A continuación, se detallan las directrices clave para garantizar un ambiente seguro y proteger la información institucional.

- La información sensible solo debe ser impresa en casos estrictamente necesarios y cuando sea indispensable contar con un documento físico que respalde dicha información. La impresión innecesaria de documentos con datos confidenciales debe evitarse siempre que sea posible.

- Es esencial que los documentos impresos que contienen información confidencial se recojan de inmediato de las impresoras para evitar que personas

no autorizadas tengan acceso a dicha información. El control de acceso a estos documentos es clave para preservar la seguridad de la información.

- La información confidencial o de uso interno (como papeles, documentos, o medios de almacenamiento electrónico) debe mantenerse guardada en lugares seguros cuando no se requiera, como cajas fuertes o gabinetes con llave. Esta medida es especialmente importante cuando la oficina esté desocupada o fuera del horario laboral, para proteger la información de accesos no autorizados.

- Los puestos de trabajo ubicados cerca de zonas de atención o áreas de tránsito frecuente deben organizarse de manera que las pantallas de los equipos no sean visibles para terceros o personal no autorizado. Esto ayuda a evitar que la información sensible sea vista accidentalmente por personas ajenas a la tarea.

- El CSI implementará soluciones de seguridad, como el bloqueo automático de sesión, para proteger las estaciones de trabajo cuando los usuarios se ausenten temporalmente. Estas soluciones son parte de un enfoque integral para garantizar que la información no esté expuesta de manera inadvertida.

- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo cuando se retiren de su puesto, incluso si es solo por un corto período de tiempo. La sesión solo podrá ser desbloqueada con la contraseña del usuario, lo que garantiza que la información no quede accesible a personas no autorizadas.

- Al finalizar la jornada laboral, el usuario debe asegurarse de cerrar todas las aplicaciones y apagar los equipos o dejar la sesión debidamente bloqueada. Esta medida es crucial para evitar que información sensible quede expuesta cuando el equipo no está en uso.

4.7. Seguridad de las Operaciones.

La seguridad de las operaciones tecnológicas es crucial para mantener la integridad, confidencialidad y disponibilidad de la infraestructura tecnológica de la Universidad. Los usuarios, administradores de sistemas y otros actores involucrados tienen la responsabilidad de seguir protocolos y directrices que minimicen los riesgos y garanticen la correcta gestión de la información. A continuación, se presentan las políticas clave que deben observarse para asegurar que las operaciones tecnológicas se realicen de manera segura y eficiente.

- Todos los usuarios son responsables de realizar el respaldo de la información

almacenada en los activos de información bajo su responsabilidad. Este proceso debe seguir los lineamientos establecidos para garantizar la disponibilidad de los datos ante posibles fallos.

- No está permitido desinstalar ni deshabilitar el software preinstalado en los equipos de cómputo proporcionados por la Universidad, ni formatear el sistema operativo. Cualquier cambio en la configuración debe ser autorizado y realizado por personal del CSI.

- Todos los equipos de cómputo de la Universidad deben estar en el dominio institucional, y los usuarios deben iniciar sesión utilizando sus credenciales de dominio. Las cuentas locales solo se autorizarán en casos excepcionales, con la aprobación previa del CSI. En estos casos, los usuarios deberán firmar un compromiso de buen uso en términos de seguridad.

- Queda estrictamente prohibido la posesión, descarga y uso de archivos con contenido obsceno o ilegal, así como la instalación de software, música, videos y gráficos sin la licencia correspondiente, en los equipos de cómputo proporcionados por la Universidad.

- Los equipos de terceros que se conecten a la red de la Universidad deben cumplir con los requisitos mínimos de seguridad, tales como contar con un sistema operativo licenciado, actualizado y con protección antivirus. Los usuarios de estos equipos también deberán aceptar y cumplir con la Política y los Lineamientos de Seguridad de la Información.

- Deben establecerse procedimientos claros para el control de los cambios en la infraestructura tecnológica o en las aplicaciones, con el fin de asegurar que estos no comprometan la seguridad operativa.

- Los sistemas de información deben conservar registros de auditoría (logs) que documenten cada cambio realizado. Estos registros deberán mantenerse mediante una herramienta de control de cambios que garantice la trazabilidad y seguridad de las modificaciones.

- Antes de implementar cualquier cambio en los sistemas, estos deben ser evaluados y probados en colaboración con los líderes de procesos y los usuarios. Además, deberán ser aprobados por el Comité de Cambios del CSI, para asegurar su cumplimiento con los estándares de seguridad y funcionalidad.

- Deben establecerse procedimientos específicos para la ejecución de copias de seguridad, con la definición de períodos de rotación de los medios y la frecuencia

de las copias, con el fin de asegurar la continuidad de los procesos y el cumplimiento de las normativas vigentes.

- Al menos dos veces al año, se deben realizar ejercicios de restauración de copias de respaldo en ambientes controlados, para garantizar la disponibilidad de los medios de respaldo y minimizar los riesgos durante una restauración de la información.

- Las copias de respaldo deben almacenarse en instalaciones adecuadas, garantizando que la información y los sistemas puedan recuperarse adecuadamente tras un desastre o falla del medio.

- Los medios de respaldo deben ser adecuados para asegurar que toda la información esencial, datos personales y software puedan ser recuperados tras un desastre o fallo de los medios de almacenamiento.

- Los cambios en los sistemas de producción y aplicaciones deben probarse previamente en un ambiente de pruebas antes de ser implementados en producción. Los procedimientos deben ser definidos, comunicados y actualizados periódicamente.

- Se debe contar con una estrategia de reversión (rollback) que permita volver al estado anterior de los sistemas antes de implementar un cambio, asegurando la estabilidad de los sistemas ante cualquier contratiempo.

- Se debe realizar una revisión periódica del contenido de software y datos en los equipos que soportan procesos críticos, con el fin de detectar la presencia de programas no aprobados o modificaciones no autorizadas.

- Los administradores de sistemas no tienen permiso para borrar ni desactivar los registros de auditoría de sus propias actividades. Estos registros deben archivarse de manera segura, preferiblemente en un equipo diferente al que los genera, y de acuerdo con los requisitos de retención establecidos.

- Las actividades de los administradores y operadores del sistema deben ser registradas, y dichos registros deben protegerse y revisarse de manera regular para garantizar la integridad de las operaciones.

- Los relojes de los equipos deben ajustarse para coincidir con la hora oficial del Instituto Nacional de Metrología, y deben tomarse medidas correctivas ante variaciones significativas, para evitar registros inexactos que dificulten futuras investigaciones.

- Debe existir un procedimiento para asegurar el control de las actualizaciones de los sistemas operativos, con la información previa sobre la implementación de estas actualizaciones.

- El CSI debe revisar periódicamente las nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de las aplicaciones para su pronta mitigación.

- La mitigación de vulnerabilidades detectadas se debe realizar después de ejercicios de pentesting (pruebas de penetración) y análisis de vulnerabilidades, garantizando que los sistemas operativos, soluciones de antimalware (antivirus) y navegadores estén actualizados y parchados.

- Si la actualización de los sistemas no es viable, se deberá realizar un análisis de riesgos y adoptar medidas compensatorias para reducir los riesgos a un nivel aceptable.

- Deben elaborarse y ejecutarse planes de acción para mitigar las vulnerabilidades técnicas detectadas, tanto en la plataforma tecnológica como en los sistemas de información.

- Los indicadores de riesgo de los activos críticos deben mantenerse dentro de niveles aceptables, monitoreando continuamente su evolución.

- Los procedimientos operativos deben ser documentados y estar disponibles para todos los colaboradores y profesores involucrados en la ejecución de las actividades, asegurando su correcta aplicación.

- Las pruebas de auditoría que afecten la disponibilidad del sistema deben realizarse fuera del horario laboral para evitar interrumpir las operaciones.

- La Universidad debe someter su Plan de Continuidad de Negocio a pruebas periódicas para garantizar su efectividad ante situaciones adversas.

- El CSI definirá y comunicará una lista actualizada de software y aplicaciones autorizadas para ser instaladas en las estaciones de trabajo de los usuarios, y se llevará a cabo un control exhaustivo para verificar el cumplimiento de los licenciamientos correspondientes.

- Los usuarios no podrán modificar la configuración de las estaciones de trabajo, incluyendo conexiones de red, cuentas locales de usuario, configuraciones

institucionales (como papel tapiz o protector de pantalla) ni archivos de configuración. Cualquier cambio deberá ser realizado exclusivamente por personal autorizado por el CSI.

4.8. Conexiones Remotas y Trabajo en Casa.

La seguridad de la información en el contexto de trabajo remoto es crucial para proteger los activos de información de la Universidad. Los colaboradores y profesores deben seguir las pautas establecidas para garantizar la integridad, confidencialidad y disponibilidad de los datos mientras trabajan de manera remota. A continuación, se detallan las políticas y responsabilidades clave para asegurar la protección de los dispositivos y la información institucional en entornos fuera de las instalaciones universitarias:

- Las pérdidas por hurto, extravío o daño de un equipo de cómputo deben ser reportadas de inmediato al jefe directo, al Centro de Servicios Informáticos (CSI) y a la oficina de activos fijos correspondiente, para tomar las medidas necesarias de recuperación o reposición.

- Los contratos, acuerdos u otros documentos relacionados con el trabajo en casa deben incluir cláusulas que regulen la seguridad de la información, especificando claramente las responsabilidades de los colaboradores respecto a la protección de los equipos y la información mientras trabajan de forma remota.

- Los colaboradores y profesores deben asegurar físicamente sus equipos de cómputo y medios de almacenamiento tanto en el hogar como en cualquier lugar desde donde trabajen remotamente. Esto incluye: Mantener los dispositivos en lugares seguros y evitar la exposición innecesaria de los dispositivos a personas no autorizadas.

- En el trabajo en casa, se debe evitar el uso de redes públicas o no seguras para acceder a los sistemas institucionales. Los colaboradores deben priorizar el uso de conexiones VPN (Red Privada Virtual) y otras soluciones seguras.

- Los colaboradores y profesores que trabajen de manera remota deben ser responsables de seguir todas las pautas de seguridad establecidas para la protección de la información institucional. Además, deben reportar inmediatamente cualquier incidente de seguridad relacionado con sus dispositivos de trabajo remoto.

- Es esencial asegurar que el equipo de cómputo cuente con las medidas de seguridad necesarias para proteger la información. Al menos, los dispositivos

deben incluir: conexión VPN (Red Privada Virtual), software antivirus y antimalware, firewall, actualizaciones controladas del sistema operativo, restricción para la instalación de software no autorizado, cifrado, herramienta de borrado remoto, activación de servicios de geolocalización, autenticación en dos factores, protección antirrobo, entre otras medidas de seguridad.

4.9. Seguridad Física.

La seguridad física de las instalaciones y equipos de la Universidad es fundamental para proteger la información sensible y garantizar que la infraestructura tecnológica funcione correctamente. Las políticas siguientes establecen las responsabilidades y procedimientos para asegurar la integridad física de los activos de información, equipos y documentos en la Universidad.

- La Oficina de Recursos Físicos deberá verificar que todas las puertas de las áreas restringidas estén correctamente cerradas al ingresar o salir. Esto garantiza la protección de la información almacenada y el acceso solo a personal autorizado.

- La Oficina de Recursos Físicos es responsable de garantizar la seguridad de los equipos de cómputo contra hurtos o pérdidas dentro de las instalaciones de la Universidad. Esta acción incluye la protección de la información almacenada en dichos equipos.

- Ningún usuario podrá manipular los equipos de cómputo de la Universidad sin la autorización del Centro de Servicios Informáticos (CSI). Los estudiantes solo podrán hacerlo bajo supervisión y en un ambiente controlado para evitar el acceso no autorizado a información sensible.

- La documentación física de la organización debe ser almacenada en archivos o repositorios seguros que sigan las condiciones establecidas por la función archivística de la Universidad, garantizando así la protección de la información.

- La información física y los dispositivos de almacenamiento removibles deben ser protegidos adecuadamente para evitar accesos no autorizados, pérdidas o daños.

- La Oficina de Recursos Físicos debe validar las condiciones ambientales de las instalaciones de procesamiento de información para evitar daños a los equipos que gestionan datos sensibles. Esto incluye el control de factores como temperatura, humedad, entre otros.

- Los cables de energía eléctrica deben estar separados de los cables de

comunicaciones para evitar interferencias que puedan afectar la seguridad de la información y el funcionamiento adecuado de los sistemas.

- Los centros de cableado y gabinetes de comunicaciones deben estar protegidos con llave para evitar accesos no autorizados, garantizando la integridad de la infraestructura que soporta la información.

- Las instalaciones deben contar con un sistema de alimentación ininterrumpida (UPS) que garantice la continuidad de los procesos y evite la pérdida de información en caso de interrupciones en el suministro eléctrico.

- Se mantendrá un inventario actualizado de los equipos críticos que protegen la infraestructura de información de la Universidad, permitiendo un control efectivo sobre los activos tecnológicos.

- Los equipos y medios de almacenamiento deben someterse a procesos de borrado seguro antes de ser reutilizados o dados de baja, para evitar que la información sensible quede accesible o sea recuperada indebidamente.

- Se debe realizar un análisis de riesgos anual de las instalaciones y procesos críticos relacionados con la seguridad de la información, para identificar posibles amenazas y tomar acciones correctivas.

- Los proveedores de tecnología deben cumplir con los requisitos de seguridad física para soportar adecuadamente la infraestructura tecnológica de la Universidad, asegurando que todos los elementos proporcionados cumplan con las normativas de seguridad física establecidas.

- La Oficina de Recursos Físicos debe programar y realizar un seguimiento periódico de los sistemas de control de acceso a las instalaciones, con el fin de proteger la información de accesos no autorizados. Esto incluye el monitoreo de entradas, salidas y la autenticación de personal autorizado.

4.10. Gestión de Sistemas de Información.

La gestión de los sistemas de información es clave para garantizar la seguridad y el adecuado funcionamiento de las aplicaciones tecnológicas dentro de la Universidad. El Centro de Servicios Informáticos (CSI) es el encargado de implementar políticas y procedimientos que aseguren el acceso controlado, el desarrollo seguro, la gestión de vulnerabilidades y el uso adecuado de datos sensibles, tanto en los sistemas internos como con proveedores externos.

- El CSI es responsable de asignar los permisos de acceso a los sistemas de información y de monitorear periódicamente la validez de los usuarios y sus perfiles de acceso, asegurando que estos se ajusten a las funciones y cargos de cada persona dentro de la Universidad.

- El CSI garantiza que los desarrollos y mejoras de los sistemas de información apliquen metodologías de desarrollo seguro en todas las fases del ciclo de vida del sistema: análisis, diseño, codificación, pruebas, implementación y mantenimiento.

- El CSI asegura que las aplicaciones desarrolladas cuenten con una matriz de roles y responsabilidades al momento de su entrega. Esta matriz facilita la creación de una matriz de perfiles que se asocian con cada cargo para definir claramente los permisos y responsabilidades.

- El CSI realizara análisis de vulnerabilidades durante la fase de pruebas de nuevos sistemas de información o mejoras, antes de su despliegue en producción, para garantizar que no existan brechas de seguridad que puedan comprometer la integridad del sistema.

- El CSI asegura que se utilicen datos distintos a los de producción en entornos de desarrollo, pruebas y réplicas. En caso de ser necesario el uso de datos reales, se aplicarán medidas estrictas para restringir el acceso a la información sensible y proteger la privacidad de los usuarios.

- Todo proyecto institucional que implique el desarrollo, adquisición, integración o uso de tecnologías de información deberá ser socializado y evaluado por el CSI, con el fin de analizar riesgos y asegurar el cumplimiento de los principios de seguridad de la información.

Cuando se contraten proveedores externos para el desarrollo de software, deben cumplirse los siguientes compromisos y requisitos:

- Es necesario definir contractualmente las disposiciones sobre la propiedad intelectual del código y paquetes de software desarrollados por el proveedor.

- El proveedor debe comprometerse a no divulgar información crítica o sensible obtenida durante el contrato, firmando un acuerdo de confidencialidad para garantizar la seguridad de los datos.

- El proveedor deberá demostrar que su proceso de desarrollo sigue las mejores prácticas de seguridad, asegurando que el software desarrollado es seguro desde su inicio.

- Se deben establecer criterios de aceptación del producto final, que incluyan pruebas funcionales y de seguridad (pruebas de estrés, penetración y contingencia). Cualquier hallazgo de vulnerabilidades deberá ser corregido antes de la entrega final.

- El proveedor debe certificar que el software entregado está libre de malware, troyanos o puertas traseras que puedan comprometer la seguridad del sistema.

- La Universidad podrá realizar auditorías para verificar el cumplimiento del ciclo de desarrollo seguro del proveedor, asegurándose de que las mejores prácticas de seguridad sean seguidas durante todo el proceso de desarrollo del software.

Adicionalmente, se deberán cumplir las siguientes disposiciones:

- Se deben establecer acuerdos de nivel de servicio con los proveedores que definan las responsabilidades en materia de seguridad y calidad del software, incluyendo pólizas de cumplimiento y garantías para asegurar la calidad y protección del software desarrollado.

- Los proveedores de desarrollo solo tendrán acceso a los programas fuente que hayan desarrollado o mantenido específicamente para la Universidad, garantizando que el acceso a los recursos sea controlado y específico.

- El proceso de actualización de los sistemas incluirá control de cambios, pruebas de funcionalidad, revisión de calidad del código, y análisis de riesgos y vulnerabilidades. Antes de la actualización, se realizarán pruebas de contingencia para garantizar que la implementación de nuevas versiones no afecte la seguridad ni la operatividad de los sistemas.

4.11. Servicios en la Nube.

Los proveedores de servicios en la nube que prestan sus servicios a la Universidad deben cumplir con un conjunto de disposiciones que garanticen la seguridad, disponibilidad y protección de la información institucional. Estas disposiciones aseguran que los servicios en la nube sean confiables, estén alineados con las normativas legales vigentes, y protejan adecuadamente los datos sensibles.

- Los proveedores de servicios en la nube deben acreditar experiencia y conocimiento en la materia, demostrando que cumplen con la normativa legal vigente en cuanto a la protección de datos y seguridad informática.

- El desempeño de los proveedores será supervisado de manera continua a través del procedimiento de gestión de proveedores de TI, para asegurar que se cumplan los estándares de seguridad establecidos.

- Los proveedores deben cumplir con acuerdos de nivel de servicio (SLA) que aseguren la disponibilidad, confidencialidad e integridad de la información almacenada y procesada en la nube.

- Estos acuerdos deben especificar claramente las expectativas y responsabilidades de las partes en cuanto a los niveles de servicio y medidas de seguridad.

- Los proveedores deben someterse a al menos dos pruebas anuales para evaluar la eficacia de los servicios, los canales y las soluciones de almacenamiento y recuperación de la información. Estas pruebas aseguran que los servicios en la nube mantengan los estándares de seguridad y funcionalidad a lo largo del tiempo.

- Los proveedores deberán ajustar la frecuencia de los respaldos de acuerdo con la criticidad de la información protegida. Esto garantiza que la información crítica para la Universidad sea respaldada con la frecuencia necesaria para evitar pérdidas de datos en caso de incidentes.

Los contratos de prestación de servicios en la nube deben incluir cláusulas específicas que cubran los siguientes aspectos:

- El contrato debe especificar cómo el proveedor asegura la confidencialidad, disponibilidad e integridad de los datos alojados en la nube, incluyendo medidas de protección como cifrado, controles de acceso y monitoreo de actividades.

- El proveedor debe comprometerse a cumplir con las leyes de protección de datos personales, garantizando que los datos privados de los usuarios y empleados de la Universidad estén debidamente protegidos.

- El proveedor debe incluir en el contrato cláusulas de confidencialidad que aseguren que la información a la que tenga acceso no será divulgada sin el consentimiento explícito de la Universidad, incluso después de la finalización del servicio.

- El contrato debe autorizar a la Universidad a realizar auditorías aleatorias a los sistemas del proveedor. Esto tiene el fin de verificar que el proveedor está cumpliendo con las medidas de seguridad, confidencialidad y protección de la privacidad especificadas en el acuerdo.

- Las auditorías deben ser accesibles para el personal autorizado de la Universidad, y deben llevarse a cabo en intervalos apropiados para garantizar la continua compliance.

4.12. Dispositivos Personales.

El uso de dispositivos personales dentro de las instalaciones de la Universidad está sujeto a ciertas restricciones y condiciones de seguridad para garantizar la integridad y confidencialidad de la información institucional. A continuación, se detallan las disposiciones para el uso de estos dispositivos:

- El uso de equipos personales (como laptops, teléfonos móviles, tablets, etc.) de colaboradores, profesores, proveedores y contratistas dentro de las instalaciones de la Universidad debe limitarse estrictamente a fines personales.

- Queda prohibido almacenar información organizacional o datos sensibles de la Universidad en los equipos personales, ya que esto pone en riesgo la seguridad de la información y puede comprometer la confidencialidad.

- Está prohibido conectar equipos personales a la red cableada de la Universidad sin previa autorización del CSI. En caso de ser autorizados, los equipos deben cumplir con condiciones mínimas de seguridad, como tener el sistema operativo y antivirus actualizados.

- La Universidad no se hace responsable por el uso inadecuado de los recursos tecnológicos institucionales que pueda resultar en la infección o compromiso de equipos personales. Es responsabilidad de cada usuario seguir las buenas prácticas de seguridad y cumplir con las políticas establecidas.

4.13. Gestión de la Seguridad en Proveedores.

La seguridad de la información no solo depende de los recursos internos de la Universidad, sino también de los proveedores con los que se trabaja. Para garantizar la protección de los activos tecnológicos y de la información sensible, se deben cumplir con los siguientes lineamientos y condiciones en la gestión de proveedores.

- Los proveedores deben presentar y mantener un plan de contingencia y continuidad del negocio, específicamente para los servicios que prestan a la

universidad, garantizando la recuperación de operaciones ante cualquier incidente.

- Todos los proveedores de TI, tanto de productos como de servicios, deben integrar criterios de seguridad de la información en sus procesos de evaluación, garantizando que se cumplan los estándares de seguridad exigidos por la universidad.

- Los proveedores de TI deben asegurar que, durante el traslado, eliminación o cualquier movimiento de activos de información y datos personales, se mantenga la confidencialidad, disponibilidad e integridad de la información en todo momento.

- El CSI será responsable de garantizar que el proceso de Gestión de Proveedores de TI se implemente adecuadamente, asegurando su cumplimiento y realizando auditorías periódicas para verificar la eficacia de las medidas de seguridad.

4.14. Uso del Internet.

El uso adecuado de internet es fundamental para la seguridad y funcionamiento eficiente de la infraestructura tecnológica de la Universidad. Si bien la Universidad garantiza la disponibilidad del servicio de internet, los usuarios tienen la responsabilidad de seguir las directrices establecidas para proteger los equipos y la información institucional. A continuación, se detallan las responsabilidades tanto de los usuarios como de la Universidad:

- Descargar archivos de internet únicamente para fines administrativos, académicos o relacionados con el ámbito universitario, de acuerdo con el cargo y la función de cada usuario, de manera razonable y sin afectar las actividades ni el servicio.

- Se recomienda evitar navegar por sitios web de mala reputación o desconocidos que puedan comprometer la seguridad de los sistemas y redes de la Universidad, minimizando el riesgo de infección por malware.

- Tomar las precauciones necesarias al descargar documentos o archivos, asegurándose de que no comprometan la seguridad de los equipos y redes de la universidad

La universidad, por su parte, deberá:

- Implementará controles para evitar la descarga de documentos o archivos de gran tamaño, con el fin de prevenir la fuga de información sensible.

- En caso de violación de las políticas de uso de internet, los usuarios involucrados podrán ser bloqueados temporalmente de la red o del acceso a internet, de acuerdo con las normativas internas de la Universidad.

- Diseñar, implementar y ejecutar procedimientos para el control y monitoreo de la red y los servicios de internet, con el objetivo de proteger la infraestructura tecnológica.

4.15. Seguridad de las Comunicaciones.

Las comunicaciones, tanto electrónicas como físicas, son un aspecto crucial para proteger la información confidencial de la Universidad. Es necesario aplicar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos transmitidos o compartidos. A continuación, se detallan las políticas que deben seguirse:

- Toda información confidencial o de uso interno que se envíe a través de medios digitales (correo electrónico, DVD, CD, USB, entre otros) hacia un dominio externo debe ser cifrada para asegurar su confidencialidad durante su transmisión.

- Los documentos físicos que contengan información sensible deben enviarse en sobres cerrados para garantizar que no sean accesibles durante el envío.

- Se debe utilizar exclusivamente las cuentas de correo electrónico institucionales para gestionar cualquier asunto relacionado con la Universidad.

- El uso de correos electrónicos personales o no institucionales está prohibido para tratar temas universitarios, para evitar la exposición de información institucional a riesgos.

- Las reuniones o conversaciones que involucren información confidencial deben realizarse en oficinas o salas de reuniones cerradas, de manera que no se pueda ver ni escuchar lo que ocurre en su interior. Estas reuniones no deben llevarse a cabo en lugares públicos.

- Las comunicaciones impresas con información confidencial, una vez cumplida su función, no deben ser utilizadas como material reciclable. Deben ser destruidas preferentemente mediante una picadora de papel.

- Se deben definir, comunicar y mantener actualizados los procedimientos necesarios para garantizar la protección adecuada de la información contenida en la mensajería electrónica, incluyendo correo electrónico, intercambio electrónico de datos y redes sociales.

- Se debe establecer y mantener procedimientos actualizados para evitar el acceso no autorizado a los mensajes almacenados en equipos multifuncionales y teléfonos IP (teléfonos de red).

- Los correos enviados a destinatarios fuera de la Universidad deben incluir un aviso legal en el pie del mensaje, informando sobre las políticas de seguridad y confidencialidad de la Universidad.

- Para el envío de correos electrónicos masivos, se deben utilizar los canales oficiales establecidos por la Universidad, como la Dirección de Comunicaciones o las listas de distribución creadas por el CSI, siempre que los destinatarios pertenezcan a la comunidad educativa.

- Al enviar correos electrónicos a destinatarios externos, es obligatorio utilizar la opción de copia oculta (CCO) para proteger la privacidad de las direcciones de los destinatarios.

- Los correos institucionales deben reflejar el comportamiento ético y transparente de la Universidad. No deben ser utilizados para enviar mensajes que expresen opiniones, conflictos, ni contenidos que puedan dañar la integridad, dignidad de las personas o la reputación de la Universidad.

- Antes de compartir cualquier información clasificada como confidencial o de uso interno con terceros, se deberá firmar un acuerdo de confidencialidad que garantice la protección y el manejo adecuado de la información.

5. DOCUMENTOS ASOCIADOS

IDENTIFICACIÓN DEL DOCUMENTO	NOMBRE
INTERNO	Estatutos de la Universidad Javeriana
	Directriz de Seguridad de la Información – PUJ Cali
EXTERNO	Política de Seguridad de la Información – Javeriana Colombia
	Lineamientos para cuentas de servicios de tecnología institucionales – PUJ Bogotá

6. CONTROL DE VERSIÓN

Versión	Fecha Aprobación	Cambios Realizados
Versión 01	Noviembre del 2016	Documento Original
Versión 02	Junio del 2025	Documento Original

Carlos Rodrigo Montehermoso Jaramillo
Vicerrector Administrativo de la Seccional

Mónica Perdomo Lozano
Directora del Centro de Servicios informáticos