Pontificia Universidad
JAVERIANA
Bogotá

ACUERDO N° 765

Política de Seguridad de la Información

EL CONSEJO DIRECTIVO
DE LA PONTIFICIA UNIVERSIDAD JAVERIANA

CONSIDERANDO:

1. Que el Código de Buen Gobierno reconoce el valor estratégico que la información tiene para la Universidad en el cumplimiento de la misión y su Proyecto Educativo; en ese sentido, la Universidad garantizará que la información que envía o que conserva por medios físicos o electrónicos, cumpla con las condiciones de integridad, consistencia, homologación y suficiencia.

2. Que la Universidad incorpora la gestión efectiva de seguridad de la información como un elemento esencial en sus procesos, para salvaguardar la información en su quehacer dinámico, y su actuar proactivo ante un entorno y una sociedad en constante cambio.

3. Que la Universidad en su política de Cultura y Desarrollo Digital, reconoce que la seguridad digital es componente esencial de un desarrollo digital sólido y sostenible.

4. Que la Política de Seguridad de la Información y el Sistema de Gestión de Seguridad de la Información constituyen el marco mediante el cual se consolida el gobierno de Seguridad de información en la Universidad con el objetivo de minimizar el riesgo de seguridad de información en sus procesos y proteger su información ante amenazas de ciberseguridad.

5. Que el texto de la política propuesta fue considerado y aprobado por este Consejo, en su sesión del 4 de diciembre de 2024, según consta en el acta número 963.

6. Que de acuerdo con lo establecido en los Estatutos de la Universidad en el Numeral 116, literal a) es función del Consejo Directivo Universitario "Adoptar, ..., las políticas generales de la Universidad...".

ACUERDA:

ARTÍCULO PRIMERO - Adoptar para la Universidad (Sede Central y Seccionales), la siguiente Política de Seguridad de la Información.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

2024

TABLA DE CONTENIDO

1. OBJETIVO

La presente política establece los lineamientos para gestionar adecuadamente la seguridad de la información de la Pontificia Universidad Javeriana, en su Sede Central y Seccional, incluyendo, sin limitaciones, la información de sus estudiantes, profesores, empleados, y demás grupos de interés, y dando cumplimiento a la reglamentación y legislación aplicable.

La política de Seguridad de la Información cubre los aspectos administrativos y de control que deben ser cumplidos por los grupos de interés y demás personas que tengan relación con la Universidad. Adicionalmente, permite establecer el alcance de sus responsabilidades en la preservación de la confidencialidad, integridad y disponibilidad de la información.

Esta política constituye el marco en el cual la información será protegida contra toda clase de riesgos y amenazas de ciberseguridad, internos o externos, intencionales o accidentales, en las diferentes formas en las cuales se pueda encontrar esta información, tanto dentro de la Universidad como "en nube", y así preservar la operación, la reputación, y los aspectos financieros y legales de la Pontificia Universidad Javeriana.

2. ALCANCE

Las disposiciones contempladas en la presente política, así como los lineamientos asociados al Sistema de gestión de Seguridad de la Información, son aplicables a:

- Toda la comunidad educativa y grupos de interés, clientes, contratistas y proveedores, entes de control y otros terceros, que acceden interna o externamente o tengan acceso alguno a la información de la Universidad en su Sede Central y Seccional,
- Todos los procesos, servicios, actividades, proyectos y recursos de tecnología de la Universidad,
- Toda información de la Universidad, creada, procesada, almacenada, intercambiada, divulgada, dispuesta, sin importar el medio, formato (físico o digital) o ubicación.

3. TERMINOS Y DEFINICIONES

- Activo: Recurso tangible o intangible que se genera a través de una operación, se puede controlar y permite obtener un beneficio.
- Activo de Información: Cualquier componente (humano, hardware, *software*, información digital o física o de infraestructura) que soporta uno o más procesos de la Institución y, en consecuencia, debe ser protegido.
- Acuerdo de Confidencialidad: Es un documento en el que los funcionarios de Referencia o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Institución, comprometiéndose a no divulgar, usar o explotar la información confidencial restringida o confidencial a la que tengan acceso en virtud de la labor o contrato que desarrollan dentro y fuera de la misma.
- Amenazas: Se entiende por amenaza, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo de seguridad de la información. Son amenazas el talento humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos. Las amenazas en un contexto de seguridad de la información incluyen actos dirigidos, deliberados (por ejemplo, por crackers) y sucesos no dirigidos, aleatorios o impredecibles (como puede ser un rayo). Amenaza es la causa de riesgo que crea aptitud dañina sobre personas y bienes.
- Análisis de Riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- Análisis de Riesgos de Seguridad de la Información: Proceso sistemático de identificación de fuentes (amenazas y vulnerabilidades), estimación de impactos y probabilidades y

comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

- Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- Ciberseguridad: Es el conjunto de procedimientos, prácticas y técnicas para la protección, prevención de daños y restauración tanto de los servicios tecnológicos y sistemas de comunicaciones electrónicas, como la información digital allí gestionada, mitigando riesgos asociados a amenazas y ataques cibernéticos (*malware, phishing, ramsomware*, denegación de servicio, y otras formas de intrusión), asegurando que la institución pueda operar de manera segura y resiliente en entornos digitales.
- Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.
- Confidencialidad: Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- Contraseña: Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a uno o más usuarios para acceder a un determinado recurso, por lo general una herramienta tecnológica o accesos físicos que son validados por herramientas tecnológicas. Las claves suelen tener limitaciones en sus caracteres (no aceptan algunos) y su longitud.
- Controles: Medidas dispuestas para reducir el nivel de riesgo, tales como políticas, procedimientos, directrices, prácticas o estructuras de la institución que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
- Dato: Representación convencional de un hecho o idea que puede ser tratada por un ordenador.
- Derechos de Autor: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
- Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada cuando esta la requiera.
- Equipo de Cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
- Evento de Seguridad de la Información: Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un incumplimiento posible de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.
- Hacking Ético (Ethical Hacking): Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.
- Incidente de Seguridad de la Información: Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de la institución y amenazar la seguridad de la información.
- Información: Está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

- Información sensible: Información o cualquier tipo de dato que si se difunde podría resultar perjudicial para personas u organizaciones. Los datos sensibles pueden incluir información personal identificable (IPI), datos financieros, entre otros, Particularmente en datos personales los datos sensibles son aquellos que afectan la intimidad de su titular o cuyo uso indebido puede generarle discriminación, vulneración a su derecho de igualdad.
- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.
- Medio Removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
- Mitigar el Riesgo: Cuando se decide prevenir o reducir el impacto o probabilidad del riesgo. Si el riesgo no se puede evitar porque crea grandes dificultades operacionales, el siguiente paso es reducirlo a un nivel aceptable. Se consigue, por ejemplo: mediante la optimización de los procedimientos, la implementación de controles, fortalecimiento del ejercicio del autocontrol, fortalecimiento del ejercicio de la autoevaluación de la gestión, las auditorías internas, entre otros. Existen dos formas de reducir el riesgo: prevenir, que apunta a la disminución de la probabilidad o proteger.
- No Repudio: Condición en la que quien envía un mensaje o realiza una operación con los sistemas de información no puede negar la validez del resultado del proceso que se utilizó para autenticar la información.
- Política: Directrices y normas que deben cumplir los integrantes de una institución las cuales reflejan las intenciones y dirección de una institución.
- Propietario de la Información: Es la unidad organizacional o proceso donde se crean los activos de información.
- Recursos Tecnológicos: Son aquellos componentes de *hardware* y *software* tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Institución.
- Riesgo: Se entiende por riesgo, la posibilidad de incurrir en pérdidas económicas, operativas o de imagen por deficiencias, fallas o inadecuaciones, en el talento humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas.
- Servicios tecnológicos: conjunto de soluciones o recursos que se ofrecen a través del uso de tecnologías de información y comunicación (TIC). Puede incluir desde *software*, infraestructura tecnológica, almacenamiento y procesamiento de datos, redes y comunicaciones, hasta nuevas tecnologías (inteligencia artificial, *blockchain*, etc), dispuestos físicamente en la institución o "en nube", y administrados directamente por la Universidad o a través de un tercero.
- Sistema de gestión de seguridad de la información: se refiere a un conjunto de procesos sistemáticos y estructurados que a través de políticas, procedimientos y controles busca, basado en el riesgo, proteger de manera proactiva y continua la confidencialidad, integridad y disponibilidad de la información crítica en una institución.
- Sistema de Información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de *software* ya sea de origen interno, es decir desarrollado por referencia o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado a la medida.
- Sistemas de Control Ambiental: Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características de este, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

- *Software* Malicioso: Es una variedad de *software* o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- Grupos de interés: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.
- Vulnerabilidad: Es el grado de debilidad de un activo frente a una amenaza. La capacidad que tiene la amenaza de afectar el activo.

4. CONTEXTO DE LA UNIVERSIDAD

Mediante el Acuerdo No. 0066 del Consejo Directivo Universitario del 22 de abril de 1992, establece el Proyecto Educativo de la Pontificia Universidad Javeriana junto con las directrices para el ejercicio de las funciones universitarias, en el marco de la Formación Integral de sus miembros, la cual procura el desarrollo armónico de todas las dimensiones del individuo.

De otra parte, el Código de Buen Gobierno reconoce el valor estratégico que la información tiene para la Universidad para el cumplimiento de la misión y su Proyecto Educativo, por lo tanto, la Universidad garantizará que la información que envía o que conserva por medios físicos o electrónicos, cumpla con las condiciones de integridad, consistencia, homologación y suficiencia.

La gestión adecuada de la información no solo corresponde a una medida preventiva, y se consolida como un componente estratégico que impulsa el logro de los objetivos institucionales estipulados en los estatutos de la Universidad; por lo anterior la Universidad incorpora la seguridad de la información como un elemento esencial en sus procesos, para salvaguardar la información y los componentes tecnológicos que apalancan la ejecución del Proyecto Educativo.

La Universidad en su Política de cultura y desarrollo digital, reconoce que la seguridad digital es componente esencial de un desarrollo digital sólido y sostenible. Por ello, trabajará en el fortalecimiento de las garantías para la seguridad y protección de la infraestructura de sistemas, los datos y la información, así como en los mecanismos de ciberseguridad necesarios para reducir los riesgos y mitigar los impactos negativos potenciales. Así mismo, fomentará una cultura de seguridad en la comunidad universitaria orientada a que las personas estén informadas sobre las mejores prácticas y asuman comportamientos seguros al utilizar tecnologías digitales para prevenir incidentes.

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El sistema de gestión de seguridad de la información proporciona la estructura general para establecer un marco de referencia para la gestión adecuada y eficaz de la seguridad de la información.

Mediante este sistema de gestión se desarrollarán las estrategias para implementar y monitorear de forma adecuada, los lineamientos de seguridad de la información definidos por la Universidad en la presente política.

5.1. Objetivo General

Contribuir en el cumplimiento de la misión de la Universidad, en el fortalecimiento de la calidad y la disponibilidad de sus servicios a través de la gestión de la seguridad de la información e implementando la política y controles necesarios para la protección de su información.

5.2. Objetivos Específicos

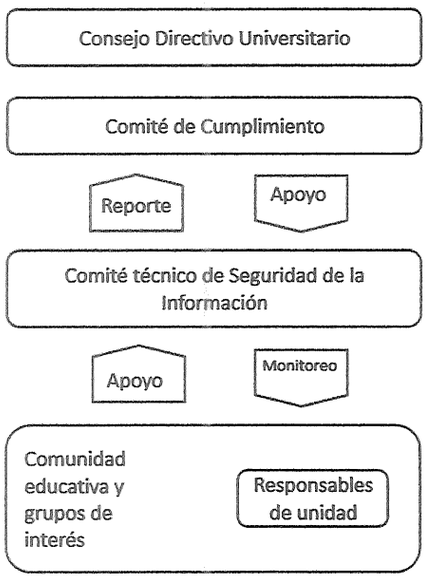
- Establecer los lineamientos para la gestión adecuada de las diferentes etapas que se contemplan en la gestión de seguridad de la información.

- Establecer una estructura de gobierno que permita soportar el Sistema de gestión de seguridad de la información de la Universidad.
- Establecer la identificación y administración proactiva de los riesgos de seguridad de la información asociados a las actividades universitarias y procesos de la Universidad.
- Definir las medidas de seguridad que deben ser implementadas para proteger y garantizar la seguridad de la información de la Universidad,
- Establecer medidas de gestión de incidentes de seguridad de la información, garantizando la continuidad de los servicios críticos y la protección de los activos de información.
- Dar seguimiento a la gestión de seguridad de la información con el fin de minimizar la afectación en las actividades universitarias y procesos de la Universidad y propender por el mejoramiento continuo en su gestión.
- Promover y establecer una cultura de la seguridad de la información y la ciberseguridad en la comunidad educativa.

5.3. Estructura de gobierno de la seguridad de la información

Teniendo en cuenta las funciones de los diferentes estamentos de la Universidad y las actividades relacionadas con la seguridad de la información que tienen a su cargo, la Universidad ha adoptado la siguiente estructura de gobierno donde se definen roles y responsabilidades, con el objetivo de dar cumplimiento al Sistema de gestión de seguridad de la información.

5.3.1. Estructura



5.3.2. Consejo Directivo Universitario

El Consejo Directivo Universitario será la instancia a la que corresponde la aprobación de la política de Seguridad de la Información y tomar decisiones particulares del Sistema de gestión de seguridad de la información, a las que haya lugar.

5.3.3. Comité de Cumplimiento

El Comité de Cumplimiento será el encargado de:

I. Realizar seguimiento a las actualizaciones a la política de seguridad de la Información de acuerdo con la identificación de nuevos riesgos, cambios de legislación o tecnológicos,
II. La verificación del cumplimiento de la política aquí mencionadas cuando lo considere y dar seguimiento a las no conformidades a la Política Institucional de Seguridad de la Información.
III. Revisar y analizar el informe de gestión que presenten los responsables de seguridad,
IV. Conocer y emitir conceptos en relación con las debidas diligencias que presenten los responsables de Seguridad,

5.3.4. Responsables de Unidades

Los responsables de Unidades serán los garantes de la seguridad de la información y de los activos de información de acuerdo con su gestión y con los procesos de la Universidad. Entre sus funciones se encuentra:

I. Adoptar los lineamientos y las prácticas de seguridad de la información para la Universidad,
II. Identificar, clasificar y mantener actualizados los activos de información de los procesos,
III. Comunicar a los responsables de seguridad informática cualquier variación respecto a la información y los servicios a su cargo,
IV. Reportar a los responsables de seguridad informática, los incidentes de seguridad y privacidad detectados,
V. Participar y promover los planes y actividades de prevención, capacitación y sensibilización del Sistema de gestión de gestión de seguridad de la información,

5.3.5. Comunidad educativa y grupos de interés

La comunidad educativa y los grupos de interés deberán cumplir con los lineamientos establecidos en la política de Seguridad de la Información, protegiendo la información a su cargo, reportando de manera inmediata cualquier antecedente, evento o actividad que se perciba como inusual o sospechosa y que pueda estar relacionado con un posible evento o incidente de seguridad de la información.

5.3.6. Comité técnico de seguridad de la información

Estará conformado por los responsables de los sistemas tanto de la Sede Central como de la Seccional: el Director(a) de Tecnologías de Información (DTI) y el Director(a) del Centro de Servicios Informáticos (CSI) y los Jefes y Coordinadores respectivos. Entre sus principales funciones se encuentran:

I. Garantizar la implementación la política de Seguridad de la Información, de acuerdo con los controles definidos por los miembros del comité,
II. Identificar, gestionar, tratar y monitorear los riesgos de seguridad de la información.
III. Garantizar la configuración y actualización de los sistemas de información y servicios de TI a fin de minimizar el impacto de las vulnerabilidades identificadas, gestionando las acciones necesarias en la configuración,
IV. Asegurar que los controles de seguridad establecidos y los procedimientos aprobados, son cumplidos estrictamente.
V. Atención inmediata a eventos o incidentes de seguridad de la información desde su detección hasta su resolución,
VI. Reporte del desempeño del Sistema de gestión de seguridad de la información.

5.3.7. Responsables de los sistemas y servicios de tecnologías de información

Serán los responsables del sistema: i) en la Sede Central el Director(a) de Tecnologías de Información (DTI) y ii) en la Seccional Cali el Director(a) del Centro de Servicios Informáticos (CSI), a través de los Jefes y Coordinadores respectivos. Entre sus principales funciones se encuentran:

I. Garantizar la disponibilidad de los sistemas de información durante todo su ciclo de vida, manteniendo los procedimientos operativos necesarios.
II. Definir la gestión de los sistemas y servicios de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
III. Asegurar que los lineamientos y controles de seguridad establecidos son implementados y mantenidos de manera estricta,
IV. Gestionar y asegurar la configuración y actualización de los sistemas y servicios de información a fin de minimizar el impacto de las vulnerabilidades identificadas,
V. Gestionar las instalaciones de *hardware* y *software*, sus modificaciones y mejoras, para asegurar que la seguridad sea incluida durante todo el ciclo del sistema y servicios de información,
VI. Participar en la elaboración e implementación de los planes de mejora de la seguridad,
VII. Informar al responsable de seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad,
VIII. Disponer de lo que sea requerido en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

5.3.8. Responsables de seguridad informática

Corresponde a los responsables de la seguridad en cada sede: i) para la Sede Central el jefe de Seguridad Informática de la Dirección de Tecnologías de la Información y ii) para la Seccional Cali el coordinador de Seguridad de la Información del Centro de Servicios Informáticos, entre sus principales funciones se encuentran las siguientes:

I. Elaborar y presentar propuesta la actualización y mejoramiento de la política de seguridad de la información de acuerdo con las directrices legales y los lineamientos internos, adoptando las correcciones necesarias para su óptimo funcionamiento,
II. Realizar seguimiento a la efectiva ejecución y monitoreo de los controles contemplados en el Sistema de gestión de seguridad de la información,
III. Realizar un informe de gestión anual, el cual será presentado al Comité de Cumplimiento,
IV. Promover la formación y concientización en materia de seguridad de la información a través de plan de comunicación de seguridad de la información para la comunidad educativa,
V. Promover y apoyar al oficial de protección de datos y cumplimiento frente a la identificación y gestión de riesgos de seguridad de la información y de ciberseguridad.
VI. Atender las solicitudes de las unidades en relación en cuanto a la seguridad de la información y emitir concepto de viabilidad en la implementación de medidas de seguridad para alcanzar una adecuada implementación del Sistema de gestión de seguridad de la Información
VII. Generar la declaración de aplicabilidad e identificar las medidas de seguridad.
VIII. Elaborar, actualizar y revisar los documentos y procedimientos necesarios para gestionar adecuadamente el Sistema de gestión de seguridad de la información
IX. Efectuar monitoreo a los sistemas y servicios de información para el reporte de las vulnerabilidades identificadas.
X. Monitorear el estado de seguridad a través de los servicios y de las herramientas de gestión de eventos de seguridad.
XI. Gestión a eventos o incidentes de seguridad de la información desde su detección o reporte hasta su resolución.
XII. Atender los requerimientos de la Auditoría Interna y la Revisoría Fiscal en los temas relacionados con la seguridad de la información y ciberseguridad, y proponer los planes de acción y medidas correctivas según sea necesario.

5.4. Compromiso y recursos

La Pontificia Universidad Javeriana a través de su compromiso en el cuidado y protección de su información a través del Sistema de gestión de Seguridad de la Información, determinará los recursos necesarios para el mantenimiento y mejoramiento continuo de la seguridad de la información de la Universidad.

5.5. Gestión de los riesgos de seguridad de la información

El Sistema de gestión de seguridad de la información de la Universidad se fundamenta en el análisis y gestión de riesgos de seguridad de la información y amenazas de ciberseguridad.

La Universidad ejecutará la gestión del riesgo de seguridad de la información conforme al Manual de Gestión de Riesgos expedido mediante la resolución N°722. Este manual proporcionará el marco y la metodología para identificar, evaluar y mitigar los posibles riesgos de seguridad de la información que puedan afectar a la institución.

La adopción de esta metodología no limita a la Universidad a incluir dentro del análisis de riesgo de seguridad de la información y amenazas de ciberseguridad, factores adicionales y complementarios tales como vulnerabilidades y amenazas, entre otros.

La revisión de riesgos de seguridad de la información se deberá realizar al menos una (1) vez al año o cuando se presenten cambios que afecten de manera significativa la información.

5.6. Seguimiento y Mejora continua

El Sistema de gestión de seguridad de la información incluye un proceso de revisión y mejora continua, que permitirá evaluar la evolución de los servicios e información, la pertinencia de su categorización, así como de las medidas de seguridad y la necesidad de actualización de las normas y procedimientos.

El comité de Cumplimiento evaluará el desempeño del Sistema de gestión de seguridad de la información de forma periódica. Estas evaluaciones contemplarán, entre otros:

- Informes de estado de las acciones correctivas y preventivas,
- Acciones de mejora,
- Cambios institucionales en procesos que afecten el Sistema de gestión de seguridad de la información,
- Cambios en el riesgo residual en las matrices de Riesgos de seguridad de la información conforme lo definido en el manual de gestión de riesgos,
- Reportes de auditoria al Sistema de gestión de seguridad de la información, entre otras que se consideren,
- Informes de panorama de riesgos tanto local como internacional,

El comité de auditoría ejecutará los planes de auditorías necesarios, sobre los procesos aplicables, así mismo definirá un cronograma y alcance para el año calendario, de acuerdo con las necesidades de la Universidad.

5.7. Gestión de cambio al Sistema de gestión de seguridad de la información

Con el fin de garantizar la estabilidad y pertinencia del Sistema de gestión de seguridad de la información cualquier cambio que afecte de forma significativa debe ser comunicado por parte del Comité de Cumplimiento, y si así lo considera, aprobado por el Consejo Directivo Universitario; algunos de estos cambios incluyen, entre otros:

- Cambios a nivel institucional y de procesos que modifiquen la política de seguridad de la información,
- Cambios de estrategia o servicios que ofrece la Universidad (se debe realizar un análisis de contexto y verificar los riesgos de nuevos servicios,
- Cambios en legislación, normativa, buenas prácticas,

- Cambios en la estructura del gobierno de seguridad de la información,
- Cambios en la infraestructura tecnológica y/o componentes que afecten el Sistema de gestión de Seguridad informática,
- Establecimiento nuevas sedes o ubicación de componente de tecnologías de información; asó como la reubicación de las ya existentes,
- Adecuación y/o remodelación de zonas que contengan información sensible de seguridad de la información.

Estos cambios serán los insumos para desarrollas los ajustes y actualizaciones pertinentes sobre los documentos y prácticas del Sistema de gestión, así como en sus procedimientos, directrices, manuales asociados a cada uno de los lineamientos.

5.8. Despliegue y comunicación

La estrategia para el despliegue de la política de Seguridad de la Información, el Sistema de gestión y sus lineamientos será liderada por los responsables de Seguridad de la Información, apoyado con las unidades de Comunicaciones y Gestión Humana correspondientes, quienes servirán de facilitadores para comunicar a todos los grupos de interés de la Universidad la política, lineamientos y recomendaciones en seguridad de la información y ciberseguridad.

La comunidad educativa atenderá a sesiones de concientización y sensibilización en materia de seguridad de la información y ciberseguridad conforme al plan de concientización definido tanto para la inducción como para reentrenamientos.

6. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

6.1. Declaración de la política de seguridad de la información

Para la Pontificia Universidad Javeriana la información constituye un recurso estratégico en el cumplimiento de su misión y es su prioridad protegerla y tratarla apropiadamente, teniendo en cuenta los principios de disponibilidad, integridad y confidencialidad, buscando asegurar el cumplimiento de los requisitos operativos, técnicos, normativos y regulatorios, a los cuales está sujeta la información, tomando como base la gestión de riesgos que, de manera continua, redunde en la mejora y eficacia del Sistema de gestión de Seguridad de la Información.

6.2. Lineamientos generales

Al adoptar esta política, se busca fortalecer la seguridad de la información de la Universidad y fomentar una cultura de responsabilidad compartida en el uso y protección de la información y de las tecnologías de información.

A continuación, se establecen los lineamientos generales que la comunidad educativa y los grupos de interés deben cumplir en la gestión responsable de la información:

- Como parte de su gestión, es un deber de la Universidad y de su comunidad cumplir con sus compromisos contractuales, las leyes y la regulación que le aplique.
- La comunidad educativa y los grupos de interés con algún vínculo con la Universidad serán responsables de proteger la información y los servicios tecnológicos a los que la Universidad les proporcione acceso o sobre los cuales tengan responsabilidad, ya sea que se encuentren alojados en servicios y repositorios dispuestos en la Universidad o "en nube", con el fin de evitar su pérdida, alteración, destrucción o uso indebido.

- La política y lineamientos contenidos en este documento deberán ser divulgados, aceptados, y cumplidos por la comunidad educativa y por los grupos de interés con algún vínculo con la Universidad.
- Los activos de información de la Universidad serán identificados y clasificados, para así establecer los mecanismos de protección necesarios de acuerdo con el plan de gestión de riesgos y amenazas de ciberseguridad.
- La comunidad educativa recibirá formación mediante el programa de capacitación y sensibilización.
- Es responsabilidad de la comunidad educativa y otros grupos de interés con algún vínculo con la Universidad, reportar incidentes de seguridad que identifiquen (eventos sospechosos, de mal uso o abuso) sobre recursos de información y servicios tecnológicos. Todo incidente que afecte o pueda colocar en riesgo la seguridad de la información debe ser reportado inmediatamente, así:

    - en la sede Central al correo: dti-mesaservicios@javeriana.edu.co o a través del registro en la plataforma SERVIR-T en https://www.javeriana.edu.co/servir-t
    - en la Seccional al correo seguridad.ti@javerianacali.edu.co o a través del registro en la mesa de servicios https://mesadeservicio.javerianacali.edu.co

- El incumplimiento de esta política se considerará un incidente de seguridad, que, según el caso, podrá dar lugar a la aplicación de sanciones disciplinarias estipuladas en los reglamentos, acuerdos o contratos correspondientes, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.
- La Universidad tendrá la potestad de intervenir y eliminar el acceso a los servicios de tecnología de información en cualquier momento, cuando se considere un uso inadecuado de la información o de los servicios, que hayan sido utilizados para realizar prácticas ilícitas o mal intencionadas, que atenten contra las normas internas de la Universidad, terceros, el orden público, las buenas costumbres, las legislaciones nacionales o internacionales vigentes, entre otras que se consideren.

6.3. Lineamientos específicos

Los siguientes lineamientos detallan la política de seguridad de la información establecida por la Universidad para la protección y uso adecuado de la información por parte de la comunidad educativa y otros grupos de interés.

6.3.1. Gestión de activos de información

Es responsabilidad de cada miembro de la comunidad garantizar el uso adecuado de los activos de información que hacen parte y usa para su gestión; así mismo es responsable de identificar, clasificar y etiquetar de forma adecuada los activos de información a su cargo.

Todo aquel que tenga acceso y responsabilidad sobre información institucional deberá gestionarla de acuerdo con los lineamientos sobre el acceso, uso, transmisión, almacenamiento, divulgación, y en general el tratamiento de la información, así como los demás lineamientos de seguridad dispuestos por la Universidad.

Está prohibido duplicar o realizar copias no autorizadas a cualquier documento físico o digital propiedad de la Universidad, así mismo, está prohibida la reproducción parcial o total de material sujeto a derechos de autor de terceros mediante los recursos de la Universidad, (documentos, artículos, bases de datos, libros, revistas entre otros).

La Universidad definirá una metodología de clasificación etiquetado y lineamientos específicos en la gestión de activos de información, de manera que se garanticen los criterios de confidencialidad, integridad y disponibilidad.

6.3.2. Gestión de usuarios y credenciales

La Universidad asignará una cuenta como llave de acceso a la información y a los servicios de tecnología de información de la Universidad de acuerdo con lo establecido y autorizado para cada miembro de la comunidad o grupo de interés.

Las credenciales, usuarios y contraseñas asignadas a los miembros de la comunidad y grupos de interés, son de carácter personal e intransferible.

Las solicitudes de usuarios y permisos de usuario, así como los cambios de privilegios a los servicios tecnológicos de la Universidad, se presentarán mediante los canales de comunicación autorizados, y estará sujeta a autorización de la correspondiente facultad o unidad administrativa quienes darán su visto bueno para su respectiva asignación.

La Universidad define a través de los procedimientos de gestión de usuarios correspondiente, el método para la creación, modificación, des habilitación, revisión periódica, eliminación, bloqueo y desbloqueo de usuarios en servicios de información y tecnologías de información.

La Universidad ejecutará depuraciones periódicas tomando como base los reportes de las fuentes vigentes de miembros de la comunidad educativa, así como de otros grupos de interés.

6.3.3. Mecanismos de autenticación

La Universidad establecerá mecanismos de autenticación seguros, apropiados según su uso y posibilidades tecnológicas, que restrinjan el acceso no autorizado a los servicios de tecnología de información; todos los servicios tecnológicos deben contar con los mecanismos de autenticación y protección de la autenticación que la Universidad considere e informe.

6.3.4. Manejo de incidentes de seguridad

Las oficinas de Seguridad Informática de cada sede serán los responsables de realizar la investigación y seguimiento a los eventos o incidentes de seguridad y ciberseguridad reportados, e informar de forma periódica al Comité de Cumplimiento, para su gestión en caso de requerir del apoyo de otras áreas de la Institución o de entidades externas.

El procedimiento de gestión de incidentes de seguridad determina la metodología, procedimiento, registros formales y consideraciones especiales para la correcta gestión de incidencias de seguridad de la información y de ciberseguridad.

6.3.5. Seguridad para empleados y colaboradores

La Universidad reconoce la importancia que tienen los empleados y colaboradores en la protección de la información, por lo que define los siguientes lineamientos:

- Todo el personal administrativo y docente, independiente de su tipo de contrato, deberá cumplir con los lineamientos de seguridad de la información, así mismo debe asistir a los programas de capacitación y sensibilización en materia de seguridad de la información, con el fin de fortalecer la conciencia en seguridad de la información.
- El personal administrativo o docente no deberá divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la Institución.
- El personal docente y administrativo debe firmar acuerdos de confidencialidad que contemplen dentro de los acuerdos contractuales, las responsabilidades antes durante y después del vínculo laboral, determinados en la presente política.
- La Dirección de Gestión Humana en la sede central y la Oficina de Gestión del Talento Humano en la seccional, deberá reportar de manera oportuna las novedades de personal en los momentos adecuados, con el fin de garantizar que la información al momento del cese de actividades sea entregada de forma controlada y segura.

- Todos los empleados y colaboradores se comprometen a no divulgar información confidencial una vez culmine la relación laboral, así mismo, cualquier tipo de información bajo su responsabilidad, debe ser entregada previo su retiro de la Universidad.
- En caso de incumplimiento de los lineamientos de seguridad de la información, la Dirección de Gestión Humana y la Dirección Jurídica en la sede Central, o la Oficina de Gestión del Talento Humano y la Oficina Jurídica en la seccional Cali, tomarán las acciones siguiendo el procedimiento de acuerdo con los reglamentos o cláusulas vigentes.

6.3.6. Escritorio y pantalla limpia

Cada miembro de la comunidad deberá bloquear su equipo de trabajo o equipo personal conectado a la red de la Universidad, cada vez que se retire del equipo y sólo se podrá desbloquear con la contraseña de usuario. Al finalizar sus actividades diarias o sesiones de trabajo deberán salir y cerrar todas las aplicaciones y bloquear la estación de trabajo.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla institucional, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, cada miembro de la comunidad educativa deberá dejar la información confidencial protegida bajo llave. Esto incluye: documentos impresos, medios ópticos (CD, DVD, etc.), dispositivos de almacenamiento USB y otros medios removibles en general.

De acuerdo con la política institucional de cero papel, en caso de requerir imprimir documentos confidenciales, deberán retirarse de forma inmediata de las impresoras. Así mismo, no se deberá reutilizar papel que contenga información confidencial.

6.3.7. Gestión de copias de seguridad

La información contenida en los servicios, aplicaciones, servidores, contenedores de la Universidad, así como la configuración de los equipos de comunicaciones y seguridad, se respaldará de forma periódica, según lo definido en el procedimiento copias de seguridad, con el objetivo de garantizar la integridad y disponibilidad de la información cuando sea requerida.

La Dirección de Tecnologías de Información (DTI) y el Centro de Servicios Informáticos (CSI) realizarán las copias de seguridad proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades.

Para el caso de equipos especializados, salas de cómputo y laboratorios, el responsable de proceso debe realizar copias de seguridad por medio del proveedor o a través de los colaboradores de la institución, para los componentes que considere críticos, tales como configuraciones, imágenes de sistema operativo, información, manuales, entre otros.

Toda la comunidad educativa y grupos de interés son responsables de realizar o solicitar las copias de respaldo necesarias. La Dirección de Tecnologías de Información (DTI) y el Centro de Servicios Informáticos (CSI) indicarán las alternativas para realizar las copias de respaldo de su información.

La Universidad no se hace responsable por la pérdida de información, causadas por amenazas y ataques cibernéticos o acciones voluntarias o involuntarias de los usuarios sobre sus equipos de cómputo y equipos personales.

6.3.8. Conexiones remotas, trabajo en casa y horario flexible.

Las conexiones desde sitios externos hacia información o servicios tecnológicos críticos de la Universidad deben contar con controles técnicos para proteger los activos de información, por esto:

- La comunidad educativa y otros grupos de interés debe abstenerse de realizar este tipo de conexiones a través de redes de acceso público en internet.
- La conexión remota se debe realizar únicamente mediante conexiones seguras, indicadas autorizadas por la Universidad, tales como redes virtuales privadas - VPN, portal de acceso unificado, entre otros.
- En caso de hurto, extravío o daño de los equipos y dispositivos móviles institucionales, se debe reportar de manera inmediata a la Dirección de Tecnologías de Información (DTI) o el Centro de Servicios Informáticos (CSI, así mismo, dar reporte a la Oficina de Activos Fijos según corresponda.

6.3.9. Áreas seguras

La seguridad física es un factor primordial para la protección de la información, por esto la Universidad establecerá medidas de control en áreas seguras:

- La Universidad definirá áreas seguras, las cuales contarán con restricción de acceso para el personal ajeno al personal asignado; todos los visitantes que requieran acceso a las áreas seguras deben ser acompañados por un funcionario encargado del área y su acceso será sujeto a previa autorización
- Todas las instalaciones que contengan información de la Universidad deben contar con control de acceso físico que garantice el uso de al menos un mecanismo de protección física (vigilancia humana o control de acceso electrónico)
- Todas las sedes de la Universidad deben contar con circuito cerrado de TV y se instalarán cámaras conforme lo requiera la Universidad.

6.3.10. Salas especializadas, centros de datos y laboratorios

La Universidad establecerá los siguientes mecanismos de protección en las salas de cómputo, centros de datos, laboratorios y salas especializadas:

- Se debe contar con mecanismos de acceso mediante tarjeta de proximidad o control biométrico,
- Mecanismos para la detección y extinción de incendios,
- Higrómetros para el control ambiental,
- Sistema de cámaras conectada al CCTV,
- Sistema de ventilación y control de temperatura,
- Los encargados de laboratorios son responsables de gestionar adecuadamente el mantenimiento y actualización de los equipos especializados y de cómputo,
- Cada vez que se integre un equipo o *software*, se debe modificar las credenciales de administrador, por ningún motivo se deben mantener las credenciales por defecto.

6.3.11. Mantenimiento, disposición y reutilización de equipos de cómputo

Con el objetivo de garantizar el óptimo estado de la infraestructura tecnológica y así la protección de la información, los responsables de los equipos de cómputo deben ejecutar o solicitar los mantenimientos periódicos de los equipos a cargo, de acuerdo con las necesidades de cada dispositivo: incluyendo actualizaciones de *software*, aplicación de paches de seguridad, actualizaciones de sistemas operativos y mantenimiento físico, entre otros que apliquen.

Cada vez que un equipo sea reasignado o dado de baja se debe ejecutar un proceso de eliminación segura de los datos almacenados.

Si el dispositivo contiene licencias propiedad de la Universidad se deberán eliminar del dispositivo y si es posible resguardar para su reutilización.

Para discos duros de servidores o equipos de usuario final que contengan información confidencial y/o sensible, se deberá realizar un proceso de borrado seguro de acuerdo con el procedimiento de borrado seguro.

6.3.12. Gestión de usuarios privilegiados

Para la Universidad la gestión de usuarios privilegiados es fundamental para garantizar la seguridad de las credenciales de administración de los servidores y de las plataformas tecnológicas, por ello se deben implementar medidas rigurosas para la asignación, monitoreo y revocación de privilegios, asegurando que solo personal autorizado tenga acceso a recursos críticos, así mismo se establecerán revisiones y auditorías – internas o externas- periódicas para garantizar la alineación con las necesidades de la Universidad y la minimización de riesgos.

Es responsabilidad de los encargados de servidores y servicios tecnológicos en cualquier dependencia de la Universidad – por ejemplo, laboratorios-, gestionar de manera adecuada las credenciales de administración de los equipos especializados, de acuerdo con los procedimientos establecidos.

6.3.13. Control de Cambios en Tecnologías de Información

Todo cambio a la arquitectura de información, así como a la infraestructura para el procesamiento de la información, será controlado y realizado de acuerdo con el procedimiento de Gestión de Cambios, con el fin de gestionar que los cambios autorizados no afecten la disponibilidad, integridad y confidencialidad de la información.

Los cambios de impacto que sean requeridos realizar sobre las plataformas críticas deben ser revisados por el Comité de Cambios en Tecnologías de Información, el cual establecerá adicionalmente a sus funciones, los requerimientos de seguridad asociados a los cambios presentados, conforme a los lineamientos establecidos por la Universidad, como el fin de prever un resultado adverso en las operaciones de la institución.

6.3.14. Configuración de equipos de cómputo, servidores y máquinas físicas y virtuales

Todos los equipos de cómputo de la Universidad deben cumplir mínimo las siguientes condiciones:

- El sistema operativo debe estar licenciado o ser de código abierto, y en cualquier caso con soporte activo,
- El sistema operativo debe estar actualizado a la última versión y con el ultimo parche de seguridad liberado,
- El equipo debe contar con protección *antivirus antimalware*; dicha protección será la autorizada por la Dirección de Tecnologías de Información (DTI) y el Centro de Servicios Informáticos (CSI),
- El equipo debe tener activado el *firewall* del sistema operativo y solo deben estar habilitados los puertos de comunicación en red necesarios para la prestación del servicio.

La gestión oportuna de las vulnerabilidades y oportunidades de mejora propuestas, deberán ser atendidas por los responsables de los equipos y/o del proceso, de acuerdo con lo estipulado en el procedimiento de gestión de vulnerabilidades

Periódicamente la Universidad realizará las pruebas, revisiones y auditorias de seguridad que considere teniendo en cuenta las buenas prácticas y la criticidad del servicio asociado a los equipos y servidores.

6.3.15. Adquisición, desarrollo y mantenimiento de *software*

La Universidad adoptará y solicitará metodologías de desarrollo seguro durante el ciclo de vida del *software*, por ello el responsable de la gestión de *software* y sus proveedores deben cumplir el procedimiento correspondiente.

Durante todo el ciclo de desarrollo de *software* se deben tener en cuenta entre otros los siguientes lineamientos de seguridad de la información:

- Contar con todas las licencias del *software* que se utilicen en el proceso de desarrollo (interno o externo) de *software* y el que respalda el uso del producto final,
- Garantizar en todo momento la segregación de ambientes: ambiente de desarrollo, ambiente de pruebas y ambiente de producción.
- Realizar un adecuado control de cambios,
- No utilizar datos reales en ambientes no productivos y si es necesario hacerlo, utilizar un método de enmascaramiento de datos y realizar un borrado seguro de la información cuando se culmine la prueba programada,
- Documentar totalmente la aplicación a nivel técnico y de usuario final,
- Para el paso a ambiente productivo el *software* previamente deberá superar con suficiencia, las pruebas de requerimientos funcionales, no funcionales y de seguridad.
- Contar con contratos de mantenimiento y soporte del *software* y del desarrollo, así como la gestión de aplicación frecuente y oportuna de parches y actualizaciones en las diferentes capas del *software*
- Para portales y sitios web se seguirán los mismos lineamientos aquí expuestos para el *software*, así como los indicados en manuales de gobierno de sitios web de la Universidad.

Periódicamente la Universidad realizará las pruebas, revisiones y auditorias de seguridad que considere teniendo en cuenta las buenas prácticas y la criticidad del servicio asociado al *software*. La gestión oportuna de las vulnerabilidades y oportunidades de mejora deberán ser atendidas por los responsables del *software* y/o del proceso de acuerdo con lo estipulado en el procedimiento de gestión de vulnerabilidades.

6.3.16. Seguridad de redes

La Universidad debe contar con los mecanismos de control necesarios para garantizar la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, debe velar por que se cuente con los mecanismos de seguridad que protejan la disponibilidad, integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos, por ello dispondrá de mecanismos de autenticación y protección para acceder a las conexiones de red a través de los servicios tecnológicos de la Universidad.

También dispondrá de los controles que considere necesarios para la segmentación, cifrado y filtrado del tráfico de red, entre otros con el fin de minimizar posibles riesgos de seguridad de la información y amenazas de ciberseguridad; así mismo, podrá restringir el tráfico de regiones o servicios web que considere un riesgo para la institución;

El uso de *software* de evasión de cualquiera de las protecciones de la red de la Universidad está prohibido, ya que representa un riesgo para la información y sus servicios tecnológicos.

6.3.17. Servicios "en nube"

Cuando los procesos sean soportados a través de servicios tecnológicos "en nube" (*cloud*), los responsables del servicio deberán:

- Solicitar un concepto la Dirección de Tecnologías de Información (DTI) o el Centro de Servicios Informáticos (CSI), según corresponda. Los cuales tendrán en cuenta, entre otros, los siguientes aspectos:

    - Verificar que el proveedor ofrezca una disponibilidad de al menos el 99.95% en los servicios prestados en la nube en los modelos Iaas y PaaS. Para aquellos proveedores del servicio de computación en la nube en el modelo SaaS, la disponibilidad debe ser de al menos el 99.5%.

- Verificar que el proveedor de servicios en la nube en el sitio de procesamiento cuente y mantenga vigente al menos la certificación ISO 27001, ISO 20000, aplique o se encuentre certificado con el marco de ciberseguridad del NIST *cybersecurity framework*, en sus versiones más recientes. El proveedor deberá demostrar sus certificaciones con estándares o mejores prácticas que reemplacen o sustituyan las anteriormente mencionadas de acuerdo con el mejor estándar disponible en el mercado. De igual manera, deberá disponer de informes de dicha gestión.

- Identificar las salvaguardas, controles y protecciones que el proveedor ofrezca para minimizar posibles riesgos de seguridad de la información y amenazas de ciberseguridad, derivadas de la utilización de servicios computacionales en la nube, considerando, entre otros factores:

    - El tipo de información y datos a procesar,
    - El tipo de nube contratada,
    - Los sitios de procesamiento,
    - Los servicios contratados,
    - Datos y servicios que allí se presten.

- Verificar que las jurisdicciones en donde se procesará la información cuenten con legislación equivalente o superior a las aplicables en Colombia, relacionadas con la protección de datos personales y penalización de actos que atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los servicios tecnológicos.

- Establecer mecanismos que permitan contar con respaldo de la información que se procesa en la nube, la cual debe ser tecnológicamente independiente al hosting principal.

- Que el proveedor garantice la independencia de la información y de las copias de respaldo de la información, de las otras entidades que procesen en la nube. La independencia se puede dar a nivel lógico o físico.

- Mantener cifrada la información clasificada como confidencial en tránsito o en reposo, usando estándares y algoritmos reconocidos internacionalmente que brinden al menos la seguridad ofrecida por los mejores algoritmos disponibles en el mercado.
- El responsable del servicio debe tener bajo su control la administración de usuarios y de privilegios para el acceso a los servicios ofrecidos, así como a las plataformas, aplicaciones y bases de datos que operen en la nube, dependiendo del modelo de servicio contratado.
- El responsable debe monitorear los servicios contratados – incluyendo los acuerdos de seguridad de la información- para detectar operaciones o cambios no deseados y/o adelantar las acciones preventivas o correctivas cuando se requiera.
- Debe verificar el cumplimiento de los acuerdos y niveles de servicio – incluyendo los acuerdos de seguridad de la información- establecidos con el proveedor de servicios en la nube y sus subcontratistas o *"partners"*, cuando sean estos quienes prestan el servicio, así como establecer dentro de los acuerdos contractuales cláusulas de protección de recursos ante escenarios de ciber-crisis.

6.3.18. Dispositivos personales

El personal docente y administrativo podrá utilizar sus dispositivos personales para acceder a recursos de la Universidad, siempre y cuando cumplan con las medidas de seguridad mínimas:

- Cumplir con el numeral Configuración de equipos de cómputo,
- El personal docente y administrativo deben contar con una clara demarcación entre la información propiedad de la Universidad y la personal en sus dispositivos. Esto implica almacenar, procesar y compartir datos institucionales de manera exclusiva en aplicaciones y espacios designados, asegurando así la confidencialidad y la integridad de la información,

- Únicamente se permitirá conexión mediante redes inalámbricas a la red de internet de la Universidad,
- Las terceras partes tales como proveedores, consultores entre otros, deben ser autorizados antes de conectarse a la red de la Universidad, y de igual manera, deben cumplir con el numeral Configuración de equipos de cómputo.

Las unidades de la Universidad que tengan acceso a información crítica de la Universidad deben seguir adicionalmente los siguientes lineamientos con el fin de asegurar una gestión adecuada de la seguridad de dicha información:

- El uso de dispositivos personales estará sujeto a previa autorización,
- Se deberá instalar el agente antimalware autorizado y tener en cuenta los demás controles de seguridad que apliquen,
- El dispositivo deberá contar con un perfil independiente; este perfil no deberá almacenar por ningún motivo información de la Universidad.

6.3.19. Gestión de la seguridad en proveedores

Con el fin de garantizar la seguridad de la información durante la cadena de suministro de servicios hacia la Universidad, los responsables del bien o servicio y los supervisores del contrato con el proveedor, deben tener en cuenta:

- Identificar y determinar el nivel potencial de los riesgos de seguridad de información y amenazas de ciberseguridad, derivados en la utilización de los servicios del proveedor.
- Como parte del proceso de evaluación de proveedores deben solicitar un concepto de la Dirección de Tecnologías de Información, con el fin de revisar y verificar las condiciones y seguridad de los servicios de tecnología asociados.
- Dentro de la elaboración de contratos o convenios con terceras partes, asegurar la inclusión de la política, normas y procedimientos de seguridad de la información y de ciberseguridad que apliquen en los acuerdos contractuales.
- Realizar revisiones periódicas a los proveedores, teniendo en cuenta el procedimiento de evaluación de proveedores.

Los lineamientos mínimos de seguridad de la información que deben cumplir dichos proveedores deben ser, entre otros:

- Cumplir con los lineamientos de seguridad y ciberseguridad aquí establecidos,
- Contar con un programa para gestionar los riesgos de seguridad de la información y amenazas de ciberseguridad,
- Contar con políticas de seguridad de la información de acuerdo con los niveles de riesgo identificados por el proveedor,
- Aplicar las medidas de control para los riesgos identificados,
- Corregir las situaciones que hayan sido identificadas en visitas o auditorias y que pongan en riesgo la seguridad de la información y ciberseguridad,
- Informar de inmediato a la Universidad de cualquier evento o incidente de seguridad que pueda afectar directa o indirectamente los servicios tecnológicos de la Universidad,
- Si el proveedor almacena información propiedad de la Universidad, deberá cifrar la información en tránsito, así como la que este almacene.

6.3.20. Recuperación ante desastres

La Universidad gestionará proactivamente potenciales riesgos de interrupción y los impactos que éstos puedan tener sobre sus procesos críticos a través del proceso de continuidad de la institución, con el fin de garantizar la continuidad y restauración de sus procesos, buscando el mínimo impacto en los servicios.

La Universidad establecerá planes y medidas de prevención ante eventos que generen potenciales interrupciones de los servicios de tecnología de información que soportan los servicios críticos de la institución, y actuará diligentemente frente a una situación de crisis o emergencia, recuperando los servicios en el menor tiempo posible, dentro de sus capacidades.

Estos planes estarán documentados y aprobados, y deberán ser probados de forma periódica, con el fin de verificar su efectividad e identificar mejoras aplicables.

7. DOCUMENTOS ASOCIADOS

IDENTIFICACION DEL DOCUMENTO	NOMBRE
EXTERNO	NTC:ISO 27001
	NTC:ISO 27005
	NTC:ISO 27017
	NTC:ISO 27018
	NTC:ISO 27032
	NTC:ISO 31001
	NIST *Cybersecurity* Framework 2.0
INTERNO	Política de cultura y desarrollo digital

ARTÍCULO SEGUNDO- El presente Acuerdo tiene vigencia a partir de su fecha de expedición y promulgación en las páginas web de la Universidad.

Dado en Bogotá, a los 12 días del mes de febrero de 2025.

LUIS FERNANDO MÚNERA CONGOTE, S.J.
Presidente del Consejo Directivo Universitario

JAIRO H. CIFUENTES MADRID
Secretario del Consejo Directivo Universitario