Manual del Sistema de Gestión de Seguridad de la Información

Gestión informática

Administración y soporte de tecnologías de información

Índice

1. Introducción

La Universidad Libre cuenta con activos de información que son fundamentales para el desarrollo de sus operaciones y, por ende, para alcanzar sus objetivos estratégicos.

Consciente de la importancia de sus activos de información, la Universidad decide implementar, mantener y mejorar un Gobierno de Seguridad de la Información y Ciberseguridad (GSIC), que establece las directrices y lineamientos para planear, implementar, operar, monitorear, revisar y mejorar la seguridad de la información, definir responsabilidades, aplicar buenas prácticas de seguridad de la información y ciberseguridad, dar cumplimiento a las disposiciones legales, contractuales, regulatorias y normativas vigentes relacionadas con seguridad de la información y ciberseguridad, y apoyar la toma de decisiones alineadas con los objetivos estratégicos, para mitigar los riesgos de seguridad de la información y ciberseguridad.

El Gobierno de Seguridad de la Información y ciberseguridad (GSIC) de la Universidad Libre se encuentra compuesto principalmente por personas, Políticas, un sistema de gestión, acciones y controles para proteger los activos de información.

En el presente documento se consolidan los aspectos más importantes del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad Libre.

2. Alcance

Este manual aplica para todas las partes que tienen acceso a los activos de información propia o bajo custodia de la Universidad Libre, y los procesos que se encuentren dentro del alcance de su Sistema de Gestión de Seguridad de la Información (SGSI).

3. Objetivo

Definir los aspectos más importantes del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad Libre.

4. Glosario

La definición de los términos se incluye al final del documento en la sección de Anexos.

5. Referencias normativas

Este documento complementa los siguientes lineamientos de la Universidad Libre:

- Política General de Seguridad de la Información y Ciberseguridad

6. Manual

En esta sección se presentan los aspectos y componentes más importantes del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad Libre.

6.1 Definición del Sistema de Gestión de Seguridad de la Información (SGSI)

El Sistema de Gestión de Seguridad de la Información (SGSI) hace parte del Gobierno de seguridad de la información y Ciberseguridad (GSIC) de la Universidad Libre.

Está alineado con la norma ISO/IEC 27001 y se estructura principalmente sobre un proceso de gestión de riesgos de seguridad de la información y ciberseguridad, integrado con los procesos incluidos en su alcance. Asimismo, se soporta en directrices definidas mediante políticas y procedimientos que permiten planear, implementar, operar, monitorear, revisar y mejorar de manera continua la seguridad de la información, establecer responsabilidades, aplicar buenas prácticas y asegurar el cumplimiento de las disposiciones legales, contractuales, regulatorias y normativas vigentes en materia de seguridad de la información y ciberseguridad.

6.2 Contexto de la Universidad Libre

En esta sección se referencian y describen los aspectos internos y externos que pueden afectar la capacidad para lograr los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) y, por ende, los objetivos estratégicos de la Universidad Libre.

6.2.1 Contexto interno

6.2.1.1 Misión y visión de la Universidad Libre

La Misión y Visión de la Universidad Libre se encuentra descrita en el siguiente sitio web:

https://www.unilibre.edu.co/wp-content/uploads/2025/01/Resolucion-14-24-Expide-el-Codigo-de-Buen-Gobierno-de-la-Universidad-Libre-W.pdfPrincipios

6.2.1.2 Principios

Los principios de la Universidad Libre se encuentran descritos en los Estatutos de la Universidad Libre, publicado en el siguiente sitio web:

https://www.unilibre.edu.co/wp-content/uploads/2025/01/Resolucion-14-24-Expide-el-Codigo-de-Buen-Gobierno-de-la-Universidad-Libre-W.pdfPrincipios

6.2.1.3 Objetivos estratégicos de la Universidad Libre

Los objetivos estratégicos de la Universidad Libre están definidos en el Plan Integral de Desarrollo Institucional (PIDI) 2025 – 2029, publicado en el siguiente sitio web:

https://www.unilibre.edu.co/normativas/acuerdo-n-o-6-de-2024/

6.2.1.4 Partes interesadas

Según la Resolución n.º 14 de 2024 (8 de agosto), «Por el cual se expide el Código de Buen Gobierno de la Universidad Libre» dentro del Artículo 11. De los grupos de interés. Son partes interesada dentro de la Universidad.

6.2.1.5 Partes interesadas internas

A continuación, se listan las partes interesadas internas, y se describen sus requisitos y expectativas identificadas frente al Sistema de Gestión de Seguridad de la Información (SGSI).

- Integrantes Activos y Benefactores de la Sala General.
- Consiliarios principales y suplentes.
- Consejeros Directivos principales y suplentes.
- Consejeros Académicos principales y suplentes.
- Integrantes de los Comités de Unidad Académica principales y suplentes.
- Profesores, investigadores, instructores y catedráticos.
- Empleados administrativos.
- Estudiantes de pregrado y posgrado.
- Egresados.
- En el caso de menores de edad los padres o tutores.

Requisitos	Expectativas
Proteger la información que esté bajo custodia de la Universidad; Conocer información establecidas en la Universidad. Conocer los mecanismos y controles que la Universidad dispone para proteger la información. Conocer los medios y procedimientos dispuestos por la Universidad para notificar eventos, incidentes, o solicitudes de seguridad de la información. Adquirir conciencia y cultura en seguridad de la información. Contar con acceso controlado y seguro a información bajo custodia de la Universidad Libre, a la cual tengan autorización de acceso.	Preservar la seguridad de su información. Contar con acceso controlado y seguro a información propia o bajo custodia de la Universidad. Que se evite la materialización de incidentes de seguridad de la información y ciberseguridad que puedan afectar su información personal, o de su proceso académico. Obtener conocimiento en seguridad de la información y ciberseguridad, que le permita proteger la información y reaccionar de forma adecuada ante un incidente.

Tabla 1. Partes interesadas internas – Requisitos y expectativas

6.2.2 Contexto externo

6.2.2.1 Partes interesadas Externas

A continuación, se listan las partes interesadas externas, y se describen sus requisitos y expectativas identificadas frente al Sistema de Gestión de Seguridad de la Información (SGSI).

- Sociedad
- Entidades del Estado
- Sector Productivo
- Redes Académicas

Requisitos	Expectativas
Contar con medios y mecanismos para notificar novedades y hacer solicitudes referentes a seguridad de la información y ciberseguridad. Que su información personal o propia que pueda ser conocida por la Universidad sea protegida de forma adecuada. Que la Universidad aplique controles de seguridad de la información y ciberseguridad, que eviten la materialización de incidentes que les afecten. Que se dé cumplimiento a los requisitos contractuales y legales referentes a la protección de datos personales y la seguridad de la información. Contar con información verídica de seguridad de la información que pueda ser requerida con justificación. Contar con acceso controlado y seguro a información bajo custodia de la Universidad Libre, a la cual tengan autorización de acceso. Que la Universidad colabore en procesos de investigación relacionados con incidentes de seguridad de la información en los que pueda encontrarse vinculada.	Que la información propia que esté bajo custodia de la Universidad sea protegida de forma adecuada. Contar con acceso seguro a la información de interés de la Universidad, cuando lo requiera. Contar con mecanismos para reportar o solicitar a la Universidad temas relacionados con seguridad de la información y ciberseguridad. Que la Universidad evite la materialización de incidentes de seguridad de la información y ciberseguridad sobre sus sistemas de información, que puedan generar un impacto sobre la sociedad. Que la Universidad responda de forma adecuada ante la materialización de incidentes de seguridad de la información y ciberseguridad.

Tabla 2. Partes interesadas externas – Requisitos y expectativas

6.2.2.2 Requisitos externos generales

En esta sección se presentan, de forma general, los requisitos externos que la Universidad Libre

Requisitos legales	
Entidad del Estado	**Requisitos**
Congreso de la República	Ley 1273 de 2009. Ley de Delitos Informáticos.
	Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
	Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales
	Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
	Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Tabla 3. Requisitos externos - Legales

Requisitos reglamentarios y regulatorios	
Entidad del Estado	**Requisitos**
Ministerio de Tecnologías de la Información y las Comunicaciones	Decreto 1078 de 2015 (Título 9, Capítulo 1). Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
	Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
	Decreto 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Ministerio de Comercio, Industria y Turismo	Decreto Único 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
	Decreto 1115 de 2017. Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
Superintendencia de Industria y Comercio	Circular Externa 001 del 8 de noviembre de 2016. Instrucciones para el realizar la inscripción de sus bases de datos en el Registro Nacional de Bases de Datos - RNBD a partir del 9 de noviembre de 2016.
	Circular Externa 001 del 11 de enero de 2017. Modifica los numerales 2.2, 2.3, 2.6 y 2.7 del Capítulo Segundo del Título V de la Circular Única de la Superintendencia de Industria y Comercio.

Requisitos reglamentarios y regulatorios	
Entidad del Estado	**Requisitos**
El Consejo Nacional de Política Económica y Social, CONPES	CONPES 3701. Lineamientos de política para la Ciberseguridad y Ciberdefensa. CONPES 3854. Política Nacional de Seguridad Digital.

Tabla 4. Requisitos externos – Reglamentarios y regulatorios

6.3 Alcance del Sistema de Gestión de Seguridad de la Información (SGSI)

La Universidad Libre define como alcance para el Sistema de Gestión de Seguridad de la Información - SGSI, los activos de información necesarios para el correcto funcionamiento del proceso Gestión Informática de la Universidad, el cual opera en diferentes sedes a Nivel Nacional, y conforme a las exclusiones que se encuentran documentadas en la declaración de aplicabilidad.

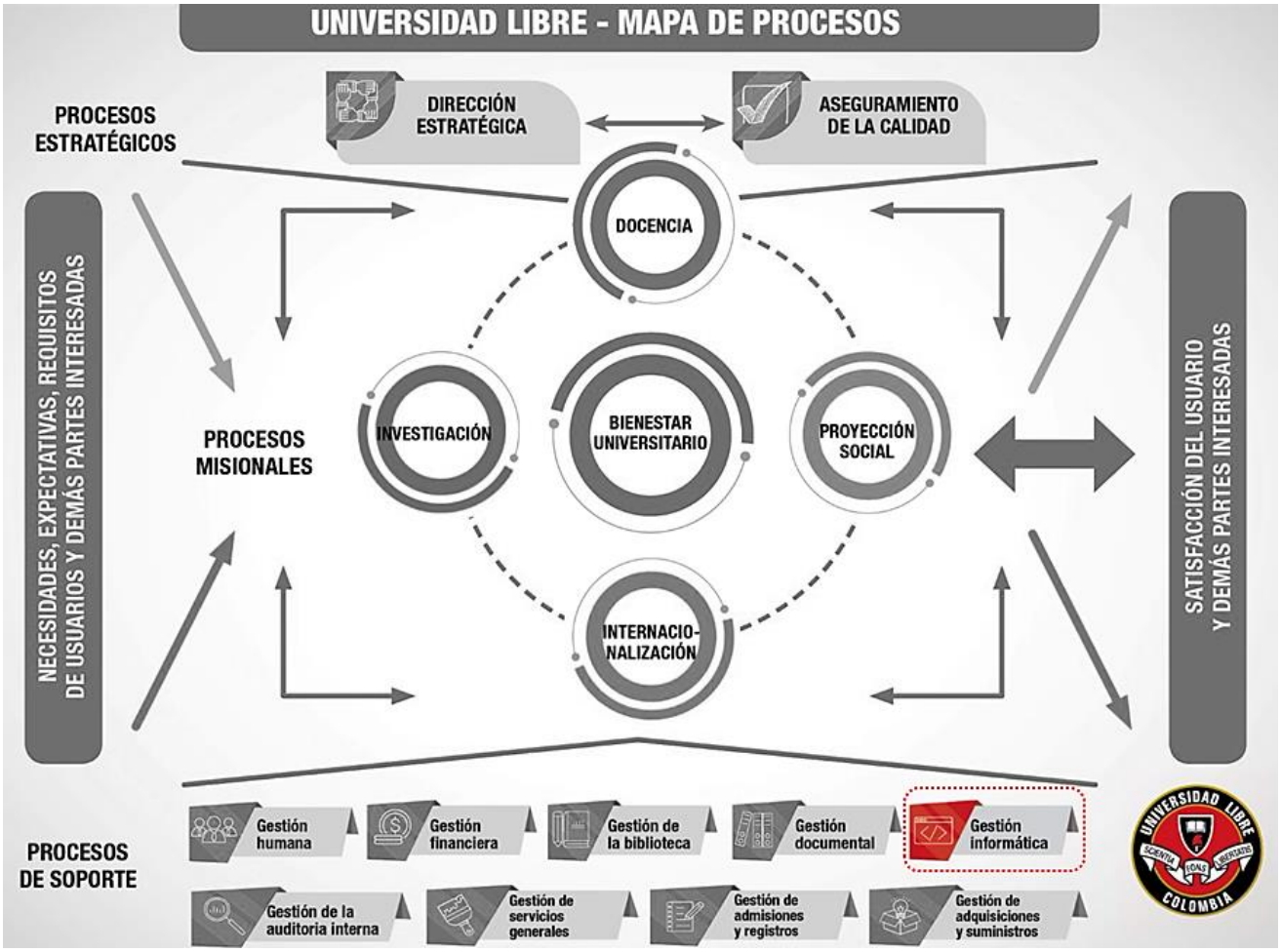

Ilustración 1. Alcance del Sistema de Gestión de Seguridad de la Información (SGSI) dentro del mapa de procesos

6.4 Objetivos del Sistema de Gestión de Seguridad de la Información (SGSI)

A continuación, los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad Libre:

- Gestionar los riesgos de seguridad de la información y ciberseguridad sobre los procesos que se encuentren dentro del Sistema de Gestión de Seguridad de la Información (SGSI), en alineación con la metodología de gestión de riesgos definida en la Universidad.
- Gestionar de forma adecuada y diligente los incidentes de seguridad de la información y ciberseguridad.
- Promover la formación de una cultura y conciencia de Seguridad de la Información y ciberseguridad entre el personal interno de la Universidad y terceros vinculados a esta.
- Velar porque sean establecidos niveles adecuados de seguridad informática y ciberseguridad.
- Velar por la aplicación de buenas prácticas y el cumplimiento de los lineamientos como políticas y procedimientos de seguridad de la información y ciberseguridad, en los procesos que se encuentren dentro del Sistema de Gestión de Seguridad de la Información (SGSI).
- Cumplir con las obligaciones de seguridad de la información y ciberseguridad aplicables a la Universidad y vigentes de tipo legal, normativo, regulatorio y contractual.
- Velar por la evaluación periódica del desempeño del Sistema de Gestión de Seguridad de la Información (SGSI) y su mejora continua.

6.5 Riesgos y oportunidades del Sistema de Gestión de Seguridad de la Información (SGSI)

En esta sección se describen los riesgos y oportunidades del Sistema de Gestión de Seguridad de la Información, identificados en la Universidad Libre, y las acciones definidas para abordarlos.

Riesgos	Acciones
Falta de presupuesto para la ejecución de las actividades definidas dentro del SGSI.	Asignación de presupuesto y recursos necesarios por parte de la Presidencia y Rectorías de la Universidad.
Incremento significativo en los costos y complejidad asociados a la implementación de herramientas de seguridad avanzadas y a la operación del Sistema de Gestión de Seguridad de la Información.	Evaluación del SGSI para optimizar su implementación y operación.
Falta de compromiso del personal responsable del SGSI del Comité de Seguridad.	Seguimiento periódico de la operación del SGSI, desde el Comité de seguridad de la información y la Presidencia.
Retraso o incumplimiento en las actividades definidas dentro del SGSI.	Seguimiento periódico de la operación del SGSI en la Universidad, desde el Comité de seguridad de la información y la Presidencia.
Desconocimiento de las partes interesadas de la existencia o los efectos del SGSI.	Socialización del SGSI y la ejecución de las actividades definidas en este.

Resistencia de los procesos y las personas de la Universidad en la adopción de los controles de seguridad de la información	Sensibilización y capacitación de las personas de la Universidad.
Desconocimiento de la Presidencia en el estado de ejecución de las acciones definidas en el SGSI y la efectividad de su operación.	Reporte periódico a la Presidencia acerca de las actividades desarrolladas dentro del SGSI y la efectividad de las acciones.

Tabla 5. Riesgos del Sistema de Gestión de Seguridad de la Información (SGSI) y acciones para abordarlos

Oportunidades	Acciones
Incorporar a los procesos institucionales el SGSI fortaleciendo la confianza de la comunidad universitaria y de las partes interesadas en el manejo adecuado y seguro de la información institucional.	Ofrecer como valor agregado de la Universidad la seguridad de la información soportada con la implementación del SGSI basado en ISO 27001.
Reducción del riesgo de materialización de incidentes de seguridad de la información.	Ofrecer como valor agregado de la Universidad la seguridad de la información soportada con la implementación del SGSI basado en ISO 27001.
Estructuración de procedimientos y actividades en un sistema de gestión integrado en la operación de la Universidad	Optimización de los procesos de la Universidad.

Tabla 6. Oportunidades del Sistema de Gestión de Seguridad de la Información (SGSI) y acciones para abordarlas

6.6 Estructura organizacional del Gobierno de Seguridad de la Información y Ciberseguridad

El Gobierno de Seguridad de la Información y Ciberseguridad (GSIC) de la Universidad Libre está conformado principalmente por los siguientes actores:

- Comité de Seguridad de la Información y ciberseguridad.
- Equipo de Seguridad de la Información y ciberseguridad.

6.6.1.1 Comité de seguridad de la información y ciberseguridad

Grupo interdisciplinario de colaboradores de la Universidad Libre, con conocimiento amplio de la operación de la organización, poder para tomar decisiones sobre la gestión de seguridad de la información y ciberseguridad de los procesos, y potestad para proponer a la Alta Dirección la toma de decisiones de este ámbito que tengan competencia con la estrategia y los objetivos de la organización.

Se reúne al menos una vez al año, o de forma extraordinaria por convocatoria del Oficial de Seguridad de Información o de alguno de sus integrantes, y está conformado por los siguientes miembros:

- Presidente
- Rector Nacional

- Coordinador Nacional del Sistema de Gestión de la Calidad
- Director nacional de planeación
- Secretario general
- Administrador de personal
- Director nacional para las TIC
- Oficial de seguridad de la información y ciberseguridad o quien haga sus veces

El Comité de Seguridad de la Información y ciberseguridad tiene la potestad de invitar a su sesión a personas vinculadas o no a la Universidad, para tratar algún tema relacionado con su gestión. Si la persona es externa (no tiene vínculo), es importante que cuente con un compromiso formal para preservar la confidencialidad de los temas que serán tratados en su presencia en la reunión del Comité a la que asista.

En caso de requerir que se incluya en el Comité de seguridad de la información y ciberseguridad de manera permanente un cargo específico que no se encuentre en el listado relacionado, éste debe definirse mediante acta de comité.

Cuando un miembro del comité no pueda asistir, debe designar formalmente una persona que lo represente en la sesión, quien asumirá sus responsabilidades y poderes.

6.6.1.2 Equipo operativo de seguridad de la información y ciberseguridad

Personas encargadas de desarrollar, mantener y administrar la seguridad de la información y la ciberseguridad en la Universidad Libre. Puede estar conformado por los siguientes roles, cuyas funciones y responsabilidades están definidas en la descripción de cada cargo correspondiente:

- Oficial de seguridad de la información y ciberseguridad o quien haga sus veces
- Jefes de Sistemas de las seccionales

6.7 Políticas de Seguridad de la Información

6.7.1 Directrices de la Política general de seguridad de la información y ciberseguridad

La Universidad Libre reafirma su compromiso con la protección, confidencialidad, integridad y disponibilidad de la información siendo un activo fundamental que respalda los procesos académicos, administrativos y transversales a nivel institucional. Entendiendo la información de todos los grupos de interés que interactúan con la Universidad, incluyendo estudiantes, docentes, egresados, colaboradores, proveedores entre otros.

En coherencia con este propósito, la Universidad reconoce la seguridad de la información y la ciberseguridad como componentes fundamentales para garantizar la continuidad, confiabilidad y transparencia de sus servicios, promoviendo una cultura institucional orientada a la gestión responsable y segura de la información teniendo en cuenta las siguientes consideraciones:

- Establecer, operar, mantener y mejorar un SGSI conforme a la norma ISO/ 27001 vigente.

- Definir, aplicar y revisar una metodología de gestión de riesgos en seguridad de la información y ciberseguridad.
- Desarrollar programas anuales de capacitación y concienciación dirigidos a toda la comunidad universitaria y terceros vinculados.
- Implementar controles técnicos, organizativos y físicos para proteger los activos de información.
- Garantizar que todos los líderes de proceso difundan, supervisen y velen por el cumplimiento de esta política en sus áreas.
- Establecer procedimientos claros de gestión de incidentes de seguridad de la información y ciberseguridad.
- Revisar periódicamente esta política, sus manuales y procedimientos asociados, asegurando su actualización y aprobación por la Presidencia Nacional.
- Garantizar la asignación de recursos humanos, técnicos y financieros necesarios para implementar esta política.

6.7.2 Política de Seguridad de la Información y Ciberseguridad

Es compromiso de la Universidad Libre proteger la confidencialidad, integridad y disponibilidad de la información, mediante el Sistema de Gestión de Seguridad de la Información y Ciberseguridad orientado a gestionar riesgos, atender incidentes, cumplir requisitos legales y promover una cultura de seguridad, fortaleciendo la confianza institucional y garantizando la continuidad de la prestación del servicio con los más altos estándares de excelencia universitaria.

6.7.3 Políticas específicas de seguridad de la información

La Universidad Libre tiene definidas políticas de seguridad de la información, que hacen parte integral del Gobierno de seguridad de la información y ciberseguridad (GSIC), y complementan la Política general de Seguridad de la Información y Ciberseguridad. Se definen a continuación.

6.7.3.1 Política de gestión de activos de información

Se consideran activos de información de la Universidad Libre la información, en cualquier formato (físico o digital), que es fundamental para el desarrollo de las actividades y procesos que soportan la operación de la organización.

Los activos de información propios de la Universidad Libre son creados o custodiados al interior de sus procesos y su operación, y sobre estos se deben aplicar los controles definidos con base en su nivel de clasificación.

Sobre los activos de información de terceros (proveedores, clientes, entes de control, etc.), que la Universidad Libre pueda tener bajo custodia o procesamiento, se deben aplicar las medidas de protección que el tercero (propietario) ha definido.

En la Universidad Libre los propietarios de los activos de información son los líderes de proceso.

Se debe crear y mantener un inventario de los activos de información de los procesos comprendidos en el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad Libre, y ser actualizado al menos una vez cada año.

Los propietarios de los activos de información son los responsables de realizar y mantener actualizado el inventario de estos, clasificarlos y valorarlos en función de su confidencialidad, integridad y disponibilidad.

Clasificación de los activos de información

En la Universidad Libre se definen los siguientes tres niveles de clasificación de los activos de información, y para cada uno medidas de protección que se deben aplicar:

Nivel de clasificación	Descripción	Ejemplos
Confidencial	Información sensible de la Universidad Libre o bajo su custodia, la cual, si sufre afectación en su seguridad, puede generar impactos leves y graves a la organización. Debido a esto, sólo puede ser accedida por personal de la Universidad Libre con autorización formal y que la requieran para el desarrollo de sus funciones. No está permitida su difusión a terceros sin autorización formal de su propietario.	Estrategias comerciales, Alianzas estratégicas, Movimientos financieros, Información comercial, Planes estratégicos, Información de clientes, Información de empleados, Contratos
Privada	Información de la Universidad Libre o bajo su custodia, que habitualmente se genera al interior de sus procesos para el desarrollo de sus operaciones. En principio solo debe ser de conocimiento interno y su divulgación o conocimiento a terceros debe realizarse dentro de procedimientos o procesos autorizados, exclusivamente por razones de negocio justificadas.	Información, documentación de procesos de negocio, Comunicaciones internas, Circulares, Borradores de contratos, Propuestas, Informes de gestión, Actas
Pública	Información de uso público, su difusión no causa perjuicios a la Universidad Libre ni a sus terceros vinculados.	Información de entes gubernamentales (leyes, circulares, decretos), información publicada en medios de comunicación, sitio web.

Tabla 7. Niveles de clasificación de activos de información

6.7.3.2 Política de control de acceso

Se deben implementar controles de seguridad física y lógica en torno a los activos de información propios y bajo custodia de la Universidad Libre, para puedan ser accedidos únicamente por entes previamente autorizados, cuando así lo requieran para el desarrollo de sus funciones y de la operación de la Universidad, protegerlos frente a alteraciones y daños no autorizados, y frente a fugas.

Control de acceso general

Es responsabilidad de los propietarios de los activos de información de la Universidad Libre velar por la seguridad de los activos que tienen bajo su propiedad y, por ende, deben definir las reglas y autorizaciones de acceso sobre estos.

Los permisos de acceso a los activos de información deben ser asignados teniendo en cuenta su nivel de clasificación de seguridad, mediante un modelo RBAC (roles y privilegios), y aplicando el principio del mínimo privilegio (solamente se concede privilegio a lo que necesita conocer y lo que necesita usar).

Los jefes inmediatos, líderes de proceso y supervisores son responsables de notificar cuando los permisos de acceso asignados a una cuenta de usuario bajo su cargo ya no sean necesarios, deban ser modificados o revocados, por cambio de funciones asignadas o retiro, y solicitar su ajuste, deshabilitación o eliminación, de forma oportuna y diligente.

Las facultades son responsables de definir los permisos de acceso que requieren los estudiantes para el desarrollo de sus actividades, y solicitar al proceso de Gestión Informática de forma oportuna y diligente la asignación y revocación de estos.

Control de acceso para terceros

Los supervisores de los vínculos con terceros son responsables de gestionar los permisos de acceso que estos requieren para el desarrollo de sus funciones, de velar porque los permisos únicamente sean utilizados para realizar actividades propias del objeto del vínculo, y de notificar de forma oportuna y diligente cuando los permisos de acceso ya no sean requeridos, o cuando deban ser modificados, para que sean ajustados, retirados, deshabilitados o eliminados.

Los mecanismos de control de acceso implementados para los terceros deben tener rigurosidad igual o superior a la de los usuarios internos de la organización (trabajadores, estudiantes, otros).

Control de acceso lógico

- El acceso a los sistemas de información, equipos de cómputo, aplicaciones, componentes y soluciones de tecnología de la Universidad, se debe realizar únicamente por medio del uso de cuentas de usuario.
- Cada cuenta de usuario debe estar asignada formalmente a un ente (trabajador, docente, estudiante, egresado, tercero).
- Las cuentas de usuario deben contar únicamente con los permisos de acceso aprobados por el propietario de los activos de información.
- Las cuentas de usuario deben tener configurado el tiempo de vigencia indicado por la persona que solicitó su creación o activación.
- Las cuentas de usuario, sus contraseñas y mecanismos de autenticación son de uso personal e intransferible.
- Los usuarios deben evitar a la mayor diligencia posible que las cuentas de usuario que tienen asignadas sean utilizadas por otra persona o ente diferente, al igual que sus contraseñas y mecanismos de autenticación.

- Los usuarios deben evitar a la mayor diligencia posible que las contraseñas y mecanismos de autenticación de las cuentas de usuario que tienen asignadas sean conocidas o adivinadas por personas o entes diferentes.
- Las actividades realizadas con cada cuenta de usuario son responsabilidad exclusiva del usuario al cual se fue asignada formalmente la cuenta.
- Se deben revisar las cuentas de usuario en el directorio activo, para identificar las cuentas en hibernación (deshabilitadas o sin uso por más de 4 meses), y confirmar que aquellas que deben haberse eliminado ya no se encuentren en el sistema.
- Se debe notificar a los líderes de proceso las cuentas de usuario bajo su cargo que se encuentren activas o en hibernación, para confirmar cuáles deben ser deshabilitadas o eliminadas.
- Se deben implementar controles de acceso para proteger y separar los ambientes de desarrollo, pruebas y producción de sistemas, software, servicios y componentes de tecnología.
- Cuando se crea cada cuenta de usuario debe tener configurada una contraseña temporal que sea única, y que cumpla con lo definido en la presente política según el tipo de cuenta, y ser entregada de forma segura al usuario que la tiene asignada.
- Los usuarios deben cambiar la contraseña temporal de las cuentas que les son asignadas, tan pronto como las reciban.
- Se debe configurar en cada sistema de información o solución de tecnología un control mediante el cual las cuentas de usuario sean bloqueadas si se realizan múltiples intentos fallidos de autenticación. La reactivación de las cuentas en estos casos debe ser gestionada directamente por el usuario que tiene asignada la cuenta, y esta solo podrá ser reactivada luego de validar su identidad y lo ocurrido.
- Se deben aplicar como mínimo los siguientes controles de seguridad sobre las contraseñas de las cuentas de usuario estándar:
    - Cambio de contraseña máximo cada 180 días;
    - Longitud mínima de 8 caracteres;
    - Contener diferentes tipos de carácter, entre mayúsculas, minúsculas, números y símbolos;
- Las contraseñas de las cuentas de usuario configuradas por defecto o fábrica en los sistemas, software o componentes de tecnología deben ser modificadas luego de su instalación, siguiendo los parámetros definidos en la presente política para cada tipo de cuenta.

Cuentas privilegiadas

Las cuentas privilegiadas de la Universidad Libre son aquellas que tienen asignados accesos o acciones privilegiadas sobre sistemas de información, componentes tecnológicos y activos de información sensibles de la organización. En algunos casos, las cuentas privilegiadas, dependiendo los privilegios que tengan asignados, pueden servir para administrar los sistemas, soportarlos, hacer mantenimiento, entre otros. Por su criticidad, estas cuentas deben tener implementados controles más robustos de seguridad.

Las cuentas privilegiadas deben utilizarse única y exclusivamente para realizar las funciones que designó el propietario del activo de TI (sistemas de información, aplicaciones, servicios o componentes de tecnología).

Las cuentas privilegiadas y sus privilegios deben ser registradas en un inventario que se actualice cada vez que se haga creación, modificación, deshabilitación o eliminación de al menos una de ellas.

Las cuentas privilegiadas deben tener configuradas contraseñas con un nivel de complejidad superior al de las cuentas estándar, y que sea suficiente para evitar que sean descifradas o interpretadas por personas o entes ajenos, teniendo en cuenta el interés que pueden tener sobre estas atacantes y ciber-criminales.

Se deben implementar mecanismos de trazabilidad y auditoría (logs) sobre las cuentas privilegiadas, que permitan registrar evidencia de la actividad desarrollada con estas.

Los privilegios de administración de los activos informáticos deben otorgarse únicamente al personal autorizado por el proceso de Gestión Informática.

El Administrador de cada activo de tecnología es el responsable de otorgar los demás accesos al mismo.

El acceso a bases de datos debe ser seguro y asignarse únicamente a los administradores de bases de datos (DBA).

Se deben recolectar y custodiar de forma segura y centralizada los nombres y contraseñas de las cuentas privilegiadas de administración de los activos informáticos.

Control de acceso físico

Centros de cómputo y de cableado

Los centros de cómputo y de cableado de la Universidad Libre se consideran zonas seguras, porque alojan activos informáticos, que a su vez contienen activos de información sensibles de la organización, que requieren ser protegidos y por tanto deben contar con controles de acceso rigurosos.

Se deben implementar mecanismos de control de acceso físico para garantizar que únicamente el personal autorizado pueda ingresar a cada centro de cómputo o de cableado de la Universidad.

El ingreso y salida de los centros de cómputo y cableado debe ser registrado por medio del instrumento (bitácora, acta, minuta, etc.) que designe la Jefatura de Informática de cada seccional, y ser diligenciado de forma rigurosa para garantizar que exista trazabilidad que permita establecer quién accede a estas zonas y la actividad que se desarrolla.

El ingreso a los centros de cómputo y de cableado por parte de terceros como proveedores debe ser justificado, y estos deben estar acompañados durante toda la visita por al menos un trabajador de la Universidad, designado por la Jefatura de Informática de la seccional correspondiente.

La persona que acompañe un visitante de un centro de cómputo o de cableado debe velar porque este cumpla en todo momento las directrices de seguridad de la información definidas en la Universidad, no realice actividades distintas a las definidas en el objeto de la visita, o que atenten contra la seguridad de la información, integridad o correcto funcionamiento de los activos informáticos de la Universidad.

Los permisos de acceso físico a centros de cómputo o de cableado deben ser modificados o retirados de forma oportuna y diligente por las Jefaturas de Informática de cada seccional, para evitar ingresos no autorizados.

Seguridad física de activos informáticos

Para retirar activos informáticos de las instalaciones de la Universidad se deben seguir los procedimientos y directrices establecidos en cada seccional, para garantizar que su salida sea justificada y cuente con autorización.

6.7.3.3 Política de seguridad en la gestión del recurso humano

Se deben realizar capacitaciones a los trabajadores de la Universidad en las cuales se hable de las políticas de seguridad de la información establecidas, detección reporte y atención de incidentes de seguridad de la información, y las consecuencias del incumplimiento de las directrices definidas teniendo en cuenta que el desconocimiento de estas, no los exonera de los procesos disciplinarios que apliquen.

De la misma forma, se debe sensibilizar a la comunidad académica de la Universidad en seguridad de la información, la importancia del uso adecuado de los activos informáticos, de la aplicación de las buenas prácticas de seguridad de la información, el reporte de eventos e incidentes de seguridad, y las amenazas más frecuentes a las cuales se puede ver expuesta.

Se debe realizar una inducción a los trabajadores, en la cual se les comuniquen las políticas y directrices de seguridad de la información y las consecuencias que puede tener su incumplimiento.

Cuando un trabajador sea trasladado de dependencia o retirado de la Universidad, el jefe de área responsable debe informar a los líderes funcionales y técnicos de los sistemas de información según corresponda y al proceso de Gestión Informática, para que sean retirados o ajustados los permisos de acceso asignados, procurando siempre aplicar el principio de mínimo privilegio, y contando siempre con la autorización de los propietarios de los activos de información.

6.7.3.4 Política de seguridad de la información en vínculos con terceros

Los terceros de la Universidad Libre son todos aquellos entes, naturales y jurídicos, que no tienen un contrato de trabajo directo con la organización, pero tienen un vínculo contractual que implica una relación en la cual pueden llegar a tener acceso a información o activos informáticos de la Universidad y, por ende, deben cumplir con las políticas y directrices de seguridad de la información y ciberseguridad establecidas en esta. Entre los terceros pueden encontrarse (sin limitarse a): proveedores, contratistas y clientes.

Para los terceros que aplique, se deben generar Acuerdos de Niveles de Servicio (ANS) que hagan parte integral del contrato, definidos con base en las necesidades de la Universidad, para evitar la afectación de su operación.

La asignación, uso y retiro de accesos para los terceros vinculados a la Universidad debe cumplir las directrices establecidas en la Política de control de acceso de la Universidad.

Los proveedores que tengan acceso a activos de información propios o bajo custodia de la Universidad, deben cumplir con lo definido en la Política de gestión de activos de información.

Los terceros que proveen servicios o componentes de tecnología deben identificar y remediar de forma oportuna las vulnerabilidades de seguridad de la información y ciberseguridad existentes en su entorno.

El proveedor debe entregar a la Universidad Libre, si aplica, la documentación que demuestre el cumplimiento de las políticas de seguridad de la información en toda la cadena de suministro que involucre los servicios contratados.

Los terceros vinculados a la Universidad deben reportar a la mayor brevedad y diligencia posible incidentes de seguridad que constituyan o puedan significar la vulneración de la seguridad de la información de la Universidad Libre, o de sus activos informáticos.

El proveedor debe contar con un Plan de Continuidad de Negocio acorde al bien, servicio u obra adquirido por la Universidad Libre; si la empresa requiere el envío y resultado de las pruebas de este plan, debe ser suministrado sin inconveniente por el proveedor.

Cuando ocurra un evento de interrupción de los servicios prestados por el proveedor que sea imputable totalmente a éste, debe asegurar la prestación del servicio cumpliendo con el Tiempo Objetivo de Recuperación (RTO) requerido por el (los) proceso (s) de la Universidad Libre según las necesidades expuestas en el documento de Análisis de Impacto al Negocio – BIA el cual se debe desarrollar por la Universidad.

El proveedor debe informar los datos de contacto y horarios de disponibilidad de los responsables que durante la vigencia del contrato atenderán situaciones críticas y de indisponibilidad de los servicios suministrados; el proveedor debe garantizar que el recurso disponible para la atención cuente con los conocimientos técnicos requeridos.

6.7.3.5 Política de uso adecuado de activos informáticos

La Universidad Libre pone a disposición de sus trabajadores, docentes, estudiantes, egresados, proveedores y otros terceros, activos informáticos como servicios (por ejemplo correo electrónico, aplicaciones, sistemas de información), equipos (por ejemplo equipos de cómputo de escritorio y portátiles, servidores, puntos de acceso de red inalámbrica), dispositivos de tecnología (por ejemplo teléfonos celulares, tabletas), infraestructura (por ejemplo instalaciones, salas, cableado), información en cualquiera de sus formatos, permisos, entre otros, para apoyar la realización de las actividades y funciones de su operación, y deben ser utilizados acorde con lo definido en la presente política, cuyo incumplimiento implica consecuencias disciplinarias que deben ser asumidas por el responsable del recurso.

Los trabajadores, docentes, estudiantes, egresados, y proveedores vinculados a la Universidad Libre deben cumplir todas las políticas y directrices de seguridad de la información y ciberseguridad cuando hacen uso de los activos informáticos que la Universidad dispone, y deben:

- Utilizar los activos informáticos que disponga y asigne la Universidad única y exclusivamente para fines laborales o académicos que esta defina, realizar las actividades propias de su cargo y aquellas que promueven el cumplimiento de los objetivos estratégicos, tácticos y académicos de la Universidad, y nunca para fines personales, ni para transmitir, procesar o almacenar información personal;
- Evitar a la mayor diligencia posible transmitir, almacenar o procesar información que atente contra la propiedad intelectual o derechos de autor;
- Abstenerse de transmitir, almacenar o procesar mensajes de correo maliciosos como SPAM (Correo no deseado o no solicitado), Spoofing (correos de suplantación), Phishing (correos de engaño o suplantación), o cualquier tipo de correo, archivo o vínculo con contenido desconocido o con contenido malicioso.
- Abstenerse de consultar, transmitir, procesar o almacenar material relacionado con pornografía o contenido sexual explícito, compra, venta, uso o distribución ilícitos de armas y alcohol, u otros hechos ilícitos;
- Abstenerse de obtener, almacenar, utilizar o instalar software ilegal, sin licenciar o no autorizado en la Universidad, así como todo tipo de programas que puedan afectar la confidencialidad, integridad o disponibilidad de la información.

- Tener en cuenta que los activos informáticos asignados o dispuestos por la Universidad pueden ser accedidos y monitoreados por un ente de control de esta, contando con autorización previa del propietario de la información, sin incurrir en violación de la privacidad, puesto que dichos activos informáticos son asignados para fines laborales.
- Custodiar los activos informáticos que tienen a su disposición o asignados, para evitar la fuga, pérdida o alteración de la información contenida en los mismos, teniendo en cuenta las directrices definidas en esta política.

Escritorio limpio y pantalla limpia

Todo documento, medio magnético u óptico removible que contenga información confidencial o sensible, debe ser almacenado en lugar seguro. Estos elementos solo pueden estar por fuera de estos sitios cuando estén siendo usados por la persona autorizada, una vez termine la actividad se debe guardar inmediatamente.

Todos los empleados y contratistas de la Universidad Libre deben bloquear la sesión del equipo de cómputo cada vez que lo vaya a dejar desatendido, o deba ausentarse por un momento de su puesto de trabajo.

Todos los equipos de cómputo deben tener configurado el bloqueo automático de sesión por tiempo de inactividad.

Todos los empleados y contratistas deben mantener el escritorio del equipo de cómputo (virtual) libre de información confidencial y datos personales sensibles.

Equipos de cómputo de escritorio y portátiles

El proceso de Gestión Informática es el único autorizado para la asignación e instalación de los equipos de cómputo requeridos para la operación de la Universidad Libre.

La instalación y administración de todo componente de software, hardware y/o Infraestructura tecnológica en general, está a cargo de la Jefatura de Sistemas, al ser de su responsabilidad y, por tanto, se debe realizar una solicitud siguiendo los lineamientos y los mecanismos diseñados para tal fin en cada sede de la Universidad.

Cualquier traslado de hardware dentro o fuera de las instalaciones de la Universidad, debe ser solicitado siguiendo lo descrito en el Procedimiento que defina el Sistema de Gestión de la Calidad.

Para retirar cualquier equipo de cómputo de la Universidad, sea portátil o de escritorio, se debe contar previamente con autorización formal del Jefe Inmediato y conforme a lo descrito en el Procedimiento que defina el Sistema de Gestión de la Calidad.

Debe respetarse y no modificarse la configuración de hardware y software establecido por la Jefatura de Sistemas, en cada uno de los equipos de cómputo. En caso de presentarse algún requerimiento de cambio de configuración se debe seguir el procedimiento diseñado para tal fin.

Los usuarios deben abstenerse de utilizar medios de almacenamiento removible como memorias flash USB, celulares, discos externos, CD, DVD, para almacenar información de la Universidad, con excepción de las personas vinculadas a esta, que lo requieran para el desarrollo de sus funciones designadas y la operación de la organización, y acorde con lo definido en el Procedimiento de Gestión de Medios Removibles.

Es responsabilidad de todos los empleados, apagar o poner a hibernar los equipos que no estén usando o al finalizar la jornada laboral.

La seguridad física e integridad de los equipos de cómputo o demás activos, que ingresen a las instalaciones de la Universidad Libre y que no sean propiedad de la misma, son responsabilidad única y exclusiva de sus propietarios. Por lo que la Universidad no se hará responsable en caso de pérdida o daño de estos equipos.

Los trabajadores o personas vinculadas a la Universidad, a quienes les sea permitido el retiro de activos físicos de tecnología, deben protegerlos con la mayor diligencia posible ante daño, pérdida y robo.

Uso de los servicios de red informática

Se deben implementar herramientas tecnológicas y controles de seguridad informática para proteger las redes informáticas de accesos no autorizados.

El acceso a la Internet debe ser controlado para evitar que sea utilizado de forma indebida y procurando proteger a los usuarios y los sistemas de amenazas que puedan provenir de las redes públicas.

Los usuarios deben utilizar el acceso a las redes informáticas y el servicio de navegación en la Internet únicamente para realizar las actividades que la Universidad defina, necesarias para el desarrollo de su operación y el cumplimiento de su misión, visión y principios. Los usuarios deben asumir la responsabilidad de toda actividad que realicen haciendo uso de las redes informáticas y el servicio a navegación en la Internet.

Únicamente el personal autorizado del Proceso de Gestión Informática cuenta con autorización para ejecutar herramientas de monitore, escucha o diagnóstico de redes y tráfico. Cualquier otra persona debe abstenerse de utilizar herramientas, soluciones o software de este tipo. El uso no autorizado de dichas herramientas y cualquier tipo de intento que se realice para burlar los controles de seguridad implementados en las redes informáticas es considerado un incidente de seguridad de la información y, como tal, está sujeto a medidas y consecuencias disciplinarias.

Está prohibido conectar módems o cualquier dispositivo móvil (en modo Access Point) para acceder a Internet, dentro de la red de la Universidad Libre.

Cuando lo considere necesario, un delegado del proceso de Gestión Informática podrá monitorear la infraestructura tecnológica (Software y Hardware) de la Universidad, a fin de preservar la seguridad informática de la Universidad.

Correo electrónico

La Universidad Libre puede asignar a los empleados, estudiantes, docentes, egresados, colaboradores, procesos y servicios, cuentas de correo electrónico institucional en el dominio @unilibre.edu.co, y deben ser utilizadas únicamente como herramienta de comunicación y para el desarrollo de las actividades definidas por la Universidad Libre.

Las cuentas de correo electrónico institucional son de uso personal e intransferible y, por ende, los usuarios a quienes estas fueron asignadas, son completamente responsables de todas las actividades realizadas con estas.

Los usuarios deben abstenerse de utilizar la cuenta de correo electrónico asignada para transmitir o almacenar información personal, datos personales, difundir información de forma masiva, envío o reenvío de cadenas, esquemas piramidales, terrorismo, pornografía, programas ilegales, proselitismo político, religioso, racial, amenazas, estafas, malware, o cualquier actividad ilegal o que vaya en contra de los principios de la Universidad.

El envío masivo de mensajes de correo electrónico debe realizarse únicamente para el desarrollo de las actividades o funciones definidas por la Universidad, y a través de las cuentas y herramientas autorizadas para tal fin.

Los usuarios de las cuentas de correo electrónico deben ser precavidos al abrir mensajes no esperados, de origen desconocido o sospechoso, y también al inspeccionar o abrir su contenido, enlaces o archivos adjuntos, debido que pueden poner en riesgo la seguridad de los sistemas, redes informáticas y la información de la Universidad.

Toda la información contenida en los buzones de correo institucionales es propiedad de la Universidad por lo tanto puede ser inspeccionada en cualquier momento por solicitud de los organismos de control interno o por requerimientos judiciales sin previo consentimiento del usuario de la cuenta de correo.

6.7.3.6 Política de respaldo de información

- Se deben obtener copias de respaldo de la información en formato digital, y de los componentes esenciales de los activos informáticos como software, configuraciones y parámetros, para que puedan ser restaurados o recreados en caso de no encontrarse disponibles por fallas o daños.
- Se deben realizar pruebas regulares de restauración de las copias de respaldo, para verificar que su contenido es válido y que los procedimientos de restauración funcionan correctamente.
- Se deben implementar herramientas tecnológicas para obtener y custodiar de forma segura, preferiblemente automatizada, las copias de respaldo y protegerlas frente a accesos y modificaciones no autorizadas.
- Los tiempos de obtención (frecuencia) y de retención de las copias de respaldo se debe determinar con base en las necesidades, tiempos y puntos objetivo de recuperación definidos por los procesos de la Universidad.
- Se debe generar y mantener un registro que contenga información relacionada con la gestión de las copias de respaldo, como el listado de aquellas que deben generarse, los tiempos de obtención, de retención, fechas de prueba, ubicación, el resultado de las pruebas, y otros datos que se consideren relevantes.
- Cuando se presenten fallas en la obtención o prueba de copias de respaldo, se debe validar lo ocurrido, dar una solución y verificar lo ocurrido.
- La responsabilidad de la obtención de las copias de respaldo de información en los equipos de usuario final son los propietarios o custodios de cada equipo, y son quienes deben garantizar que la información respaldada es suficiente acorde con las necesidades de cada proceso y las directrices definidas por la Universidad en los procedimientos definidos en el SGC.
- La obtención, mantenimiento y eliminación de copias de respaldo de información de los sistemas de información, debe ser solicitada al proceso de Gestión Informática por el propietario de cada uno de estos.

Respaldo de servicios hospedado en Internet o sitios alternos de proveedores:

Colocación:

La responsabilidad de la realización de las copias de respaldo recae en los responsables designados por la Universidad.

Se realizan copias de respaldo de aplicaciones y datos según la evaluación de las necesidades asociadas a cada uno de los servicios.

Alojamiento Web:

Cuando se contrate o configure un servicio en la modalidad de hosting, a través del contrato.

El proveedor debe garantizar la realización de copias de respaldo periódicas a los datos, las aplicaciones y demás información según las necesidades de cada servicio.

Las copias de respaldo realizadas son entregadas de forma periódica al líder técnico de la aplicación, ya sea en medios magnéticos o mediante el acceso a un repositorio.

Si las copias de respaldo se entregan en medios magnéticos, estos se revisan y se envían debidamente etiquetados con el proveedor del servicio de custodia que tiene contratado la Universidad.

El proveedor garantiza contractualmente la confidencialidad de la información que se encuentre alojada en sus equipos, teniendo en cuenta los lineamientos definidos en el contrato vigente.

Se tiene en cuenta las tablas de retención de información para las copias de respaldo de acuerdo a lo definido en la Universidad.

Al finalizar el contrato, el proveedor debe entregar copia de toda la información de la Universidad en un formato estándar y legible.

Nube (IaaS, PaaS, SaaS):

Cuando se contrate o configure un servicio con información en la nube (Cloud) bajo cualquiera de las modalidades de Infraestructura como servicio, Plataforma como servicio o Servicio como servicio, a través del contrato el proveedor debe garantizar la realización de copias de respaldo periódicas a los datos acordados según la evaluación de necesidades (información en archivos o estructurada, aplicaciones, sistemas operativos o cualquier otro tipo de información aplicable).

Las copias de respaldo realizadas son entregadas de forma periódica al líder técnico de la aplicación, ya sea en medios magnéticos o mediante acceso a un repositorio.

Las copias de respaldo se entregan en medios magnéticos, estos se envían debidamente etiquetados con el proveedor del servicio de custodia que tiene contratado la Universidad.

El proveedor garantiza contractualmente la confidencialidad de la información que se encuentre alojada en sus equipos, teniendo en cuenta los lineamientos definidos en el contrato de transmisión de datos vigente.

Se tiene en cuenta las tablas de retención de información para las copias de respaldo de acuerdo a lo definido en la Universidad.

Al finalizar el contrato, el proveedor debe entregar copia de toda la información de la Universidad en un formato estándar y legible.

6.7.3.7 Política de gestión de incidentes de seguridad de la información

La Universidad Libre con el fin de asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, define las siguientes directrices:

- Se deben implementar herramientas tecnológicas y mecanismos para recibir reportes y detectar eventos que puedan afectar la seguridad de la información y de los activos de información de la Universidad.
- Se debe definir e implementar un procedimiento para gestionar los eventos que puedan afectar la seguridad de la información y de los activos informáticos de la Universidad.
- Todas las personas vinculadas a la Universidad deben reportar a la mayor brevedad y diligencia posible al proceso de Gestión Informática cualquier situación o evento que pueda afectar la seguridad de la información o de los activos informáticos, o que constituya un incumplimiento a las políticas definidas en la Universidad, o los controles de seguridad implementados.
- Se debe contar con registros (logs) en los activos informáticos de la Universidad, que permita identificar el responsable, el momento y la forma en la cual se materializó un incidente de seguridad de la información, y que sirva como evidencia de lo ocurrido. Estos registros deben ser protegidos contra alteraciones o accesos no autorizados, y custodiados por el proceso de Gestión Informática por el período que considere prudente.
- Se debe definir un procedimiento de gestión de incidentes de seguridad de la información que integre las buenas prácticas y necesidades de la Universidad, mediante el cual se prevenga la materialización de eventos que puedan afectar la seguridad de la información y de los activos informáticos, y se definan actividades para minimizar el impacto que estos pueden generar.
- Los eventos e incidentes de seguridad de la información deben ser gestionados acorde con lo definido en el procedimiento de gestión de incidentes de seguridad de la información.
- Se debe llevar un registro de todos los incidentes de seguridad de la información ocurridos en la Universidad Libre con sus respectivas soluciones de tal forma, que permitan reducir el tiempo de respuesta en caso de ocurrencia de nuevos incidentes.

6.7.3.8 Política de eliminación y destrucción segura de información

Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe garantizarse la eliminación de toda información residente en los equipos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando tecnologías para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.

6.7.3.9 Política de seguridad informática y ciberseguridad

Seguridad de los activos informáticos

- Se deben implementar unidades de potencia sin interrupción (UPS) que garanticen la provisión de energía a los activos informáticos durante fallas en el suministro principal, acorde con las necesidades de los equipos.
- Las conexiones cableadas de red deben estar claramente etiquetadas para identificar fácilmente los elementos conectados, evitar desconexiones erróneas y facilitar la atención de actividades de soporte y mantenimiento.

- La asignación de espacio, ubicación, movimiento y demás requerimientos físicos para los recursos informáticos de los Centros de cómputo deben ser autorizados por la Jefatura de Informática de cada seccional, acogiéndose a los procedimientos de administración y operación de los Centros de cómputo.
- Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno (por ejemplo, incendio, inundación, humedad).
- Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
- El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.
- Se deben ejecutar de forma oportuna y diligente actividades de mantenimiento sobre los equipos y componentes de tecnología para asegurar su disponibilidad e integridad continuas.
- Deben existir planos que describan las conexiones del cableado (voz y eléctricos).

Gestión de cambios

La Universidad Libre es consciente de que cualquier cambio realizado sobre las aplicaciones, los sistemas de información o la infraestructura tecnológica puede generar riesgos para la seguridad de la información. Por esta razón, define los siguientes controles para su adecuada gestión, define los siguientes controles:

- Todo cambio a un componente de la plataforma tecnológica relacionado con: modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, debe realizarse de tal forma que no disminuya los niveles de seguridad de la información existentes en la Universidad Libre.
- La Universidad Libre debe asegurar que los cambios efectuados sobre la plataforma tecnológica, considerando tanto el software operativo como los sistemas de información, son adecuadamente controlados y debidamente autorizados por las áreas.
- Cualquier tipo de cambio debe quedar formalmente documentado desde su solicitud hasta su implantación.
- Los propietarios de la información o los activos de información deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus activos de información, acorde con los procedimientos internos definidos en el SGC.
- Los propietarios o solicitantes del cambio son los responsables de efectuar las pruebas suficientes de funcionalidad y operación, documentarlas y aprobar formalmente los cambios solicitados.
- Cualquier tipo de cambio sobre las plataformas e infraestructura tecnológica de la Universidad Libre debe cumplir con lo estipulado en el procedimiento de Gestión de Cambios de la Universidad Libre.
- A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos de cómputo como computadores, monitores, los otros elementos deben conectarse a la red no regulada. Esta labor debe ser revisada periódicamente.

- Deben existir planos que describan las conexiones del cableado (voz y eléctricos) custodiados por la custodiados por el Coordinador asignado de la Subdirección Administrativa y de datos custodiados por el Líder del Centro de Servicios.

Controles relacionados con la plataforma tecnológica

La plataforma tecnológica es el conjunto de software, hardware e infraestructura de comunicaciones y seguridad, que soportan los diferentes servicios y procesamiento de la información dentro y fuera de la Universidad.

Para reducir los riesgos identificados en la plataforma tecnológica, se debe buscar la planeación, implantación, mantenimiento y monitoreo de la misma, incluyendo los siguientes aspectos:

- La definición de perfiles,
- La asignación y establecimiento de controles de acceso,
- La gestión de privilegios,
- La existencia en la red de datos de dispositivos de seguridad como firewall e IDS,
- La habilitación de filtros de acceso y contenido en Internet y en los mensajes de correo,
- La segmentación de las redes de datos,
- La Universidad Libre debe mantener las redes de datos segmentadas por dominios, grupos de servicios, usuarios o sistemas de información.
- Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
- Se debe implementar una solución antimalware sobre todos los equipos de cómputo y servidores de la Universidad, para protegerlos frente a infecciones de todo tipo de malware. Esta solución debe tener capacidad de reportar automáticamente a un componente central los registros de eventos de todos los sistemas, actualizar automáticamente los patrones y definiciones más recientes de malware, y efectuar acciones sobre los equipos que se consideren bajo riesgo.
- Se debe implementar un mecanismo mediante el cual se garantice la sincronización de los relojes de los activos informáticos de información, para que los eventos registrados en estos tengan una fecha y hora consistente.
- Se deben desarrollar e implementar en los activos informáticos de información configuraciones base de seguridad, mediante las cuales se restrinja el uso de funcionalidades y servicios del sistema que puedan ser utilizadas para manipular la configuración y vulnerar la seguridad, y se aborden posibles brechas y vulnerabilidades de seguridad.

Controles relacionados con los sistemas de información

Los sistemas de información de la Universidad Libre apoyan el cumplimiento de los objetivos estratégicos, dando soporte a sus diferentes procesos.

Con el fin de mitigar los riesgos identificados en los sistemas de información, se deben considerar y aplicar los aspectos definidos, de conformidad con la metodología de gestión de riesgos establecida en el Manual de Riesgos y en el *Procedimiento de Gestión de Riesgos*, asegurando su alineación con los requisitos de la norma ISO/IEC 27001.

- Los requisitos para la construcción, pruebas y administración de los sistemas de información de acuerdo con los requerimientos de seguridad definidos,
- La separación de ambientes de desarrollo, pruebas y producción,
- La existencia de metodologías y estándares que involucren seguridad en el desarrollo e implantación del software,
- La documentación de los desarrollos,
- El control sobre las versiones,
- El soporte sobre los sistemas de información y el control de los cambios realizados, la existencia de repositorios de software,
- La existencia de un programa de entrenamiento basado en las tecnologías de desarrollo utilizadas.

Seguridad del correo electrónico

Se deben bloquear o inactivar las cuentas de correo electrónico de remitentes internos o externos que generen mensajes inapropiados o que vayan en contravía de lo definido en la Política de uso adecuado de recursos, y notificar a las instancias correspondientes para que sean aplicadas las medidas disciplinarias a que haya lugar.

Seguridad para servicios y recursos en la nube

El proceso de Gestión Informática debe considerar los siguientes aspectos cuando se evalúe la implementación, modificación o suspensión de recursos y servicios en la nube digital, con el objetivo de proteger la información de la Universidad:

- Solicitar al proveedor de servicios en nube el listado de los sitios geográficos y países en los cuales están ubicados sus trabajadores, recursos físicos (como servidores, medios de almacenamiento, de procesamiento, centros de datos, redes, componentes tecnológicos, entre otros), y procurar que no se encuentren dentro de los países sancionados en la lista **OFAC.**
    - Podrá ser necesario restringir conexiones a recursos y servicios ubicados en la nube, originadas desde países sancionados en la lista OFAC.
- Los servicios en la nube deben contar con controles de acceso que cumplan con los requerimientos indicados en la Política de control de acceso. En caso de encontrarse una limitación técnica, que evite la aplicación de dichos controles de acceso, se deben implementar controles complementarios para que únicamente tengan acceso a los datos e información en la nube los usuarios autorizados.
- En caso de ser configurados componentes de tecnología en la nube como bases de datos, servidores, conectores de comunicaciones, estos deben estar aislados y protegidos de acuerdo con las mejores prácticas de arquitectura de seguridad en cada caso, generando barreras de protección entre las capas de acceso a

los datos y la información. Por ejemplo, asegurando los componentes de infraestructura, plataformas, software, bases de datos, aplicaciones, servicios, comunicaciones y conexiones.

- Previo a la contratación de servicios en nube, se debe confirmar que el contrato con el proveedor incluya lo siguiente:
    - Que la información contenida y procesada en los servicios y componentes tecnológicos en la nube, es propiedad exclusiva de la Universidad.
    - El proveedor no cuenta con autorización para interpretar la información de la Universidad contenida y procesada en los servicios y componentes tecnológicos en la nube, y realiza de forma periódica auditoría sobre los controles y registros de acceso para verificar su correcto funcionamiento.
    - Una vez finalizado el contrato con el proveedor de servicios en la nube, y dada instrucción de la Universidad, el proveedor se encontrará en la obligación de eliminar con mecanismos seguros la información contenida en los componentes tecnológicos de la nube.
    - El proveedor debe reportar a la mayor diligencia posible los eventos e incidentes de seguridad de la información y ciberseguridad que tienen o pueden tener un impacto sobre los servicios, componentes, datos e información involucrados en el contrato con la Universidad.
- Los componentes y servicios de tecnologías de información alojados en la nube deben estar contemplados dentro de los escenarios de respuesta y recuperación.
- La información contenida y procesada en los componentes en la nube, debe ser descargable para que, en caso de verse terminado el contrato con el proveedor de servicios de nube, esta pueda ser cargada en infraestructura local, o en componentes de otro proveedor de servicios en la nube.
- Prevenir infecciones con software malicioso en los activos informáticos en la nube, por medio de la implementación de soluciones automatizadas y especializadas como herramientas antimalware.
- Definir e implementar mecanismos para detectar eventos sobre los componentes alojados en la nube, que puedan generar impacto en la seguridad de la información y la ciberseguridad, tales como ataque de fuerza bruta, denegación de servicio, phishing e infecciones con malware.
- Se debe procurar que los datos alojados en los servicios en la nube cuenten con cifrado, para evitar el acceso no autorizado a los datos.
- Los activos informáticos en la nube deben ser incluidos en los programas de mantenimiento, actualización, revisión e inspección que se encuentren definidos.
- Los activos informáticos en la nube deben estar contemplados dentro de lo establecido en la Política de gestión de vulnerabilidades.
- La solución y sus componentes deben tener capacidad de generar y procesar los registros (logs) de eventos, e integrarse con las soluciones de monitoreo de la Universidad.

Redes inalámbricas:

- Cada una de las redes inalámbricas que operen en las sedes de la Universidad Libre son para servicio de dispositivos móviles de usuarios externos, terceros y de aquellos empleados a quienes se les haya autorizado el uso de dichos dispositivos en la Universidad; este acceso permite el uso de Internet con las restricciones

que establezca la Universidad para el uso adecuado del activo. No se debe permitir conexión a las redes institucionales en las cuales operen los servicios críticos de la Universidad, a usuarios externos y estudiantes.

- La Universidad Libre se reservará el derecho de monitorear y revisar el cumplimiento de la política para dispositivos móviles conectados a las redes inalámbricas de la misma, cuando lo estime conveniente.

6.7.3.10 Política de seguridad en el desarrollo de software

- Se deben definir e implementar directrices y controles para garantizar la seguridad de la información en todo el ciclo de vida del software, sea desarrollado al interior de la Universidad o para esta por terceros contratados.
- Se deben definir e implementar requerimientos de seguridad mínimos que debe cumplir el software desarrollado al interior de la Universidad y por terceros contratados.
- Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
- El ambiente de prueba debe simular el ambiente de producción. Sin embargo, los datos de prueba utilizados, a pesar de corresponder a una estructura similar a la de producción, deben utilizarse traslapados, para garantizar la seguridad y protección de los datos sensibles.
- Se debe establecer, documentar y mantener principios para la construcción de sistemas seguros y aplicarlos a cualquier actividad de implementación de sistemas de información.
- Se deben incluir las opciones de autenticación de acuerdo con los requerimientos de seguridad de la información, esto incluye diferentes factores de autenticación, adicionales al de usuario y contraseña, como son: tokens de seguridad, controles biométricos y contraseñas de un solo uso enviadas al dispositivo móvil.
- Se deben gestionar las vulnerabilidades técnicas de seguridad del software adquirido o implementado, acorde con lo descrito por los proveedores de tecnología y las agencias especializadas (CVE, OWASP) o detectados por cualquier usuario y proponer las medidas de mitigación al riesgo definido y documentarlo.
- Toda migración de datos entre ambientes de desarrollo, pruebas y producción o entre sistemas de información debe ser aprobada por los propietarios de los activos de información.
- Cuando las migraciones de datos son realizadas por un tercero, éste debe adjuntar el plan de migración completamente documentado, donde se incluya la metodología a utilizar y los planes de contingencia en caso de falla. De igual forma, se deben documentar los inconvenientes y resultados de cada migración.
- Los desarrollos deben garantizar la creación de la funcionalidad que permita configurar el cierre de las sesiones por desuso o tiempo de conexión de acuerdo los requerimientos de seguridad de la información.

6.7.3.11 Política sobre el uso de controles criptográficos

Se deben implementar controles y definir responsables del cifrado de la información con el fin de asegurar la confidencialidad, integridad, autenticidad y no repudio de la información de la Universidad. Todas las partes descritas en el alcance deben cumplir las siguientes directrices:

- Identificarse el nivel de protección necesario, teniendo en cuenta el tipo, la fortaleza y la calidad del algoritmo de cifrado requerido.

- El uso de controles criptográficos únicamente es válido cuando sea el resultado de un análisis de riesgos y su implementación sea autorizada por el propietario de la información correspondiente.
- Se debe hacer uso de técnicas de cifrado autorizadas para proteger la confidencialidad e integridad de la información clasificada como confidencial y datos personales sensibles.
- La Universidad Libre tendrá en cuenta la reglamentación y restricciones nacionales que puedan resultar aplicables al uso de técnicas criptográficas.
- Para realizar la distribución de la contraseña de cifrado de un archivo, esta debe hacerse a través de un medio diferente al del envío de este.
- La Universidad Libre permitirá únicamente aquellos algoritmos autorizados, teniendo en cuenta la información de los grupos de interés, con el fin de descartar algoritmos de cifradas débiles. Se debe considerar el uso de técnicas de cifrado simétricas, asimétricas y protocolos SSL/TLS actualizados en su última versión.

6.7.3.12 Política de seguridad para dispositivos móviles

- Se deben implementar controles que propendan por la Seguridad de la Información asociada a los dispositivos móviles que sean propiedad de la Universidad o aquellos dispositivos de uso personal de los empleados y/o terceros que sean puestos a disposición de la misma y tengan la autorización respectiva para hacerlo. Por lo que se debe dar cumplimiento a los siguientes lineamientos:
- Son catalogados como dispositivos móviles: Los computadores portátiles, Smartphone, dispositivos de almacenamiento externo y tabletas, utilizados por los empleados de la Universidad Libre para gestionar información.
- Los líderes de los procesos deben autorizar el uso de dispositivos móviles y definir los activos tipo información que podrán ser gestionados en los mismos; esta autorización se podrá realizar a través de correo electrónico. Previa instalación o configuración de los controles de seguridad de la información acorde con las políticas y procedimientos de la Universidad.
- En caso de requerirse el uso de dispositivos móviles de propiedad privada o personal, se debe documentar cláusulas contractuales para evitar disputas acerca de derechos de propiedad intelectual de la información o contenidos desarrollados en estos equipos; el acceso al equipo para verificar la seguridad de la máquina y el acceso durante una auditoría.
- El usuario del dispositivo móvil debe aceptar la instalación de los controles de seguridad y estos no podrán ser modificados mientras se gestionen activos de información de la Universidad Libre.
- La instalación de software en dispositivos móviles de propiedad de la Universidad y privados debe cumplir con las políticas y los procedimientos de Seguridad de la Información de Institución.
- La conexión remota empleada para el uso de dispositivos móviles, en los sistemas de información de la Universidad Libre debe realizarse a través de una conexión VPN (Red Privada Virtual) suministrada por la institución.
- Todos los dispositivos móviles propiedad de la institución deben estar registrados y clasificados en el inventario de activos de información de la Universidad Libre, de acuerdo a los procedimientos establecidos para tal fin.

- Los dispositivos móviles propiedad de la Universidad Libre, asignados a los empleados, son personales e intransferibles, y deben contar con una contraseña o clave (password) que impida el acceso directo a la información que este contiene o el acceso de personal diferente a que se asignó como custodio del activo.
- Aceptar y permitir que la información de la Universidad Libre que se encuentre almacenada en el dispositivo móvil puede borrarse de forma remota si el dispositivo es afectado por un incidente de seguridad de la información o si el responsable del dispositivo termina su relación contractual con la empresa.
- Para los dispositivos que son propiedad de la Universidad está prohibido ejecutar volcado de pila o reinstalación del sistema operativo por parte del empleado a quien fue asignado el dispositivo.
- Está prohibido almacenar datos personales sensibles e información confidencial en los dispositivos móviles propiedad de la organización, sin los respectivos controles de seguridad y criptografía.

6.7.3.13 Política de seguridad en las conexiones remotas

- Se deben implementar controles que permitan asegurar los activos de información, a los que se tiene acceso mientras se realice la ejecución de actividades bajo la modalidad de trabajo en casa, teniendo en cuenta la Ley 2088 de 2021, *"por la cual se regula el Trabajo en Casa en Colombia*".
- Los empleados o contratistas autorizados para ejercer su trabajo por fuera de las instalaciones de la Universidad deben hacerlo manteniendo los controles de seguridad de la información, establecidos en la institución.
- Cualquier empleado o contratista autorizado y que requiera tener acceso a la información de la Universidad Libre desde redes externas de manera temporal, podrá acceder remotamente mediante un proceso de autenticación, a través del uso de conexiones seguras y cumplimiento los requisitos de seguridad de los equipos desde los que se accede, acorde con las condiciones dadas por el proceso de Gestión Informática.
- Reportar cualquier evento anormal de acuerdo al Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- Se debe verificar la seguridad física existente en el sitio propuesto, teniendo en cuenta la seguridad de la edificación y del entorno local.
- Se debe documentar cláusulas contractuales para evitar disputas acerca de derechos de propiedad intelectual de la información o el procesamiento de la misma, que se haya desarrollado en equipos de propiedad privada; de igual forma que permitan el acceso al equipo para verificar la seguridad de la máquina y durante una auditoría.
- Se deben definir los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas de información de la empresa y la confidencialidad de la información a la que se tendrá acceso.
- La conexión remota empleada para realizar activades laborales externas de acceso a recursos tecnológicos locales debe realizarse a través de una conexión VPN (Red Privada Virtual) suministrada por la Universidad.

6.7.3.14 Política de seguridad en la transferencia e intercambio de información

Se deben definir formalmente e implementar mecanismos o protocolos para transferir o intercambiar información sensible de la Universidad o bajo su custodia, sea con un ente interno o externo de la organización.

Se deben implementar herramientas o soluciones de tecnología con controles de seguridad que:

- Permitan transferir e intercambiar información sensible de forma segura cuando esto sea necesario.
- Permitan garantizar la integridad de la información.
- Permita realizar análisis antimalware de los paquetes de datos.

La transferencia e intercambio de información sensible de la Universidad o bajo su custodia debe:

- Realizarse únicamente cuando esté justificado por una necesidad de la operación de la Universidad o las actividades que ha definido en sus objetivos, y cuando se cuente con autorización del propietario de la información a ser transferida o intercambiada.
- Realizarse siguiendo el procedimiento definido para tal fin.
- Realizarse utilizando únicamente las herramientas y soluciones dispuestas y autorizadas por el proceso de Gestión Informática, por ejemplo, el correo electrónico institucional.
- Siempre contar con análisis antimalware.

6.7.3.15 Política de gestión de vulnerabilidades

La Universidad Libre conocedora de la importancia de la gestión de vulnerabilidades sobre sus sistemas de información, y con el fin de evaluar la exposición de éstos a las amenazas y tomar las medidas apropiadas para minimizar los riesgos de Seguridad de la Información, establece los siguientes controles:

- El proceso de Gestión Informática de la Universidad Libre deben revisar de manera periódica la aparición de vulnerabilidades técnicas, la información publicada por parte de los fabricantes, proveedores y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar la infraestructura y plataformas tecnológicas de la institución, y reportarlo tanto a los administradores de los recursos informáticos como incluirlo como requerimiento para los nuevos desarrollos internos y externos de software.
- Se deben ejecutar por lo menos una vez al año un plan de análisis de vulnerabilidades y/o hacking ético para las plataformas críticas de la Universidad Libre y se deben aplicar los correctivos necesarios de acuerdo con los resultados arrojados por las pruebas.
- Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad del Líder del proceso de Gestión Informática, y se deben seguir los lineamientos del Procedimiento de Gestión de Cambios, para proceder a su implementación.
- Los servidores, dispositivos de comunicación y seguridad, las estaciones de trabajo, equipos portátiles y las bases de datos de la Universidad Libre deben ser configurados de manera segura, utilizando controles de seguridad robustos y software licenciado; en especial aquellos que almacenan y procesan información crítica o sensible para la institución.
- Se deben implementar las reglas para la instalación de software por parte de los usuarios finales, en cumplimiento del Procedimiento de Instalación de Software en Sistemas Operativos.

- Se deben implementar herramientas que ayuden a correlacionar e identificar posibles amenazas utilizando los diferentes eventos y logs que se almacenen en las soluciones tecnológicas de la Universidad.

6.7.3.16 Política de seguridad de la información en la continuidad del negocio.

Esta política define las directrices de seguridad de la información que deben ser implementadas sobre los escenarios de continuidad del negocio.

- Se deben definir e implementar en el proceso de Gestión Informática estrategias y soluciones para darle continuidad a los servicios de tecnologías de información y un plan de recuperación ante desastres (DRP) de tecnologías de información, alineados con los tiempos y puntos objetivo de recuperación y las necesidades definidas por los procesos de la Universidad (RTOs y RPOs).
- Los activos informáticos destinados a darle continuidad a la operación de la Universidad deben contar con controles que permitan conservar la seguridad de la información.
- Se deben realizar pruebas periódicas del plan de recuperación ante desastres y documentar los resultados de dichas pruebas.
- Se debe capacitar al personal a cargo de la definición e implementación de las estrategias de continuidad y recuperación de los servicios de tecnologías de información, para que estas tengan integradas las buenas prácticas en gestión tecnológica y en seguridad de la información.
- Se deben realizar pruebas periódicas de las estrategias de continuidad y recuperación definidas e implementadas en tecnologías de información de la Universidad.
- Los Centros de Cómputo deben contar con un plan de recuperación ante desastres y un conjunto de procedimientos de contingencia para los servicios y activos informáticos.
- Las estrategias y planes de continuidad y recuperación de los servicios y activos informáticos deben ser actualizados para que se encuentren alineados con las necesidades definidas por los procesos de la Universidad.

6.7.3.17 Política de seguridad para la educación virtual

En esta política se describen las directrices de seguridad de la información que la Universidad establece para el entorno de educación virtual.

- El acceso a las plataformas de educación virtual debe tener implementado un mecanismo de múltiple factor de autenticación.
- Los contenidos educativos, registros asociados con los cursos y el proceso de aprendizaje como trabajos, evaluaciones y desempeño del personal vinculado con el proceso de educación virtual, debe ser respaldada y protegida frente al acceso y modificación no autorizados.
- Se debe realizar una gestión de capacidad rigurosa sobre los servicios y sistemas que soportan el proceso de educación virtual, que garantice el nivel de disponibilidad requerido.
- Se deben implementar mecanismos o herramientas en el sistema de educación virtual, que permitan realizar un análisis anti-malware de los archivos y datos que la comunidad educativa carga en este, y que evite la infección de los activos informáticos o la vulneración de los controles de seguridad.

- Los sistemas que soportan el proceso de educación virtual deben protegerse ante ataques de denegación directos y distribuídos (DoS y DDoS).
- De ser viable, se deben ejecutar pruebas de hacking ético con usuario sobre las aplicaciones de educación virtual, mediante las cuales se permita confirmar que los usuarios no puedan acceder a información o privilegios sin autorización, ni realizar modificación no autorizada de los datos.
- Las clases virtuales y sesiones relacionadas con el proceso de educación virtual deben realizarse utilizando únicamente las soluciones de tecnología que provee la Universidad y aquellas que esta autoriza, utilizando de forma adecuada los recursos y controles implementados.

6.7.3.18 Política de derechos de propiedad intelectual

Para apoyar el cumplimiento de la ley de protección de los derechos de propiedad intelectual aplicable, y a las obligaciones relacionadas con estos, la Universidad Libre define esta política.

El software instalado en los activos informáticos de la Universidad debe ser licenciado acorde con la actividad y operación de esta.

Los usuarios de activos informáticos de la Universidad deben evitar a la mayor diligencia posible almacenar, transferir, ejecutar, descargar o instalar medios digitales, contenido, software, programas, o cualquier tipo de objeto digital, que infrinjan la ley de protección de derechos de propiedad intelectual aplicable y vigente.

La Jefatura de Sistemas de cada seccional debe velar porque en los equipos y sistemas de la Universidad únicamente se encuentre instalado software autorizado.

7 Anexos

7.1 Glosario de términos

En esta sección se presentan las definiciones de términos relacionados con la seguridad de la información y la ciberseguridad. Están basadas en las definiciones dadas por las Normas ISO 27000:2018 y 73: 2009.

Activo de información

Información de la organización o bajo su custodia que, por su importancia para los procesos y la operación de La Compañía, es fundamental para alcanzar sus objetivos estratégicos y tácticos, y por ende debe ser protegida.

Alcance del SGSI

Ámbito de la organización que queda sometido al SGSI.

Alta dirección

Persona o grupo de personas que dirige y controla una organización al más alto nivel.

La alta dirección (o alta gerencia) tiene el poder de delegar autoridad y proporcionar recursos dentro de la organización. Si el alcance del sistema de gestión cubre solo una parte de una organización, la alta dirección se refiere a aquellos que dirigen y controlan esa parte de la organización. A la alta dirección a veces se le llama gerencia ejecutiva y puede incluir directores ejecutivos (CEO), directores financieros (CFO), directores de información (CIO) y funciones similares.

Amenaza

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos.

Ataque

Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

Autenticación

Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad

Propiedad de que una entidad es lo que afirma ser.

Competencia

Capacidad de aplicar conocimientos y habilidades para lograr los resultados previstos.

Compromiso de la Dirección

Alineamiento firme de la dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Confidencialidad

Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Continuidad de la seguridad de la información

Procesos y procedimientos para garantizar una operativa continuada de la seguridad de la información.

Consecuencia

Resultado de un evento que afecta los objetivos.

Un evento puede llevar a una serie de consecuencias. Una consecuencia puede ser segura o incierta y, en el contexto de la seguridad de la información, suele ser negativa. Las consecuencias pueden expresarse cualitativa o cuantitativamente. Las consecuencias iniciales pueden incrementarse a través de los efectos secundarios.

Contexto externo

Ambiente externo en el que la organización busca alcanzar sus objetivos.

El contexto externo puede incluir el entorno cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo, ya sea internacional, nacional, regional o local. También factores y tendencias clave que tienen impacto en los objetivos de la organización o relaciones y percepciones y valores de partes interesadas externas.

Contexto interno

Ambiente interno en el que la organización busca alcanzar sus objetivos. El contexto interno puede incluir:

- gobernanza, estructura organizativa, roles y responsabilidades;
- políticas, objetivos y las estrategias que existen para lograrlos;
- las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías);
- sistemas de información, flujos de información y procesos de toma de decisiones (tanto formales como informales);
- relaciones y percepciones y valores de las partes interesadas internas;
- la cultura de la organización;
- normas, directrices y modelos adoptados por la organización;
- forma y alcance de las relaciones contractuales.

Control

Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control.

Control correctivo

Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

Control de acceso

Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.

Control preventivo

Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Declaración de aplicabilidad

Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Directriz

Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad

Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Estimación de riesgos

Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

La estimación de riesgos ayuda en la decisión sobre el tratamiento de riesgos.

Evaluación de riesgos

Proceso global de identificación, análisis y estimación de riesgos.

Evento

Ocurrencia o cambio de un conjunto particular de circunstancias.

Un evento puede ser una o más ocurrencias y puede tener varias causas. Un evento puede consistir en que algo no suceda. Un evento a veces puede ser referido como un "incidente" o "accidente".

Evento de seguridad de la información

Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

Gestión de incidentes de seguridad de la información

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Gobierno de seguridad de la información

Sistema mediante el cual las actividades de seguridad de la información de una organización se dirigen y controlan.

Identificación de riesgos

Proceso de encontrar, reconocer y describir riesgos. La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas.

Impacto

El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.

Incidente de seguridad de la información

Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Indicador

Medida que proporciona una estimación o evaluación.

Indicador de Compromiso

Es un conjunto de datos sobre un objeto o una actividad que indica acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso.

Información documentada

Información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida. La información documentada puede estar en cualquier formato y medio y desde cualquier fuente y puede referirse al sistema de gestión (incluidos los procesos relacionados), información creada para que la organización funcione (documentación) y/o evidencias de resultados alcanzados (registros).

Integridad

Propiedad de la información relativa a su exactitud y completitud.

ISO/IEC 27001

Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ISO/IEC 27002

Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

ISO 9001

Norma que establece los requisitos para un sistema de gestión de la calidad.

Mejora continua

Actividad recurrente para aumentar el rendimiento.

Monitoreo

Determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente.

Nivel de riesgo

Magnitud de un riesgo expresado en relación a la combinación de consecuencias y su probabilidad.

No repudio

Capacidad de probar la ocurrencia de un evento o acción reclamada y sus entidades de origen.

Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Objetivo

Resultado a alcanzar. Un objetivo puede ser estratégico, táctico u operativo. Los objetivos pueden relacionarse con diferentes disciplinas (como las metas financieras, de salud y seguridad y ambientales) y pueden aplicarse a diferentes niveles (como estratégico, de toda la organización, proyecto, producto y proceso). Un objetivo puede expresarse de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, como un objetivo de seguridad de la información o mediante el uso de otras palabras con un significado similar (por ejemplo, propósito, meta o hito).

En el contexto de los sistemas de gestión de seguridad de la información, la organización establece los objetivos de seguridad de la información, de acuerdo con la política de seguridad de la información, para lograr resultados específicos.

Organización

Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos. El concepto de organización incluye, pero no se limita a un comerciante individual, compañía, corporación, agencia, empresa, autoridad, sociedad, organización benéfica o institución, o parte o combinación de las anteriores, ya sea sociedad anónima o no, pública o privada.

Parte interesada

Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

PHVA

Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

Plan de continuidad del negocio

Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política

Intenciones y dirección de una organización, expresada formalmente por su alta dirección.

Probabilidad

Posibilidad de que ocurra algo.

Proceso

Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Proceso de gestión del riesgo

Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicación, consultoría, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos.

Profesional del Sistema de Gestión de Seguridad de la Información (SGSI)

Persona que establece, implementa, mantiene y mejora continuamente uno o más procesos del Sistema de Gestión de Seguridad de la Información.

Propietario del riesgo

Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Requisito

Necesidad o expectativa que es establecida, generalmente de forma implícita u obligatoria. “Generalmente implícita” significa que es costumbre o práctica común para la organización y las partes interesadas donde la necesidad o expectativa bajo consideración está implícita. Un requisito especificado es uno que se establece, por ejemplo, en información documentada.

Revisión

Actividad realizada para determinar la idoneidad, adecuación y efectividad del objeto de estudio para lograr los objetivos establecidos.

Riesgo

Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad. El riesgo a menudo se caracteriza por la referencia a posibles "eventos" y "consecuencias" o una combinación de estos.

El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la "probabilidad" asociada de ocurrencia.

En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información.

El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

Riesgo residual

El riesgo que permanece tras el tratamiento del riesgo. El riesgo residual puede contener un riesgo no identificado. El riesgo residual también puede denominarse "riesgo retenido".

Segregación de tareas

Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.

Selección de controles

Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI

Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión

Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos.

Un sistema de gestión puede abordar una sola disciplina o varias disciplinas. Los elementos del sistema incluyen la estructura, roles y responsabilidades, planificación y operación de la organización. El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones en un grupo de organizaciones.

Sistema de Gestión de la Seguridad de la Información

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Sistema de Información

Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información.

Tratamiento de riesgos

Proceso para modificar el riesgo. Las acciones de tratamiento del riesgo pueden contemplar:

- evitar el riesgo al decidir no comenzar o continuar con la actividad que da lugar al riesgo;
- asumir o aumentar el riesgo para aprovechar una oportunidad;
- eliminar la fuente de riesgo;
- modificar la probabilidad;
- modificar las consecuencias;
- compartir el riesgo con otra parte o partes (incluidos contratos y financiación del riesgo);
- retener el riesgo mediante una elección informada.

Las acciones de tratamiento del riesgo sobre consecuencias negativas a veces se denominan "mitigación de riesgos", "eliminación de riesgos", "prevención de riesgos" y "reducción de riesgos".

El tratamiento del riesgo puede crear nuevos riesgos o modificar los riesgos existentes.

Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas