SANMARTÍN
Fundación Universitaria

FUNDACIÓN UNIVERSITARIA SAN MARTIN
CONSEJO SUPERIOR

ACUERDO N° 17
07 de octubre de 2025

"Por el cual se aprueba Política General de Seguridad de la Información de la Fundación Universitaria San Martín"

El Consejo Superior de la Fundación Universitaria San Martín en uso de sus facultades legales y estatutarias, en especial las consagradas en los artículos 18 numerales 5 y 7, y 56 de los Estatutos y

CONSIDERANDO

Que la Fundación Universitaria San Martín con domicilio en Bogotá D.C., es una Institución universitaria de carácter privado, con Personería Jurídica reconocida mediante Resolución No. 12387 del 18 de agosto de 1981, expedida por el Ministerio de Educación Nacional.

Que la Constitución Política en el artículo 69, garantiza la autonomía universitaria, y establece que las instituciones de educación superior podrán darse sus directrices y regirse por sus propios estatutos de acuerdo con la ley.

Que la Ley 30 de 1992 desarrolla los alcances de la autonomía universitaria y regula la educación superior en los aspectos generales de los programas académicos; así, en su artículo 29 dispone que en ejercicio de su autonomía, las Instituciones de Educación Superior podrán darse y modificar sus estatutos, designar sus autoridades académicas y administrativas, crear, desarrollar sus programas académicos, lo mismo que expedir los correspondientes títulos, definir y organizar sus labores formativas, académicas, docentes, científicas, culturales y de extensión, y arbitrar y aplicar sus recursos para el cumplimiento de su misión social y de su función institucional.

Que la Fundación Universitaria San Martín está comprometida con la implementación de un Sistema de Gestión de Seguridad de la Información y Ciberseguridad, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información a fin de fortalecer la continuidad de las operaciones de la Fundación, protegiendo adecuadamente los activos de información, reduciendo los riesgos y apoyando la transformación digital.

Que el Plan de Desarrollo Institucional 2022-2026 contempla la línea 5 referida al Desarrollo y Fortalecimiento Financiero y Administrativo Institucional, donde se incorpora el programa de Transformación Digital y el subprograma de Seguridad Informática, que propende porque los servicios tecnológicos y de comunicaciones sean con calidad, confiabilidad, integridad, brindando un nivel de seguridad óptimo y que permita disminuir las amenazas a la seguridad de la información y los datos.

Que en virtud del anterior, se hace necesario contar con una Política General de Seguridad de la Información, aplicable a todos los miembros de la comunidad Sanmartiniana, cuyo objetivo general será proteger la confidencialidad, integridad, disponibilidad y privacidad de los activos de la Fundación Universitaria San Martín, así como, la de sus partes interesadas,

SANMARTÍN
Fundación Universitaria

FUNDACIÓN UNIVERSITARIA SAN MARTIN
CONSEJO SUPERIOR

ACUERDO N° 17
07 de octubre de 2025

"Por el cual se aprueba Política General de Seguridad de la Información de la Fundación Universitaria San Martín"

por medio de la gestión de riesgo de seguridad de la información dentro de todas las etapas contempladas en el sistema general de seguridad.

Que en la sesión del Consejo Superior celebrada el 7 de octubre de 2025, se presentó la propuesta de la Política General de Seguridad de la Información de la Fundación Universitaria San Martín; una vez revisada y encontrándola ajustada, fue aprobada por el Consejo Superior, según consta en Acta No. 13 del 7 de octubre de 2025.

Que en mérito de lo expuesto,

ACUERDA:

ARTÍCULO PRIMERO: Aprobar la Política General de Seguridad de la Información de la Fundación Universitaria San Martín, según documento adjunto que forma parte integral del presente Acuerdo,

ARTÍCULO SEGUNDO: El presente Acuerdo rige a partir de su aprobación.

COMUNÍQUESE Y CÚMPLASE

Dado en la ciudad de Bogotá D.C., a los siete (7) días del mes de octubre del año dos mil veinticinco (2025).

LUIS JAVIER GIRALDO MÚNERA
Presidente Consejo Superior

ALEJANDRO SUAREZ PARADA
Secretario General

POLÍTICA GENERAL Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

SAN MARTÍN
Fundación Universitaria

Bogotá, D.C., septiembre de 2025

DIRECTIVOS
Consejo Superior

Luis Javier Giraldo Múnera – Presidente del Consejo
María Juliana Araujo Oñate – Miembro externo
Oscar Manco López – Miembro externo
Alejandro Olaya Dávila – Miembro externo
Carlos Eugenio Solarte Portilla – Miembro externo
Javier Pérez Montenegro – Decano miembro del Consejo Superior
Yuranis Del Carmen De La Hoz Pantoja– Representante de los profesores
Andrés Felipe Márquez Acosta – Representante de los estudiantes
Hans Diederichs Quirós - Egresado Miembro del Consejo Superior

Rector y Representante Legal
Fernando José Restrepo

Vicerrector Académico
Javier Daza Lesmes

Vicerrectora Financiera y Administrativa
María Fernanda Juliao Ferreira

Vicerrector de Desarrollo Estratégico
Yezid Orlando Pérez Alemán

Secretario General
Alejandro Suárez Parada

Responsable del documento
Dirección de Informática y Tecnología

Soporte técnico
Misael Barragán Sánchez – Director de Informática y Tecnología
Ricardo Andrés Toro Cerón – Líder de Seguridad de la Información.

Contenido

1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Fundación Universitaria San Martín con domicilio principal en la ciudad de Bogotá D.C. como Institución Universitaria de carácter privado, se compromete con la implementación de un Sistema de Gestión de Seguridad de la Información y Ciberseguridad, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información a fin de fortalecer la continuidad de las operaciones de la Fundación, protegiendo adecuadamente los activos de información, reduciendo los riesgos y apoyando la transformación digital.

Esta política aplica a todos los estudiantes, docentes, trabajadores, administrativos y directivos de nivel gerencial, de facultades y sedes; así como, contratistas y proveedores en el ámbito de su relación contractual con la Fundación.

Adicionalmente la alta dirección promueve, gestiona, apoya el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI). Por medio del desarrollo de las siguientes acciones:

- Estableciendo las responsabilidades frente a la seguridad de la información, compartiéndolas y publicándolas a todos los estudiantes, docentes, trabajadores administrativos y directivos.
- Protegiendo la información generada, procesada o resguardada por los procesos de la Fundación, su infraestructura tecnológica y activos, del riesgo que se genera los accesos otorgados a terceros (ejemplo.: proveedores o estudiantes), o como resultado de un servicio interno tercerizado.
- Protegiendo la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta, para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Resguardando su información de las amenazas originadas por parte del personal.
- Protegiendo las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Implementando el control de acceso a la información, sistemas y recursos de red.
- Asegurando la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Garantizando una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información a través de la mejora continua de su modelo de seguridad.
- Estableciendo manuales de uso, mejores prácticas, procedimientos, instructivos y entrenamiento permanente en materia de Seguridad de la información y Ciberseguridad.
- Fortaleciendo la cultura de Seguridad de la información en los trabajadores, en la comunidad universitaria, proveedores y demás terceros relacionados.

1.1. OBJETIVO GENERAL

Proteger la Confidencialidad, Integridad, Disponibilidad y Privacidad de los activos de la Fundación Universitaria San Martín, así como, la de sus partes interesadas, por medio de la gestión de riesgo de seguridad de la información dentro de todas las etapas contempladas en el sistema general de seguridad.

1.1.1 OBJETIVOS ESPECÍFICOS

- Gestionar de forma adecuada y permanente los riesgos de seguridad de la información a los que pueda estar expuesta la Fundación y aquella que pertenezca a sus partes interesadas.
- Reducir la cantidad de incidentes que atenten contra la disponibilidad, confidencialidad e integridad de la información a través del procedimiento de gestión de incidentes de seguridad.
- Fortalecer la cultura con respecto a seguridad de la información a los empleados, proveedores y demás terceros relacionados.
- Generar las herramientas necesarias para el desarrollo, maduración y mejoramiento continuo del sistema de gestión de seguridad de la información.

1.2 MEDICIÓN DEL CUMPLIMIENTO DE OBJETIVOS (Indicadores)

Con el fin de evaluar el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información la Fundación definió los indicadores a través de los cuales hace el seguimiento de la gestión del SGSI y son el insumo para la toma de decisiones que propendan por el mejoramiento continuo de sistema y logro de sus objetivos, para lo cual se establecieron las acciones a realizar, los recursos, el responsable de la medición, la periodicidad de la evaluación y las instancias donde serán revisados los resultados generados por los indicadores, los cuales están descritos en el documento: *objetivos SGSI* Fundación *xls.*

1.3 DEFINICIONES

Acceso: En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas de la Fundación en un momento dado.

Acceso físico: Se refiere al acceso a áreas restringidas dentro de una organización, donde se almacenan datos sensibles o recursos valiosos. Este nivel de acceso requiere múltiples capas de seguridad, como autenticación biométrica, vigilancia constante y autorización de alto nivel, garantizando así que solo el personal autorizado pueda ingresar a estas zonas críticas.

Acceso lógico: En general, el acceso lógico es un acceso electrónico o digital, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas...) que tenga valor para la Fundación.

Activo de Información: Es todo aquello que en la Fundación es considerado importante o de alta validez para el mismo, porque contiene información importante, como son los datos creados o utilizados por procesos de la organización, en medio digital, en papel o en otros medios. Ejemplos: bases de datos con usuarios, contraseñas, números de cuentas, informes etc.

Acuerdos de Niveles de Servicio (ANS - SLA): son parámetros, tiempos y requisitos establecidos para la entrega de productos o servicios de un proceso a los usuarios internos y externos, con los cuales se medirá la oportunidad de este.

Ambiente de Pruebas: es el ambiente en que el usuario ejecuta las pruebas funcionales de la versión liberada a pruebas.

Ambiente de Producción: es el ambiente en el que se mantienen las últimas versiones de los programas objeto que se ejecutan.

Áreas seguras: Sitio donde se maneja información sensible o valiosos equipos informáticos, es decir, refugios con los que alcanzar los objetivos de la FUNDACIÓN.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

Autenticación: Procedimiento informático que permite asegurar que un usuario de un sitio web u otro servicio similar es auténtico o quien dice ser, valida la veracidad.

Trabajadores Autónomos: Son aquellos que utilizan su propio domicilio o un lugar escogido para desarrollar su actividad profesional, puede ser una pequeña oficina, un local comercial, etc. En este tipo se encuentran las personas que trabajan siempre fuera de la organización y sólo acuden a la oficina en algunas ocasiones.

Aviso de Privacidad: Comunicación física, verbal o electrónica generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de los lineamientos de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

Acuerdo de Confidencialidad: Documento donde se plasma el compromiso para mantener la confidencialidad de la información de la Fundación, a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud del desarrollo de las funciones desempeñadas en la Fundación.

Áreas seguras: Son todas aquellas instalaciones como centros de datos (principal y alterno), racks de comunicaciones de los puntos de atención y en cada piso de las sedes; en las que se realiza el procesamiento y envío de información del negocio. De igual forma, se consideran áreas seguras las que manejan información confidencial o privada.

Backup / Copia de Seguridad: es el proceso de resguardar de manera segura los archivos o datos críticos contenidos en un sistema informático, transfiriéndolos desde un medio de almacenamiento de origen (como un disco duro) a un medio de almacenamiento distinto (como otro disco duro o un servidor de copias). Este proceso se realiza con el fin de mantener la integridad y disponibilidad de la información, permitiendo su restauración en caso de pérdida o daño.

Base de Datos: Conjunto organizado de datos personales que corresponde con el objeto de Tratamiento.

Cintas Magnéticas: Dispositivo de almacenamiento masivo de datos.

Cifrado: Es el proceso que se aplica a unos datos para hacerlos incomprensibles. Este proceso o transformación precisa de una clave de cifrado, que es una cadena aleatoria de bits, de una medida determinada (longitud de clave). Sólo aplicando el proceso contrario, denominado descifrado, a los datos cifrados será posible regenerar los datos originales y, por tanto, hacerlas otra vez comprensibles.

Código Malicioso: El software malicioso o Malware es cualquier programa que busca deliberadamente causar un daño y/u obtener acceso no autorizado a los activos de información digital.

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Fundación. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Clave o contraseña: Toda forma de autenticación secreta para controlar el acceso a sistemas de información y/o red de la Fundación.

Confidencialidad: Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.

Copia de seguridad completa (full): Una copia de seguridad que incluye la totalidad de archivos previamente seleccionados de un sistema informático. Es un proceso donde se copian todos los archivos y directorios seleccionados.

Copia de seguridad incremental: Una copia de seguridad que respalda los archivos creados o modificados desde la última copia de seguridad completa. La restauración de los datos debe realizarse con la última copia de seguridad completa y las copias de seguridad incrementales posteriores.

Custodia de Medios: Corresponde al almacenamiento seguro de los medios magnéticos fuera de la Fundación, a cargo de un proveedor externo, solo incluye el almacenamiento.

Consulta: Solicitud del titular del dato o de las personas debidamente autorizadas por éste o por la ley, para conocer la información que reposa sobre él, en las bases de datos de la Institución.

Contratista- Prestación de Servicios (consultor externo/freelance): Es toda persona natural o jurídica, nacional o extranjera, en forma individual o conjunta, que suscribe un contrato. Se establece una vinculación de una persona natural en forma excepcional, para suplir actividades o labores relacionadas con la administración o funcionamiento de la organización, o para desarrollar actividades especializadas que no puede asumir el personal de planta.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato Privado: Aquel que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato Público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato semiprivado: Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector personas o a la sociedad en general, como el dato financiero y crediticio.

Datos Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Dirección IP: Número que identifica, de manera lógica y jerárquica en una red informática a un dispositivo (computadora, tableta, portátil, Smartphone).

Dispositivo móvil: Equipos de procesamiento electrónicos de información que, por su pequeño tamaño, permiten que sean transportados fácilmente y que cuentan con capacidades de procesamiento de datos, conexión a Internet y memoria; entre algunos se encuentran los ordenadores portátiles, teléfonos inteligentes, Tablets, entre otros.

Disponibilidad: Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, fundaciones o procesos autorizados cuando lo requieran.

Dato: Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

Desarrollo de Software: es el ambiente en el cual se hace creación y modificación de programas fuente, así como las pruebas técnicas que se requieren antes de liberar una versión para pruebas de usuario.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta y riesgo del responsable del Tratamiento.

Escritorio Limpio: Hacer referencia a la limpieza y el orden de una estación de trabajo, en donde no se manifiesta sólo en tener los papeles en un cajón, todo en su lugar y nada a la vista, sino en tener un control exhaustivo del uso que damos a nuestro escritorio, no exponiendo la información y los datos críticos a personas que podrían hacer mal uso de ellos.

Firma Electrónica: Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente, este conjunto de datos electrónicos acompañan o están asociados a un documento electrónico y cuyas funciones básicas son (i) identificar a una persona de manera inequívoca, (ii) Asegurar la exclusividad e integridad del documento firmado y (iii) los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede negarse la firma el documento.

Hardware: Activos que representan toda la infraestructura física que permite el procesamiento, transporte y almacenamiento de información. Por ejemplo: Las Estaciones de Trabajo, los equipos de comunicaciones, router, switch, firewall y cualquier otro elemento de una red de computadoras por donde transita la información, los equipos portátiles, los medios de almacenamiento y los servidores.

Información: corresponde a todo dato Institucional (tecnológico administrativo, financiero, entre otros) propio y de terceros, con las cuales se asume un rol como responsable y/o encargado.

Información pública: Es aquella en poder de los sujetos obligados, contenida en documentos, archivos, datos, bases de datos, comunicaciones y todo tipo de registros que documenten el ejercicio de sus facultades o actividades, que consten en cualquier medio, ya sea impreso, óptico o electrónico, independientemente de su fuente, fecha de elaboración, y que no sea confidencial o reservada. Dentro de la información pública se

encuentra un subconjunto de información denominado “información oficiosa”, la cual debe de ser publicada de forma inmediata sin que ninguna persona lo solicite. Esta información puede estar impresa o colgada en los sitios web de las instituciones y deben entregársela en el mismo momento en que lo solicites.

Información reservada: Es la información pública cuyo acceso se restringe de manera expresa, debido a un interés general durante un periodo determinado y por causas justificadas. Por ejemplo, los planes militares secretos, las negociaciones internacionales o cualquier tipo de negociación o discusión que se tenga, mientras no se adopte una decisión definitiva. O toda aquella información que esté relacionada con la investigación o persecución de actos ilícitos o que genere una ventaja indebida en perjuicio de un tercero.

Información confidencial: Es la información privada en poder de los sujetos obligados, cuyo acceso público se prohíbe por mandato constitucional o legal en razón de un interés personal jurídicamente protegido. Es decir, la información referente a la intimidad personal y familiar, al honor y propia imagen, así como archivos médicos cuya divulgación constituye una invasión a la privacidad de la persona. A esta información sólo tendrán acceso las personas que son dueñas de ella. Dentro de la información confidencial están los datos personales la cual es la información privada de una persona, como por ejemplo su nacionalidad, domicilio, patrimonio, dirección electrónica, número de teléfono o cualquier otra parecida. Por su carácter sensible, no puede ser conocida por el público en general, como: planes estratégicos, datos personales, salario de los empleados, información financiera, entre otros.

Incidente de seguridad: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a un Lineamiento de Seguridad de la Información.

Integridad: Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Librería de Cintas: Sistema de Backup robotizado que utiliza como medio de almacenamiento cintas magnéticas. Es el puente de conexión entre la red de datos y las cintas de respaldo.

Lugar seguro: Espacio que permite tener resguardada la información o medios físicos (Cajoneras, archivadores, entre otros).

Malware: Un programa malicioso, también conocido como programa maligno, programa malintencionado o código maligno, es cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Medios de almacenamiento de información: Son dispositivos para grabar o almacenar información (datos). Un dispositivo de almacenamiento puede guardar la información y

procesarla. Dispositivos como los discos duros, CD´s, memorias USB y algunas cintas de copia, son los medios de almacenamiento que generalmente se utilizan para almacenar información.

Medios removibles: Dispositivos tecnológicos de almacenamiento de información diseñados para ser extraídos del computador.

MFA – Autenticador de Factor Múltiple: Es un sistema de seguridad que requiere más de una forma de autenticación para verificación de la legitimidad de una transacción.

Móviles **o trabajadores remotos**: Son aquellos que no tienen un lugar de trabajo establecido y cuyas herramientas primordiales para desarrollar sus actividades profesionales son las Tecnologías de la Información y la comunicación, en dispositivos móviles.

Nuevas Tecnologías: Cualquier medio, plataforma, software, programa, equipo, dispositivo y/o equipo que permita la comunicación, interacción y/o ejecución del contrato de trabajo de manera remota mediante una conexión a internet o a cualquier otra red que permita ejecutar dichas acciones. Lo anterior con base en las disposiciones contempladas en el artículo 6 de la ley 1341 de 2009.

OTP – One Time Password: es un mecanismo de autenticación, el cual consiste en un código temporal que le llega a la persona a través de mensaje de texto SMS o correo electrónico certificado, para que este pueda de manera segura realizar acciones virtuales, en donde se certifica la identidad de la persona, ya sea vía internet o mediante la aplicación para teléfonos móviles (APP).

Pantalla Limpia: Hace referencia a la limpieza y el orden de los archivos presentes en el escritorio de los equipos de cómputo.

Propietario de la Información: Persona o entidad que tiene la autoridad y responsabilidad sobre los datos, incluyendo su uso, acceso y protección. Este rol implica la toma de decisiones sobre cómo se gestionan y resguardan los datos dentro de un Sistema de Gestión de Seguridad de la Información (SGSI).

Proveedor de Bienes y Servicios: Persona natural o jurídica o empresa que suministra bienes y/o presta servicios a la Fundación, para su funcionamiento.

Ransomware: También llamado 'secuestro de datos' en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. La Fundación actúa como responsable del tratamiento de datos personales frente a todos los datos personales sobre los cuales decida directamente, en cumplimiento de las funciones propias reconocidas legalmente.

Recuperación: Hace referencia a las técnicas empleadas para recuperar la información (archivos) a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Seguridad digital: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante, incluye la seguridad de la información (Política, Lineamientos, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).

SGSI: Sistema de Gestión de Seguridad de la Información, es el encargado de asegurar la confidencialidad, integridad y disponibilidad de la información. La seguridad de la Información implica la aplicación y gestión de controles apropiados que involucran la consideración de un amplio rango de amenazas, con el objetivo de asegurar el éxito empresarial sostenido, así como su continuidad, y minimizar las consecuencias de los incidentes de la seguridad de la información.

Sistemas de Información: Un sistema de información es una infraestructura tecnológica que permite a una organización procesar datos y transformarlos en información útil para la gestión y la toma de decisiones. Conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una organización o negocio. Estos elementos pueden incluir hardware, software, datos, procedimientos y personas.

Tareas de respaldo: Programación de las copias de seguridad que incluyen: la fuente, el destino y la periodicidad.

Tecnología de la Información: Se refiere al hardware y software operados por la Fundación o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Compañía, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Titular: Persona natural cuyos datos personales corresponden con el objeto de Tratamiento. Para el caso son los Estudiante, Egresados, Proveedores, Contratistas, así como Empleados y personas que se encuentren en proceso de vinculación contractual de cualquier naturaleza con la Fundación.

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio nacional (de la República de Colombia), cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Usuario: Trabajador que tiene contrato con la Fundación a quien se le asigna un dispositivo para la ejecución de sus labores y hacen uso de los servicios tecnológicos o insumos físicos que proporciona la FUNDACIÓN.

De acuerdo con el artículo 2 de la ley 1221 de 2008, existen 3 modalidades las cuales se clasifican de acuerdo con las tareas a realizar y el perfil del trabajador. Su clasificación se establece de la siguiente manera:

- Tiempo completo: el trabajador no asiste a la organización, pero está en contacto permanente de forma remota por medio de las TIC para realizar sus actividades.
- Tiempo parcial: se aplica la modalidad de teletrabajo por lo menos una vez a la semana.
- Tiempo complementario: asiste a la Fundación entre 2 y 3 días a la semana y el tiempo restante en forma remota. Alternan sus tareas en distintos días de la semana entre la Fundación y un lugar fuera de ella usando las TIC para sus actividades. [1]

Vulnerabilidad: Es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

2. LINEAMIENTO SOBRE DISPOSITIVOS MÓVILES

2.1. INTRODUCCIÓN

El Lineamiento de Uso de Dispositivos Móviles suministrados por la Fundación se adelanta con el fin de dar cumplimiento al tratamiento y protección, preservación y aseguramiento de la integridad, confidencialidad y disponibilidad definidos para los activos de información. Teniendo en cuenta los avances tecnológicos de software y hardware en los dispositivos móviles, se considera directamente proporcional el nivel de riesgo, de adulteración o pérdida que puede llegar a tener la información almacenada en las bases de datos de la institución.

Así mismo, es necesario precisar que si bien los dispositivos móviles, son reconocidos como herramientas útiles en casos de emergencia, también pueden llegar a constituirse en un

[1] Definición de Teletrabajo bajo la ley 1221 de 2008 Congreso de la República, artículo 2.
[2] ley 2121 del 2021. Artículo 4.

distractor que impide el desarrollo normal de las labores cumpliendo estándares de seguridad, eficiencia y calidad. Para el uso de dispositivos móviles como: equipos portátiles, teléfonos celulares, tabletas, entre otros, la Fundación Universitaria San Martín debe implementar controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

2.2. OBJETIVO

Establecer por parte de la Fundación las condiciones para el manejo de los dispositivos móviles, únicamente los pertenecientes al inventario de la Fundación, los lineamientos y medidas de seguridad de la información sobre el uso de dispositivos móviles (portátiles), garantizando las mejores prácticas con el uso adecuado y responsable de servicios eficientes hacia la comunidad académica; velando siempre por el uso responsable de éstos.

2.3. ALCANCE

El Lineamiento sobre dispositivos móviles, es aplicable a todo el personal que tengan asignado un dispositivo móvil (equipo computador portátil), que haya sido proporcionado por la Fundación para el desarrollo de las actividades propias de sus funciones; y para el personal encargado (los trabajadores de la Mesa de Soporte) de configurar de manera segura los dispositivos móviles al servicio de la Fundación.

2.4. RESPONSABLES

- Dirección de Informática y Tecnología
- Personal de la Mesa de Soporte
- Trabajadores de la Fundación

2.5. LINEAMIENTO DE USO DE DISPOSITIVOS MÓVILES

La Fundación proporciona las condiciones a sus trabajadores para el manejo de los dispositivos móviles (computadores portátiles) a nivel corporativo de tal manera que les permita desarrollar las funciones para el cargo al cual le fue asignado el activo. Así como, el cuidado y uso responsable por parte del dueño de dicho activo. La asignación de cualquier dispositivo móvil a un trabajador de la Fundación se realizará con evidencia, mediante acta de entrega y el registro del control de inventario asociado a los activos de información.

Los usuarios que hagan uso de dispositivos móviles para almacenar o acceder a la información de la Fundación a través de estos dispositivos como teléfonos inteligentes (Smartphones), Tabletas (tablets) u otros dispositivos corporativos electrónicos, deberá:

- Aceptar las configuraciones de seguridad, en caso de que estas se requieran, que se aplicarán en el dispositivo móvil, las mismas no podrán modificarse mientras se acceda o almacene información de la Fundación.

- Se prohíbe compartir la configuración y/o contraseñas de dispositivos móviles para acceder a las redes institucionales de la Fundación, con los demás usuarios, trabajadores y/o terceros. Únicamente el personal autorizado de Soporte Fundación está autorizado a instalar las configuraciones necesarias en cada dispositivo móvil.
- En caso de pérdida o hurto del dispositivo móvil, el usuario deberá reportar la novedad ante el jefe inmediato y reportar a la mesa de soporte en el correo soporte.fusm@sanmartin.edu.co , considerando que cada usuario será responsable de las actividades realizadas a través del dispositivo.
- Cada equipo cuenta con un software de antivirus que no debe alterarse y se actualiza cada vez que el usuario apaga el equipo. A su vez cada dispositivo cuenta con mecanismos de control de acceso, bloqueo de pantalla por inactividad de máximo dos minutos. La información del equipo es manejada como contenido cifrado.
- Los dispositivos móviles corporativos no se deben conectar a computadores públicos o a redes Wifi-públicas. (por ejemplo, aquellas que se pueden encontrar en hoteles, cafés internet, entre otros).
- Está prohibido almacenar vídeos, fotografías o información personal en los dispositivos asignados, dichos dispositivos son para uso exclusivo de actividades laborales.
- Cuando se trate de dispositivos móviles personales, el soporte técnico únicamente cumplirá con la función de brindar la conectividad de red a estos dispositivos, más no estarán disponibles para realizar soporte técnico y/o ningún tipo de mantenimiento.

No se autoriza el uso de WhatsApp para efectos de comunicación, debido a que la herramienta en mención no cuenta con soporte técnico por parte de la mesa de soporte de la Fundación. Las herramientas permitidas para la comunicación interna son Microsoft Teams, chat y correo de Google.

2.6. USO DE CONTRASEÑA

Los trabajadores deben considerar que:

Todos los dispositivos móviles pertenecientes a la Fundación que se encuentren asignados para un trabajador autorizado deben contar con una contraseña o clave (password) personal e intransferible, que limite solamente a su responsable a contar con el acceso directo a la información que éste contiene.

Las contraseñas utilizadas para el acceso a los dispositivos móviles tipo portátil, deberán seguir los lineamientos indicados, en longitud de contraseñas y uso de combinaciones (alfanuméricos, con o sin caracteres especiales), la periodicidad de cambio, el almacenamiento en memoria de las últimas contraseñas; a su vez resulta importante que

dichas contraseñas no contengan información de carácter personal (fechas de nacimiento, nombres familiares u otra información de fácil reconocimiento).

2.7. PROTECCIÓN FÍSICA

- Todos los dispositivos móviles de la Fundación deben estar registrados e inventariados.
- Los dispositivos móviles asignados a los trabajadores son personales e intransferibles.
- Los equipos asignados, en particular aquellos que almacenen información sensible, no deben ser entregados a personal ajeno a la Fundación
- En caso de pérdida o hurto del equipo, el trabajador deberá interponer la denuncia ante las autoridades competentes (Fiscalía) e informar inmediatamente a su jefe. quien deberá escalar la novedad con el responsable de tecnología e infraestructura tan pronto tenga conocimiento de los hechos.
- Cuando se reporte la novedad, la Dirección de Informática y Tecnología inmediatamente deberá bloquear los sistemas de información con las plataformas utilizadas a disposición de estos eventos.

2.8. INSTALACIÓN Y CONFIGURACIÓN DE APLICACIONES

Está prohibida la descarga e instalación de aplicaciones diferentes a las que se encuentran por defecto en los dispositivos al momento de la entrega por parte de la Fundación. En caso de necesitar una aplicación diferente a las entregadas inicialmente, deberá ser autorizada y aprobada por parte del Coordinador Técnico.

El proceso de instalación y configuración de las aplicaciones en los dispositivos móviles sólo puede ser realizado por los profesionales designados por el Coordinador Técnico.

2.9. SEGURIDAD DEL SISTEMA OPERATIVO

Para garantizar la disponibilidad, confidencialidad e integridad de la información contenida en los dispositivos móviles, el profesional designado por el proceso de tecnología e infraestructura será quien otorgue los respectivos permisos.

Los trabajadores no podrán descargar el sistema operativo en los portátiles o dispositivos móviles, sin la autorización o aprobación de la Dirección de Informática y Tecnología.

La Fundación cuenta con una actualización automática del sistema operativo designado para las funciones de la Fundación. El trabajador deberá apagar el equipo al momento de finalizar su jornada de trabajo, con el fin de garantizar que las actualizaciones se ejecuten de manera adecuada y no provoque efectos de ralentización.

2.10. REGISTRO DE INGRESO Y SALIDA DE LOS DISPOSITIVOS MÓVILES

Los Dispositivos Móviles que ingresen o salgan de las instalaciones de la Fundación por parte de personal externo deben ser registrados en una planilla de ingreso y salida de visitantes.

Los trabajadores que tengan asignado un dispositivo móvil (portátil) por la Fundación, estarán registrados en una lista de control para omitir el registro diario de entrada y salida de este dispositivo. La actualización de este listado estará a cargo del Coordinador de soporte de la Dirección de Informática y Tecnología.

2.11. USO DE DISPOSITIVOS MÓVILES FUERA DE LAS INSTALACIONES

Los trabajadores deben ser responsables del manejo y cumplir las recomendaciones de uso y cuidado físico. Adicionalmente, debe contar con el control de intercambio de información de acuerdo con los lineamientos de copias de respaldo, usando la herramienta de Google Drive.

2.12. NORMAS DIRIGIDAS A TODOS LOS TRABAJADORES

- No dejar desatendidos los equipos o dispositivos móviles.
- No llamar la atención acerca de portar un equipo o dispositivo valioso.
- No registrar información de contacto del personal técnico de la Fundación. Lo anterior, para evitar posibles ataques informáticos.
- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física mínimas necesarias para evitar accesos no autorizados al dispositivo, pérdida, mala manipulación o hurto de estos.
- Los usuarios no deben almacenar vídeos, fotografías o información personal en los dispositivos móviles asignados.
- No hacer uso de redes de acceso público en cafeterías, restaurantes, centros comerciales, aeropuertos, entre otros.

3. LINEAMIENTO DE USO DE INTERNET

3.1. INTRODUCCIÓN

El Lineamiento de Uso de Internet establece las normas para garantizar un adecuado uso del internet; se definen las reglas sobre las cuales todo usuario que tenga con una cuenta con acceso a internet en la Fundación Universitaria San Martín debe seguir para que así la organización pueda administrar sus riesgos de seguridad de uso de internet; esto de la mano con la educación a sus usuarios y promoviendo el uso correcto de los sistemas tecnológicos corporativos.

Todos los usuarios están obligados a acatar los lineamientos plasmados en la presente política, con el fin de realizar sus operaciones u actividades diarias minimizando el riesgo de llevar a cabo el uso inadecuado o prácticas impropias en dichos recursos.

3.2. OBJETIVO

Establecer las responsabilidades, normas y lineamientos mínimos que deben cumplir todos los usuarios que utilicen Internet al interior de la Fundación, con el fin de garantizar el correcto uso de este, cumplimiento de requisitos técnicos, legales y asegurar un mejor aprovechamiento del servicio de internet como una herramienta de trabajo y apoyo académico en beneficio de toda la comunidad.

- Mitigar los riesgos de seguridad asociados con el uso de internet, garantizando con ello la seguridad, disponibilidad, integridad y confidencialidad de los activos de información de la Fundación.
- Promover un entorno de trabajo productivo y seguro, estableciendo directrices claras sobre el uso adecuado de Internet en el lugar de trabajo, se busca fomentar la productividad de los empleados al tiempo que se protege la red y los sistemas de la Fundación. Contra amenazas cibernéticas, malware, acceso no autorizado y actividades no relacionadas con la actividad laboral.
- Establecer, difundir y verificar el cumplimiento de buenas prácticas en el internet para los usuarios de la Fundación, conociendo sus responsabilidades como usuarios. Delimitar el acceso a páginas o sitios WEB que representen un riesgo para la información y reputación de la Institución, tales como la Deep web y páginas de contenido explícito.

3.3. ALCANCE

El presente lineamiento de uso de internet es aplicable a todos los trabajadores de la Fundación, el cuerpo docente, directivos, proveedores, trabajadores, los consultores, contratistas y a quienes tengan acceso al servicio de internet dentro de la FUNDACIÓN, independientemente de la sede.

3.4. RESPONSABLES

Todos los trabajadores, cuerpo docente, directivos, proveedores, Dirección de Informática y Tecnología (quien vela por el cumplimiento del presente lineamiento para garantizar el adecuado control de acceso lógico y físico, consultores, contratistas y todo aquel que cuente con una cuenta de correo electrónica corporativa de la Fundación.

3.5. GENERALIDADES DEL LINEAMIENTO DE USO DE INTERNET

La Fundación establece las medidas de control del uso de internet con el objeto de implementar soluciones de seguridad y de monitoreo que permitan rastrear el cumplimiento de las políticas corporativas.

La Fundación cuenta con soluciones de seguridad y monitoreo diseñadas para rastrear el cumplimiento de las políticas corporativas. Los controles de acceso son idóneos y robustos, con el fin de impedir la extracción de los activos de información de la Fundación. Estas restricciones son conocidas por todos los trabajadores y terceras partes que cuentan con acceso a la información de la Fundación y en este sentido la Fundación controla los privilegios sobre los activos de información de acuerdo con lo permitido y según lo estrictamente necesario para el desempeño de su función.

- El servicio de Internet es un recurso que la Fundación suministra a toda la comunidad universitaria para contribuir con las actividades académicas y/o laborales. El uso personal, ocasional o eventual de este recurso es permitido, en tanto, no interfiera con la productividad académica y que no afecte su desempeño laboral. El uso de este recurso implica la aceptación íntegra de los términos, normas, lineamientos y condiciones contenidas en la presente política.
- Las solicitudes de nuevos permisos de usuario y los cambios de privilegios de acceso a internet se presentarán por escrito a la correspondiente facultad o unidad administrativa quien dará su visto bueno para su respectiva gestión.
- La Fundación en cualquier momento podrá implementar las medidas necesarias en las plataformas tecnológicas que brindan el servicio de internet, en aras de incrementar los niveles de seguridad y/o de brindar un mejor servicio. En este sentido la Fundación se reserva el derecho de deshabilitar, modificar o eliminar las cuentas institucionales, en las cuales se evidencie un uso inadecuado o que incurran en el incumplimiento de los lineamientos plasmadas en el presente documento. El incumplimiento del presente lineamiento expone al usuario a medidas disciplinarias según corresponda.
- La Fundación es dueña de la infraestructura, servicios y tecnologías utilizadas para el acceso a Internet, por lo que se reserva el derecho de supervisar el tráfico de la red y el acceso a la información.

3.6. RESPONSABILIDADES DE LOS USUARIOS DE INTERNET

- Con el fin de resguardar la integridad y confidencialidad de la información, se prohíbe el acceso a páginas web que contengan material pornográfico, relacionado con drogas, terrorismo, hacktivismo, segregación racial, juegos, apuestas, y actividades ilegales en general.
- Se restringe el acceso a redes sociales como Facebook, Twitter, TikTok, Instagram, entre otras. Esto se aplica a menos que el acceso tenga un propósito laboral y/o académico, y el usuario cuente con los permisos correspondientes.
- Evite la descarga no autorizada de archivos o software, incluyendo contenido de audio, vídeo, herramientas para eludir las políticas de seguridad, programas de prueba y software para descargas.
- Los usuarios deben asumir la responsabilidad de todas las actividades realizadas desde su cuenta institucional, utilizada para acceder a los servicios de Internet.

- Los usuarios deben emplear las herramientas ya instaladas en sus computadoras para acceder a Internet. Si es necesaria una herramienta adicional, el usuario debe realizar la solicitud a la mesa de soporte.
- Es su responsabilidad exclusiva mantener la confidencialidad de sus datos de acceso a internet y garantizar su uso adecuado en todo momento.
- Si nota algún uso no autorizado de su cuenta o detecta cualquier problema de seguridad, es crucial informar de inmediato a la mesa de soporte, al correo: soporte.fusm@sanmartin.edu.co.
- Solo se debe manejar correos electrónicos institucionales y se debe limitar el acceso a los datos confidenciales de la organización.
- La Fundación filtra el tráfico web y monitorea el acceso a páginas no permitidas. Si es necesario acceder a una página restringida, se debe solicitar a la mesa de soporte al correo: soporte.fusm@sanmartin.edu.co.
- Todo usuario deberá comunicar a la Dirección de Informática y Tecnología al mail soporte.fusm@sanmartin.edu.co cualquier incumplimiento de las directrices plasmadas en el presente documento.
- Los usuarios son responsables de todas las actividades que se realicen desde su cuenta institucional con la cual accede a los servicios de internet.
- Cada usuario se responsabilizará de cualquier efecto NO deseado que provoque al intentar visitar algún sitio no permitido o bien instalar un programa NO autorizado ni licenciado.
- La cuenta institucional con la que se accede al servicio de internet es de uso personal e intransferible, por lo tanto, es responsabilidad del usuario salvaguardar la contraseña, cambiarla periódicamente, y no compartirla bajo ninguna circunstancia.
- El usuario se compromete a aceptar las condiciones estipuladas en el presente lineamiento en el que se señala el uso de los servicios con fines puramente laborales, educativas y de investigación, lo que excluye cualquier uso comercial del internet, así como prácticas desleales (hacking) o cualquier otra actividad que voluntariamente tienda a afectar a otros usuarios de la red, tanto en las prestaciones de ésta como en la privacidad de su información.
- Los usuarios deben utilizar las herramientas previamente instaladas en el equipo de cómputo para el consumo del internet.

3.7. RESTRICCIONES DEL USO DE INTERNET

- Está estrictamente prohibido el uso del Internet con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral o educativo.
- Diseminar virus, gusanos, troyanos, o malware u otros tipos de programas dañinos que puedan afectar la integridad física o lógica de cualquier componente de la infraestructura tecnológica; ya sea propiedad de la Fundación o de algún usuario que haga uso de la misma.

- Congestionar enlaces de internet mediante la transferencia, ejecución de archivos o programas que no son de uso propio en el ambiente laboral o académico.
- El acceso a páginas web con contenido pornográfico, sexual, de drogas, hacking, explosivos, juegos, apuestas, actividades ilegales en general, redes sociales (facebook, twitter, linkedInd, etc.), páginas para evasión de políticas o enmascaramiento del tráfico, entre otras; que podrían poner en riesgo la integridad y confidencialidad de la información de la Fundación, salvo que sea con fines académicos y en cuyo caso el usuario lo pueda demostrar.
- El uso de cualquier página o herramienta de chat o mensajería instantánea a menos que la universidad disponga o autorice alguna herramienta para estos fines, y en cuyo caso, sólo se deberá usar para fines académicos y/o laborales y que vayan en pro del desarrollo institucional.
- Se controlará el uso del internet de la Fundación para descarga de archivos o software sin su debida autorización tales como: archivos de audio, vídeo, software para evasión de las políticas de seguridad o enmascaramiento del tráfico, software trial o de prueba, software para descarga o intercambio de archivos en redes P2P (Peer to Peer (Ej. Ares, Kazaa, Morpheus, Limeware, emule, edonky, torrents, etc.)), el acceso a redes sociales, correos personales, llamadas telefónicas sobre internet, audio o video on-line (Streaming), entre otros.

4. LINEAMIENTO DE RESPALDO, ALMACENAMIENTO Y RECUPERACIÓN DE INFORMACIÓN

4.1. INTRODUCCIÓN

La Fundación Universitaria San Martín, ha determinado la necesidad de contar con un lineamiento de respaldo, almacenamiento y recuperación de la información crítica que garantice la disponibilidad e integridad de los activos informáticos dispuestos en el centro de datos de su sede principal.

El presente documento describe los lineamientos de copias de respaldo de información y almacenamiento junto con los procedimientos y mecanismos para la realización de las actividades relacionadas, con el fin de apoyar a los administradores y líderes de servicios de tecnología a reducir los impactos de los riesgos generados por fallas en la prestación de servicios internos y externos de la Fundación que involucren la pérdida total o parcial de información.

4.2. OBJETIVO

Definir los lineamientos generales aplicables a los sistemas de información y a la infraestructura de servidores ubicados en el centro de datos de la Fundación, en lo referente a los procedimientos de respaldo, custodia y recuperación o restauración de las copias de respaldo de la información, garantizando la disponibilidad de la misma siempre que se requiera.

4.3. ALCANCE

El presente lineamiento de Respaldo, Almacenamiento y Recuperación de Información es aplicable a todos los sistemas de información y dispositivos de almacenamiento de datos que contengan información catalogada como reservada o crítica para la prestación de servicios internos y externos de la Fundación alojada en los servidores del centro de datos ubicado en la sede principal de la Fundación

Va dirigida a todos los responsables de administrar, liderar, gestionar e interactuar con la infraestructura tecnológica y/o que tengan cualquier relación con información de la Fundación incluidos terceros.

4.4. RESPONSABLES

Dirección de Informática y Tecnología
Trabajadores de la Fundación Universitaria San Martín.

4.5. LINEAMIENTOS

- Es responsabilidad de los líderes de procesos y jefes de áreas garantizar que la información institucional catalogada como crítica “aquella necesaria para mantener operativos los procesos de la Fundación”, sea almacenada en los servidores de Google Drive. Para la gestión de archivos compartidos de los usuarios, la Dirección de Tecnología utiliza la herramienta de Google Drive para el manejo y almacenamiento de la información.
- Por ningún motivo se permite alojar en servidores información catalogada como personal, música, videos, documentos transitorios, documentos confidenciales, backups de equipos de escritorio, backups de correo electrónico y demás que no sea relevante en el cumplimiento de los objetivos de la Fundación.
- Es responsabilidad de los líderes de proceso y jefes de dependencias identificar claramente la información crítica a su cargo, identificar los riesgos y generar el plan de continuidad. Los líderes de proceso y jefes de dependencias son los únicos autorizados para solicitar el respaldo y/o recuperación de información mediante el formato dispuesto para tal fin (formato Respaldo y Recuperación de Información, indicando los siguientes datos: del solicitante, de la aplicación, de los archivos (tipo y ubicación), de la Base de Datos (ubicación, motor y versión), accesos, periodicidad de respaldo y tipo de respaldo.
- Siempre que exista alguna modificación o adición en la fuente de la información, se debe generar el formato descrito y entregarlo al administrador de copias.
- El software de respaldo y restauración de información (en el caso de contar con el mismo) debe estar instalado en los servidores para los cuales se haya hecho solicitud de backup. Se debe contar con las licencias necesarias que garanticen el cumplimiento de dicha solicitud.

- Cada trabajador de la Fundación es responsable de resguardar la información generada para el desarrollo de sus funciones dentro de los recursos asignados para tal fin, como es el caso de carpeta de Google Drive.
- Ningún tipo de información que se refiera a la misión de la Fundación debe ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo. Para estos casos, es responsabilidad de cada usuario replicar la información en las carpetas de archivos que residen en Google Drive.

4.6. RESPONSABILIDADES DE LA DIRECCIÓN DE INFORMÁTICA Y TECNOLOGÍA

- La Dirección de Informática y Tecnología verifica que las copias de seguridad sean tomadas con la periodicidad definida y las restauraciones hayan sido verificadas.
- Las pruebas de restablecimiento de los backups se deben ejecutar de forma periódica, validando contenido y completitud.
- Realizar en forma adecuada las copias de respaldo de la información que garanticen la continuidad de los servicios tecnológicos de la Fundación y mantener su inventario actualizado. Para esto tendrá en cuenta:

  - Determinar el nivel de criticidad de la información, las frecuencias de ejecución y el periodo de retención de las copias de respaldo. Según las necesidades de la compañía y definiciones dentro de la Tabla de Retención Documental (TRD) definidas.

  - Definir los tipos de respaldos (completa, incremental o diferencial) que se van a generar.

  - Registros exactos y completos de las copias.

  - Alcance y frecuencia de los respaldos, que indique los requisitos de negocio, de seguridad de la información y la importancia de la operación.

- Es responsabilidad de la Dirección de informática y Tecnología la gestión adecuada de las versiones relacionadas a las aplicaciones en el medio de almacenamiento utilizado en su momento que le permita atender requerimientos operacionales internos y legales
- Los operadores del centro de datos verificarán constantemente la ejecución correcta de las copias de respaldo, suministrarán los medios y/o espacio de disco requeridos para cada trabajo de copia, controlarán la vida útil de cada respaldo o medio y el procedimiento de limpieza de las plataformas de grabación.

- El administrador de las bases de datos realizará pruebas periódicas de restauración de la información en un ambiente de pruebas adaptado para tal fin, con el objetivo de garantizar que los respaldos son adecuados para una eventual restauración.
- El respaldo de información confidencial debe protegerse por medio de cifrado.

4.7. PROCESO DE RESTAURACIÓN

Se debe tener en cuenta los siguientes requerimientos tanto para la restauración de carpetas, archivos y/o correos electrónicos:

- Los líderes de proceso y jefes de áreas son los únicos autorizados para solicitar la recuperación de información ante una pérdida total, parcial o para realizar pruebas controladas.
- Se debe diligenciar en su totalidad el formato Respaldo y Recuperación de Información y ser entregado al administrador de copias.
- Es responsabilidad del administrador de copias informar la disponibilidad de los respaldos, realizar el trámite para obtener los medios magnéticos, ejecutar el procedimiento de recuperación e informar los resultados.
- Al finalizar el procedimiento se debe devolver el medio magnético solicitado en el proceso de restauración a la empresa de custodia.
- La información de los equipos de escritorio y portátiles se resguarda en la carpeta Google Drive asignada a cada usuario.
- Todos los trabajadores deben guardar la información en la carpeta compartida de cada usuario en su Google Drive, la cuál es la única carpeta autorizada para la gestión de las copias de respaldo.
- El equipo de la Dirección de Informática y Tecnología o quién haga sus veces realizará el Backup del Google Drive de cada usuario de forma mensual.
- La Fundación resguarda la información de correo electrónico de las cuentas corporativas por medio de una herramienta automatizada, con periodicidad semestral.
- Se lleva a cabo la prueba de restauración de backup, seleccionando de manera aleatoria un archivo de restauración de correo electrónico, esta actividad se ejecuta con periodicidad semestral.
- La información de las cuentas de correo se mantiene de manera permanente en el servidor de correo electrónico de Google WorkSpace, hasta la finalización del contrato laboral de los trabajadores en la cual se realizará un borrado seguro de la cuenta.

4.8. COPIAS DE RESPALDO DE SERVIDORES

Las copias de respaldo relacionadas con la configuración de los servidores e información contenida se realizan de forma trimestral en el respectivo servidor de backup.

Cuando se presentan cambios en la configuración, se realizan los backup correspondientes antes y después de dicho cambio.

4.9. COPIAS DE RESPALDO DE INFORMACIÓN EN LA NUBE

Las copias de respaldo de la información del cliente (arquitectura, implementación, logs, informes, correo electrónico de clientes) se realizan de forma manual y se alojan de manera segura en las instalaciones de la Fundación.

5. LINEAMIENTO DE TRATAMIENTO DE DATOS PERSONALES

5.1. INTRODUCCIÓN

En cumplimiento de las normas establecidas para regular el tratamiento de datos personales y promoviendo el respeto de los derechos fundamentales consagrados en los artículos 15 y 20 de la Constitución Política, la Fundación adopta los siguientes Lineamientos para el Tratamiento de Datos Personales de obligatorio cumplimiento en todas las actividades que desarrolle la Fundación, que involucre el tratamiento de datos personales por parte de sus directivos, trabajadores administrativos y docentes, estudiantes, egresados, jubilados, ex empleados, proveedores, contratistas o aspirantes.

Particularmente, estos lineamientos contemplan el manejo de solicitudes de aceptación, consultas y solicitudes relacionadas con el tratamiento de este tipo de información.

5.2. PRINCIPIOS

Para dar cumplimiento a los lineamientos de Protección de Datos Personales, como a las obligaciones impartidas por la ley 1581 de 2012 y su decreto reglamentario, en la Fundación se emplean los siguientes principios:

- Principio de legalidad: El tratamiento de los datos personales es una actividad reglada que debe sujetarse a lo establecido en la ley 1581 de 2012 en el decreto 1377 de 2013 y en las demás disposiciones que las desarrollen.
- Principio de finalidad: El tratamiento de los datos personales debe obedecer a una finalidad legítima de acuerdo con la constitución y la ley, la cual debe ser informada al titular.
- Principio de dignidad: Toda acción u omisión asociada al tratamiento de datos personales debe ejecutarse siempre salvaguardando la dignidad del titular y amparando los demás derechos constitucionales, en especial el derecho al buen nombre, a la honra, a la intimidad y el derecho de información.
- Principio de no discriminación: Queda prohibido realizar cualquier acto de discriminación por las informaciones recaudadas en la base de datos.
- Principio de integridad: En el tratamiento debe garantizarse el derecho del titular a obtener del responsable o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de sus datos personales.

- Principio de libertad: El tratamiento de los datos personales sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización.
- Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a especulación.
- Principio de transparencia: En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de sus datos personales.
- Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley.
- Principio de temporalidad del dato: Se refiere a la necesidad de que el dato del titular no podrá ser suministrado a los usuarios cuando deje de servir para la finalidad del banco de datos.
- Principio de seguridad: La información sujeta a tratamiento por el responsable o encargado del tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado a la información.
- Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la norma.
- Deber de información: La Fundación, informará al titular de los datos personales, así como a los responsables y encargados del tratamiento, del régimen de protección de datos adoptado, así como la finalidad y demás principios que regulen el tratamiento de esos datos. Además, informará sobre la existencia de las bases de datos de carácter personal que custodie, los derechos y el ejercicio del hábeas data por parte de los titulares procediendo al registro que exige la ley.

5.3. FINALIDADES Y TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS PERSONALES

Con el objetivo de dar cumplimiento a la legislación vigente en materia de protección de datos personales, en especial a la Ley 1581 de 2012 (y demás normas que la modifiquen, adicionen, complementen o desarrollen) y al Decreto 1377 de 2013, a continuación informamos a todos los titulares de los datos que reposan en las bases de datos de la Fundación , sobre los aspectos relevantes en relación con la recolección, almacenamiento, uso, circulación, supresión, manejo y/o transferencia de datos personales que la Fundación realiza de los datos, en virtud de la autorización otorgada para adelantar dicho tratamiento.

En armonía con lo previsto en el artículo 15 de la Constitución Política de Colombia, la Ley 1266 de 2008, Ley 1581 de 2012, Decreto 1377 de 2013 y todas aquellas normas que las reglamenten, adicionen, deroguen o modifiquen. En este lineamiento se plasman las políticas Institucionales, con las cuales la Fundación realiza el tratamiento de los datos personales, la finalidad del tratamiento, los derechos como titular, así como los mecanismos previstos en la Ley para el ejercicio de tales derechos.

En general, el lineamiento de privacidad y manejo de datos personales tiene como finalidad informar que la obtención, manejo y utilización de información personal de terceros, que tengan una relación contractual con FUNDACIÓN recolectados con ocasión de los servicios prestados, en desarrollo de la misión social para efectos principalmente de establecer y mantener una relación estrecha con los beneficiarios de servicios ofertados, la cual, se adelantará, única y exclusivamente, si ésta se ha suministrado de manera voluntaria, bajo su pleno conocimiento y consentimiento previo y expreso.

En atención a que al titular de los datos personales le asiste el derecho a contar con la privacidad de estos, la Fundación informa que los datos personales recolectados serán utilizados para las siguientes finalidades:

a) Establecer y mantener una relación cercana con los interesados.
b) Realizar retroalimentación de la atención brindada con el fin de proporcionar un efectivo servicio al cliente.
c) Cobro de cuentas por pagar debido a los servicios prestados.
d) Envío de avisos publicitarios o comerciales sobre los servicios de la Fundación.
e) Contacto con clientes, estudiantes, egresados, empleados, proveedores, Contratistas y así como personas que se encuentren en proceso de vinculación contractual de cualquier naturaleza con la Fundación para el envío de información relacionado con la relación contractual, comercial y obligacional que tenga lugar.
f) Recolección de datos para el cumplimiento de los deberes que como **responsable** de la información y datos personales, le corresponde a la Fundación.
g) Con propósitos de seguridad o prevención de fraude.
h) La remisión de cualquier información de carácter financiero, comercial, crediticio o de servicios con fines estadísticos, de control, o supervisión que deban procesarse,

reportarse, conservarse, consultarse, suministrarse o actualizarse ante las centrales de información o bases de datos debidamente constituidas para tal fin, que se estime conveniente, en los términos y durante el tiempo que los sistemas de bases de datos, las normas y las autoridades lo establezcan.

i) Solución de dudas o inquietudes, preguntas generales.
j) Cualquier otra finalidad que resulte en el desarrollo del contrato o la relación comercial existente entre el titular y la Fundación.

De acuerdo con las finalidades enunciadas, los datos personales podrán ser puestos a disposición del personal encargado de la labor correspondiente, dentro de la Fundación, sin excluirse la posibilidad de ser transferidos a encargados, consultores, asesores, personas y oficinas externas según sea necesario para cumplir con las finalidades citadas en el presente numeral

5.4. EXCLUSIONES

Es importante aclarar que la autorización del titular no será necesaria cuando:

a) Dicha información sea requerida por una entidad pública o administrativa.
b) Se emplee en el tratamiento de fines históricos, estadísticos o científicos.
c) Se requieran datos de naturaleza pública.
d) Datos relacionados con el registro civil de los estudiantes.
e) Casos de urgencia médica o sanitaria.

5.5. EN RELACIÓN CON LA BASE DE DATOS DE USUARIOS DE LA FUNDACIÓN

Esta base de datos es generada por el área comercial de la organización en calidad de persona jurídica, para gestión de mercadeo y gestión de servicios específicos dirigidos a los beneficiarios, potenciales beneficiarios y/o clientes.

5.6. EN RELACIÓN CON LA BASE DE DATOS DE LOS TRABAJADORES Y/O CONTRATISTAS DE LA FUNDACIÓN

El tratamiento de los datos es realizado por la institución en calidad de persona jurídica, para la vinculación, desempeño de funciones o prestación de servicios, retiro o terminación, dependiendo del tipo de relación jurídica entablada con la Fundación Universitaria San Martín (incluye entre otros, trabajadores, aprendices y aspirantes a cargos).

5.7. EN RELACIÓN CON LA BASE DE DATOS DE PROVEEDORES DE LA FUNDACIÓN UNIVERSITARIA SAN MARTIN

Esta base de datos corresponde a la información relacionada con los proveedores de la institución en calidad de persona jurídica, en distintos frentes desde infraestructura física, tecnológica y servicios.

5.8. EN RELACIÓN CON LA BASE DE DATOS DE SERVICIOS DE PREVENCIÓN DIGITAL DE LA FUNDACIÓN

Esta base de datos se encuentra asociada con el servicio de “Prevención Digital” y corresponde al tratamiento de datos de personas naturales y jurídicas que contraten el servicio de la Fundación, y sobre las cuales se realiza un monitoreo de aproximadamente cinco (5) patrones en cada caso.

5.9. EN RELACIÓN CON LA BASE DE DATOS DE ESTUDIANTES Y EGRESADOS DE LA FUNDACIÓN

El tratamiento de los datos es realizado por la institución en calidad de persona jurídica, para la gestión académica, servicios académicos, redes de profesionales y requisitos legales y/o normativos, encaminados a los estudiantes activos y egresados de la Fundación.

5.10. DERECHOS DEL TITULAR

En cualquier momento, el titular de los datos personales objeto de tratamiento puede ejercer los derechos que le otorgan la Constitución Política de Colombia y las Leyes, expresamente consagrados en el artículo 8 de la Ley 1581 de 2012, a saber:

- Conocer, actualizar y rectificar los datos personales frente a los **responsables** del tratamiento o encargados del tratamiento. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada al **responsable** del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, lo anterior de conformidad con lo previsto en el artículo 10 de la precitada ley.
- Ser informado por el **responsable** del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el **responsable** o encargado han incurrido en conductas contrarias a esta ley y a la Constitución.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

5.11. DATOS SENSIBLES

El titular tiene derecho a optar por no suministrar cualquier información sensible solicitada por la Fundación, relacionada, entre otros, con datos sobre su origen racial o étnico, la pertenencia a sindicatos, organizaciones sociales o de derechos humanos, convicciones políticas, religiosas, de la vida sexual, biométricos o datos de salud.

5.12. DATOS MENORES DE EDAD - NIÑOS, NIÑAS Y ADOLESCENTES

El suministro de los datos personales de menores de edad es facultativo y debe realizarse con autorización de los padres de familia o representantes legales del menor. Los adolescentes son considerados incapaces relativos, lo que significa que pueden otorgar su consentimiento para el tratamiento de sus datos personales en ciertas circunstancias, como en actividades educativas, culturales o de salud, siempre que se cumplan ciertos requisitos de madurez y comprensión.

5.13. AUTORIZACIÓN DEL TITULAR

Sin perjuicio de las excepciones previstas en la ley, en el tratamiento se requiere la autorización previa, expresa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

5.14. DATOS BIOMÉTRICOS – SISTEMAS DE VIGILANCIA

La Fundación, utiliza diversos medios de vigilancia, dentro de los cuales se emplean circuitos cerrados de televisión, los cuales cuentan con cámaras de video y monitoreo, en todas las oficinas y sedes, estos se encuentran debidamente identificadas y notificadas con avisos en lugares visibles donde todos los involucrados conozcan que están siendo grabados y monitoreados.

La Fundación utilizará la información recolectada con el único fin de proteger la integridad de su personal, visitantes, estudiantes, sus bienes y sus instalaciones. El titular entiende y acepta dicha finalidad y consecuentemente su uso. Esta información puede ser empleada como prueba en cualquier tipo de proceso ante cualquier tipo de autoridad y organización.

5.15. PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS DEL TITULAR

La Fundación dispone de un área responsable de la atención a peticiones, quejas, consultas y reclamos por medio de la cual el titular de los datos puede ejercer sus derechos antes reseñados, los canales de comunicación son: el correo juridicasanmartin@sanmartín.edu.co o dirección física: Carrera 18 No. 80-45 en la ciudad de Bogotá D.C. o al teléfono fijo 622 4422122.

Las solicitudes presentadas ante el área correspondiente, y que versen sobre el tratamiento de datos personales, podrán ser presentadas por medio físico o electrónico a través de los

canales de contacto descritos anteriormente y en comunicación dirigida a la Fundación, siendo necesario que la comunicación expresa de manera clara sus datos de contacto físicos y electrónicos con la finalidad de responder su solicitud.

Presentada la solicitud, la Fundación contará un término de quince (15) días hábiles, desde el día hábil siguiente al recibo de la petición, para atender la solicitud o tomar las medidas que el titular exija.

Si la solicitud no contiene los datos de contacto suficientes, o no refleja de manera expresa los hechos que permitan a la Fundación atender y dar trámite a la petición, se le comunicará tal situación al remitente dentro de lo estipulado en la Ley 1755 de 2015. Para efectos de que allegue la información necesaria dentro del mes siguiente al recibo del requerimiento, so pena de considerarse desistida la petición.

5.15. VIGENCIA

La FUNDACIÓN se reserva el derecho de modificar el presente lineamiento en cualquier momento, previa comunicación electrónica dirigida a los titulares de la información, razón por la cual le invitamos a consultar regular o periódicamente nuestra página web https://www.sanmartin.edu.co/, donde se encuentra publicada la última versión de la presente Política.

La vigencia de la base de datos será el tiempo razonable y necesario para cumplir con las finalidades del tratamiento, teniendo en cuenta lo dispuesto en el artículo 11 del Decreto 1377 de 2013.

El presente lineamiento de tratamiento de datos entra en vigencia a partir del treinta (30) de abril de dos mil veinticuatro (2024).

6. LINEAMIENTO SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON PROVEEDORES

6.1 INTRODUCCIÓN

La Fundación Universitaria San Martín establece directrices y requisitos de seguridad de la información con sus proveedores con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información; asegurando que se cumplen con los objetivos y acuerdos según lo establecido en las políticas de contratación de la Fundación, para lograr el cumplimiento del objeto contratado en los términos establecidos.

Este lineamiento se relaciona con los proveedores y/o terceros que prestan servicios y tienen acceso a información o activos de información de la Fundación y se enmarca en los controles de seguridad de la información y ciberseguridad

6.2 OBJETIVO

Establecer las condiciones para la prestación de los servicios, responsabilidades y controles que ayuden a proteger la información involucrada en las relaciones entre la Fundación Universitaria San Martín con sus terceros, frente a interceptaciones, copia, modificación, divulgación y destrucción no autorizada, que puedan afectar los principios de integridad, disponibilidad y confidencialidad de la información. Definiendo los lineamientos, las condiciones y las medidas en seguridad de la información empleada con los terceros, con el fin de salvaguardar la información, garantizando la confidencialidad, integridad y disponibilidad de la información de la compañía.

6.3 ALCANCE

El presente lineamiento aplica para todos los proveedores que para la ejecución de su trabajo requieran acceder a la información o infraestructura tecnológica de la Fundación.

6.4 RESPONSABLES

Dirección de Informática y Tecnología
Vicerrectoría Financiera y Administrativa.

6.5 LINEAMIENTOS DE SEGURIDAD EN LA RELACIÓN CON PROVEEDORES

Para establecer un entorno donde se minimicen las probabilidades de materialización de riesgos asociados con el acceso de proveedores y contratistas a los activos de información de la Fundación, se establecen los siguientes lineamientos de Seguridad de la Información al momento de una relación entre Fundación y sus proveedores y/o contratistas:

- Con el objetivo de asegurar la protección de los activos de información de la Fundación que sean accesibles a los proveedores, se establece que los proveedores y/o contratistas que tengan acceso a los activos de información, están obligados a cumplir los lineamientos de seguridad definidas y reportar los incidentes de seguridad de la información, al trabajador con quien se encuentre acompañado y él a su vez, escalará al responsable de la gestión del incidente.
- La Fundación exige que, en todos los contratos o acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Fundación, se deben realizar acuerdos de confidencialidad y/o acuerdos de protección de datos sobre el manejo de la información. La Fundación hará firmar un acuerdo de confidencialidad al proveedor con quien establezca relación, en el cual se describe la criticidad del activo que se vaya a compartir con él.
- Los proveedores y/o contratistas no podrán tener acceso a áreas o zonas donde se encuentre información sensible en la Fundación. Sí fuese necesario su ingreso a determinadas áreas, debe ser autorizado por el Director de informática y tecnología o quien él designe, a su vez éste debe acompañar al contratista durante todo el tiempo que este permanezca en dicha área.

- La Fundación es la encargada de gestionar las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que sea necesario mover, y asegurar para que la seguridad de la información se mantenga durante todo el período de transición.

6.6 CONTROLES DE SEGURIDAD PARA EL INTERCAMBIO DE INFORMACIÓN CON PROVEEDORES

Para el intercambio de información entre la Fundación y sus proveedores y/o contratistas, se deberán implementar estándares y procedimientos formales asociados al intercambio de información, que permitan garantizar la seguridad en el acceso y la transferencia de información, considerando la aplicación de cifrado en las comunicaciones y la validación de identidad.

Los proveedores y/o contratistas que apliquen relaciones contractuales con la Fundación, deben incluir dentro de su contrato las cláusulas de confidencialidad de la información pertinentes y los lineamientos establecidos por la Fundación.

6.7 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON LOS PROVEEDORES

- Todo control físico y lógico sostenido entre el proveedor y/o contratista y la Fundación, deberá contar con un soporte contractual garantizando que se cumplirá acorde a las condiciones de servicio y el alcance de cada una de las partes.
- La Fundación deberá contar con un seguimiento del personal externo (proveedor y/o contratista) que esté autorizado para acceder a la información de la Fundación o recibirla por parte de ella.
- Si la Fundación contrata un proveedor y/o tercero para la modificación y/o adquisición de una aplicación o software, se deberá realizar pruebas con el solicitante del nuevo desarrollo o cambio, con el fin de validar la funcionalidad y disponibilidad del sistema a implementar. Adicionalmente, el desarrollador deberá entregar un manual de usuario y administración donde se encuentren las especificaciones técnicas y funcionales de la aplicación o programa diseñado para su correcta operación.
- Los proveedores notificarán a la Dirección de Informática y Tecnología o quien haga sus veces, sobre los incidentes de seguridad de la información que hayan sucedido o materializado en el marco del servicio prestado, así mismo reportará a la Fundación la gestión y acciones tomadas para el cierre del incidente.

6.8 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

Toda adquisición de Software y Hardware realizada por la Dirección de Informática y Tecnología para la Fundación se debe notificar al comité de seguridad de la información. Lo anterior, con el objetivo de poder definir los requisitos y condiciones de seguridad

mínimas requeridas, los cuales deben contar con soportes documentales aprobados por las partes en el contrato o acuerdo de servicio.
Los proveedores y contratistas que acuerdan externamente servicios de otras compañías, que estén relacionados con el suministro de tecnología de información y comunicación que prestan a la Fundación, deberán proporcionar información sobre los requisitos y prácticas de seguridad de la información manejada; quienes serán objeto de seguimiento por parte de la Fundación, según los acuerdos iniciales establecidos con el proveedor del servicio.

6.9 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES

Es importante asegurar que los términos y condiciones de seguridad de la información en los acuerdos realizados entre la Fundación y los proveedores y/o contratistas, se cumplan; así como. los incidentes que se generen sean gestionados oportunamente. Para lo anterior:

- Se realizará seguimiento y revisión a los productos y/o servicios prestados por los proveedores y/o contratistas, de acuerdo con las condiciones iniciales establecidas dentro del contrato.
- De acuerdo con el proveedor y/o contratista, se definirán los mecanismos que permitan realizar el seguimiento, dependiendo de la criticidad de la información que maneja, evaluando criterios de seguridad física y lógica. En caso de proveedores que almacenen, procesen o transmitan datos del cliente o en la medida que puedan afectar la seguridad del entorno de los datos de los titulares, se debe realizar un seguimiento periódico. Así mismo se tendrá en cuenta algunos requerimientos del estándar ISO/IEC 27001- 2022 y la normatividad asociada con el estándar ISO 9001:2015.
- De ser posible y si aplica, para proveedores de alto impacto en seguridad de la información, se evaluará el plan de continuidad que emplea el proveedor y/o contratista.
- El seguimiento o auditoría a los procesos y controles a los proveedores y/o contratista se realizará con una periodicidad no mayor a un año.
- El líder del proceso de tecnología o delegado tendrá la responsabilidad de verificar y validar la configuración de los equipos o programas instalados, de igual manera, reportar las debilidades y oportunidades de mejora al proveedor del servicio a través de los procedimientos internos establecidos.
- Los proveedores y/o contratista que entreguen sus servicios a la Fundación deben contar con certificaciones vigentes de seguridad de la información y/o firmas digitales aplicado a los servicios que se contratarán, en especial, en los casos en que se externalizan los procesos de tratamiento y resguardo de información, ya sean hosting, housing, entre otros.
- Para los proveedores que tengan relación con almacenamiento, comunicación, infraestructura, plataforma o software que sean entregados a la Fundación, en modalidad de servicio, como: servicios en la nube, equipos tecnológicos adquiridos o sistemas de información desarrollados por terceros y sobre los cuales existan garantías del fabricante; se deben establecer y documentar los procedimientos

requeridos para la gestión de incidentes de seguridad, los que serán gestionados a través la Dirección de Informática y Tecnología de la Fundación, bajo los procedimientos internos definidos por la Fundación.

- Es necesario establecer Acuerdos de Niveles de Servicio (ANS), los cuales deben ser formalizados a través de acuerdos complementarios que contengan criterios relacionados con el nivel de servicio, entrega continua del mismo, tiempos de respuesta de atención para su entrega, tiempos de resolución de problemas, entre otros; que serán aplicados por el área respectiva que solicita el servicio y asesorados por el personal del proceso de tecnología e infraestructura y el personal asociado al proceso de gestión de calidad.
- Para el monitoreo sobre los servicios tecnológicos tercerizados, será responsabilidad del personal técnico de tecnología e infraestructura y del personal directivo del proceso de operación del servicio, el incorporar un control de monitoreo que asegure la disponibilidad de los servicios tecnológicos, plataformas de infraestructura y los sistemas de información que sean entregados por el proveedor; con el propósito de medir los niveles del servicio y gestionar de manera oportuna cualquier incidente que puedan afectar el principio de disponibilidad.

6.10 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES Y/O CONTRATISTAS

Cuando se presentan cambios como:

- Acuerdos con los proveedores: tanto el proveedor y/o contratista como el responsable en la Fundación deberán establecer y notificar los cambios que se generen o se estimen realizar con respecto a los acuerdos contractuales iniciales.
- Cambios que la Fundación requiera implementar, como: mejoras al servicio ofrecido, desarrollo de nuevas aplicaciones y sistemas, actualizaciones o modificaciones a los lineamientos de la compañía; será el comité de seguridad de la información, quien definirá los lineamientos de seguridad que se deben aplicar para cumplir con los requisitos de seguridad de la información y el sistema de gestión integrado.

- Todo cambio en el servicio que el proveedor y/o contratista desee o requiera implementar, como: uso de nuevas tecnologías, cambios y mejoras en las redes, versiones o ediciones recientes, herramientas nuevas y ambientes de desarrollo; deben ser informados a la Fundación, antes de ser implementados.

7 LINEAMIENTO DE ESCRITORIO Y PANTALLA LIMPIA

7.1 OBJETIVO

Definir y establecer las normas, directrices, lineamientos y condiciones generales relacionadas con los puestos de trabajo, para mantener el escritorio limpio y la pantalla despejada, con el fin de reducir las brechas existentes ante el riesgo de acceso no autorizado, pérdida y daño de la información de la Fundación, que se encuentran bajo la responsabilidad de los trabajadores de la Fundación.

7.2 ALCANCE

El presente Lineamiento de escritorio y pantalla limpia, es aplicable a todos los trabajadores de la Fundación, el cuerpo docente, directivos, proveedores, trabajadores, los consultores, contratistas y todo aquel que se encuentre realizando actividades o funciones específicas y diarias con la Fundación independientemente de la sede.

7.3 RESPONSABLES

Todos los trabajadores, cuerpo docente, directivos, proveedores, consultores y contratistas de la Fundación.

7.4 LINEAMIENTOS DE ESCRITORIO Y PANTALLA LIMPIA

Este Lineamiento busca asegurar la confidencialidad, disponibilidad e integridad de la información en los puestos de trabajo y los activos de información que son propiedad de la Fundación. Por lo anterior, todos los trabajadores de la FUNDACIÓN deberán cumplir los siguientes lineamientos:

7.5 LINEAMIENTO ESCRITORIO LIMPIO

- Todos los trabajadores deben mantener su puesto de trabajo limpio y organizado; deben contar con los implementos básicos para poder desarrollar las funciones propias de su cargo.
- Cada uno de los trabajadores debe mantener su puesto de trabajo libre de información, propia de la Fundación, susceptible de ser alcanzada, visualizada, copiada o utilizada por personal sin autorización para su uso o conocimiento.
- Todo documento, medio magnético o memoria extraíble autorizada, CD, DVD o unidad extraíble que contenga información confidencial o sensible de la Fundación, debe ser almacenado en lugares seguros o en los sistemas de información autorizados con los controles de acceso acordes al cargo.
- Los puestos de trabajo con equipos de cómputo deben estar estratégicamente ubicados, para que la información desplegada en sus monitores no pueda ser visualizada por personas no autorizadas.
- Al finalizar la jornada de trabajo, el trabajador debe cerrar todos los sistemas de información y/o aplicaciones salvaguardando la información que desarrolló durante su jornada laboral y posteriormente apagar el equipo. En caso de conservar

documentación en físico con información reservada o confidencial, ésta se debe guardar en un lugar seguro bajo llave.

- Toda información impresa en los equipos de oficina de la Fundación de clasificación confidencial o sensible debe ser retirada de manera inmediata de la impresora y no se debe dejar en el puesto de trabajo sin custodia del trabajador responsable.
- Las contraseñas no se pueden dejar en notas adhesivas publicadas en o debajo de una computadora, ni pueden dejarse escritas en un lugar accesible.
- Para eliminar documentos confidenciales o sensibles que están de manera impresa, se debe usar una trituradora de papel.
- Es importante tener en consideración que elementos alimenticios en el lugar de trabajo pueden llegar a ocasionar problemas en caso de ser regados sobre los dispositivos móviles, razón por la cual se recomienda en las situaciones en las que se desee consumir alguna bebida esta se encuentre en un recipiente hermético que no ocasione inconvenientes en caso de ser involuntariamente tropezado al realizar el trabajo normal.
- Todo trabajador debe salvaguardar la información que reposa en sus agendas o cuadernos de trabajo diario, por tanto, los mismos siempre deben quedar resguardados en un lugar seguro, bajo llave y siempre deben estar custodiados.
- Si se emplean pizarras o tableros de marcador o tiza resulta fundamental que luego de ser utilizados el contenido sea borrado, con el objeto de salvaguardar la información que pueda llegar a ser empleada por personal ajeno al propietario de esta. Es importante siempre salvaguardar el activo de la información de la Fundación.

7.6 LINEAMIENTO DE PANTALLAS LIMPIAS

- El equipo de soporte tecnológico implementa el bloqueo automático de las sesiones de los usuarios en los equipos de cómputo, después de 2 minutos de tiempo de inactividad, con el objeto de restringir la posibilidad de fuga de información.
- El equipo de mesa de ayuda realiza inspecciones periódicas para revisar que los equipos de hardware no se encuentren encendidos, al finalizar la jornada laboral y en caso de incumplimiento realiza los respectivos reportes y alertas.
- Es fundamental que todo trabajador bloquee la pantalla de su equipo de cómputo cuando no esté haciendo uso de este, o cuando por algún motivo deba ausentarse de su puesto de trabajo. Si utiliza el sistema operativo Windows puede hacer uso del bloqueo de la sesión con la combinación simultánea de las teclas Windows + L.
- Es responsabilidad del trabajador mantener cerrado y bloqueado cualquier archivo que contenga información restringida y/o confidencial cuando no esté en uso o sin supervisión.
- Reportar cualquier problema de seguridad o pérdida de información de inmediato a soporte al correo: soporte.fusm@sanmartin.edu.co.
- El protector y fondo de pantalla deben ser autorizados por la Fundación.

- Asegurarse que las pantallas de computadoras no muestren información confidencial cuando el escritorio esté desatendido.
- Los trabajadores no deben almacenar información sensible en el escritorio de los equipos de cómputo.
- Los trabajadores deben almacenar la información de forma ordenada, haciendo uso de carpetas y jerarquías de almacenamiento en los sistemas de información utilizados por la Fundación. De igual manera debe mantener la información en los repositorios de información de cada área bajo el esquema de etiquetado propio definido por gestión documental. Por ningún motivo se deben dejar documentos anclados al escritorio que resulten de fácil acceso a personas inescrupulosas que no están autorizadas para visualizar documentos confidenciales para la Fundación.
- En lo posible se recomienda que los trabajadores no almacenen información como: videos, fotografías o información personal en los equipos de cómputo asignados.

7.7 CONSIDERACIONES

Para tener un alto grado de certeza en el cumplimiento de los lineamientos planteados en este Lineamiento la Fundación realiza los siguientes controles:

La Dirección de Informática y Tecnología, verificará el cumplimiento de los lineamientos planteados en este lineamiento a través de varios métodos (cada vez que se escale requerimientos de gestión por medio de acceso remoto se evidenciará el correcto cumplimiento de las directrices, igualmente todo soporte en sitio contará con la respectiva inspección), a su vez dentro del cronograma de actividades del equipo de mesa de soporte se tendrán establecidos recorridos periódicos de monitoreo; los resultados de dichas inspecciones se presentarán como informes al oficial de seguridad, quien a su vez lo escalará al área de control interno o a quien corresponda, auditorías internas y externas, entre otros.

Cualquier excepción al lineamiento debe ser aprobada con anticipación ante la Dirección de Informática y Tecnología.

8 LINEAMIENTO DE CONTROL DE ACCESOS

8.1 INTRODUCCIÓN

El presente documento establece los lineamientos y normas para garantizar un adecuado control de acceso a los sistemas de información de la Fundación.

Para la Fundación es prioritario definir el personal que tiene acceso a información sensible, por lo cual, limita el acceso de usuarios de aplicaciones tecnológicas únicamente a los trabajadores y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial.

En tal sentido, se hace necesario controlar y restringir el acceso a toda la información sin importar si se encuentra en medios físico y/o digitales, garantizando así, la confidencialidad e integridad de ésta.

8.2 OBJETIVOS

- Gestionar y regular el personal que tiene permiso y atribuciones a los diferentes recursos, sistemas e información de la Fundación; limitando el acceso físico y lógico a solo aquellos usuarios autorizados con lo cual se previenen fugas de información y se protegen los datos sensibles.
- Reducir las brechas existentes ante el riesgo inminente de acceso no autorizado, pérdida y daño de la información de la Fundación, que se encuentran bajo la responsabilidad de los trabajadores de la Fundación.
- Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de la Fundación se encuentren debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

8.3 OBJETIVOS ESPECÍFICOS

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas y de la información.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de claves, equipos de cómputo e información.
- Garantizar la seguridad de la información cuando se utiliza computación móvil y/o trabajo remoto.

8.4 ALCANCE

El presente Lineamiento de control de accesos, es aplicable a todos los trabajadores de la Fundación, el cuerpo docente, directivos, proveedores, trabajadores, los consultores, contratistas y a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos, documentación, programas o servicios de información, sin importar la función que desempeñe en la Fundación independientemente de la sede.

8.5 RESPONSABLES

Todos los trabajadores.
Dirección de Informática y Tecnología (quien vela por el cumplimiento del presente Lineamiento para garantizar el adecuado control de acceso lógico y físico), consultores y contratistas de la FUNDACIÓN.

8.6 DESCRIPCIÓN DEL LINEAMIENTO DE CONTROL DE ACCESOS

La Fundación establece las medidas de control de acceso a toda la información propiedad de la Fundación, sin importar el medio en el que se almacene, procese, utilice, transmita, lo cual incluye, pero no limita a recursos de físicos y digitales; también a los ambientes públicos, privados, propios, de terceros o en nube; redes, sistemas operativos, aplicaciones, sistemas de información; servicios de TI, entre otros.

Los controles de acceso deben ser idóneos y robustos, con el fin de impedir el acceso no autorizado a los activos de información de la Fundación. Éstos deben ser conocidos por todos los trabajadores y terceras partes que cuentan con privilegios de acceso a la información y deben controlar los privilegios sobre los activos de información de acuerdo con lo permitido y según lo estrictamente necesario para el desempeño de su función. Se deben implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, bases de datos y servicios, estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

8.7 RESPONSABILIDADES DE LA DIRECCIÓN DE INFORMÁTICA Y TECNOLOGÍA

El responsable de la Seguridad y Privacidad de la Información estará a cargo de definir normas y procedimientos para la gestión de accesos e identidades a todos los activos de información, así como, de las instalaciones en donde se procesa o almacena información confidencial. Los accesos y privilegios deben ser limitados únicamente a personas autorizadas. Además, es responsable de:

- Definir las directrices y los lineamientos para la conexión a los activos de información, de forma segura y confiable.
- Verificar la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para el control de acceso a los activos de información y servicios de la Fundación, así como, verificar su cumplimiento y su efectividad.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de claves, utilización de servicios de red, uso controlado de utilitarios del sistema, registro de eventos, verificación de que se ejecuten los procesos de auditoría.
- Apoyar a los usuarios sobre el uso apropiado de claves y de equipos de trabajo. o Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Acceder a los registros de auditoría a fin de realizar el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

8.8 RESPONSABILIDAD DE LOS PROPIETARIOS DE LA INFORMACIÓN

Los propietarios de los activos de información deben determinar las normas de control de acceso y la asignación de los privilegios sobre ésta, de acuerdo con la política de seguridad de la información y el análisis de riesgos. Así mismo, son los responsables de:

- Identificar toda la información que corresponda a su área de responsabilidad cualquiera que sea su forma y medio de conservación.
- Clasificar todos los datos de su propiedad de acuerdo con el grado de criticidad de éstos y mantener un registro actualizado de la información más sensible.
- Autorizar el acceso sobre sus activos de información a trabajadores, contratistas o terceros de la Fundación, de acuerdo con sus respectivas funciones.
- Aprobar y solicitar la asignación de privilegios sobre la información a los diferentes usuarios, ya sea en situaciones rutinarias como excepcionales.

8.9 LINEAMIENTO PARA EL ACCESO A LA RED

El acceso a los activos de información y a los servicios y recursos tecnológicos provistos por la Fundación debe ser otorgado únicamente a los usuarios que les hayan sido otorgados específicamente dichos accesos según a las funciones y responsabilidades que tiene a su cargo.

- Son usuarios de red todos aquellos trabajadores y consultores externos que se encuentren en la Fundación.
- Para la gestión de identidades cada una de las cuentas de acceso se compone de un nombre de usuario o “username” y una contraseña o “password”. El nombre de usuario se determina por el nombre más el apellido del usuario, y la contraseña es generada por cada uno de los usuarios.
- El acceso a la red por parte de terceros se encuentra estrictamente restringido y permitido únicamente con previa autorización Dirección de Informática y Tecnología
- La gestión de contraseñas para el acceso a la red se realiza por medio de autorización de la Dirección de Informática y Tecnología.
- La Fundación cuenta con normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso. Cuenta con un inventario de control procedimental de gestión que protege el acceso a la información y a los servicios de red.
- La gestión de los usuarios para el ingreso a la red corporativa de la Fundación se realiza a través del Directorio Activo.
- El ingreso a la red corporativa se encuentra protegido, mediante el inicio seguro de sesión; los trabajadores tendrán acceso a la red corporativa en función del perfil asignado para el desarrollo de sus funciones, así mismo es de su responsabilidad cumplir los lineamientos de seguridad de la información establecidas para el acceso.

- El acceso privilegiado a la red debe otorgarse siguiendo el principio de otorgar la cantidad mínima necesaria de privilegios para que el usuario realice su trabajo de manera efectiva, de acuerdo con las necesidades específicas de su función laboral.
- Los trabajadores no deben acceder a sus dispositivos con privilegios de administrador.
- Todos los trabajadores y terceras partes jurídicas o naturales deben cumplir las Lineamientos de Seguridad y Privacidad de la Información y firmar todos los acuerdos y cláusulas estipuladas para tener acceso a los sistemas de información de la Fundación.

8.10 IDENTIFICACIÓN DE LOS EQUIPOS EN LAS REDES

La Fundación tiene identificados automáticamente los equipos, como medio para autenticar conexiones y ubicaciones específicas, indicando con claridad a qué red está permitido conectar el equipo, si existe más de una red y si éstas tienen sensibilidad diferente.

Los dispositivos de cómputo y comunicaciones tienen un nombre lógico que permite al administrador de red identificar la ubicación y responsable del mismo.

8.11 PROTECCIÓN DE LOS PUERTOS DE CONFIGURACIÓN Y DIAGNÓSTICO REMOTO.

El acceso lógico a los puertos de configuración y diagnóstico se controla con mecanismos de autenticación que restringe dicho acceso exclusivamente a los responsables de las actividades en los respectivos dispositivos. Los puertos, servicios o prestaciones instaladas en un dispositivo o red que no se requieren para la funcionalidad de la institución se inhabilitarán o retirarán una vez que no sean requeridos.

8.12 LINEAMIENTO DE ACCESO A INTERNET

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. Los accesos serán autorizados formalmente por el líder del área correspondiente y a cargo del personal que lo solicite. Así mismo, se debe dar un uso adecuado y racional por parte de los trabajadores.

8.13 LINEAMIENTO DE ACCESO A LAS APLICACIONES

- La Dirección de Informática y Tecnología es responsable de la creación, modificación, verificación, retiro o bloqueo de las cuentas de usuario. Aquellas cuentas de usuario redundantes no serán otorgadas a otros usuarios; de igual manera el responsable asegurará que los proveedores del servicio solo permitan el acceso a los usuarios autorizados de acuerdo con lo establecido en el Acceso a sistemas de información GDT-SDI-PR-002.
- El jefe de cada área de la Fundación es quien debe realizar la solicitud de creación o asignación de usuarios a las aplicaciones a la Dirección de Informática y Tecnología.

- Todos los sistemas y/o aplicativos cuentan con mecanismos de control de acceso y medidas de seguridad apropiadas para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Los usuarios solo pueden usar las redes y servicios de red para los cuales se les fue otorgado el permiso específico, los cuales son monitoreados.
- El acceso a la información debe ser gestionado mediante la autorización de administradores y la asignación de roles de control de acceso a las cuentas de la aplicación.
- Cada sistema y/o aplicación debe tener un sistema de gestión de contraseñas que utilice criterios de fuerza, longitud y complejidad.
- Se deben emplear medidas de seguridad adicionales, como certificados de dos factores o respaldados por hardware, cuando el acceso a los sistemas proviene desde el exterior.
- Se requiere la autenticación de doble factor como mínimo para acceder a servidores, y se sugiere implementar el mismo método en las estaciones de trabajo.

8.14 REVISIÓN Y RETIRO DE LOS DERECHOS DE ACCESO A USUARIOS

La Dirección de Informática y Tecnología será responsable de controlar los derechos de acceso a los usuarios (lectura, escritura, modificación y eliminación) y a otras aplicaciones, según solicitud del jefe de área encargado.

Los derechos de acceso a usuarios se revisan periódicamente, si se presentan cambios en los roles y/o responsabilidades de los trabajadores, estos deben ser autorizados por el jefe inmediato y modificados por parte de la Dirección de Informática y Tecnología.

La inactivación, bloqueo o retiro de acceso a usuarios en el caso de trabajadores: en vacaciones, licencias o terminación de contrato laboral se realiza con autorización enviada por el jefe dirección administrativa, Decanos y/o Coordinadores de programa Facultades, por medio de correo electrónico. Es responsabilidad del departamento de recursos humanos informar oportunamente a la Dirección de Informática y Tecnología sobre el personal que ha dejado de trabajar, para que se puedan cancelar sus cuentas de acceso.

La Dirección de Informática y Tecnología debe revisar las cuentas inactivas catalogadas así porque llevan más de 90 días sin movimiento, inactivas.

8.15 GESTIÓN DE PRIVILEGIOS

La Fundación aplica el principio de menor privilegio posible, que consiste en que sólo se otorgan los permisos necesarios para la ejecución de las funciones, por tal motivo, el departamento, dueño de la información es el responsable de autorizar formalmente los privilegios (permisos) o niveles de acceso correspondientes a las cuentas de los usuarios autorizados.

8.16 USO DE LAS UTILIDADES DEL SISTEMA

La Fundación adoptó buenas prácticas para restringir y controlar estrictamente el uso de programas utilitarios que puedan anular los controles del sistema, de la aplicación o herramientas del sistema. Se ha considerado las siguientes directrices para dicho control:

- Identificación, autenticación y autorización para las utilidades del sistema limitando su uso a la cantidad mínima de usuarios.
- Separación de las utilidades del sistema del software de aplicaciones y limitación de la disponibilidad de las utilidades y registro del uso de estas.
- Retiro e inhabilitación de todas las utilidades del sistema o el software, retiro de la disposición de las utilidades a los usuarios que tengan acceso a aplicaciones del sistema en donde se requiere distribución de funciones.

9 LINEAMIENTO DE DESARROLLO SEGURO

9.1 INTRODUCCIÓN

El Lineamiento de Desarrollo Seguro establece las reglas básicas para sus aplicaciones y/o servicios; aplica al desarrollo y mantenimiento de todos los servicios, arquitectura, software y sistemas de la cadena de valor de la Fundación.

9.2 OBJETIVO

Establecer por parte de la Fundación los lineamientos de Seguridad de la Información dentro del ciclo de vida de desarrollo de software.

9.3 ALCANCE

El presente Lineamiento aplica para los proveedores, a quienes se contrata para realizar los desarrollos para la Fundación, y se enmarca en los controles del SGSI.

Con el fin de crear y mantener mecanismos que incluyan los requerimientos de seguridad en todo el ciclo de vida de desarrollo de las aplicaciones, los desarrolladores revisarán y determinarán la acción a seguir para el tratamiento de las posibles vulnerabilidades, para evitar que tengan brechas que afecten la seguridad.

9.4 RESPONSABLES

Dirección de Informática y Tecnología

9.5 LINEAMIENTOS DE DESARROLLO SEGURO

La Fundación establecerá e implementará un conjunto de lineamientos y controles para garantizar la Seguridad de la Información durante todo el ciclo de vida de los desarrollos realizados por terceros a los sistemas de información de la Fundación

Para la Fundación es importante asegurar la confidencialidad, disponibilidad e integridad de la información que se encuentra almacenada en los diferentes sistemas de información, por esta razón se considera que para todas las fases del ciclo de vida de desarrollo de software se deben incluir requisitos de seguridad, y estos deben ser obligatorios, con el fin de minimizar vulnerabilidades que podrían aparecer en caso de no implementar planes de seguridad al desarrollo realizado.

- Se deben identificar, justificar, acordar y documentar los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software.
- Se deben incluir puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.
- El cambio de versión en el ambiente de producción debe contar con controles de seguridad, para esto se debe hacer una copia de respaldo en caso de que se deba dar marcha atrás, para mantener la integridad de los datos y de los sistemas de información.
- Se deben realizar pruebas de seguridad en el ambiente de pruebas, con el fin de identificar vulnerabilidades, las cuales deben ser resueltas antes del paso a producción.
- Los ambientes de desarrollo, pruebas y producción deben estar separados.
- Los usuarios y/o terceros que están involucrados en esta instancia, deben utilizar perfiles diferentes en el ambiente de desarrollo, pruebas y producción; además, asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente.
- 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.
- En caso de requerirse hacer copia de la información del ambiente de producción al ambiente de pruebas, se podrá realizar únicamente si la información se encuentra enmascarada, con el fin de que no se llegue a comprometer.

9.6 SUPERVISOR DE CONTRATO

Cuando los supervisores de los contratos de los proveedores relacionados con desarrollo de software evidencian una oportunidad de mejora con respecto a los servicios prestados por dichos proveedores en cuanto al ciclo de vida de desarrollo de software, esta debe ser informada de manera oportuna al Líder de seguridad de la Información o quien haga sus veces, y/o a la Dirección de Informática y Tecnología quien comunicará a la Vicerrectoría Financiera y Administrativa con el fin de tener en cuenta la etapa del contrato y los costos que podrían ocasionarse.

10 LINEAMIENTO DE GESTIÓN DE CONTRASEÑAS

10.1 INTRODUCCIÓN

El Lineamiento de Gestión de Contraseñas establece las normas para garantizar una adecuada gestión de las contraseñas y autenticación de acceso a los sistemas de información de la Fundación.

Al ser la Fundación consciente que el tratamiento diario de la información de la Fundación requiere el acceso a distintos servicios, dispositivos y aplicaciones por parte de los usuarios, para los cuales se requiere el uso de credenciales de acceso compuestas por un usuario y una contraseña. Por tanto, por seguridad de los servicios y sistemas en los que existen cuentas de usuarios para la autenticación, se garantiza que las credenciales de autenticación se generan, actualizan y revisan de forma óptima y segura.

10.2 OBJETIVOS

- Garantizar la seguridad de la información y de los sistemas informáticos de la Fundación, mediante la implementación de buenas prácticas que promuevan la protección y creación de contraseñas sólidas y seguras.
- Reducir las brechas existentes ante el riesgo inminente de acceso no autorizado, pérdida y daño de la información de la Fundación, que se encuentran bajo la responsabilidad de los trabajadores de la Fundación.
- Establecer, difundir y verificar el cumplimiento de buenas prácticas en el uso de contraseñas para los usuarios estándar y para los usuarios con privilegios de administrador de los diferentes sistemas de información.

10.3 ALCANCE

La presente es aplicable a todos los trabajadores de la Fundación y en general a la comunidad académica a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos, documentación, programas o servicios de información, sin importar la función que desempeñe en la Fundación e independientemente de la sede.

10.4 RESPONSABLES

Trabajadores de la Fundación y en general a la comunidad académica que cuente con un usuario asignado por la Fundación.

Dirección de Informática y Tecnología (quien vela por el cumplimiento del presente lineamiento para garantizar el adecuado control de acceso lógico y físico).

10.5 DESCRIPCIÓN DE LA LINEAMIENTO DE CONTRASEÑAS

La Fundación establece las medidas de control de acceso a toda la información propiedad de la Fundación, sin importar el medio en el que se almacene, procese, utilice, transmita, lo cual incluye, pero no limita a recursos de físicos y digitales; también a los ambientes

públicos, privados, propios, de terceros o en nube; redes, sistemas operativos, aplicaciones, sistemas de información; servicios de TI, entre otros, a través de asignación de usuarios y contraseñas de acceso personales e intransferibles a cada usuario de la Fundación.

Los controles de acceso son idóneos y robustos, con el fin de impedir el acceso no autorizado a los activos de información de la Fundación. Éstos son conocidos por todos los trabajadores y terceras partes que cuentan con privilegios de acceso a la información de la Fundación y deben controlar los privilegios sobre los activos de información de acuerdo con lo permitido y según lo estrictamente necesario para el desempeño de su función. Se deben implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, bases de datos y servicios, estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

10.6 SISTEMA DE GESTIÓN DE CONTRASEÑAS

Las contraseñas constituyen uno de los principales medios de validación y autorización de permisos a un usuario para acceder a un servicio informático. Los sistemas de administración de credenciales deben constituir una herramienta eficaz e interactiva que garantice contraseñas robustas. En este sentido, con el fin de evitar el acceso no autorizado a los sistemas informáticos y equipos de cómputo de la Fundación, el sistema de administración de credenciales a través de las contraseñas se indica que como mínimo deben cumplir con las siguientes condiciones:

- Imponer el uso de mecanismos de acceso individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas.
- Imponer el uso de contraseñas robustas y rechazar contraseñas débiles.
- Obligar a los usuarios a cambiar las claves temporales en su primer procedimiento de autenticación.
- Evitar mostrar las claves en pantalla cuando son ingresadas.
- Durante la inducción inicial a nuevos trabajadores, se debe explicar la importancia de las contraseñas y proporcionar instrucciones sobre cómo usarlas y protegerlas de manera adecuada.
- Las contraseñas empleadas deben ser robustas, difíciles de adivinar. Por ejemplo, una buena práctica es cambiar las letras por números o caracteres especiales.
- Uso de combinaciones. Las contraseñas utilizadas por los usuarios de la red corporativa de la Fundación deben cumplir con los siguientes requerimientos:

- ✓ La longitud de las contraseñas de ingreso a equipos de cómputo debe ser mínimo de diez (10) caracteres. Entre más caracteres tenga la contraseña es más difícil de descifrar por algún delincuente informático (hacker.)
- ✓ Contener caracteres alfabéticos (a-z, A-Z), es importante tener en consideración que se discrimina entre mayúsculas y minúsculas. Preferiblemente no consecutivas ni repetidas.

- ✓ Numéricos (0-9) Preferiblemente no números consecutivos ni repetidos.
- ✓ Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: “qwerty”, “asdf” o las típicas en numeración: “1234” o “98765”)
- ✓ No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
- ✓ Caracteres especiales (!@#$%^&*() _+|~- =\`{}[]:";'<>?,./) (Opcional).

- No se deben emplear palabras ni nombre de familiares o personales; se recomienda combinaciones entre números y letras que no puedan ser identificables fácilmente.
- Evite almacenar contraseñas de forma legible en archivos dentro de la computadora, en notas, en papeles o cualquier lugar accesible por personas no autorizadas.
- No divulgue las contraseñas por correo electrónico o teléfono.
- No es aconsejable activar la opción de recordar contraseña en navegadores web.
- Nunca comparta su usuario y contraseña con otras personas, como amigos, familiares o compañeros de trabajo. Compartirlos expone a las consecuencias de las acciones realizadas por otros con esas cuentas.
- Las credenciales asociadas a un usuario que se encuentre de vacaciones deberán ser inactivadas durante el periodo de vacaciones del trabajador.
- Si sospecha que alguien más conoce tu contraseña, cámbiala de inmediato o informa a tu jefe o informa a la mesa de soporte al correo: soporte.fusm@sanmartin.edu.co.
- Si olvida su contraseña o desea cambiarla, puede enviar un correo solicitando el restablecimiento a:soporte.fusm@sanmartin.edu.co.
- Para garantizar una mayor seguridad en línea, se aconseja el uso de un gestor de contraseñas. Este método implica el empleo de un administrador de contraseñas que opera con una única contraseña maestra. Con esta aplicación, es posible generar y recuperar las contraseñas de todas las cuentas, proporcionando así una capa adicional de protección para la información en línea.

10.6.1 RESTRICCIONES DE USO DE CONTRASEÑAS

- Las contraseñas utilizadas para el acceso a los equipos de cómputo y sistemas informáticos de la Fundación no deben utilizar cadena de caracteres duplicados, nombre de usuario del equipo, fechas de nacimiento o cualquier otro dato personal, conjuntos de letras o caracteres de fácil identificación (ejemplo: abcd1234).
- No se permitirá la reutilización de las últimas cuatro contraseñas.
- Se debe exigir el cambio de contraseña al primer uso acceso de los equipos de cómputo y sistemas informáticos; ya que las primeras fueron suministradas por la Dirección de Informática y tecnología y deben ser secretas, personales e intransferibles.

10.6.2 PRIVACIDAD DE LAS CONTRASEÑAS

La contraseña de acceso a los equipos de cómputo y sistemas de información de la Fundación de cada usuario es personal e intransferible, por tanto, cada usuario se compromete a no revelar, prestar, transferir y difundir sus contraseñas de acceso.

10.6.3 PERIODICIDAD DE LAS CONTRASEÑAS

Las contraseñas de acceso a los equipos de cómputo y sistemas de información de la Fundación deben ser cambiadas cada 90 días para los usuarios.

10.6.4 GESTIÓN DE CLAVES CRÍTICAS

En los diferentes ambientes de procesamiento existen códigos de usuarios con los cuales es posible efectuar actividades críticas como la instalación de plataformas o sistemas, habilitación de servicios, actualización de software y configuración de componentes informáticos. Dichas cuentas no serán de uso habitual, sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por claves con un mayor nivel de complejidad que el habitual. Las cuentas con accesos privilegiados deben ser controladas y gestionadas a través de los mecanismos necesarios para garantizar el gobierno y protección sobre éstas.

11 LINEAMIENTO DE USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN

11.1 INTRODUCCIÓN

La Fundación en su función de salvaguardar el uso adecuado de los activos de información de la Fundación y velar por que todos los usuarios de la información conozcan y apliquen los lineamientos y controles que ésta defina. La Fundación reconoce la información y los sistemas de información como un componente indispensable para el cumplimiento de sus objetivos estratégicos; por tanto, se compromete a adoptar lineamientos de seguridad de la información de alto nivel que permitan que sólo las partes interesadas y autorizadas que tienen la necesidad legítima en cumplimiento de sus funciones (confidencialidad) puedan acceder a los activos de información, que no se realicen modificaciones sin autorización, se salvaguarde su exactitud y completitud (la integridad), y que estén disponibles y utilizables cuando sean requeridos para el desarrollo de las actividades propias del negocio.

11.2 OBJETIVO

Establecer las especificaciones de seguridad para el uso aceptable de los activos de información pertenecientes a la Fundación Universitaria San Martín.

11.3 ALCANCE

Este documento define las directrices y lineamientos para garantizar que todo el personal de la Fundación Universitaria San Martín, incluidas las partes interesadas, trabajadores, contratistas o terceros, den buen uso a los activos de información de esta.

11.4 RESPONSABLES

Trabajadores de la Fundación Universitaria San Martín.
Comunidad Universitaria

11.5 GENERALIDADES

Por lo anterior, se establecen los siguientes lineamientos para el uso aceptable de los activos de información. Las personas son responsables del uso apropiado de los activos de la Fundación de acuerdo con los siguientes lineamientos, estándares y directrices establecidos por la compañía:

- Está prohibido compartir credenciales de acceso o contraseñas con otros usuarios, en caso de requerir soporte se debe iniciar sesión previamente, así mismo, no se puede ceder la sesión para que otros usuarios realicen actividades sobre estas, toda actividad realizada bajo las cuentas asignadas a cada usuario será responsabilidad de este ya sea él u otro usuario quien las ejecute y deberá comparecer los procesos disciplinarios definidos por la Fundación.
- La Fundación como propietario de los equipos, cuentas y/o buzones de correo electrónico podrá acceder a cualquier cuenta de un empleado sin previa autorización de éste, siempre y cuando exista sospecha de actos ilícitos, extorsiones u otro acto que amerite dicha intervención.
- Se prohíbe la transmisión de mensajes por cualquier medio que pueda comprometer hostigamiento de raza, edad, sexo, religión, política, nacionalidad, origen, incapacidad u orientaciones personales, comentarios despectivos, noticias informales o mal intencionadas, mensajes masivos de índole personal y en general, cualquier tipo de información que cause congestión en la red o interfiera con el trabajo de otros.
- Se prohíbe el uso de medios de almacenamiento en la nube, correos electrónicos, mensajería instantánea, entre otros de propiedad personal para guardar y/o transferir información sensible o critica corporativa.
- La comunicación o el intercambio de documentos corporativos con contactos externos o internos deberá realizarse exclusivamente a través de las cuentas de correo electrónico o mensajería instantánea asignadas por la Fundación.
- Es responsabilidad de la Fundación entregar al trabajador y/o contratista un equipo de cómputo bajo previa solicitud con el software estándar corporativo (sistema operativo, herramientas de ofimática, navegador, antivirus, aplicaciones y políticas o lineamientos de seguridad) definido para la Fundación.
- Por motivos de seguridad, cumplimiento y mantenimiento, el personal autorizado de la Dirección de Informática y Tecnología podrá monitorear y auditar el equipo, los sistemas, aplicaciones, el tráfico de la red y demás plataformas o servicios tecnológicos prestados de acuerdo con al presente lineamiento y demás directrices relacionadas al control de acceso.
- La Fundación no faculta, ni autoriza a ningún trabajador o consultor externo a establecer un acuerdo o ejecutar el pago por rescate de información en caso de ser víctima de ciberataque, infección (malware) o secuestro de información (Ransomware).

11.6 LINEAMIENTO DE USO DE LOS EQUIPOS DE CÓMPUTO O SISTEMAS INFORMÁTICOS

Los computadores, cuentas de usuario, teléfonos (incluyendo los celulares), buzones de correo de voz y otros recursos similares que son propiedad de la Fundación, son asignados para asistir a sus trabajadores en el desempeño de su trabajo diario.

- Es responsabilidad de cada trabajador de la Fundación velar por el transporte, cuidado y buen uso de los equipos tecnológicos asignados. Dado que los equipos portátiles son especialmente sensibles a robo o pérdida y requieren unas medidas de seguridad más altas. En ningún momento se deben dejar descuidados en sitios públicos.
- El Coordinador de soporte o quien haga sus veces es responsable de que ningún activo de información adquirido y que sea parametrizable, deberá ser instalado con la configuración por defecto de fábrica, se deben eliminar claves por defecto y establecer cuentas de administrador y cuentas de usuario seguras.
- La Dirección de Informática y Tecnología es la responsable que todo activo de información parametrizable sea configurado de acuerdo con los parámetros establecidos por la Fundación, eliminando toda configuración.
- La Dirección de Informática y Tecnología es el único autorizado para realizar actividades de soporte preventivo y/o correctivo a los equipos de cómputo y/o servidores tales como: instalación y/o desinstalación de software, cambios de configuración, limpieza, optimizaciones del sistema operativo, cambios de protector de pantalla, fondos, entre otros.
- Solo podrán ser instalados componentes de software y hardware adquiridos por la Fundación, ningún usuario se encuentra autorizado para adquirir o ejecutar instalación de ningún tipo de software o herramientas, en caso de necesitar, deberá hacer una solicitud directa al jefe inmediato, así como la Dirección de Informática y Tecnología quien evaluará y definirá el proceso de adquisición.
- La Dirección de Informática y Tecnología es el único autorizado para asignar o reasignar equipos y/o periféricos tecnológicos, ningún usuario podrá auto asignarse hardware (monitores, teclados, ratón entre otros) sin autorización previa.
- La Dirección de Informática y Tecnología deberá garantizar que el software estándar esté siempre actualizado, así como los parches de seguridad de Windows y firmas de antivirus.
- Los equipos de cómputo asignados deben ser devueltos en buen estado a la Dirección de Informática y Tecnología, cuando el empleado o proveedor responsable de dicho equipo finalice su vinculación con la Fundación.

11.7 LINEAMIENTOS DE USO DEL HARDWARE Y SOFTWARE

Corresponde a la Dirección de Informática y Tecnología, proveer las especificaciones técnicas de cualquier equipo informático, la instalación de software y equipos computacionales, como también la realización de las pruebas técnicas respectivas.

- Todo equipo de cómputo (impresora, scanner, monitor y otros recursos informáticos) perteneciente a la Fundación o en uso bajo cualquier modalidad de contratación, deberá permanecer en el lugar asignado por la institución. El traslado o cambio de cualquier equipo debe ser autorizado por el Director de Informática y Tecnología.
- No deben abrir o romper los sellos de seguridad instalados en cada computador y/o equipo por la Dirección de Informática y tecnología.
- No abrir, retirar o cambiar componentes de los equipos.
- Evitar prestar e intercambiar los equipos de cómputo.
- Evitar instalar dispositivos o periféricos sin la supervisión y autorización expresa de la Dirección de Informática y Tecnología.
- No retirar o sacar equipo de la institución sin previa autorización del área de almacén.
- El usuario deberá mantener los archivos de su equipo ordenados, siendo de su responsabilidad conservar espacio suficiente en el disco duro para poder ejecutar sus aplicaciones.
- Se debe respetar la propiedad intelectual y licencias.

11.8 LINEAMIENTOS DE USO DE LA INFORMACIÓN IMPRESA

- El material impreso producido utilizando los recursos de tecnología de la Fundación, debe ser tratado con la misma precaución con la que se manejan los datos almacenados electrónicamente. Todo el material impreso debe ser tratado de acuerdo con los lineamientos de seguridad establecidos por la Fundación.
- El envío de material impreso que contenga información confidencial o estrictamente confidencial, a través de correo físico, debe ser enviado con las medidas necesarias para garantizar su protección, confidencialidad e integridad y emplear sobre sellado marcado con una etiqueta que lo distinga y que indique que es “sólo para el destinatario”.
- Cuando se requiera el envío de información confidencial o restringida de la Fundación, se deben utilizar servicios que permitan realizar seguimiento y trazabilidad del material enviado como los servicios de correo certificado.
- Para prevenir cualquier lectura no autorizada o búsqueda de información, en dispositivos de reproducción de información como impresoras, fotocopiadoras, multifuncionales, entre otras, no se debe dejar abandonado el material impreso.
- Los documentos que contienen información sensible se deben retirar de las impresoras inmediatamente.

- Todo el material impreso que no sea retirado de los dispositivos de reproducción podrá ser destruido.

11.9 DESTRUCCIÓN DEL MATERIAL IMPRESO

El material impreso con información interna, confidencial o restringida debe ser destruido utilizando una máquina de destrucción de papel, o debe romperse en varios pedazos y, en todo caso, debe distribuirse en diferentes depósitos de papel.

Por ningún motivo material con información interna, confidencial o restringida debe ser reutilizado.

11.10 GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Fundación mantiene los activos de información claramente identificados, referenciados, inventariados y actualizados.

Como mínimo una vez al año o si se presenta alguna novedad con periodicidad inferior al Comité de Seguridad de la Información la revisión detallada de los inventarios de los activos de información de la Fundación, con el objetivo de verificar que todos los activos se encuentren actualizados, asegurando la disponibilidad, confidencialidad e integridad de la información allí relacionada.

Toda adquisición de hardware, así como cambios de ubicación física de los mismos, requiere la evaluación técnica y aprobación por parte de la Dirección de Informática y Tecnología, quién es la encargada de controlar los activos de información dentro de la compañía.

11.11 LINEAMIENTOS DE USO DE SERVICIO DE INTERNET

Se deben adoptar las medidas necesarias para propiciar el correcto uso del servicio de Internet, con el propósito de minimizar los riesgos para la FUNDACIÓN, derivados de su uso.

- El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la Fundación y, debe ser utilizado por los trabajadores y contratistas para realizar las funciones establecidas bajo su cargo.
- Los trabajadores y/o contratistas son responsables de mantener su imagen profesional dentro de internet, así como proteger la imagen y reputación de la Fundación.
- No está permitido el acceso a páginas cuyo contenido pueda resultar ofensivo o puede llegar a atentar contra la dignidad humana. Así mismo, no se permite el acceso a páginas de contenido no adecuado, ilegal o poco ético.
- No visitar páginas no fiables o sospechosas con el fin de evitar posibles incidentes de seguridad y privacidad de la información.

- En ninguna circunstancia se podrá dejar configuraciones y contraseñas por defecto en los sitios web, como credenciales de acceso a correo o cuentas bancarias, entre otros.
- Se debe garantizar que el acceso al servicio de internet por parte de personal externo y que se encuentre dentro de las instalaciones de la Fundación se encuentra configurado en segmentos totalmente independientes a los segmentos de red, para evitar accesos no autorizados a la información.
- Se encuentra prohibida la descarga, reproducción y acceso a sitios web de música, videos, emisoras, televisión online, películas, descarga de software ilegal o no licenciado entre otros. Así mismo, la publicación, envío o adquisición de material sexualmente explícito, discriminatorio, todo aquello que implique un delito informático.
- Se prohíbe la publicación de anuncios comerciales o material publicitario a nombre de la Fundación, salvo del área asignada para ello por parte de la Institución.
- Se prohíbe promover, asuntos o negocios personales bajo la navegación de internet de la Fundación.
- Se prohíbe la divulgación, él envió de documentos o aplicaciones con fines maliciosos o ilegales a nombre de la Fundación.
- El uso de Internet no definido dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la seguridad de la información.

11.12 LINEAMIENTOS DE USO DEL CORREO ELECTRÓNICO

- Las cuentas de correo electrónico de la Fundación son un servicio de red que permite a los usuarios de la Fundación enviar y recibir mensajes para el desarrollo de sus funciones. En este sentido todos los usuarios, trabajadores y/o consultores externos que la requiera para el desempeño de sus funciones el mismo, deben asegurar el buen uso del recurso para garantizar la protección del servicio y de la información de la Fundación.
- Se asigna un buzón de correo electrónico previa solicitud del jefe inmediato pertinente (área a la que ingresa), se creará teniendo en cuenta el usuario asignado para acceder a la red y el dominio @sanmartin.edu.co.
- Tanto los mensajes y la información contenida en los buzones de correo son de propiedad de la Fundación, cada usuario como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Las cuentas de correo electrónico asignadas por la Fundación son de carácter corporativo por tal razón no podrán ser usadas para registros personales como cuentas en redes sociales, entidades bancarias, registros de páginas web, universidades o cualquier otro, salvo previa autorización y que sea necesario para el cumplimiento de sus funciones. A su vez, estas cuentas son de carácter personal e intransferible y por tanto no se debe ceder el uso de la cuenta a terceros.

- Todos los mensajes o correos electrónicos enviados deben respetar el estándar de formato e imagen corporativa definido y deben conservar, en todos los casos, el mensaje legal institucional de confidencialidad.
- La Fundación establecerá métodos de control y seguridad para el acceso a las cuentas o buzones de correo electrónicos, sin embargo, es también responsabilidad del usuario identificar con claridad los remitentes del correo recibido, validando su veracidad al igual evitar abrir archivos de remitentes desconocidos o archivos no solicitados.
- La clave de acceso al servicio de correo electrónico no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión se debe seguir los controles de protección de contraseñas definidos por el Sistema de Gestión de Seguridad de la Información.
- Toda información generada que requiera ser transmitida fuera de la compañía, y que por sus características de confidencialidad e integridad debe ser protegida, es importante exportar en formatos no editables como (PDF) y con mecanismos de seguridad (contraseñas y cifrado). Sólo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

  La Fundación protege el servicio de correo electrónico y los activos de información que pueden ser accedidos a través de éste, frente a las amenazas y vulnerabilidades identificadas de los resultados de la gestión de riesgos de seguridad digital, como la suplantación de identidad, el acceso no autorizado a información, indisponibilidad del servicio, y en general cualquier riesgo que afecte la disponibilidad, confidencialidad e integridad de la información.

- Los siguientes usos del servicio de correo electrónico se consideran usos no autorizados y prohibidos los siguientes:

  - Envío de correos masivos sin autorización oficial.
  - Está estrictamente prohibido el envío de cadenas.
  - Envío, reenvío o intercambio de mensajes no deseados o considerados spam.
  - Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, cualquier contenido que represente riesgo para la seguridad de la información de la Fundación o esté prohibido por la leyes, regulaciones o normas a las cuales está sujeta la Fundación.
  - Creación, almacenamiento o intercambio de mensajes que violen las leyes de material protegido por la ley de derechos de autor, normas sobre seguridad de la información y protección de datos personales.

- Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario, o Abrir, usar o revelar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.

11.13 ARCHIVOS ADJUNTOS Y CONTENIDOS EN LOS CORREOS ELECTRÓNICOS

- Enviar archivos adjuntos en los correos electrónicos es una de las formas más fáciles de transmitir un virus. Por tanto, se debe prestar especial atención para asegurar que los archivos recibidos correspondan con una fuente confiable. Su contenido debe ser conocido antes de ser abierto o enviado.
- Los archivos recibidos serán chequeados automáticamente por el sistema, para verificar si contienen programas maliciosos. Si un correo electrónico tiene archivos con programas maliciosos, los archivos serán removidos automáticamente del correo.
- El emisor de un correo debe describir lo que contiene el(los) archivo(s) que anexa.
- El correo debe tener, al menos, la siguiente información:
  - Número de archivos.
  - Nombre y extensión de cada uno.

- No abrir archivos que se encuentren en correos electrónicos recibidos de remitentes desconocidos.

11.14 CONFIDENCIALIDAD

La información confidencial o reservada no debe ser enviada por correo a través de redes públicas (por ejemplo, Internet) a menos que vaya protegida.

En los casos en los que se requiera envío o recepción de información pública clasificada con carácter reservado, el usuario del servicio de correo electrónico debe cifrar dicha información, de acuerdo con los lineamientos establecidos.

Se debe garantizar que la información se protege adecuadamente al ser enviada por el servicio de correo electrónico corporativo, para lo cual se debe escribir en el asunto del correo la clasificación de la información que está enviando.

11.15 REENVÍO DE CORREO ELECTRÓNICO

El reenvío de mensajes con información confidencial o restringida está prohibido.

La información enviada por correo electrónico por defecto está clasificada como interna. Los usuarios deben tener cuidado al enviar mensajes, debido a que puede no ser apropiado distribuirlos.

El uso de reglas que permitan reenviar de manera automática correos electrónicos a direcciones que no sean de la Fundación (direcciones externas) está prohibido.

Cuando se responde o reenvía un mensaje se deben revisar las direcciones de correo a las cuales se va a remitir dicha respuesta o reenvío. Además, deben borrarse todas las direcciones que pudieran aparecer en el correo enviado con anterioridad y que aparezcan reflejadas en el nuevo correo reenviado o respondido.

11.16 TRATAMIENTO DE CUENTAS DE CORREO ELECTRÓNICO CUANDO UN TRABAJADOR SE RETIRA

Se deberá realizar una copia de respaldo para la cuenta y almacenarla según lo establecido en el lineamiento de respaldo de la Fundación.

Se debe contar con los procedimientos e instructivos necesarios para el restablecimiento de las cuentas que hayan sido eliminadas y que sea necesaria su recuperación.
El superior jerárquico debe definir el tiempo de retención de dicha información o quedar como responsable de la misma, según los intereses y necesidades del área.

11.17 CUENTAS DE CORREO ELECTRÓNICO INACTIVAS

Periódicamente se debe realizar la revisión de las cuentas que llevan más de 60 días sin ningún acceso, en caso tal, se procederá a enviar una comunicación de las cuentas sin uso al propietario de la cuenta y/o al responsable superior inmediato para obtener respuesta de la actividad de esta y se darán 30 días adicionales a partir de la fecha de la comunicación para la utilización de la cuenta. Vencidos los treinta días, de no presentarse uso y/o respuesta del responsable superior inmediato, se procederá a su eliminación y se entenderá que el usuario ya ha sido comunicado y se tomaran las medidas necesarias para hacer uso de la licencia.

11.18 USO DE VIDEOCONFERENCIA Y MENSAJERÍA INSTANTÁNEA

La Fundación restringe el uso de programas de Mensajería Instantánea que no están bajo el control de la compañía, con el objetivo de incorporar buenas prácticas sobre la seguridad de la información, lo únicos medios para ejecutar o establecer una videoconferencia y/o mensajería instantánea son Zoom, Microsoft Teams y Meet.

No se permite enviar o recibir por este medio archivos confidenciales, sensibles o de alta criticidad.

Está prohibido descargar documentos, aceptar invitaciones o enlaces de conexión desconocidos o de dudosa procedencia.

11.19 RECURSOS COMPARTIDOS

El trabajador que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.

Se debe definir el tipo de acceso y los permisos estrictamente necesarios sobre la carpeta (lectura, ejecución, escritura, modificación y borrado).

El acceso a carpetas compartidas debe delimitarse a los trabajadores que las necesitan y deben ser protegidas con contraseñas.

11.20 CONTROL DE ACCESO FÍSICO

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

Los ingresos y salidas de personal a áreas restringidas de tecnología de la Fundación deben ser registrados; por consiguiente, los trabajadores y proveedores deben cumplir completamente con los controles físicos implementados.

Los trabajadores y consultores externos deben portar el carnet que los identifica en un lugar visible; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible a la Dirección de Recursos Humanos.

Los visitantes pueden ingresar y permanecer en las áreas restringidas solamente cuando esté presente un empleado designado; quien debe acompañar al visitante durante toda su estadía en las instalaciones.

12 NO CUMPLIMIENTO

Todos los trabajadores de la Fundación, comunidad académica, proveedores y demás terceros relacionados con los activos de información de la institución tienen la responsabilidad de cumplir esta Política y Lineamientos de Seguridad de la Información. Cualquier incumplimiento, que ponga en riesgo algún aspecto de Seguridad de la Información y Ciberseguridad, puede constituir una falta y se aplicarán las sanciones pertinentes.

Los proveedores de la Fundación, que tengan a su cargo el desarrollo de software, tienen la obligación de cumplir con los Lineamientos de seguridad de la información establecidos

por la Fundación cualquier incumplimiento a las mismas y que puedan poner en riesgo algún aspecto del SGSI constituye una falta la cual conlleva a sanciones.

El incumplimiento de la política general y los Lineamientos del SGSI afectan a nivel normativo y operativo, esto trae consigo consecuencias administrativas, disciplinarias o legales relacionadas con la seguridad y la privacidad de la información.

13 DOCUMENTOS DE REFERENCIA

El presente documento se basa en las buenas prácticas, leyes y normas relacionadas con la seguridad de la información:

13.1 Lineamiento de uso de dispositivos móviles

- Procedimiento GDT-SDI-PR-001 Asignación de equipos a funcionarios.
- Procedimiento GDT-SDI-PR-002 Acceso a sistemas de información.
- Norma ISO 27001:2022 bajo la guía de controles ISO 27002:2022. Anexo 5.2. Funciones y responsabilidades en materia de seguridad de la información; 7.8 Ubicación y protección de equipos; 8.1 Dispositivos finales del usuario.

13.2 Lineamiento de uso de internet

- ISO NTC/IEC 27001:2022, Anexo 27002:2022 8.3 Restricción del Acceso a la Información; 8.12 Prevención de la fuga de datos, 8.23 Filtrado Web.
- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

13.3 Lineamiento de respaldo, almacenamiento y recuperación de información

- ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información (SGSI), Anexo B. 8.13.
- ISO 22301:2019 – Seguridad de la Sociedad: Sistemas de Continuidad del Negocio.
- La ley 594 de 2000 Ley General de Archivos.

13.4 Lineamiento seguridad de la información en la relación con proveedores

Norma Técnica Colombiana NTC-ISO/IEC 27001:2022 Anexo 5.19 Seguridad del Información en las relaciones con proveedores. Anexo 5.20 Abordar la Seguridad de la información en los acuerdos con los proveedores; 521 Gestión de la Seguridad de la Información en la Cadena de Suministro.

13.5 Lineamiento de escritorio y pantalla limpia

Norma ISO 27001:2022 Anexo 7.7. Lineamiento de escritorio y pantalla limpios.

13.6 Lineamiento de control de accesos

ISO NTC/IEC 27001:2022 Anexo A. 5.15 Control de Acceso y A 5.16 Gestión de Identidad.

13.7 Lineamiento de desarrollo seguro

Norma ISO 27001:2022 bajo la guía de controles ISO 27002:2022. Anexo 8.25 Lineamiento de Desarrollo Seguro; 8.30 Desarrollo tercerizado

13.8 Lineamiento de gestión de contraseñas

ISO NTC/IEC 27001:2022 Anexo A.5.17 Información de autenticación.

13.9 Lineamiento de uso aceptable de activos de información

ISO 27001:2022 Anexo A 5.2. Funciones y responsabilidades en materia de seguridad de la información; 5.10 Uso aceptable de la información y otros activos asociados.

FUNDACIÓN UNIVERSITARIA SAN MARTÍN-Nit: 860.503.634-9
Personería Jurídica N° 12387 de Agosto 18 de 1981 Ministerio de Educación
Sede Norte: Carrera 18 No. 80-06 PBX: (1) 530-1001
Sede Calle 60: Calle 61A No. 14-28
www.sanmartin.edu.co

www.sanmartin.edu.co