



POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**Aprobado por el Consejo Académico
Acta 028 del 21 de septiembre de 2021**

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA FUNDACIÓN UNIVERSITARIA SALESIANA

OBJETIVOS	3
APLICABILIDAD	3
PRINCIPIOS RELACIONADOS CON LA GESTIÓN DE LA INFORMACIÓN	4
RESPONSABILIDAD	5
LINEAMIENTOS	6
ACCESO A SISTEMAS Y RECURSOS DE INFORMACIÓN INSTITUCIONAL	6
USO DE LAS CUENTAS Y GESTIÓN DE CONTRASEÑAS DE ACCESO	6
INFRAESTRUCTURA DE COMUNICACIONES Y DE LOS SERVICIOS DE INTERNET	7
USO DEL CORREO ELECTRÓNICO INSTITUCIONAL	8
DEFINICIONES	9

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Fundación Universitaria Salesiana con respecto a la protección de sus activos de información¹, que soportan los procesos institucionales y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información, por medio de la generación y publicación de principios, políticas, lineamientos, procedimientos y guías, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Objetivos

- Establecer los procedimientos y guías en materia de seguridad y privacidad de la información.
- Cumplir con los principios de seguridad de la información definidos en la Política de Seguridad y Privacidad de la Información.
- Orientar a las instancias de decisión de SALESIANA en materia de Seguridad y Privacidad de la Información, de acuerdo con los requerimientos institucionales y normativos.
- Preservar y administrar la información producida por los procesos de SALESIANA por medio de tecnologías de ciberseguridad, con el fin de garantizar el cumplimiento de las características de confidencialidad, integridad, disponibilidad y no repudio de la Información.
- Mantener la Política de Seguridad y Privacidad de la Información actualizada y vigente de acuerdo con los requerimientos institucionales y normativos.
- Fortalecer la cultura de seguridad de la información en los estudiantes, profesores, administrativos, contratistas, terceros y demás miembros de la Comunidad Universitaria.

Aplicabilidad

Esta política aplica a toda la institución, miembros y unidades académicas y administrativas de SALESIANA, a sus procesos institucionales², a externos

¹ Estudiantes, profesores, administrativos, otros miembros de la comunidad universitaria, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software.

² Procesos estratégicos, misionales y de apoyo.

vinculados por medio de contratos de prestación de servicios, convenios, acuerdos con la Institución y a todo el personal que haga uso de los servicios de TI, sistemas de información e infraestructura tecnológica de la Fundación Universitaria Salesiana.

Principios relacionados con la gestión de la información

Entendiendo la importancia de una adecuada gestión de la información, la Dirección de Tecnologías de la Información de la **FUNDACIÓN UNIVERSITARIA SALESIANA** se compromete con la implementación del modelo de gestión de seguridad y privacidad de la información con el fin de garantizar la disponibilidad, confidencialidad e integridad de las fuentes de información de SALESIANA.

Los principios son reglas generales y directrices para guiar y apoyar a SALESIANA en el logro de sus metas y objetivos institucionales. A continuación se describen los principios relacionados con la gestión de la información:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los miembros de la Comunidad Universitaria.
- **SALESIANA** protegerá la información creada, procesada, transmitida o resguardada por sus procesos estratégicos, misionales y de apoyo, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.
- **SALESIANA** protegerá su información de las amenazas originadas por parte de los miembros de la Comunidad Universitaria.
- **SALESIANA** protegerá las instalaciones físicas de comunicaciones, procesamiento y la infraestructura tecnológica que soporta sus procesos estratégicos, misionales y de apoyo.
- **SALESIANA** implementará controles de acceso a la información, sistemas de información y recursos de comunicaciones.
- **SALESIANA** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información institucionales.
- **SALESIANA** garantizará la disponibilidad de sus procesos estratégicos, misionales y de apoyo y la continuidad de su operación basada en el impacto que pueden generar los eventos.

Responsabilidad

- La Dirección de Tecnologías de la Información diseñará y elaborará la propuesta de políticas de seguridad de Información que serán presentadas al Comité de Rectoría y demás instancias de decisión de la **FUNDACIÓN UNIVERSITARIA SALESIANA**.
- La Dirección de Tecnología de la Información será la responsable de definir las estrategias de capacitación o formación en materia de Seguridad de la Información al interior de **SALESIANA**.
- La Dirección Administrativa y Financiera cumplirá la función de notificar a través de la Unidad de Gestión Humana, a todo el personal que se vincule contractualmente con **SALESIANA**, de las obligaciones respecto del cumplimiento de la Política de Seguridad y privacidad de la Información y de todos los lineamientos, procesos, procedimientos y orientaciones que surjan de la Seguridad de la Información. De igual forma, la Dirección de Tecnología de Información será la responsable de la notificación de la Política y los cambios que de ella se produzcan a todos los miembros de la Comunidad Universitaria, por medio de los canales institucionales.
- Para la asignación de la cuenta institucional, la unidad de Gestión Humana debe crear la solicitud en la mesa de servicios o a través del correo electrónico soporteti@salesiana.edu.co.
- Los miembros de la Comunidad Universitaria y personal que haga uso de los servicios de TI, sistemas de información e infraestructura tecnológica son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.
- La Dirección de Tecnologías de Información será responsable de realizar auditorías periódicas sobre los servicios de TI, sistemas de información e infraestructura tecnológica. Es su responsabilidad informar sobre el cumplimiento de los lineamientos y medidas de seguridad establecidas por esta Política y por los procesos, procedimientos y orientaciones que de esta surjan.

Lineamientos

Acceso a sistemas y recursos de información Institucional

- Los miembros de la Comunidad Universitaria que tengan una vinculación laboral con la Fundación Universitaria Salesiana, tendrán asociada cuentas de acceso a los sistemas de información y servicios de tecnologías de información, de acuerdo con su rol en la Institución.
- La creación y asignación de cuentas institucionales, se realizará una vez Gestión Humana o un Líder de proceso, realice la solicitud mediante la mesa de servicios o a través del correo electrónico soporteti@salesiana.edu.co.
- Las unidades académicas y administrativas, podrán solicitar la asignación de permisos y privilegios de sus cuentas de usuario para los diferentes sistemas y servicios de tecnologías de información. Dicha solicitud se debe realizar mediante la mesa de servicios o a través del correo electrónico soporteti@salesiana.edu.co.
- SALESIANA tiene la potestad de suspender la cuenta institucional de cualquier miembro de la Comunidad Universitaria, cuando determine que en el uso de la misma o de los sistemas de información o servicios de tecnologías de información, el usuario ha violado las Políticas de Seguridad y Privacidad de la Información y condiciones de uso o la legislación colombiana vigente.
- Cuando existan indicios de una indebida utilización de los sistemas de información académicos y administrativos, así como los servicios de tecnologías de información, SALESIANA podrá acceder a los contenidos del usuario de forma unilateral.
- Al finalizar la relación laboral o contractual entre un miembro de la Comunidad Universitaria y SALESIANA, la unidad de Gestión Humana deberá informar a la Dirección de Tecnologías de la Información, para que se suspenda la cuenta, privilegios y permisos otorgados.

Uso de las cuentas y gestión de contraseñas de acceso

- Los miembros de la Comunidad Universitaria deben hacer un uso responsable de sus cuentas y contraseñas institucionales.
- La Dirección de Tecnologías de la Información no solicitará a ningún miembro de la Comunidad Universitaria sus contraseñas; en este sentido, los miembros no deberán compartirlas con terceros o miembros del equipo de la Dirección de Tecnologías de la Información. En los casos especiales en los que se requiera compartir una contraseña con el equipo de tecnología, la contraseña deberá ser cambiada una vez finalizada la actividad o soporte requerido.

- Las contraseñas de acceso al sistema de información académico y administrativo, correo institucional y demás servicios de TI no deben ser guardadas, registradas o almacenadas en computadores asignados, portátiles o dispositivos móviles.
- Los miembros de la Comunidad Universitaria, que sospechen o evidencien comportamientos irregulares o anómalos a través de sus cuentas asignadas, como accesos indebidos o mensajes no autorizados, debe cambiar su contraseña de forma inmediata y reportar este incidente de seguridad mediante la mesa de servicios o a través del correo electrónico soporteti@salesiana.edu.co.

Infraestructura de comunicaciones y de los servicios de internet

- Los miembros de la Comunidad Universitaria, deberán abstenerse de enviar material ofensivo o contenidos difamatorios.
- Los miembros de la Comunidad Universitaria, deberán responder por cualquier actividad llevada a cabo desde sus cuentas institucionales de acceso a los sistemas de información³ y servicios de tecnologías de información. Por lo anterior, cada usuario, se compromete a no transferir sus cuentas de acceso a los sistemas de información, compartirlas, prestarles, cederlas y a mantener la confidencialidad, control y buen manejo de su contraseña.
- Los miembros de la Comunidad Universitaria, deberán abstenerse de realizar acceso no autorizado o intento de pruebas, verificación o escaneo de vulnerabilidades de sistemas o redes, violentar medidas tecnológicas de seguridad o de autenticación local o de terceros, sin la expresa autorización de la Dirección de Tecnologías de la Información de SALESIANA.
- Los miembros de la Comunidad Universitaria, deberán abstenerse de hacer uso de los servicios tecnológicos con fines comerciales o publicitarios, o buscar beneficio económico a través de ellos.
- Los miembros de la Comunidad Universitaria, deberán abstenerse de congestionar los enlaces de comunicación o sistemas de información mediante la transferencia o ejecución de archivos o programas que no son de uso propio en el ambiente laboral o académico.
- Los miembros de la Comunidad Universitaria no tienen permitido vulnerar las restricciones que la Fundación Universitaria Salesiana tiene previstas, para realizar corrupción o destrucción de datos, o de cualquier acción que pueda impedir el acceso legítimo a estos, incluyendo difusión de virus, troyanos o cualquier tipo de software malicioso a usuarios, redes o servidores de la red de SALESIANA.

³ Sistema de Información académico y administrativo INTEGRA, BrightSpace, Google Workspace, Symphony, Porfolio, entre otros.

- Los miembros de la Comunidad Universitaria, deberán abstenerse de instalar software, cuando se trate de equipos de propiedad de SALESIANA, sin la autorización y licencia adecuada o procedente de alguna fuente no autorizada.
- Los miembros de la Comunidad Universitaria, deberán abstenerse de vulnerar las restricciones que SALESIANA tiene previstas en el uso de la red para el entretenimiento, conexión a redes P2P, sitios de pornografía u otros de similar naturaleza.
- Los miembros de la Comunidad Universitaria, deberán abstenerse de instalar dispositivos de red como Routers, Switches, Access Point, entre otros, sin previa autorización de la Dirección de Tecnologías de Información de SALESIANA.
- Los miembros de la Comunidad Universitaria, deberán evitar cualquier conducta ilegal de acuerdo con la legislación aplicable de cualquier país al que se puede tener acceso por la red.
- Los miembros de la Comunidad Universitaria, deberán informar a la Dirección de Tecnologías de la Información o a los administradores de los servicios de internet, según el caso, sobre incidencias, problemas o irregularidades relacionados con la infraestructura de comunicaciones y de los servicios de tecnologías de información, para que se puedan aplicar los correctivos oportunamente.

Uso del correo electrónico institucional

- Los miembros de la Comunidad Universitaria, deberán utilizar el correo electrónico institucional exclusivamente para las actividades propias de la Fundación Universitaria Salesiana, para el desempeño de las funciones o actividades propias dentro de los procesos y no se debe utilizar para otros fines.
- Los miembros de la Comunidad Universitaria, deberán utilizar de manera adecuada, razonable y sin generar riesgos para la operación de la Infraestructura tecnológica y sistemas de información.
- Todos los miembros de la comunidad universitaria deberán dar cumplimiento a la ley 1273 de 2009 de delitos informáticos.
- El servicio de correo electrónico institucional debe ser empleado para servir a una finalidad académica y administrativa de SALESIANA. Todas las comunicaciones establecidas mediante este servicio, se consideran como propiedad de SALESIANA y pueden ser revisadas por el administrador del servicio, en caso de una investigación o incidentes de seguridad de la información.

- El tamaño del buzón de correo electrónico se asigna de manera estandarizada, la capacidad específica es definida y administrada por la Dirección de Tecnologías de Información.
- Todos los miembros de la Comunidad Universitaria son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro de SALESIANA, para que de esta forma la Dirección de Tecnologías de Información realice la actualización de permisos requerida.
- El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus a la Dirección de Tecnologías de Información, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma el usuario debe reportar cuando no reciba correos y esté seguro que este no es de tipo SPAM, así la Dirección de Tecnología hará el análisis para evaluar el origen y así tomar las medidas pertinentes.
- Todo miembro de la comunidad universitaria es responsable de reportar los mensajes cuyo origen sea desconocido, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el miembro de la comunidad universitaria desconfíe del remitente de un correo electrónico debe remitir la consulta al correo electrónico soporteti@salesiana.edu.co.
- Si una cuenta de correo es interceptada por personas mal intencionadas o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), la Dirección de Tecnologías actuará según sea el caso.

Backup:

- La Dirección de Tecnologías de Información, debe realizar periódicamente un análisis de las necesidades institucionales para determinar la información crítica que debe ser respaldada y la frecuencia con que se debe realizar.
- La Dirección de Tecnologías de Información junto con los propietarios de la información deben determinar los requerimientos para salvaguardar la información.
- El dueño de la información es responsable de definir claramente el período de realizar su copia de seguridad según lo sensible que sea la información.

Definiciones

- **Activo:** es la información o elementos relacionados con el tratamiento de la misma y que tiene valor para SALESIANA. Todo activo contiene información, la cual posee un valor y es necesaria para el desarrollo de los procesos estratégicos, misionales de **SALESIANA**.
- **Autenticación:** es el proceso de identificar a los usuarios que están dentro de la Comunidad Universitaria y garantizar que los mismos sean quienes dicen ser, evitando que cualquier persona externa a la misma pueda entrar a un determinado sistema o iniciar sesión dentro del entorno tecnológico de Salesiana.
- **Confidencialidad:** garantizar que la información no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados.
- **Comunidad Universitaria:** En SALESIANA hace referencias a los Estudiantes, Administrativos, Profesores, ciudadanía en general, terceros, contratistas y cualquier interviniente dentro de los procesos institucionales.
- **Datos:** de acuerdo con la Ley 1581 de 2012, cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Para Salesiana los datos son uno de sus activos más valiosos y por tanto deben protegerse.
- **Disponibilidad:** garantizar el acceso y el uso oportuno y fiable de la información por parte de personas autorizadas. La información no está disponible no sólo cuando se pierde o se destruye, sino también cuando se deniega o retrasa el acceso a la información a una persona autorizada.
- **Infraestructura tecnológica:** Son todos los equipos utilizados dentro de SALESIANA para gestionar la información y comunicaciones, como equipos de cómputo, switches, puntos de acceso, tableros interactivos, micrófonos, impresoras, entre otras.
- **Integridad:** asegurar que la información sea precisa y confiable y no ha sido sutilmente cambiada o manipulada por una parte no autorizada.
- **Información:** la información constituye un importante activo, esencial para las actividades de la Comunidad Universitaria por lo tanto necesita una

protección adecuada. Esta información puede estar relacionada de muchas maneras. Puede estar impresa inscrita en papel, almacenada electrónicamente, mostrada en videos o expuesta oralmente.

- **Instancias de decisión:** es el conjunto de personas que tienen el poder de decisión dentro de la Comunidad Universitaria, en SALESIANA encontramos el Consejo Superior, Consejo Académico, Comité de Rectoría, entre otros.
- **Modelo de gestión de seguridad y privacidad de la información:** el MSPI conduce a todos los miembros de la Comunidad Universitaria al compromiso de la preservación de la confidencialidad, integridad, disponibilidad de la información, garantizando la privacidad de los datos, mediante la aplicación de los procesos de gestión del riesgo.
- **No repudio:** los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente. También definido como el servicio de seguridad que previene que un emisor niegue haber emitido el mensaje y que un receptor niegue su recepción.
- **Procesos institucionales:** en Salesiana hace referencia a la categorización dentro del mapa de procesos. procesos estratégicos, misionales y de apoyo.
- **Plan de continuidad del Negocio:** plan orientado a permitir la continuidad de los procesos estratégicos, misionales y de apoyo de SALESIANA en caso que haya un evento imprevisto y que se ponga en peligro los procesos de funcionamiento de la Comunidad Universitaria.
- **Servicios de TI:** Son los que se manejan dentro de SALESIANA como servicios de tecnología de la información prestada por parte de la Dirección de Tecnologías.
- **Funciones sustantivas:** en SALESIANA hace referencia a Formación, Docencia, Investigación y Proyección Social.