FUNDACIÓN UNIVERSITARIA INTERNACIONAL DE LA RIOJA

Política de Gestión de la Información

Fundación Universitaria Internacional de La Rioja

Acuerdo 007 del 24 de abril de 2023, Consejo Superior

Contenido

1. Introducción

La Fundación Universitaria Internacional de La Rioja UNIR, en adelante la Fundación, a partir de sus procesos académicos y administrativos procesa datos que convierte en información y luego en conocimiento para la toma de decisiones. La Fundación considera la información como un activo clave para el cumplimiento de su misión institucional, por esta razón la información debe cumplir con unos atributos de calidad:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Relevancia. (La información responde a las necesidades de los públicos de interés).

Por lo anterior, la Fundación se compromete con unos principios de gestión de la información y define las políticas que garanticen un adecuado uso y aprovechamiento de la información que se genera en los procesos de la institución. Respecto a los principios de gestión de la información, la Fundación se compromete con:

- Reconocer la información con un recurso clave.
- Brindar a las partes interesadas acceso autónomo a la información de acuerdo con su rol.
- Presentar información con el nivel de detalle que le es permito a la parte interesada de acuerdo con su rol.
- Garantizar la seguridad de la información.
- Proveer información oportuna para la toma de decisiones.
- Proveer información relevante para las partes interesadas.
- Determinar las fuentes, procesos y herramientas tecnológicas que faciliten el desarrollo de la cadena de valor del dato.

En este sentido y como un pilar fundamental complementario se presentan las políticas de gestión de la información, enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de gestión de la información establecida por los estándares internacionales para la toma de decisiones, considerando las siguientes:

- Política general de gestión de la información.
- Política de tratamiento de datos personales.
- Política de gestión a la información estadística.

- Política de registro de información en SNIES / MINCIENCIAS.
- Política de control de acceso.
- Política de tercerización u outsourcing.
- Política de controles criptográficos.
- Política de registro y seguimiento de eventos / monitoreo de logs.
- Política de seguridad en entornos cloud.
- Política de trabajo remoto.

Las anteriores políticas deben ser acatadas por los docentes, estudiantes, egresados, empleados administrativos y terceras partes que tengan relación directa con la Fundación, quienes en adelante se denominaran partes interesadas. Estas Políticas se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de gestión de la información, basadas en la norma ISO/IEC 27001:2022.

Es de anotar que la seguridad de la información en la Fundación, en un fuerte compromiso que permite brindar servicios con calidad que redunden en la confianza de la comunidad educativa, exhortando a todos a velar por el cumplimiento de las políticas establecidas en el presente manual.

2. Objetivo

Establecer las políticas que reglamentan la gestión de la información en la Fundación, presentando su estructura, intención y elementos, la cual deben conocer, acatar y cumplir todas las partes interesadas que presten sus servicios o tengan algún tipo de relación con la Fundación.

3. Alcance

Las Políticas de Gestión de la Información son aplicables a la información que se genera en los procesos administrativos y académicos de la Fundación y deben ser cumplidas por todas las partes interesadas que presten sus servicios o tengan algún tipo de relación con la Fundación.

4. Aplicabilidad

Las Políticas de Gestión de la Información aplican y son de obligatorio cumplimiento para todas las partes interesadas que presten sus servicios o tengan algún tipo de relación con la Fundación.

5. Términos y definiciones

Tomando como base lo establecido en la norma ISO/IEC 27000, la cual provee un vocabulario estándar relacionado con la gestión de la información, se relacionan los siguientes términos y definiciones que aportan una perspectiva general y lenguaje común para todos los estándares ISO sobre la seguridad de la información, aplicables al contexto actual de la Fundación.

- **Acción correctiva**: Acción para eliminar la causa de una no conformidad y para prevenir la recurrencia.

- **Alta Dirección**: Persona o grupo de personas que dirige y controla una organización (3.50) al nivel más alto. La alta dirección tiene el poder de delegar autoridad y proporcionar recursos dentro de la organización.

- **Alcance de auditoría**: El alcance de una auditoria generalmente incluye una descripción de las áreas físicas, unidades organizacionales, actividades y procesos, así como el periodo de tiempo cubierto.

- **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar hasta qué punto se cumplen los criterios de auditoría. Las auditorias pueden ser internas o externas.

- **Aceptación del riesgo**: Decisión informada de tomar un riesgo particular.

- **Amenaza**: Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.

- **Análisis de riesgo**: Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo.

- **Ataque**: Acción encaminada a destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo.

- **Autenticación**: Garantía de que una característica reivindicada de una entidad es correcta.

- **Característica reivindicada:** Término técnico referido a reivindicar, lo cual significa reclamar algo a lo que se tiene derecho (RAE, 2023). Técnicamente significa afirmar la responsabilidad por una acción cibernética. Justamente esto es lo que hace una autenticación.

- **Competencia**: Capacidad de aplicar conocimientos y habilidades para lograr los resultados esperados.

- **Confidencialidad**: Propiedad por la que la información no se pone a disposición o se divulga apersonas, entidades o procesos no autorizados.

- **Confiabilidad**: Propiedad de la conducta y resultados esperados consistentes.

- **Conformidad**: Cumplimiento de un requisito.

- **Consecuencia**: Resultado de un evento que afecta a los objetivos.

- **Contexto externo:** Entorno externo en el que la organización busca alcanzar sus objetivos.

- **Contexto interno:** Entorno interno en el que la organización busca alcanzar sus objetivos.
- **Control de acceso**: Medios para garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.
- **Corrección**: Acción para eliminar una no conformidad detectada.
- **Criterios de riesgo:** Términos de referencia contra los cuales se evalúa la importancia del riesgo.
- **Desempeño**: Resultado medible.
- **Disponibilidad**: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada.
- **Efectividad**: Medida que realizan las actividades planificadas y se logran los resultados planificados.
- **Evaluación de riesgos**: Proceso global de identificación de riesgos, análisis de riesgos y evaluación de riesgos.
- **Evento**: Ocurrencia o cambio de un conjunto particular de circunstancias.
- **Gestión de incidentes de seguridad de la información:** Conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Guía**: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad.
- **Información documentada**: Información necesaria que una organización debe controlar y mantener actualizada tomando en cuenta y el soporte en que se encuentra. la información documentada puede estar en cualquier formato (audio, video, ficheros de texto etc.) así como en cualquier tipo de soporte o medio independientemente de la fuente de dicha información.
- **Incidente de seguridad de la información:** Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.
- **Identificación de riesgo:** Proceso de búsqueda, reconocimiento y descripción de riesgos. La identificación del riesgo implica la identificación de las fuentes de riesgo, los eventos sus causas y sus posibles consecuencias.
- **Indicador**: Medida que proporciona una estimación o evaluación.
- **Integridad**: Propiedad de la exactitud y la integridad.
- **Medida**: Variable a la que se asigna un valor como resultado de la medida.

- **Mejora continua**: Actividad recurrente para mejorar el rendimiento. Control: Medida que modifica un riesgo.
- **Monitoreo**: Determinar el estado de un sistema, un proceso o una actividad.
- **No conformidad**: Incumplimiento de un requisito.
- **No repudio:** Capacidad para demostrar la ocurrencia de un evento o acción reclamada y sus entidades de origen.
- **Nivel de riesgo:** Magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad.
- **Objetivo**: Resultado a lograr. Un objetivo puede ser estratégico, táctico u operacional.
- **Organización**: Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.
- **Parte interesada:** Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.
- **Probabilidad**: Posibilidad de que algo suceda.
- **Proceso**: Conjunto de actividades interrelacionadas o interactivas que transforman entradas en salidas.
- **Procedimiento**: Los procedimientos, se definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico.
- **Riesgo residual**: Riesgo restante después del tratamiento de riesgo.
- **Riesgo**: Efecto de la incertidumbre sobre los objetivos.
- **SGSI**: Un Sistema de Gestión para la Seguridad de la Información se compone de una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que afectan a la seguridad de la información en una empresa u organización
- **Seguridad de información**: Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Sistema de gestión de seguridad de la información (SGSI) profesional:** Persona que establece, implementa, mantiene y mejora continuamente uno o más procesos del sistema de administración de seguridad de la información.

- **Sistema de información:** Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.

- **Requisito**: Necesidad o expectativa que se declara, generalmente implícita u obligatoria.

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

- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotado por una o más amenazas.

6. Política General de Gestión de la Información Fundación Universitaria Internacional de La Rioja-UNIR

La Fundación reconoce la información como un activo fundamental que debe ser protegido frente a amenazas internas o externas que puedan comprometer la confidencialidad, integridad y disponibilidad de la misma.

Manifiesta su compromiso con la preservación de la gestión de la información, los objetivos de seguridad establecidos y el cumplimiento de la legislación vigente y aplicable en lo que respecta a la protección de la información.

Consciente de la importancia de la gestión de la información de sus empleados, docentes, egresados, cuerpo administrativo y terceras partes, establece un Sistema de Gestión de la Información basado en la norma NTC-ISO-IEC 27001:2022, cuyo alcance se enfoca en las actividades sustantivas, adjetivas y de gestión en o de la educación superior.

7. Políticas específicas articuladas con la política de Gestión de la Información de la Fundación Universitaria Internacional de La Rioja- UNIR

Para la Fundación es importante contar con la política de gestión de la información articulada a políticas específicas, ya que son ellas quienes guiarán el comportamiento de las partes interesadas sobre la información obtenida, generada o procesada por la Fundación, así mismo estas políticas permitirán que la Fundación trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales determinados.

Lineamientos:

La Fundación debe asegurar que las partes interesadas ejecuten de manera apropiada todos los procedimientos de gestión de la información al interior de su área, con el propósito de lograr el

cumplimiento de las políticas y estándares definidos por la Fundación.

La Fundación debe garantizar el monitoreo de las políticas para determinar la efectividad y cumplimiento de estas, de forma periódica, dando cuenta de las evidencias de su funcionamiento o del ajustarse de la misma, por encontrarse necesario.

La Fundación periódicamente debe hacer la revisión de las políticas, determinando su actual impacto e importancia en la Fundación.
La Fundación debe asegurar que las políticas se encuentren actualizadas, integras y que contengan los ajustes necesarios y obtenidos de las retroalimentaciones.

Con el propósito de establecer la eficacia frente al cumplimiento de las políticas de seguridad de la información, la Fundación debe estructurar programas de auditoría del Sistema de Gestión de la Información. Lo anterior permitirá evaluar el cumplimiento de los requisitos, el rendimiento y señalar oportunidades de mejora.

La Fundación en el marco de la difusión y conocimiento de las políticas establecidas en la presente política, debe implementar los mecanismos internos y externos estructurados por segmentos comunicacionales, que permitan a las partes interesadas conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación documental, para ser consultados en el momento requerido. Lo anterior permitirá fomentar la cultura y conciencia de seguridad en la gestión de la información al interior de la Fundación.

7.1. Política de tratamiento de datos personales

Atendiendo lo establecido en el artículo 15 de la Constitución de la República de Colombia, la Ley Estatutaria 1581 del 17 de octubre de 2012, el Decreto 1377 del 27 de junio de 2013, la Fundación se compromete con la protección de los datos privados, semiprivados y sensibles de las partes interesadas que tengan relación directa con la Fundación. De igual manera adoptará mecanismos que aseguren la confidencialidad, integridad y disponibilidad de los mismos.

Esta política se encuentra disponible en https://unir.edu.co/politica-privacidad/ y se complementa con la implementación del principio de responsabilidad demostrada (Decreto 1377/2013), el cual se encuentra detallado en el Anexo A.

7.2. Política de gestión de la información estadística

La Fundación implementará los mecanismos que faciliten la planeación, el monitoreo y la evaluación de las actividades institucionales y la toma de decisiones relacionadas con las labores formativas, académicas, docentes, científicas, culturales y de extensión, garantizando que la información sea veraz, oportuna, precisa, completa y confiable, para ello establecerá:

a) Un sistema de indicadores clave de gestión académica y administrativa.

b) Asignar responsabilidades directas al área encargada quién realizará el cargue de la información en las plataformas y en los plazos establecidos.

c) Documentar y conservar los respectivos registros ante futuras auditorias.

d) Las demás que permitan asegurar y garantizar el monitoreo, gestión y disponibilidad estadística cuantitativa y cualitativa para la toma de decisiones.

En los anexos B: ficha de indicador y C: indicadores clave de gestión académica y administrativa, se describe, respectivamente: cómo documentar los indicadores y algunos indicadores relevantes.

7.3. Política de registro de información en SNIES / MINCIENCIAS

Atendiendo lo establecido en la Resolución 009573 del 27 de mayo de 2021 literal c) expedida por el Ministerio de Educación Nacional encaminada a efectuar *el registro de información actualizada, en los sistemas de información que administren el Ministerio de Educación Nacional y el Ministerio de Ciencia, Tecnología e Innovación, de acuerdo con los requerimientos de los mismos en cuanto a periodicidad y tiempos de suministro*, la Fundación adoptará los mecanismos requeridos que permitan dar cumplimiento a la norma en mención y normas subyacentes, atendiendo los siguientes aspectos:

a) Acatar lo establecido en la Resolución 009573 del 27 de mayo de 2021 expedida por el Ministerio de Educación Nacional.

b) Adoptar un mecanismo que permita realizar los registros de información actualizada en los sistemas que administra el Ministerio de Educación Nacional y el Ministerio de Ciencia Tecnología e Innovación.

c) Asignar responsabilidades directas al área encargada quién realizará el cargue de la información en las plataformas y en los plazos establecidos.

La Fundación realizará las actualizaciones que surjan de acuerdo con los cambios normativos realizados por el Ministerio de Educación Nacional. En el anexo D, como parte de esta política se encuentra el procedimiento de reporte de información al SNIES y MINCIENCIAS.

7.4. Política de control de acceso

La Fundación adoptará los aspectos requeridos para que los sistemas de información, las áreas de procesamiento de datos, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico, contemplando los siguientes aspectos:

a) Establecer los mecanismos para que el ingreso a plataformas de la Fundación sea únicamente con la cuenta de correo institucional.

b) Establecer controles de acceso a las plataformas institucionales por roles.

c) Establecer contraseñas seguras en plataformas institucionales, de igual manera su tiempo de caducidad como mínimo cada tres meses.

d) En servicios críticos implementar la autenticación en dos factores.

e) Implementar mecanismos de seguridad perimetral.

f) Restringir el acceso físico a las instalaciones y áreas críticas por roles, implementado medidas de verificación como soluciones biométricas.

g) Realizar pruebas de pentesting que permitan determinar vulnerabilidades a fin de corregirlas a tiempo.

7.5. **Política de tercerización u outsourcing**

Con el propósito de fortalecer y soportar la operación misional de la Fundación se recurrirán a las contrataciones de servicios con empresas externas y contratistas especializados. Estos acuerdos contractuales deben estar regidos por el precepto de confidencialidad de la información que sea suministrada por la Fundación y enmarcarse en los siguientes lineamientos de cumplimiento entre las partes:

a) Definir como criterio de selección ante un acuerdo comercial con terceras partes, que la empresa demuestre y/o certifique que implementa controles de seguridad de la información. En caso de contratistas deben firmar el acuerdo de confidencialidad establecido por la Fundación.

b) La Fundación deberá establecer controles referentes a los accesos de terceras partes que requieran interactuar con plataformas de la Institución.

c) Incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de gestión de la información.

*El acuerdo de confidencialidad se convierte en un compromiso por medio del cual todo funcionario, contratista y/o tercero vinculado a la Fundación, se compromete a no divulgar información interna y externa que conozca de la entidad, así como la relacionada con las funciones que desempeña en la misma. La firma de este acuerdo implica que la información conocida, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

7.6. **Política de controles criptográficos**

La Fundación adoptará los mecanismos técnicos y procedimentales que permitan proteger la información a través de herramientas criptográficas en los diferentes entornos digitales que soportan la operación de la institución. En este aspecto se debe garantizar la confidencialidad y autenticidad de la información que circula o se genera a través de los diferentes sistemas.

a) Utilizar técnicas criptográficas para la protección de la información con base al inventario y criticidad de activos de información.

b) La aplicación de medidas de cifrado debe estar alineada con el establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

c) Utilizar controles criptográficos para la protección de claves de acceso a sistemas, datos y

servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada.

d) Desarrollar procedimientos y asignar funciones respecto de la administración de claves, la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

e) El uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberán ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en técnicas de descifrado.

f) Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos y, en algunas ocasiones, podría ser necesario asesoramiento legal para establecer acuerdos especiales que respalden su uso.

7.7. **Política de registro y seguimiento de eventos / monitoreo de logs**

La Fundación consciente que los datos almacenados en los logs permiten monitorear eventos sobre el funcionamiento y uso de los sistemas de información tanto de procesos internos como la actividad de los usuarios; se establece la presente política específica con el propósito de generar alertas, determinar los eventos más significativos dentro de los sistemas de información, analizar amenazas y establecer mecanismos de monitorización que permitan la detección de intrusiones, fuga de información, errores y situaciones anómalas o potencialmente peligrosas. Es de anotar que ante un evento que requiera aplicar informática forense los logs se convierten en una pieza fundamental dentro de la investigación.

La Fundación determinará los mecanismos procedimientos, formatos, monitoreo y periodicidad para monitoreo de Logs.

7.8. **Política de seguridad en entornos cloud.**

Siendo un activo fundamental para soportar su misionalidad, la Fundación adopta directrices y aspectos para tener en cuenta para el aseguramiento de la información en entornos cloud, de tal manera que se conserve la seguridad de los datos en este tipo de ambientes.

La correcta implementación del servicio de información en la nube reducirá el riesgo de presentar incidentes de seguridad que afecten la operación de la Fundación y generen un daño irreparable.

Con base en lo anterior, y atendiendo las buenas prácticas señaladas en la NTC-ISO/IEC 27017, la Fundación impulsará los controles y lineamientos adaptables que permitan minimizar los riesgos frente a un incidente de seguridad, señalando las siguientes actividades:

a) Realizar migraciones de información en la nube basadas en el análisis de riesgos.

b) Definir roles y responsabilidades dentro de un entorno de cloud computing.

c) Implementar un servicio SIEM que permita visualizar de manera completa el monitoreo de las amenazas que afectan la seguridad informática de la Fundación.

d) Implementar una red perimetral (DMZ).

e) Implementar una solución de prevención de pérdida de datos (DLP).

f) Las demás que se definan de acuerdo con el análisis de requerimientos.

7.9. Política de trabajo remoto

La modalidad de trabajo remoto aporta a la Fundación un factor clave que coadyuva a mejorar los índices de productividad y permite a los docentes y empleados administrativos desarrollar sus actividades laborales desde escenarios distintos al entorno corporativo. Lo anterior conlleva una serie de riesgos de seguridad asociados a los dispositivos de cómputo utilizados para tal fin, siendo un compromiso mancomunado de la Fundación, minimizar el riesgo de afectación donde se pueda ver comprometida la confidencialidad, integridad y disponibilidad de la información.

De igual manera y atendiendo lo establecido en el concepto de Bring Your Own Device (BYOD) planteado por la Fundación TELEFÓNICA[1], se convierte en un factor de atención para la Fundación el uso de dispositivos y aplicaciones propias que utilizan las partes interesadas para realizar actividades personales y asociadas con la Fundación, lo cual permite brindar un escenario de flexibilidad, pero también de riesgos operacionales. Por lo anterior la Fundación adoptará las siguientes directrices generales:

a) Fortalecer el modelo Zero Trust, haciendo énfasis en el control estricto para la verificación de identidad, en relación con usuarios, dispositivos propios y personales, aplicaciones y servicios corporativos.

b) Mantener actualizados el inventario de activos de información, entendiendo que los activos de información son toda información o recurso relacionado para la creación, almacenamiento, manejo o transmisión de la información.

c) Realizar auditorías aleatorias a equipos, acceso y colaboradores que permitan y detectar vulnerabilidades e identificar aspectos de mejora relacionadas con trabajo remoto.

d) Dar soporte a partes interesadas y establecer una gestión a través de tickets.

e) Capacitar y concientizar a los colaboradores con el propósito de fortalecer las buenas prácticas en materia de seguridad de la información. En esta directriz se hace fundamental dar a conocer los riesgos cibernéticos al utilizar redes no corporativas, dando alcance a las amenazas y técnicas usadas por los ciberdelincuentes para comprometer la confidencialidad, integridad y disponibilidad de la información.

A continuación, se describen las principales responsabilidades de la Dirección de Recursos Humanos y las Partes Interesadas de la Fundación, en cuanto al trabajo remoto.

- **Dirección de Recursos Humanos**.

[1] Ciberseguridad, la protección de la información en un mundo digital / 2016

a) Informar oportunamente al Área de Tecnología y Soporte la relación de colaboradores que realiza actividades de trabajo remoto, suministrando el lugar acordado para realizar esta actividad y horarios de trabajo acordados. Lo anterior permitirá monitorear y validar el cumplimiento de los requisitos mínimos de seguridad de la información en el sitio y equipos de cómputo que se utilizarán.

b) Informar oportunamente al Área de Tecnología y Soporte cuándo un colaborador finalice su actividad de trabajo remoto o finalice su contrato con la Fundación.

c) Realizar jornadas de sensibilización que permitan a las partes interesadas adoptar buenas prácticas frente al uso de IoT, especialmente cuando se utiliza hardware, software y redes de uso personal.

d) Las demás que se consideren en el marco de asegurar la confidencialidad, integridad y disponibilidad de la información gestionada por la Fundación.

- **Partes interesadas de la Fundación**.

a) Conocer y dar estricto cumplimiento a la política de control de acceso.

b) Adoptar buenas prácticas de seguridad de la información, haciendo especial énfasis a contraseñas seguras, uso de VPN, canales para videoconferencias, uso de correo corporativo, navegabilidad segura en internet, descarga de ficheros, instalación de software no autorizado, salvaguarda del equipo de cómputo asignado o personal, entre otros.

c) Asistir a las capacitaciones convocadas por la Fundación relacionadas con seguridad de la información.

d) Tener como premisa de trabajo la seguridad digital, con el fin de evitar fugas de datos, de privacidad y ciberataques. Así mismo la perdida de dispositivos corporativos o propios que tengan información de la Fundación.

e) Informar oportunamente a la Fundación los incidentes de seguridad de la información presentados.

f) Concertar e informar oportunamente a la Dirección de Recursos Humanos cualquier cambio de lugar donde se realizará la actividad de trabajo remoto.

8. Cumplimiento

Los diferentes aspectos contemplados en esta política son de obligatorio cumplimiento para las partes interesadas, que presten sus servicios o tengan algún tipo de relación con la Fundación. En caso de que se violen las políticas de gestión de la información ya sea de forma intencional o por negligencia, la Fundación tomará las acciones administrativas, disciplinarias y legales correspondientes.

9. Marco Legal

El presente documento de Política de Gestión de la Información se rige por la normatividad legal vigente colombiana, con el fin de dar cumplimiento a los diferentes aspectos que en materia de protección de datos personales y gestión de la información rigen en el país.

Artículo 15 de la Constitución de la República de Colombia. +Artículo 20 de la Constitución de la República de Colombia.
Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1273 de 2009, Delitos Informáticos, protección de la información y los datos.

Ley 1581 de 2012, Protección de Datos personales.
Resolución 0009573 de 2021, Por la cual se modifica la resolución 20434 de 2016 modificada por la Resolución 19591 de 2017.

Decreto 1377 del 27 de junio de 2013.

Decreto 1330 de 2019, Por el cual se sustituye el Capítulo 2 y se suprime el Capítulo 7 del Título 3 de la Parte 5 del Libro 2 del Decreto 1075 de 2015 -Único Reglamentario del Sector Educación.

CONPES 3995 de 2020 Política Nacional de Confianza y Seguridad Digital.

10. Requisitos técnicos

NTC-ISO-IEC 27000:2017 Tecnología de la información. técnicas de seguridad. sistemas de gestión de seguridad de la información (SGSI). Visión general y vocabulario

Norma Técnica Colombiana NTC-ISO/IEC 27001:2022 Sistemas de gestión de la seguridad de la información.

GTC-ISO-IEC 27002:2015 Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información.

NTC-ISO-IEC 27005:2020 Tecnología de la información. Técnicas de seguridad. Gestión de riesgos para la seguridad de la información.

Norma Técnica Colombiana NTC – ISO 31000:2011 Gestión del riesgo, principios y directrices.

Norma Técnica Colombiana NTC – ISO 19011:2018 Directrices para la Auditoría de los Sistemas de Gestión.