POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

Introducción

La E.S.E Alejandro Próspero Reverend, comprometida con la mejora continua y la modernización de sus servicios, adopta la Política de Seguridad y Privacidad de la Información en concordancia con la Política de Gobierno Digital. Esta iniciativa busca optimizar la gestión pública y la prestación de servicios mediante el uso eficiente de tecnologías de la información y comunicación (TIC). En un entorno donde la información se convierte en un activo crítico, es esencial implementar medidas robustas que aseguren la confidencialidad, integridad y disponibilidad de los datos, protegiendo así tanto la información personal de los pacientes como los datos administrativos de la institución.

La adopción de esta política responde a la necesidad de cumplir con normativas nacionales e internacionales, tales como el Decreto 1078 de 2015 y la Ley 1712 de 2014, que promueven la transparencia y la protección de datos personales. Además, se alinean con los estándares de la norma técnica colombiana NTC ISO/IEC 27001:2022, estableciendo un marco sólido para la gestión de la seguridad de la información.

Esta resolución formaliza el compromiso de la E.S.E Alejandro Próspero Reverend de implementar un Modelo de Seguridad y Privacidad de la Información que no solo cumpla con los requisitos legales, sino que también mejore continuamente para afrontar las amenazas y vulnerabilidades del entorno digital. Así, se asegura la continuidad de las operaciones y la calidad de los servicios de salud ofrecidos a la comunidad, fortaleciendo la confianza y la transparencia en la gestión institucional.

Avenida del Libertador No. 25-67 819.004.070-5
www.esealejandroprosperoreverend-santamarta-magdalena.gov.co
@esealejandroprosperor ESE Alejandro Próspero Reverend @esealejandroprosperor
gerencia@esealprorev.gov.co

Objetivo

Establecer la Política de Seguridad y Privacidad de la Información junto con las Políticas Generales de Manejo y los lineamientos para su uso, con el propósito de salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de la información en la E.S.E Alejandro Prospero Reverend

Objetivos especificos

La Política de Seguridad y Privacidad de la Información, tiene los siguientes objetivos:

1. Asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información de la E.S.E Alejandro Prospero Reverend.
2. Establecer los lineamientos del modelo de seguridad y privacidad de la información en la E.S.E Alejandro Prospero Reverend.
3. Brindar los procedimientos y mecanismos necesarios para la gestión de incidentes de seguridad de la información en la E.S.E Alejandro Prospero Reverend.
4. Gestionar los riesgos para abordar las amenazas y vulnerabilidades en la seguridad y privacidad de la información de la E.S.E Alejandro Prospero Reverend.
5. Mejorar la apropiación, las capacidades y la cultura de seguridad de la información en todos los funcionarios y contratistas de la E.S.E Alejandro Prospero Reverend.

Alcance

La Política de Seguridad y Privacidad de la Información se establece para asegurar la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información de la E.S.E Alejandro Prospero Reverend, garantizando la calidad, el cumplimiento y la transparencia en los servicios de salud que ofrecemos a la población del distrito turístico, cultural e histórico de Santa Marta y sus alrededores.

Esta política es aplicable a todos los miembros de la E.S.E Alejandro Próspero Reverend, incluyendo Funcionarios, Contratistas, Terceros y cualquier otra parte que tenga acceso a la información y a los sistemas de la organización. Cubre todos los aspectos relacionados con la gestión de la información, desde su creación y almacenamiento hasta su transmisión y destrucción. Esta política se extiende a todos los activos de información, tanto digitales como físicos, así como a los sistemas tecnológicos y las infraestructuras utilizadas para su procesamiento, almacenamiento y transmisión. La implementación de esta política asegura que se apliquen las medidas de seguridad necesarias para proteger la información contra amenazas internas y externas, y garantiza el cumplimiento de las normativas legales y regulatorias vigentes. La política también promueve una cultura de seguridad en toda la organización, fomentando la conciencia y la responsabilidad entre todos los usuarios de los sistemas de información.

Las políticas y directrices establecidas se encuentran alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI). Además, están en conformidad con la norma

ISO/IEC 27001:2022, la Ley 1581 de 2012 de Protección de Datos Personales, la Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública, Clasificada y Reservada, entre otras normativas adoptadas por la entidad, que son esenciales para la protección de los activos de información de la E.S.E Alejandro Prospero Reverend

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política. Esto significa que todos los funcionarios, contratistas, proveedores y cualquier otra parte interesada que esté sujeta a esta política deben adherirse a sus lineamientos y requisitos.

A continuación, se establecen los lineamientos de seguridad que soportan el Modelo de Seguridad y Privacidad de la Información de la E.S.E Alejandro Prospero Reverend:

1. La E.S.E Alejandro Prospero Reverend ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas y terceros.

3. La E.S.E Alejandro Prospero Reverend protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

4. La E.S.E Alejandro Prospero Reverend, protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, 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.

5. La E.S.E Alejandro Prospero Reverend, protegerá su información de las amenazas originadas por parte del personal.

6. La E.S.E Alejandro Prospero Reverend, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7. La E.S.E Alejandro Prospero Reverend, controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. La E.S.E Alejandro Prospero Reverend, implementará controles de acceso a la información, sistemas y recursos de red.

9. La E.S.E Alejandro Prospero Reverend, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. La E.S.E Alejandro Prospero Reverend, garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. La E.S.E Alejandro Prospero Reverend, garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

12. La E.S.E Alejandro Prospero Reverend, garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Marco normativo

El marco de referencia de esta política se basa en las siguientes normativas y estándares:

- **Ley 1581 de 2012:** Dispone las normativas generales para la protección de datos personales.
- **Ley 1266 de 2008:** Regula las disposiciones generales del Habeas Data y el manejo de la información en bases de datos personales.
- **Ley 1712 de 2014:** Ley que regula la Transparencia y el Derecho de Acceso a la Información Pública Nacional.
- **Resolución 1995 de 1999:** Define las normas para la gestión y manejo de la historia clínica.
- **Resolución 500 de 2021:** Define lineamientos para la gestión y respuesta a incidentes de seguridad digital en entidades públicas, garantizando la protección de la información y la continuidad operativa.
- **Directiva Presidencial 02 de 2020:** Relacionada con la política de gobierno digital y ciberseguridad.
- **Política de Gobierno Digital:** Conjunto de directrices del Gobierno Nacional para el uso y aprovechamiento de las TIC en la gestión pública.
- **Modelo de Seguridad y Privacidad de la Información de MinTIC:** Estándar establecido por MinTIC para garantizar la seguridad y privacidad de la información.

Este marco de referencia proporciona una base sólida para la implementación y mantenimiento del sistema de gestión de seguridad de la información, asegurando que las prácticas de seguridad estén alineadas con las mejores prácticas y requisitos legales aplicables.

Glosario de términos

- **Activo de Información**: Recurso de información considerado valioso para la organización, que debe ser protegido mediante controles de seguridad adecuados.
- **Amenaza**: Cualquier circunstancia o evento con el potencial de causar daño a la organización, comprometiendo la confidencialidad, integridad o disponibilidad de la información.
- **Autenticación**: Proceso para verificar la identidad de un usuario, dispositivo o sistema, generalmente mediante credenciales como contraseñas o certificados digitales.
- **Confidencialidad**: Propiedad que asegura que la información no sea divulgada a personas, entidades o procesos no autorizados.
- **Clasificación de la Información**: Proceso de categorizar la información de acuerdo con su nivel de sensibilidad y el impacto potencial de su divulgación no autorizada.
- **Control de Acceso**: Mecanismos y políticas que limitan el acceso a la información y sistemas solo a usuarios autorizados.
- **Ciberseguridad**: Prácticas y tecnologías destinadas a proteger los sistemas de información y los activos de una organización contra ataques cibernéticos.
- **Disponibilidad**: Propiedad de la información que garantiza que esté accesible y utilizable cuando sea requerida por una persona, entidad o proceso autorizado.
- **Desactivación de Usuarios**: Proceso mediante el cual se revocan los permisos de acceso a sistemas e información de un usuario que ya no está autorizado, como en el caso de la desvinculación laboral **Integridad**: Propiedad que asegura la precisión y totalidad de la información, manteniéndola exacta y completa desde su creación hasta su eliminación.
- **Evaluación de Riesgos**: Proceso de identificación, análisis y evaluación de riesgos asociados a la seguridad de la información, para mitigar o aceptar los riesgos identificados.
- **Gestión de Activos**: Conjunto de prácticas y procedimientos destinados a identificar, clasificar, y proteger los activos de información, asegurando su confidencialidad, integridad y disponibilidad.
- **Información Clasificada**: Información accesible para todos los procesos de la entidad, cuya divulgación no autorizada podría afectar negativamente dichos procesos.
- **Información No Clasificada**: Activos de información que no han sido categorizados pero que deben ser tratados como de alta importancia hasta que se les asigne una clasificación adecuada.
- **Información Pública**: Información que puede ser divulgada libremente, sin riesgo de daños a terceros o a la entidad.

- **Información Reservada**: Información accesible solo para un proceso específico dentro de la entidad, cuya divulgación no autorizada podría tener consecuencias negativas como problemas legales o pérdida de reputación.
- **Incidente de Seguridad de la Información**: Cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información o los sistemas de la organización.
- **Información Personal**: Datos que identifican o podrían identificar a una persona, cuya protección es fundamental para cumplir con las leyes de privacidad y protección de datos.
- **Modelo de Seguridad y Privacidad de la Información (MSPI)**: Marco de referencia adoptado por la E.S.E Alejandro Próspero Reverend para garantizar la seguridad y privacidad de la información, alineado con normativas como la ISO/IEC 27001:2022.
- **Política de Seguridad y Privacidad de la Información**: Conjunto de directrices adoptadas por la E.S.E Alejandro Próspero Reverend para proteger la confidencialidad, integridad, disponibilidad y privacidad de la información en la organización.
- **Vulnerabilidad**: Debilidad en un sistema de información o en las medidas de seguridad que puede ser explotada por una amenaza para causar daño o comprometer la información.
- **Plan de Continuidad del Negocio**: Conjunto de procedimientos y medidas destinados a garantizar que los procesos críticos de la organización continúen operando durante y después de una interrupción significativa.
- **Política de Escritorio Limpio**: Directriz que establece que los Funcionarios y Contratistas deben asegurar que la información sensible no quede expuesta en los escritorios o en las pantallas de los computadores cuando no están presentes.
- **Privacidad**: Derecho de las personas a controlar la forma en que se recopila, utiliza, retiene y comparte su información personal.
- **Responsabilidad del Usuario**: Obligación de los usuarios de los sistemas de información de la organización de cumplir con las políticas y prácticas de seguridad establecidas.

Política de seguridad y privacidad de la información

La E.S.E Alejandro Prospero Reverend establece medidas para asegurar, proteger y gestionar la confidencialidad, integridad, disponibilidad y privacidad de la información en sus procesos, servicios, sistemas de información y su infraestructura, así como la continuidad de las operaciones, en concordancia con el mapa de procesos y cumpliendo con las normativas legales vigentes. La entidad adopta una actitud proactiva en la prevención de incidentes, gestionando riesgos asociados a la seguridad y privacidad de la

información, implementando controles físicos y digitales, y promoviendo la mejora continua con calidad y transparencia de la información que resulta de la prestación de servicios de salud para toda la población del D.T.C.H. de Santa Marta, partes interesadas y la gestión institucional.

Políticas generales de manejo de información

Organización de la seguridad de la información

La política de seguridad de la información de la E.S.E Alejandro Prospero Reverend es de cumplimiento obligatorio para todo el personal de la entidad, independientemente de su estatus jurídico, área de trabajo o nivel de responsabilidad.

Roles y Responsabilidades

Esta política busca garantizar que los Funcionarios, Contratistas y Terceros comprendan sus responsabilidades y sean competentes en sus roles relacionados con la Seguridad de la Información. Por lo tanto, la E.S.E Alejandro Prospero Reverend establece los siguientes roles y responsabilidades:

Gerente

- Aprobar las políticas de seguridad de la información.
- Evaluar el proceso de gestión de la seguridad de la información.
- Definir las estrategias y mecanismos de control para la gestión de riesgos que afecten los activos de información institucionales, basándose en los informes y recomendaciones del Comité Institucional de Gestión y Desempeño.
- Proveer los recursos necesarios para el sistema de gestión de seguridad de la información.

Comité de Seguridad de la Información

- Revisar, modificar y proponer la Política de Seguridad de la Información para su posterior aprobación por el Comité de Gestión y Desempeño.
- Supervisar la implementación de los procedimientos y estándares derivados de las políticas de seguridad de la información.
- Proponer estrategias y soluciones para implementar los controles necesarios y resolver las situaciones de riesgo identificadas.
- Resolver conflictos relacionados con la seguridad de la información y los riesgos asociados, y proponer soluciones adecuadas.
- Informar al Gerente sobre oportunidades de mejora en la seguridad de la información, así como sobre los incidentes relevantes y sus soluciones.

Jefe de Oficina Asesora de Planeación

- Integrar los aspectos de seguridad de la información en la planificación estratégica de la entidad.
- Coordinar con la Gerencia y otras áreas para asegurar la asignación adecuada de recursos financieros, humanos y tecnológicos necesarios para la implementación de las políticas de seguridad de la información.

- Participar en la revisión periódica de la Política de Seguridad de la Información, evaluando su efectividad y proponiendo ajustes para alinearla con los objetivos estratégicos de la entidad.
- Colaborar con el Comité de Seguridad de la Información y la Oficina de Sistemas para identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información en los proyectos y planes estratégicos de la entidad.
- Monitorear la correcta integración de las políticas de seguridad de la información en los proyectos institucionales, asegurando que se cumplan los estándares establecidos y que se mitiguen los riesgos identificados.

P.U. Con funciones de sistemas

- Coordinar el mantenimiento correctivo y preventivo de la infraestructura tecnológica de la entidad.
- Supervisar la ejecución de actividades, controles y planes de tratamiento relacionados con la seguridad de la información.
- Asegurar que los sistemas de información cumplan con las normativas de seguridad establecidas y sean actualizados regularmente.
- Gestionar la implementación de nuevas tecnologías, garantizando que estén alineadas con las políticas de seguridad de la entidad.
- Monitorear y evaluar el rendimiento de los sistemas y aplicaciones, tomando medidas correctivas cuando sea necesario para mantener la seguridad y el rendimiento óptimos.

Oficial de Seguridad de la Información

- Desarrollar y gestionar las políticas de seguridad de la información dentro de la entidad, garantizando su correcta implementación.
- Supervisar el avance en la implementación de las estrategias de control y tratamiento de riesgos de seguridad digital.
- Colaborar con otras áreas de la entidad para apoyar los objetivos de seguridad de la información.
- Servir de enlace con responsables de seguridad de otras entidades públicas y especialistas externos para mantenerse al día con las tendencias, normativas y metodologías en seguridad de la información.
- Coordinar con las autoridades en materia de ciberseguridad para recibir alertas y apoyo en la gestión de incidentes de seguridad de la información.
- Participar activamente en grupos de interés especializados en seguridad de la información para asegurar una comprensión actualizada del entorno y compartir conocimientos sobre nuevas tecnologías, productos, amenazas o vulnerabilidades.
- Implementar programas de capacitación continua en seguridad de la información.

Secretaria Técnica de Seguridad de la Información

- Gestionar operativamente las soluciones a los incidentes de seguridad de la información que afecten los activos institucionales.
- Monitorear el progreso de cada etapa en la implementación de la Política de Seguridad de la Información.

Propietarios de los Activos de Información Institucional

- Clasificar los activos de información según su sensibilidad y criticidad, manteniendo la documentación actualizada.
- Determinar qué usuarios tienen permisos de acceso a la información según sus funciones y competencias.
- Proporcionar directrices en materia de seguridad de la información, establecidas por la alta dirección y su equipo.
- Ejercer un liderazgo comprometido en la aplicación de la política de seguridad de la información.

P.U. Con funciones de talento humano

- Cumplir con los procedimientos relacionados con la seguridad de la información en la gestión del talento humano.
- Informar a todo el personal que se incorpore a la entidad sobre sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y las normativas relacionadas.
- Incluir en el Plan Institucional de Capacitación las actividades del Plan de Sensibilización en seguridad de la información, aprobadas por el Comité Institucional de Gestión y Desempeño.

Jefe Oficina Asesora Jurídica

- Asegurar el cumplimiento legal de la Política de Seguridad de la Información en la entidad.
- Definir, documentar y actualizar los requerimientos legales, regulatorios y contractuales relevantes en materia de seguridad de la información, y establecer el enfoque de la entidad para cumplir con dichos requisitos.
- Asesorar en aspectos legales relacionados con la seguridad de la información y establecer directrices que permitan cumplir con los requerimientos legales.

Jefe Oficina de Control Interno

- Realizar auditorías periódicas o cuando se considere necesario, sobre los sistemas y actividades relacionadas con la tecnología de información, informando sobre el cumplimiento de las especificaciones y medidas de seguridad establecidas por esta política.
- Comunicar los resultados de las auditorías al encargado de seguridad de la información.
- Recomendar acciones de mejora para abordar las debilidades encontradas en las auditorías y comunicar estas recomendaciones al Comité Institucional de Gestión y Desempeño.

Funcionarios, Contratistas y Terceros

- Conocer, cumplir y hacer cumplir la Política de Seguridad de la Información y todas las normativas y procedimientos establecidos por la entidad.
- Utilizar de manera adecuada los equipos de cómputo y periféricos asignados para el desempeño de sus funciones, registrando su uso en el Sistema de Inventarios de la entidad.

- Entregar en buen estado los equipos de cómputo y periféricos asignados al finalizar su relación con la entidad, cambiar de funciones o culminar el contrato, y proteger la información almacenada en dichos equipos.
- Cumplir con las políticas de respaldo, custodia y recuperación de la información establecidas por la Oficina de Sistemas.
- Permitir la revisión física y de software de los equipos de cómputo cuando lo requiera la Subgerencia Administrativa.

Visitantes

- Cumplir con las políticas de seguridad de la información institucionales cuando se les autorice el acceso a los activos de información institucionales.
- Solicitar la autorización de acceso al responsable del activo de información correspondiente.
- No desactivar ni interferir con los controles de seguridad implementados por la entidad para proteger sus activos de información.

Gestión de seguridad de talento humano

En relación con la vinculación y desvinculación de los Servidores Públicos

La seguridad de los recursos humanos se gestiona a través del proceso de Gestión del Talento Humano.

- Los procesos de selección de los Servidores Públicos en la entidad incluyen la verificación de antecedentes disciplinarios, fiscales y policiales, así como la validación de sus experiencias académicas y laborales.
- La selección y vinculación de Servidores Públicos sigue el procedimiento establecido por el área Talento Humano de la E.S.E Alejandro Prospero Reverend.
- Durante su permanencia en la entidad, los Servidores Públicos deben participar en las actividades de capacitación y sensibilización en Seguridad de la Información, organizadas por el área de Talento Humano y por el área de Sistemas.
- Al finalizar su relación laboral, el área de Talento Humano debe pasar una solicitud al área de Sistemas sobre la desactivación o eliminación de su cuenta en los Sistemas de Información que corresponda.
- En concordancia con los lineamientos establecidos en el código disciplinario único (Ley 734 de 2002), los Servidores Públicos adquieren la responsabilidad legal de garantizar la confidencialidad de la información que gestionan.
- Todo el personal vinculado a la entidad debe aceptar formalmente las políticas de seguridad de la información, así como las políticas operativas de la institución.

Gestión de Contratistas respecto a la Seguridad de la Información

- Los contratistas están obligados a aceptar una cláusula de confidencialidad referente a la información a la que tienen acceso, la cual deben firmar al momento de iniciar el contrato, además de comprometerse a cumplir con las políticas de seguridad de la información y las políticas operativas de la E.S.E Alejandro Prospero Reverend.

- Al finalizar la ejecución de su contrato, el Supervisor debe gestionar la eliminación de las cuentas de usuario asociadas a los Sistemas de Información utilizados. Si el Contratista recibió equipo de cómputo, el supervisor debe coordinar la devolución de este a la oficina de Sistemas de acuerdo con el procedimiento de devolución de equipos tecnológicos.
- Durante su permanencia en la entidad, los Contratistas deben participar en las actividades de capacitación y sensibilización en Seguridad de la Información, organizadas por el área de Sistemas.

Gestión de activos de información

La E.S.E Alejandro Prospero Reverend a través de la Oficina de Sistemas establecerá y divulgará los lineamientos específicos para la identificación, clasificación y buen uso de los Activos de Información, con el objetivo de garantizar su protección y asegurar su confidencialidad, integridad y disponibilidad.

Inventario de Activos

Los Activos de la E.S.E Alejandro Prospero Reverend deben ser identificados, clasificados y controlados para garantizar su uso adecuado, protección y la recuperación ante desastres. Por tal motivo, se debe llevar el inventario de los activos de información de propiedad de la E.S.E Alejandro Prospero Reverend discriminado por proceso

Para establecer los controles de seguridad tanto físicos como digitales, las áreas responsables de custodiar la información generada en el ejercicio de sus funciones deberán protegerla, así como mantener y actualizar el inventario de activos de información vinculados a sus servicios.

Clasificación de Activos

El sistema de clasificación de la información se basa en las características particulares de la información, contempla la cultura y el funcionamiento interno y busca dar cumplimiento a los requerimientos estipulados en la Gestión y Clasificación de Activos de Información del MINTIC.

- Clasificación de acuerdo con la **Confidencialidad**

  La confidencialidad implica que la información no esté accesible ni sea divulgada a personas, entidades o procesos no autorizados. Esta debe establecerse según las características de los activos, y conforme a la ley 1712 de 2014, se determinan tres niveles que se alinean con los tipos de información:

INFORMACION RESERVADA	Información accesible únicamente para un proceso específico dentro de la entidad, cuya divulgación no autorizada a terceros podría generar consecuencias negativas, tales como problemas legales, operativos, pérdidas de reputación o impactos económicos.
INFORMACION CLASIFICADA	Información accesible para todos los procesos de la entidad, cuya divulgación no autorizada a terceros podría afectar negativamente dichos procesos. Esta información, ya sea de la entidad o de terceros, puede ser utilizada por todos los Funcionarios o Contratistas para llevar a cabo las tareas propias de los procesos, aunque no debe ser compartida con terceros sin la aprobación del propietario.

INFORMACION PÚBLICA	Información que se puede compartir o divulgar libremente con cualquier persona, tanto interna como externamente, sin que ello provoque daños a terceros ni perjudique los procesos o actividades de la entidad.
NO CLASIFICADA	Activos de información que necesitan ser incorporados en el inventario y que aún no han sido categorizados.

- Clasificación de acuerdo con la **Integridad**

La integridad se refiere a la precisión y totalidad de la información (ISO 27000). Esta propiedad garantiza que la información se mantenga precisa, coherente y completa desde su creación hasta su eliminación. Según el siguiente esquema, se establecen los siguientes niveles.:

3 (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
2 (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
1 (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

- Clasificación de acuerdo con la **Disponibilidad**

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. En el siguiente esquema se clasifican tres (3) niveles:

3 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
1 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA

Etiquetado de Activos de Información

Para realizar el etiquetado de los Activos de Información se deben tener en cuenta las siguientes pautas generales, las cuales se rige de acuerdo con las directrices establecidas en la **Guía para la clasificación de la Información** de la E.S.E Alejandro Prospero Reverend

- El etiquetado se realizará de acuerdo a los niveles de clasificación de la información:
  - **PÚBLICA**
  - **CLASIFICADA**
  - **RESERVADA**
- Todo documento o archivo debe ser etiquetado con su clasificación correspondiente.
- El etiquetado de la documentación se hará de acuerdo con la criticidad de la información que esta contenga.
- No se deberá publicar en carteleras, página Web o INTRANET documentos sin etiquetado o con etiquetado de Información Clasificada o Reservada.
- Se podrá publicar en la cartelera, página Web o INTRANET los formatos con etiquetado Pública, Clasificada o Reservada que no contengan información, para que sean utilizados de apoyo a la operación de los procesos de la E.S.E Alejandro Prospero Reverend.
- Las comunicaciones oficiales como memorandos, oficios, circulares y resoluciones se deberán diligenciar en los formatos establecidos, conforme a lo estipulado por el Proceso de Planeación Estratégica, las cuales están disponibles en la Intranet de la E.S.E Alejandro Prospero Reverend en el espacio "Formatos Institucionales", así mismo deben ser rotuladas de acuerdo con la información que contengan.

Manejo y Disposición Final de Discos Duros

Todo disco duro que deje de ser utilizado en la E.S.E Alejandro Próspero Reverend deberá someterse a un proceso de borrado seguro, asegurando que toda la información almacenada sea irrecuperable. En casos donde el disco duro esté destinado a disposición final, se procederá con su destrucción física siguiendo los procedimientos establecidos por la Oficina de Sistemas. Estas acciones se toman para garantizar que no se exponga información sensible o confidencial en desuso.

Control de acceso a la información y gestión de usuarios

El acceso a las redes y servicios de red de E.S.E Alejandro Prospero Reverend está regulado para asegurar la integridad, confidencialidad y disponibilidad de la información y los recursos tecnológicos. Esta política establece las normas y procedimientos para el uso seguro y eficiente de los recursos de red.

Acceso a Redes y Sistemas de Información

1. **Autenticación y Autorización**:

- Todo usuario debe ser autorizado antes de acceder a la red o a los Sistemas de Información de la E.S.E Alejandro Prospero Reverend.
- Se utilizarán métodos robustos de autenticación, como contraseñas seguras y autenticación de dos factores (2FA) donde aplique.

2. **Gestión de Usuarios**:
   - El acceso a la red o a cualquier Sistema de Información se otorgará solo a usuarios autorizados, basándose en sus roles y responsabilidades.
   - Las cuentas de usuario serán revisadas y actualizadas periódicamente para asegurar que los privilegios de acceso se mantengan apropiados.
3. **Gestión de Contraseñas:**
   - Las contraseñas generadas por los usuarios deben tener una complejidad media a alta, incluyendo letras mayúsculas y minúsculas, así como caracteres especiales.
   - La asignación y modificación de contraseñas se gestionará mediante un proceso formal a cargo de la Oficina de Sistemas de Información y Comunicaciones
   - La contraseña inicial asignada será la cédula del usuario y deberá ser cambiada en su primer ingreso al sistema.
   - Las contraseñas no deben ser escritas ni dejadas en lugares donde puedan ser vistas por otras personas.
4. **Uso Aceptable del Internet**:
   - El acceso a Internet debe utilizarse solo para actividades relacionadas con el trabajo y en alineación con los objetivos de la organización.
   - Está prohibido el uso de Internet para actividades ilegales, no éticas o no autorizadas.
5. **Control de Dispositivos**:
   - Solo dispositivos autorizados por la Oficina de Sistemas podrán conectarse a la red.
   - Los dispositivos personales deben cumplir con las políticas de seguridad establecidas antes de acceder a la red corporativa.
6. **Monitoreo y Registro:**
   - Se monitoreará y registrará el uso de Internet para asegurar el cumplimiento de las políticas.
   - Los registros de acceso a Internet se revisarán periódicamente para detectar y responder a actividades inusuales o no autorizadas.

Uso de Dispositivos Personales

La E.S.E Alejandro Próspero Reverend reconoce el uso de dispositivos personales como una herramienta para mejorar la eficiencia y flexibilidad de sus Funcionarios y Contratistas. Sin embargo, para asegurar la protección de la información y activos digitales, se

establecen las siguientes directrices para el uso de dispositivos personales dentro de la red de la organización:

1. **Registro, Autorización y Medidas de Seguridad Obligatorias**:
   - Todos los dispositivos personales que se utilicen para acceder a sistemas de información de la organización deben estar registrados y autorizados por la Oficina de Sistemas. Esto incluye, pero no se limita a, teléfonos móviles, tabletas y computadores portátiles.
   - Los dispositivos que requieran conexión a la red LAN o WiFi de la organización deben cumplir con los requisitos mínimos de seguridad establecidos. Estos incluyen:
     - Uso de software legal y actualizado.
     - Un antivirus o software de seguridad, con actualizaciones periódicas.
     - Contraseñas seguras para el acceso al dispositivo y aplicaciones.
2. **Almacenamiento de Información**:
   - Está prohibido almacenar información reservada de la organización de manera permanente en dispositivos personales. En casos necesarios, la información debe ser eliminada de manera segura después de su uso.
3. **Uso Responsable y Restricciones**:
   - Los dispositivos personales no deben ser utilizados para actividades no autorizadas o que puedan comprometer la seguridad de la información, como descargar software no aprobado o acceder a sitios web no seguros.
   - El uso de dispositivos personales debe estar alineado con los lineamientos de uso aceptable de la organización, evitando cualquier acción que pueda poner en riesgo la integridad de la red y los sistemas de información.
4. **Responsabilidad del Usuario**:
   - Los usuarios son responsables de la protección física y lógica de sus dispositivos personales. Esto incluye la notificación inmediata a la Oficina de Sistemas en caso de pérdida o robo del dispositivo.
   - El incumplimiento de estas directrices puede resultar en acciones disciplinarias, conforme a las políticas internas de la organización.
5. **Monitoreo y Auditoría**:
   - La E.S.E Alejandro Próspero Reverend se reserva el derecho de monitorear y auditar el uso de dispositivos personales para asegurar el cumplimiento de las políticas de seguridad.

Criptografia

La E.S.E Alejandro Prospero Reverend adoptará herramientas de cifrado para salvaguardar la confidencialidad e integridad de la información. De igual manera, la Oficina de Sistemas será responsable de identificar los equipos que requieran la implementación de controles criptográficos adicionales cuando sea necesario.

Firma Digital

Se emplean firmas digitales para asegurar la autenticidad e integridad de los documentos electrónicos. Este control garantiza que los documentos no han sido alterados desde su

firma, proporcionando confianza en la veracidad y la integridad de la información manejada dentro de la empresa.

Seguridad física y del entorno

Los espacios físicos donde se encuentren los sistemas de información de la E.S.E. Alejandro Próspero Reverend deben estar adecuadamente protegidos mediante controles de acceso perimetral, sistemas de vigilancia y medidas preventivas para evitar o mitigar el impacto de incidentes de seguridad (accesos no autorizados a sistemas de información, robo o sabotaje) y accidentes ambientales (incendios, inundaciones, cortes de suministro eléctrico, etc.). Además, debe existir un control de acceso físico en formato físico mediante un registro en papel que indique quién accede a dicha información.

Seguridad Operativa

Todos los sistemas de información de la E.S.E. Alejandro Próspero Reverend que procesan o almacenan información deben contar con medidas de seguridad adecuadas que optimicen su nivel de madurez (como la monitorización, control de cambios, revisiones, etc.). Además, se deben gestionar, controlar y monitorizar las redes de manera adecuada para protegerse de amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo los controles de acceso a la red, asegurando así la protección de toda la información transferida a través de estos medios.

Sistema de Vigilancia

La E.S.E. Alejandro Próspero Reverend cuenta con cámaras de vigilancia para el monitoreo continuo de sus instalaciones, las cuales operan las 24 horas del día, los 7 días de la semana. El acceso a las grabaciones de dichas cámaras debe ser solicitado formalmente a la Subgerencia Administrativa, a través de un correo electrónico dirigido a dicha dependencia. Las grabaciones podrán ser utilizadas como soporte o evidencia ante autoridades o entes de control, siempre y cuando se presente una solicitud oficial y formal, conforme a las normativas vigentes sobre la protección de datos y el uso adecuado de la información.

Seguridad en las Telecomunicaciones

La arquitectura de red de la E.S.E. Alejandro Próspero Reverend debe contar con medidas de prevención, detección y respuesta para evitar brechas en los dominios internos y externos. El "dominio interno" se refiere a la red local compuesta por los elementos tecnológicos accesibles exclusivamente desde la red interna. El "dominio externo" se refiere a la red accesible desde el exterior de la red de la entidad.

Control de acceso a las instalaciones

- El área de Talento Humano debe proporcionar regularmente un listado de Terceros que incluya nombres, apellidos, número de identificación y el área donde desempeñan sus funciones. Esta lista podrá ser utilizada por el personal de vigilancia para la verificación de identidad al ingresar a las instalaciones de la E.S.E Alejandro Prospero Reverend.

- El área Jurídica, a través de su proceso de contrataciones, debe entregar de manera periódica un listado de los Contratistas activos y desvinculados, con detalles como

nombres, apellidos, número de identificación y área de actividad. Este listado también podrá ser utilizado por el personal de vigilancia para verificar el ingreso a las instalaciones y por la Oficina de Sistemas para activar o desactivar el acceso a los Sistemas de Información.

- La E.S.E Alejandro Prospero Reverend, como responsable del manejo de datos personales, se compromete a utilizar dicha información únicamente para los fines establecidos en la Política de tratamiento de datos personales, la cual ha sido aprobada por la entidad y publicada en su página web: *http://www.esealejandroprosperoreverend-santamarta-magdalena.gov.co/*.
- El personal de vigilancia debe solicitar a todos los visitantes un documento de identificación vigente, preferiblemente con foto, para verificar los datos y confirmar telefónicamente con la persona o área que se visita. Una vez completada la verificación, el documento de identificación será devuelto al visitante inmediatamente.
- Es responsabilidad del personal de vigilancia registrar la entrada y salida de equipos de cómputo, portátiles y otros dispositivos electrónicos en el libro de registro de elementos situado en la recepción.
- La E.S.E Alejandro Prospero Reverend no asume la responsabilidad por equipos de cómputo, portátiles, dispositivos electrónicos u otros objetos personales que ingresen a la entidad. El cuidado y protección de estos elementos es responsabilidad exclusiva de su propietario, y el personal de vigilancia debe informar esto claramente a quienes ingresen dichos bienes a las instalaciones.
- El personal de vigilancia debe garantizar que ningún visitante salga de las instalaciones con activos de información de la entidad sin previa autorización de la Subgerencia Administrativa.
- Cuando un contratista acude a prestar un servicio externo dentro de las instalaciones de la E.S.E Alejandro Prospero Reverend, el funcionario o contratista que autoriza su ingreso debe acompañarlo de manera continua hasta que finalice la prestación del servicio.
- Cualquier ingreso de Servidores Públicos, Contratistas o Terceros fuera del horario laboral debe contar con la previa autorización de Subgerencia Administrativa

Seguridad en las operaciones y comunicaciones

La Oficina de Sistemas tiene la responsabilidad de:

- Gestionar la infraestructura tecnológica de la E.S.E Alejandro Prospero Reverend.
- Llevar a cabo el mantenimiento tanto preventivo como correctivo de equipos de cómputo, servidores, y UPS.
- Administrar el centro de datos, la gestión de licencias de software, y proporcionar la infraestructura tecnológica necesaria para el correcto funcionamiento de los servicios de información.
- Desarrollar y mantener los procedimientos relacionados con la gestión y

operación tanto de la plataforma tecnológica como de los servicios de información.

- Salvaguardar las claves de acceso a todos los servicios tecnológicos.
- Asegurar la protección de los recursos tecnológicos y bases de datos.
- Proveer y mantener actualizadas las herramientas de protección contra software malicioso.

Protección contra software malicioso

- La Oficina de Sistemas se encargará de configurar y administrar Windows Defender como la herramienta de seguridad antimalware oficial de la entidad, para minimizar el riesgo de infección por software malicioso.

- La Oficina actualizará regularmente Windows Defender para garantizar que las definiciones de virus y las actualizaciones de seguridad estén al día.
- Los Funcionarios y Contratistas no deben alterar o desactivar la configuración de Windows Defender en los equipos de propiedad de la E.S.E Alejandro Prospero Reverend.
- Los equipos de cómputo pertenecientes a los Contratistas deberán contar con una herramienta de antimalware, preferiblemente Windows Defender, que esté licenciada y actualizada.
- En caso de que Windows Defender detecte una infección en un equipo o archivo, los Funcionarios o Contratistas deberán notificar de inmediato a la Oficina de Sistemas.
- Si se sospecha o se confirma que un equipo está infectado por software malicioso, es responsabilidad de los Funcionarios y contratistas notificar a la oficina de Sistemas.

Gestión de seguridad en la red

- La E.S.E Alejandro Prospero Reverend asignará los recursos necesarios cada año para garantizar el correcto funcionamiento de la infraestructura de red.
- La Oficina de Sistemas será la encargada de gestionar la infraestructura de red y proporcionar la configuración necesaria para el desempeño de las funciones de cada área.
- La Oficina de Sistemas establecerá mecanismos para asegurar la disponibilidad y protección de la infraestructura de red de la entidad.
- La Oficina de Sistemas contará con medidas de seguridad que protejan contra amenazas y controlen el tráfico entrante y saliente en la red LAN de la entidad.
- La Oficina de Sistemas mantendrá la red segmentada por centros de cableado y acceso WIFI.
- La Oficina de Sistemas definirá y comunicará los estándares técnicos para la configuración de dispositivos de seguridad y de red en la plataforma tecnológica.

Seguridad de la Red WiFi

La E.S.E Alejandro Próspero Reverend implementará medidas de seguridad robustas para proteger su red WiFi. Estas medidas incluirán, pero no se limitarán a, la utilización de cifrado WPA3, autenticación de usuarios mediante credenciales seguras, y la segmentación de la red para aislar el tráfico sensible. El acceso a la red WiFi estará restringido a dispositivos

autorizados, y se realizará un monitoreo constante para detectar y mitigar cualquier intento de acceso no autorizado. Además, la Oficina de Sistemas será responsable de revisar y actualizar las configuraciones de seguridad de la red WiFi de manera periódica para asegurar la protección continua de la infraestructura.

Gestión de medios removibles

- **No Uso de Medios Removibles**: La E.S.E Alejandro Prospero Reverend prohíbe el uso de cualquier tipo de medio removible, incluyendo, USB, discos duros externos, y tarjetas de memoria, para la transferencia o almacenamiento de información corporativa.

- **Excepciones Justificadas:** En casos excepcionales donde sea absolutamente necesario el uso de medios removibles, el solicitante debe justificar la necesidad y obtener la aprobación previa por escrito del Jefe de Sistemas o del oficial de seguridad de la información.

- **Evaluación de Riesgos**: Toda solicitud de excepción será evaluada en términos de riesgo para la seguridad de la información. La evaluación debe incluir el tipo de datos a ser transferidos o almacenados, la duración del uso del medio removible, y las medidas de seguridad adicionales que se implementarán.

- **Registro y Monitoreo**: Todas las excepciones aprobadas serán registradas y monitoreadas estrictamente. El registro incluirá detalles como el tipo de dispositivo, el usuario autorizado, el propósito del uso, la fecha de emisión y cualquier medida de seguridad aplicada

- **Controles de Seguridad:** En los casos donde se haya otorgado una excepción, todos los datos almacenados en medios removibles deben ser encriptados utilizando algoritmos aprobados por la organización. La encriptación mediante BitLocker será requerida para todos los medios removibles utilizados.

- **Configuración de BitLocker:** Antes de utilizar cualquier medio removible aprobado, este deberá configurarse con BitLocker u otra herramienta de encriptación autorizada por la organización, para asegurar que todos los datos estén protegidos contra accesos no autorizados

- **Auditoría y Cumplimiento**: Se realizarán auditorías periódicas para asegurar el cumplimiento de esta política y detectar cualquier uso no autorizado de medios removibles.

- **Sanciones**: El uso no autorizado de medios removibles resultará en sanciones disciplinarias, de acuerdo con las políticas internas de la E.S.E Alejandro Prospero Reverend.

Adquisicion, desarrollo y mantenimiento de sistemas

La oficina de Sistemas velará que los sistemas de información implementados en la entidad cumplan con los requisitos de seguridad y sigan las mejores prácticas. Todos los procesos de la entidad deberán notificar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de recibir observaciones pertinentes y evaluar los aspectos técnicos necesarios para su desarrollo e implementación. Para los sistemas de información, aplicaciones y portales que manejen datos confidenciales o reservados, los líderes de Área de los servicios deben velar por el cumplimiento de los controles de seguridad que garanticen la preservación de la confidencialidad e integridad de la información.

La Oficina de Sistemas establece los lineamientos de seguridad de la infraestructura tecnológica, que garantizan el cumplimiento de los controles y la salvaguarda de la información de manera segura. Además, para la adquisición del parque computacional, se deberán cumplir con las siguientes especificaciones técnicas mínimas para garantizar un rendimiento óptimo y la compatibilidad con los sistemas de seguridad de la entidad:

- **Procesador**: Intel Core i5 11th Generación o superior
- **Memoria RAM**: 8 GB.
- **Disco Duro**: 512 GB SSD
- **Sistema Operativo**: Licencia de Windows 10 Pro o superior.
- **Suite Ofimática**: Licencia de Microsoft Office 2021 o superior.

Estas especificaciones aseguran que los equipos adquiridos cuenten con la capacidad y el rendimiento necesario para soportar las aplicaciones y sistemas utilizados en la entidad, así como para implementar los controles de seguridad requeridos.

Relaciones con los proveedores

La E.S.E Alejandro Prospero Reverend establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.

Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

Continuidad de la operación

En respuesta a los requisitos de calidad y buenas prácticas, la E.S.E. Alejandro Próspero Reverend debe disponer de un Plan de Continuidad de la operación como parte de su estrategia para garantizar la continuidad en la prestación de sus servicios esenciales o críticos y el adecuado manejo de los impactos sobre el negocio en posibles escenarios de crisis, proporcionando un marco de referencia para actuar en caso de ser necesario. Este Plan de Continuidad debe ser actualizado y probado periódicamente. Además, se debe definir y mantener actualizado un Plan de Recuperación ante Desastres alineado con la continuidad de negocio, abarcando la continuidad del funcionamiento de las tecnologías de información y comunicación.

La entidad debe encargarse de la formación y capacitación de todos sus funcionarios y contratistas en materia de Continuidad de la operación.

Gestión de incidentes de seguridad de la información

La E.S.E Alejandro Próspero Reverend establecerá un proceso claro para la gestión de incidentes de seguridad de la información. Esto incluirá la identificación, clasificación, y análisis de los incidentes, así como la implementación de medidas para contener y mitigar los daños. Se deberá notificar inmediatamente a las partes responsables, y se documentarán todos los incidentes y las acciones tomadas para su resolución. Además, se revisarán y actualizarán regularmente los procedimientos para mejorar la respuesta ante incidentes futuros.

Regulaciones para el uso de los recursos tecnológicos

Normas de Uso del Correo Electrónico

- **Uso Profesional**: El correo corporativo debe ser empleado exclusivamente para fines laborales, evitando el uso personal o el envío de mensajes masivos que no estén relacionados con la entidad. Cada usuario es responsable de la información contenida y de cualquier otra información adjunta.
- **Confidencialidad y Seguridad**: Se debe asegurar que la información sensible no se comparta sin la debida protección, y clasificación, además evitar abrir correos sospechosos que puedan contener malware o intentos de phishing.
- **Contenido Apropiado**: Está estrictamente prohibido utilizar el correo electrónico institucional para difundir o enviar mensajes anónimos, así como contenidos que sean insultantes, ofensivos, difamatorios, obscenos, que infrinjan los derechos de autor, o que de cualquier manera comprometan la integridad moral de personas o instituciones.
- **Respuestas y Reenvíos**: Se debe tener precaución al responder a todos o reenviar correos electrónicos. Los Funcionarios y Contratistas deben asegurarse de que solo los destinatarios pertinentes reciban el correo y que no se comparta información confidencial innecesariamente. Está prohibido el reenvío de correos que contengan información sensible sin la autorización correspondiente.

Normas de Navegación y Uso de Internet

- **Acceso Restringido**: El uso de internet debe limitarse a actividades relacionadas con el rol desempañado. Está prohibido visitar sitios web no relacionados con el ámbito laboral, como redes sociales o entretenimiento, salvo autorización explícita.
- **Descargas Seguras**: No está permitido la descarga de software sin la debida autorización y acompañamiento del Oficina de Sistemas. Los archivos

necesarios para el desempeño laboral se pueden descargar siempre y cuando sean de fuentes confiables.

- **Protección de la Información**: No se debe compartir información confidencial en sitios web sin las medidas de seguridad adecuadas. Se requiere el uso de conexiones seguras (HTTPS) para cualquier transmisión de datos sensibles.
- **Navegación Segura**: Se deben evitar sitios web sospechosos o potencialmente peligrosos que puedan comprometer la seguridad de la red corporativa. Los Funcionarios y Contratistas deben informar inmediatamente cualquier actividad sospechosa al Oficina de Sistemas de Información y Comunicaciones.

Normas para el Uso y Mantenimiento de Recursos Tecnológicos

- **Propiedad Corporativa**: Los equipos tecnológicos proporcionados por la empresa son para uso exclusivo en actividades laborales. El uso personal está estrictamente prohibido.
- **Mantenimiento y Cuidado**: Los Funcionarios, Contratistas y Terceros deben cuidar los equipos asignados, mantenerlos en buen estado y reportar cualquier daño o fallo técnico al Oficina de Sistemas de inmediato.
- **Control de Acceso**: Los dispositivos tecnológicos deben estar protegidos con contraseñas seguras y otras medidas de seguridad, como autenticación multi-factor, para evitar accesos no autorizados. Todos los sistemas de información deben disponer de un mecanismo de control de acceso.
- **Almacenamiento de Datos**: Toda la información y datos deben almacenarse en servidores y sistemas aprobados por la empresa. Está prohibido almacenar información corporativa en dispositivos personales o medios no autorizados.
- **Cierre de Sesión**: Los Funcionarios, Contratistas y Terceros deben asegurarse de cerrar sesión cuando no estén en uso, especialmente al final del día laboral o al dejar el puesto de trabajo.

Normas de Seguridad en Sistemas de Información

- **Control de Acceso lógico**: Solo se permite acceder a los sistemas de información con las credenciales y permisos asignados según el rol del Funcionario o Contratista. Cualquier intento de acceso no autorizado está prohibido y se considerará una violación de seguridad. Este control se centra en garantizar que solo los usuarios autorizados puedan acceder a los sistemas y así prevenir accesos no autorizados. Se incluyen medidas como la protección mediante contraseñas robustas.
- **Integridad de la Información**: Los Funcionarios y Contratistas deben asegurar que toda la información ingresada en los sistemas de la empresa sea precisa, actualizada y completa. Cualquier discrepancia o error debe ser corregido inmediatamente.
- **Uso Adecuado de Contraseñas**: Las contraseñas deben ser complejas, únicas y cambiadas regularmente. Compartir contraseñas con otras personas está prohibido.

- **Monitoreo de Actividades**: La empresa monitorea el uso de los sistemas de información para asegurar el cumplimiento de las políticas de seguridad. Cualquier actividad inusual o sospechosa debe ser reportada al Oficina de Sistemas de Información y Comunicaciones.

Ciclo de vida de usuarios en los Sistemas de Información

La E.S.E. Alejandro Próspero Reverend establece un sistema adecuado para gestionar el ciclo de vida de la identidad de los usuarios de los Sistemas de Información. La identidad es el conjunto de características que identifican de manera única a cada persona con acceso físico o lógico a los sistemas de información de la E.S.E. Alejandro Próspero Reverend. El ciclo de vida de la identidad abarca desde la creación hasta la eliminación de la identidad de un usuario.

Este ciclo incluye las siguientes actividades:

- Creación y asignación de la identidad.
- Revisión periódica.
- Modificación o eliminación.

La gestión del ciclo de vida de la identidad se encuentra enmarcada en la **Guía de Procedimientos de Sistemas de Información** la cual se encuentra alineada con la Oficina de Talento Humanos con el fin de verificar las identidades en función de las altas y bajas de Funcionarios y Contratistas y su correspondencia en los sistemas de información.

Copias de Respaldo

Se deberán realizar y verificar periódicamente copias de respaldo de la información, del software y del sistema. Estas copias incluirán aplicaciones, archivos y bases de datos y se realizarán de acuerdo al procedimiento de copias de respaldo, excepto en los casos donde no se hayan producido actualizaciones durante dicho periodo. En situaciones donde la información a proteger sea de alta importancia para la E.S.E Alejandro Prospero Reverend o de alta transaccionalidad, se puede aumentar la frecuencia de las copias de seguridad.

La periodicidad de las copias de seguridad se determinará según la sensibilidad de las aplicaciones o datos, siguiendo los criterios de clasificación de la información establecidos en procedimiento de copias de respaldo y deberán recibir el mismo nivel de protección que los datos originales, asegurando su conservación adecuada y la implementación de controles de acceso apropiados.

Se garantizará que exista una copia de respaldo de la información sensible, para asegurar su integridad en caso de necesitar una recuperación frente a posibles incidentes de seguridad, como los ataques de ransomware.

PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

La gestión de la privacidad y confidencialidad de los datos personales recolectados y tratados por la E.S.E ALEJANDRO PRÓSPERO REVEREND se rige de acuerdo con las directrices establecidas en la **Política de Tratamiento de Datos Personales E.S.E ALPROREV** en la cual se encuentra información detallada sobre los principios, derechos de los titulares, procedimientos y obligaciones respecto al tratamiento de datos personales, dando cumplimiento con lo dispuesto en la ley 1581 del 2012.
Esta Política está disponible en los canales internos de la institución y en el portal de WEB.

CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La E.S.E Alejandro Próspero Reverend en su proceso de mejora continua desarrollará e implementará programas de capacitación y sensibilización en seguridad de la información para todos sus Funcionarios y Contratistas.

Estos programas incluirán formación sobre el uso seguro de sistemas de información, la protección de datos personales, y las políticas de uso de tecnología. Se realizarán sesiones de actualización periódicas para asegurar que todos los Funcionarios y Contratistas estén al tanto de las amenazas emergentes y las mejores prácticas en seguridad de la información.

Política de Escritorio y Pantallas limpios

Se implementan las siguientes directrices para garantizar la seguridad en los puestos de trabajo:

- Los Funcionarios y Contratistas deben bloquear sus equipos cuando se ausenten de su puesto, ya sea manualmente (por el propio usuario) o automáticamente mediante la configuración de bloqueo de pantalla.
- Al final de la jornada laboral, el entorno de trabajo debe quedar ordenado. Esto incluye asegurarse de que todos los documentos o soportes de información no queden a la vista y guardar bajo llave aquellos que sean confidenciales, según los niveles de clasificación establecidos.
- El puesto de trabajo debe mantenerse organizado y libre de documentos o soportes de información que puedan ser vistos o accesibles por personas no autorizadas.

Revisión de la conformidad

La Política de Seguridad y Privacidad de la Información, será revisada anualmente, o antes si existiesen modificaciones que así lo requieran, para que se mantenga oportuna,

suficiente y eficaz. Este proceso será liderado por la oficina de Sistemas, revisado por el comité Institucional de Gestión y Desempeño o en su defecto por el Comité de Seguridad de la Información.

Sanciones disciplinarias

Cualquier violación de la presente Política de Seguridad de la Información puede resultar en la toma de acciones disciplinarias correspondientes de acuerdo con el proceso interno de la E.S.E. Alejandro Próspero Reverend. Es responsabilidad de todos los Funcionarios, Contratistas y Terceros notificar al responsable de Seguridad de la Información o a la oficina de Sistemas cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

	Elaboración	Cargo	Firma
Elaboró	Gonzalo Gonzales	Contratista sistemas	Gonzalo Gonzalez T.
Revisó	Adriana Ariza	P.U. Con funciones de sistemas	
Aprobó	Haroldo Pizarro	Gerente	
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales y/o técnicas vigentes, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma.			