## INTRODUCCIÓN.

La información es uno de los activos más valiosos para la gestión eficiente y segura de los servicios de salud. En ese sentido, la Red de Salud Ladera E.S.E., como entidad pública prestadora de servicios de salud, reconoce la importancia de proteger la confidencialidad, integridad y disponibilidad de su información, así como garantizar el adecuado manejo de los activos asociados a ella, en concordancia con la normativa vigente del Estado colombiano.

Este Manual de Políticas de Seguridad y Privacidad de la Información establece los lineamientos fundamentales para implementar y fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) en la Red de Salud Ladera E.S.E., en armonía con los principios de la Política de Gobierno Digital, adoptada mediante el Decreto 1008 de 2018 y regulada por el Manual de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Asimismo, este manual se construye con base en la normativa colombiana, especialmente en lo establecido por la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1712 de 2014 sobre transparencia y acceso a la información pública, la Ley 1273 de 2009 en materia de delitos informáticos, y el Decreto 1078 de 2015, que reglamenta el sector TIC. También incorpora buenas prácticas internacionales, tales como las definidas en la norma NTC ISO/IEC 27001:2013, promoviendo una cultura institucional orientada a la gestión de riesgos, la mejora continua y la confianza digital.

Este documento tiene como propósito establecer políticas claras, responsables y actualizadas que orienten a todos los funcionarios, contratistas y terceros vinculados a la Red de Salud Ladera E.S.E. en el uso correcto de los activos de información, previniendo incidentes, protegiendo los derechos de los ciudadanos y garantizando la continuidad de las operaciones en un entorno seguro.

VIGILADO Supersalud

## TABLA DE CONTENIDO:

INTRODUCCION. ..... 1

TABLA DE CONTENIDO: ..... 2

1. OBJETIVOS. ..... 4

2. ALCANCE: ..... 4

3. REQUISITOS LEGALES. ..... 4

4. DEFINICIONES: ..... 6

5. LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION ..... 12

5.1. ORGANIZACIÓN INTERNA: ..... 12

5.2. SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES EN LA GESTIÓN DE PROYECTOS: ..... 13

5.3. DISPOSITIVOS MÓVILES Y TRABAJO VIRTUAL: ..... 14

5.3.1. Uso de Dispositivos Móviles ..... 14

5.3.2. Seguridad y Privacidad de la Información para el Trabajo Virtual: ..... 16

5.4. LINEAMIENTO DE SEGURIDAD DE LOS RECURSOS HUMANOS: ..... 20

5.5. LINEAMIENTOS DE GESTIÓN DE ACTIVOS: ..... 22

5.5.1. Clasificación y niveles de protección ..... 24

5.5.2. Manejo de Activos de Información ..... 25

5.5.3. Disposición de los Medios Físicos y Digitales (Hardware y Software) ..... 26

5.5.4. Transferencia de Medios ..... 27

5.6.1. Lineamientos para el control de accesos lógico: ..... 29

5.6.2. Responsabilidades de los Usuarios en Control de Acceso ..... 32

5.6.3. Acceso y Servicios a Redes ..... 33

VIGILADO Supersalud

5.6.4. Claves de Acceso..... 33

5.7. Lineamiento de Criptografía:..... 35

5.8. Lineamiento de seguridad física y del entorno: ..... 35

5.9. Lineamiento de seguridad en las operaciones: ..... 36

5.10. Lineamiento de seguridad de las comunicaciones:..... 36

5.11. Lineamientos de Adquisición, desarrollo y mantenimiento de sistemas:..... 36

5.12. Lineamientos de relaciones con los proveedores: ..... 37

5.13. Lineamiento de seguridad de la información en la continuidad del negocio:..... 37

5.14. Lineamientos de gestión de incidentes: ..... 38

5.15. Lineamientos de cumplimiento: ..... 38

5.16. Lineamiento de escritorio limpio:..... 38

5.17. Lineamiento de uso adecuado del internet:..... 39

5.18. Lineamiento de uso de correo electrónico:..... 39

5.19. Lineamiento de uso de usuarios y contraseñas: ..... 40

6. SENSIBILIZACION Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACION:..... 40

6.1. SENSIBILIZACIÓN Y COMUNICACIÓN: ..... 40

6.2. CAPACITACIONES EN SEGURIDAD: ..... 41

7. PROBACION Y REVISION:..... 41

8. SANCIONES: ..... 41

9. BIBLIOGRAFIA. ..... 42

VIGILADO Supersalud

## 1. OBJETIVOS.

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la Política General de Seguridad de la Información con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de la Red de Salud Ladera E.S.E.

## 2. ALCANCE:

Aplica para todos los procesos, área y dependencias, Directivos, funcionarios, Contratistas, Proveedores y Terceros que presten sus servicios o tengan alguna relación con la Red de Salud Ladera E.S.E, y de igual manera para todos los activos de información que hacen parte de la infraestructura tecnológica.

## 3. REQUISITOS LEGALES.

| LEGALES | APLICABILIDAD |
|---|---|
| Constitución Política de Colombia (1991) | Artículo 15: Reconoce el derecho a la intimidad personal y familiar y a la protección de los datos personales.<br>Artículo 20: Garantiza la libertad de información y el acceso a documentos públicos. |
| Ley 1581 de 2012 – Ley de Protección de Datos Personales | Establece disposiciones generales para la protección de datos personales y los derechos de los titulares, así como las obligaciones de los responsables y encargados del tratamiento de información. |
| Decreto 1377 de 2013 | Reglamenta parcialmente la Ley 1581 de 2012, en aspectos como la autorización para el tratamiento de datos personales y los mecanismos para ejercer los |

VIGILADO Supersalud



icontec ISO 9001 co-sc 7215-1
IQNET CERTIFIED MANAGEMENT SYSTEM

| | |
|---|---|
| | derechos de los titulares. |
| Ley 1273 de 2009 | Introduce el delito informático en Colombia y crea nuevos tipos penales relacionados con la protección de la información y los datos |
| Ley 1341 de 2009 – Ley TIC | Define principios y conceptos sobre la sociedad de la información y establece el marco para el desarrollo del sector TIC en Colombia. |
| Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC | Compila la normatividad del sector TIC. Contiene lineamientos específicos sobre el uso y administración de tecnologías de la información por parte de entidades públicas. |
| Política de Gobierno Digital (antes Estrategia de Gobierno en Línea) | Adoptada mediante el Decreto 1008 de 2018 y actualizada por el Manual de Gobierno Digital del Ministerio TIC. Establece lineamientos para el fortalecimiento institucional, uso estratégico de las TIC, gestión de la información y servicios digitales en las entidades públicas. |
| Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC | Guía técnica y normativa para la implementación de políticas, controles y buenas prácticas en la gestión de la seguridad de la información en entidades del Estado. |
| Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública | Establece que toda información generada, obtenida o en poder de los sujetos obligados es pública y debe ser accesible a los ciudadanos, con excepciones específicas. |
| NTC ISO/IEC 27001:2013 y 27002:2013 | Normas técnicas que establecen requisitos y buenas prácticas para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Adoptadas como referencia técnica en Colombia para la implementación |

VIGILADO Supersalud

| | |
|---|---|
| | de seguridad de la información. |
| Código de Ética y Buen Gobierno | Regula la conducta de los servidores públicos, fomentando principios de transparencia, responsabilidad y compromiso en el manejo de la información institucional. |
| Código Disciplinario Único – Ley 1952 de 2019 | Contempla las faltas disciplinarias relacionadas con el uso inadecuado de la información y de los medios tecnológicos en el sector público. |

## 4. DEFINICIONES:

- **Acceso privilegiado:** Acceso dado a usuarios autorizados para el manejo de cuentas especiales relacionadas con sistemas críticos, bases de datos, redes de comunicaciones y herramientas de seguridad de la información.
- **Activo Tecnológico:** Son elementos físicos y lógicos que hacen parte de la infraestructura tecnológica (hardware y software), y redes de comunicaciones.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. [ISO/IEC 27000:2018].
- **Amenaza informática:** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado [Ministerio de Defensa de Colombia].
- **Análisis de riesgos:** Proceso de comprender la naturaleza del riesgo y determinar el nivel de riesgo. [ISO/IEC 27000:2018]. Proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para tratar el riesgo.
- **Ataques cibernéticos:** Son ataques que tienen motivaciones económicas, sociales o políticas y se llevan a cabo a través de Internet, son dirigidos al público en general, a organizaciones privadas o países.
- **Autenticación:** Permite establecer la validez de la información reconociendo la fuente y medio de verificación.

VIGILADO Supersalud

- **Autenticidad:** Capacidad de demostrar la identidad del emisor con el objetivo de certificar que los datos, o la información, provienen realmente de la fuente que dice ser.
- **Base de Datos:** Se entiende como el conjunto organizado de datos corporativos y personales que sea objeto de Tratamiento.
- **Ciberamenaza:** Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste. [Glosario de Términos (CCN-STIC 401)].
- **Ciberdefensa:** Concepto que engloba todas las actividades ofensivas y defensivas en las que se utilizan como medio aquellos relacionados con las infraestructuras TIC (Ej. Redes de computadoras, computadoras, programas informáticos, etc.), y cuyo campo de batalla es el Ciberespacio. Las actividades de desarrollo de la ciberdefensa van encaminadas hacia la capacitación de los gobiernos y naciones en la denominada Ciberguerra. (Glosario de Términos [CCN-STIC 401]).
- **Ciberespacio:** Espacio virtual que engloba todos los sistemas TIC, tanto sistemas de información como sistemas de control industrial. El ciberespacio se apoya en la disponibilidad de Internet como red de redes, enriquecida con otras redes de transporte de datos. Los sistemas interconectados en espacios aislados no forman parte del ciberespacio. (Glosario de Términos (CCN-STIC 401)).
- **Ciberincidente**: Incidente relacionado con la seguridad de las TIC que se produce en el Ciberespacio. Este término engloba aspectos como los ataques a sistemas TIC, el fraude electrónico, el robo de identidad, el abuso del Ciberespacio, etc. (Glosario de Términos (CCN-STIC 401)).
- **Ciberseguridad:** Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan. (Glosario de Términos (CCN-STIC 401)).
- **COLCERT:** Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
- **Confidencialidad:** Propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000:2018].
- **Contraseña Fuerte:** Contraseña que consta mínimo de nueve caracteres, mayúsculas, minúsculas, números y caracteres especiales.
- **Contratista:** Persona natural o jurídica contratada por la Agencia Nacional Digital para la adquisición de una obra, bien o servicio, no perteneciente al régimen laboral.

VIGILADO Supersalud

- **Control:** Es una medida que modifica el riesgo. [ISO/IEC 27000:2018]. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

- **Copias de Seguridad:** Es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla en caso de que ocurra un fallo que afecte a esta y pueda estar disponible.

- **Custodio de activo de información:** Parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar, modificar, leer, procesar y hacer efectivos los controles de seguridad definidos, tales como copias de seguridad.

- **Datos abiertos:** Todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que Terceros puedan reutilizarlos y crear servicios derivados de los mismos" (Ley 1712 de 2014. Literal J, artículo 6. Definiciones).

- **Datos biométricos:** Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. (Reglamento (UE) 2016/679 del parlamento europeo y del consejo).

- **Dato personal:** hace referencia a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

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

- **Dato privado:** es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

VIGILADO Supersalud

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

- **Dato semiprivado:** Son los datos que no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo al titular sino a cierto sector o a la sociedad general, como es el caso de los datos financieros y crediticios de la actividad comercial o de servicios.

- **Disponibilidad:** Propiedad de ser accesible y utilizable a la demanda por una entidad autorizada. [ISO/IEC 27000:2018].

- **Encargado del Tratamiento:** Es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos por cuenta del responsable del Tratamiento.

- **Activo de información**: Cualquier información que tenga valor para la entidad y los medios que permiten su tratamiento, tales como bases de datos, historias clínicas, documentos físicos o digitales, sistemas de información, dispositivos electrónicos, redes, software, servicios en la nube, personas y procesos asociados. Los activos de información deben ser identificados, clasificados y protegidos conforme a su criticidad.

- **Confidencialidad:** Propiedad de la información que asegura que solo las personas, procesos o sistemas autorizados puedan acceder a ella. Garantiza que los datos sensibles, como la información clínica de los pacientes, no sean divulgados a terceros sin autorización.

- **Integridad:** Propiedad que garantiza que la información se mantenga completa, exacta, y libre de alteraciones no autorizadas durante su almacenamiento, procesamiento o

VIGILADO Supersalud

transmisión. Preservar la integridad evita errores que puedan poner en riesgo decisiones clínicas o administrativas.

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando se requiera por los usuarios autorizados. Incluye medidas para prevenir interrupciones, garantizar respaldo y continuidad del servicio en situaciones críticas.

- **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de políticas, procedimientos, recursos, controles y estructuras organizativas que permiten gestionar de forma sistemática la seguridad de la información, con base en un enfoque de gestión del riesgo y mejora continua.

- **Datos personales:** Cualquier información vinculada o que pueda asociarse a una persona natural identificada o identificable, como nombres, cédula, dirección, número de teléfono, historia clínica, entre otros. Se clasifican como públicos, semiprivados, privados o sensibles, conforme a la Ley 1581 de 2012.

- **Datos personales sensibles:** Categoría especial de datos personales cuyo uso indebido puede afectar gravemente los derechos fundamentales del titular, como datos relacionados con la salud, orientación sexual, convicciones religiosas o políticas, entre otros. Requieren mayor protección y medidas de seguridad.

- **Incidente de seguridad de la información:** Evento o conjunto de eventos no deseados o inesperados que tienen una alta probabilidad de afectar negativamente la seguridad de la información, como accesos no autorizados, fuga de datos, virus, fallas de disponibilidad o alteraciones indebidas.

- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza explote una vulnerabilidad de un activo de información, generando un impacto negativo sobre los

VIGILADO Supersalud

objetivos de la entidad. La gestión de riesgos permite identificar, evaluar y tratar los riesgos para minimizar su impacto.

- **Control:** Medida técnica, administrativa, física o legal implementada para mitigar los riesgos que amenazan la seguridad de la información. Los controles pueden ser preventivos, detectivos o correctivos.

- **Usuario:** Persona natural que accede a los sistemas o servicios de información de la entidad en función de sus responsabilidades laborales, contractuales o de prestación de servicios. Todo usuario debe firmar el acuerdo de confidencialidad y conocer las políticas de seguridad.

- **Tercero:** Persona natural o jurídica que tiene relación contractual o legal con la entidad y que, en desarrollo de sus funciones, puede acceder a activos de información. Incluye contratistas, proveedores, asesores externos, entre otros.

- **Clasificación de la información:** Proceso mediante el cual se asigna un nivel de criticidad o sensibilidad a la información, con el fin de aplicar controles adecuados de seguridad. Los niveles comunes son: pública, interna, confidencial y restringida.

- **Criptografía:** Técnica que permite proteger la información mediante el uso de algoritmos y claves que aseguran su confidencialidad, autenticidad y/o integridad durante la transmisión o almacenamiento.

- **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que decide sobre la finalidad y tratamiento de los datos personales. En este caso, la Red de Salud Ladera E.S.E. actúa como responsable de la información personal que recolecta y gestiona.

VIGILADO Supersalud

## 5. LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

### 5.1. ORGANIZACIÓN INTERNA:

La Red de Salud Ladera E.S.E. establece una estructura organizacional y funcional para garantizar la gestión de la seguridad de la información y la privacidad de los datos personales de usuarios, colaboradores, estudiantes, contratistas y proveedores.

El proceso de Seguridad y Privacidad de la Información hace parte del direccionamiento estratégico de la Alta Dirección, constituyéndose en un eje transversal que impacta todos los procesos misionales, de apoyo y estratégicos, asegurando la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.

En este marco:

Se debe establecer y mantener contacto con las autoridades competentes en materia de seguridad de la información y protección de datos, con el fin de dar cumplimiento a la normatividad vigente en Colombia (Ley 1581 de 2012, Ley 1273 de 2009, Ley 1712 de 2014, Decreto 1377 de 2013, entre otras) y las disposiciones internas de la Red.

La Red de Salud Ladera E.S.E. debe contar con una lista actualizada de contactos de las autoridades competentes, empresas de servicios públicos (energía, agua, comunicaciones, seguridad), organismos de respuesta a emergencias (bomberos, defensa civil) y autoridades judiciales o de investigación, que permita garantizar una actuación inmediata ante incidentes o eventos de seguridad.

En caso de ataques, incidentes o delitos cibernéticos, la Red informará oportunamente a las autoridades competentes, con el fin de activar las investigaciones correspondientes y adelantar las acciones legales y técnicas que se requieran.

Se fomentará el contacto con grupos especializados en seguridad de la información y ciberseguridad, así como la participación en foros, alianzas estratégicas y eventos de actualización tecnológica que permitan fortalecer el conocimiento institucional sobre:

VIGILADO Supersalud

- Mejores prácticas en seguridad de la información.
- Alertas tempranas sobre amenazas y vulnerabilidades.
- Procedimientos de resolución de incidentes.
- Acceso a asesorías técnicas especializadas.
- Implementación de tecnologías de punta en ciberseguridad.

Todos los funcionarios, contratistas y terceros que desempeñen funciones relacionadas con el manejo de la información institucional o de los sistemas de información deben estar vinculados y comprometidos con el proceso de Seguridad y Privacidad de la Información, participando en programas de capacitación, sensibilización y control.

## 5.2. SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES EN LA GESTIÓN DE PROYECTOS:

La Red de Salud Ladera E.S.E. debe garantizar que todos los proyectos institucionales, tanto internos como externos, cuenten con información documentada en materia de seguridad de la información, asegurando la confidencialidad, integridad, disponibilidad y trazabilidad de los datos generados o utilizados durante su ejecución.

En este sentido:

- Todos los proyectos deben incorporar desde su planeación requisitos explícitos de seguridad de la información, privacidad de los datos personales y gestión de riesgos asociados.
- Dichos requisitos serán definidos por el Proceso de Seguridad y Privacidad de la Información, y deberán ser adoptados, implementados y supervisados por los Gerentes o responsables de proyecto.
- Los responsables de los proyectos deben velar por el cumplimiento de estos lineamientos, realizando revisiones periódicas y aplicando los mecanismos de

VIGILADO Supersalud

seguimiento establecidos por la Red de Salud Ladera E.S.E. para la gestión de proyectos.

- Los riesgos de seguridad y privacidad asociados a cada proyecto deben ser identificados, documentados y gestionados de acuerdo con la metodología institucional de gestión de riesgos.
- Cualquier incumplimiento de los requisitos de seguridad de la información o de protección de datos personales deberá ser reportado de forma inmediata por el supervisor del contrato, gerente o responsable del proyecto a las partes interesadas, incluyendo al área de Seguridad de la Información, para activar los planes de acción correspondientes.
- Los supervisores, gerentes o responsables de proyectos están obligados a notificar de manera oportuna los incidentes, eventos o riesgos de seguridad que se presenten, aplicando el procedimiento institucional de notificación y gestión de incidentes de seguridad de la información, así como la metodología de gestión de riesgos definida.

## 5.3. DISPOSITIVOS MÓVILES Y TRABAJO VIRTUAL:

La Red de Salud Ladera E.S.E. garantizará la seguridad de la información institucional y la protección de los datos personales a través del uso controlado de dispositivos móviles y la implementación de modalidades de trabajo virtual por parte de funcionarios de planta, contratistas y proveedores de servicios autorizados.

### 5.3.1. Uso de Dispositivos Móviles

La Red de Salud Ladera E.S.E. establece las siguientes directrices para el aseguramiento de la información en el uso de dispositivos móviles:

- Los procesos de Seguridad y Privacidad de la Información y de Tecnologías de la Información (TIC) evaluarán los requisitos mínimos de seguridad y privacidad en los

VIGILADO Supersalud

dispositivos móviles personales utilizados por funcionarios o contratistas en el desarrollo de sus actividades laborales.

- El uso de dispositivos móviles institucionales será de carácter exclusivo para el desarrollo de actividades laborales o contractuales, quedando prohibido su uso para fines personales.

- Los funcionarios y contratistas que utilicen dispositivos móviles personales deberán acatar las medidas de seguridad de la información y privacidad de los datos personales, informando de manera inmediata a su jefe inmediato o al supervisor de contrato sobre cualquier incidente o riesgo que pueda afectar la información de la entidad.

- Está prohibido descargar información institucional en dispositivos no autorizados o en repositorios personales sin la autorización expresa del proceso de Seguridad y Privacidad de la Información.

- Todos los dispositivos en los que se procese, almacenen o transmita información institucional deben cumplir con las políticas de seguridad y privacidad de la Red de Salud Ladera E.S.E.

- Los dispositivos móviles adquiridos o autorizados por la entidad deberán estar registrados en el inventario de activos de información y administrados bajo el proceso de gestión de TIC.

- Todo dispositivo móvil deberá contar con software legal y debidamente licenciado, ya sea comercial u open source.

VIGILADO Supersalud

- El uso responsable de los dispositivos móviles institucionales es obligación de cada funcionario, incluyendo su custodia, cuidado físico y cumplimiento de las normas de seguridad digital.

- La Subgerencia Administrativa y Financiera será la responsable de establecer controles tecnológicos y administrativos sobre el uso de los dispositivos móviles institucionales.

- En caso de uso de dispositivos móviles personales para labores institucionales, deberá configurarse una sesión independiente destinada exclusivamente a actividades laborales o contractuales.

- Toda información institucional deberá almacenarse únicamente en los repositorios autorizados por la Red de Salud Ladera E.S.E., evitando el almacenamiento en dispositivos móviles personales.

- El soporte y mantenimiento de software y hardware de los dispositivos personales autorizados para actividades laborales será responsabilidad directa del usuario.

### 5.3.2. Seguridad y Privacidad de la Información para el Trabajo Virtual:

La Red de Salud Ladera E.S.E. reconoce el trabajo virtual como una modalidad válida para el cumplimiento de actividades laborales o contractuales de sus funcionarios, contratistas y terceros autorizados, de acuerdo con la normatividad colombiana vigente (Ley 1221 de 2008 sobre teletrabajo, Decreto 884 de 2012, Ley 2121 de 2021 sobre trabajo remoto y demás aplicables).

Con el fin de proteger la información institucional y los datos personales de los usuarios, se establecen los siguientes lineamientos:

VIGILADO Supersalud

**Ubicación del colaborador y acceso a los activos de información:**

- Es responsabilidad de todos los colaboradores (funcionarios, contratistas y terceros) aplicar los lineamientos de seguridad y privacidad de la información al realizar actividades laborales fuera de las instalaciones físicas de la Red de Salud Ladera E.S.E.
- Previo a la autorización del trabajo virtual, se deberá realizar una identificación y análisis de riesgos de seguridad y privacidad de la información, en conjunto con los procesos de Gestión del Talento Humano, Jurídica y TIC, con el fin de garantizar el nivel adecuado de protección.
- El acceso a los sistemas institucionales (ej. RFAST, SICODA, aplicativos financieros, correo corporativo) deberá realizarse mediante conexiones seguras (VPN o mecanismos equivalentes autorizados por TIC).
- Está prohibido el uso de redes públicas no seguras (ej. aeropuertos, cafés internet, redes abiertas) para el desarrollo de actividades laborales o contractuales relacionadas con información institucional.
- El acceso a actividades virtuales deberá hacerse exclusivamente con el correo electrónico corporativo, siguiendo los lineamientos de seguridad y confidencialidad establecidos.
- Las redes WiFi personales utilizados para trabajo virtual deben configurarse bajo estándares de seguridad mínimos (WPA2 o superior) y cumplir con la política institucional de contraseñas, que exige cambios periódicos (mínimo cada 3 meses).
- En caso de que el trabajo se realice en equipos personales, el usuario deberá crear una sesión independiente exclusiva para las actividades laborales. Si el equipo es institucional, solo podrá utilizarse para fines laborales y contractuales.
- La información institucional debe ser almacenada únicamente en los repositorios oficiales y autorizados por el proceso de Gestión Documental, evitando el uso de discos locales, memorias USB o nubes personales.

VIGILADO Supersalud

- Todos los accesos deberán cumplir con las políticas de control de acceso establecidas en el marco de seguridad de la información institucional.
- Los dispositivos utilizados para trabajo virtual deberán contar con software legal y licenciado, conforme a la política de gestión de activos y a la política de derechos de autor y propiedad intelectual de la Red de Salud Ladera E.S.E.

**Obligaciones para salvaguardar y custodiar la seguridad y privacidad de la información en el trabajo virtual:**

Los colaboradores de la Red de Salud Ladera E.S.E. (funcionarios de planta, contratistas o terceros autorizados) son responsables de la seguridad y privacidad de la información que procesan, consultan o generan en el marco de sus actividades, de acuerdo con los lineamientos, controles y políticas institucionales.

**Responsabilidades de los colaboradores**

- Bloquear o apagar el equipo cuando no esté en uso, a fin de proteger la información de accesos no autorizados.
- Realizar el cambio periódico de contraseñas conforme a la política institucional de control de acceso.
- Custodiar la información conforme a lo establecido en la Ley 1581 de 2012 (protección de datos personales) y demás normativa aplicable.
- Utilizar la información y los sistemas institucionales de manera ética, garantizando el respeto a los derechos de autor y propiedad intelectual.
- Reconocer que la información institucional es propiedad de la Red de Salud Ladera E.S.E., incluyendo aquella suministrada o generada en el desarrollo de actividades laborales o contractuales.

VIGILADO Supersalud

**Consecuencias del incumplimiento:**

El incumplimiento de estas políticas por parte de los funcionarios de planta estará sujeto a medidas disciplinarias según el reglamento interno de trabajo y los procedimientos establecidos en la entidad.

El incumplimiento por parte de contratistas, proveedores o terceros será gestionado de acuerdo con lo estipulado en los contratos de prestación de servicios, pudiendo dar lugar a sanciones, declaratorias de incumplimiento o terminación contractual.

**Soporte y mantenimiento de equipos**

El proceso de Gestión de Tecnologías de la Información (TIC), en coordinación con la Gestión Administrativa, es responsable de garantizar el soporte y mantenimiento del hardware y software de los dispositivos institucionales utilizados en trabajo virtual, conforme a la política de adquisición, desarrollo y mantenimiento de sistemas de información de la Red.

Los dispositivos personales empleados para actividades laborales o contractuales no serán objeto de soporte ni mantenimiento por parte de la Red, siendo esta responsabilidad exclusiva del usuario.

La Gestión Administrativa y Financiera deberá garantizar la contratación de pólizas de seguro que amparen los dispositivos institucionales, incluyendo aquellos asignados al trabajo virtual, frente a pérdida, daño o hurto.

VIGILADO Supersalud

## 5.4. LINEAMIENTO DE SEGURIDAD DE LOS RECURSOS HUMANOS:

La Red de Salud Ladera E.S.E. implementará controles y procedimientos específicos para garantizar que el personal vinculado bajo cualquier modalidad contractual (funcionarios de planta, contratistas y terceros) cumpla con los requisitos de idoneidad, seguridad y confidencialidad en el manejo de la información institucional y de los datos personales.

**Procesos de selección, vinculación y desvinculación**

- Se establecerán procedimientos formales de selección, vinculación y desvinculación, que incluyan criterios de seguridad de la información y protección de datos personales.
- Durante el proceso de contratación o vinculación, se realizará la verificación de antecedentes laborales, disciplinarios, fiscales y judiciales, conforme a la reglamentación vigente.
- Todo cambio administrativo o contractual deberá ser notificado al proceso de Seguridad y Privacidad de la Información por parte de Talento Humano de forma semanal o bajo demanda, según corresponda.

**Confidencialidad y no divulgación**

- Todos los colaboradores (funcionarios, contratistas y terceros) deberán firmar un Acuerdo de Confidencialidad y No Divulgación al inicio de su vinculación o contrato.
- En los contratos laborales, de prestación de servicios y en las actas de posesión, se deberá incluir de manera obligatoria una cláusula de confidencialidad y protección de la información.

VIGILADO Supersalud

- La información institucional, incluidos los datos clínicos, administrativos y financieros, será considerada propiedad exclusiva de la Red de Salud Ladera E.S.E., por lo que su uso indebido generará sanciones legales, disciplinarias y contractuales.

**Responsabilidades del personal**

- Todos los funcionarios, contratistas y terceros deberán dar cumplimiento estricto a las políticas de seguridad de la información y privacidad de datos personales establecidas por la Red.

- Se deberán establecer los términos y condiciones de empleo o contratación, incluyendo responsabilidades claras en materia de seguridad de la información y privacidad.

**Capacitación y sensibilización**

- La capacitación en seguridad de la información y protección de datos personales será obligatoria para todo el personal, incluyéndose en los programas de inducción, reinducción y capacitación anual de la Red.
- Los temas relacionados con confidencialidad, protección de la historia clínica, acceso seguro a la información y ciberseguridad deberán formar parte del plan institucional de formación anual.

**Control disciplinario y gestión de accesos**

- Se establecerá un proceso formal de control disciplinario que contemple los posibles incumplimientos o violaciones a las políticas de seguridad de la información y privacidad de datos personales.

VIGILADO Supersalud

- Frente a la terminación de contratos o cambios de roles, se aplicarán controles de seguridad para proteger la información institucional, incluyendo la revocación o ajuste de accesos a los sistemas de información.

- El proceso de Gestión de Talento Humano deberá enviar mensualmente, o de manera inmediata cuando sea necesario, las novedades administrativas y contractuales al área de TIC, con el fin de realizar la adecuada gestión de accesos a los sistemas institucionales.

## 5.5. LINEAMIENTOS DE GESTIÓN DE ACTIVOS:

La Red de Salud Ladera E.S.E. debe gestionar sus activos de información de acuerdo con las políticas institucionales, asegurando su identificación, valoración, clasificación, uso adecuado, trazabilidad y mejora continua, garantizando en todo momento la confidencialidad, integridad y disponibilidad (CID) de la información institucional.

### Responsabilidades en la gestión de activos

- Los líderes de proceso son responsables de identificar, registrar y mantener actualizados en la matriz de activos de información los activos bajo su custodia.
- Todo activo de información deberá contar con un propietario y un responsable designados en el inventario institucional.
- Los activos de información podrán ser utilizados exclusivamente con fines laborales o contractuales, de acuerdo con las funciones y responsabilidades asignadas.
- Los funcionarios, contratistas y terceros deberán devolver todos los activos de información asignados al finalizar su relación laboral o contractual.

VIGILADO Supersalud

**Trazabilidad y control de activos:**

- La salida de activos de información fuera de las instalaciones deberá realizarse mediante un procedimiento formal de disposición y control, dejando registro de la trazabilidad.

- Todos los equipos de cómputo deberán contar con software antimalware institucional y configuraciones de seguridad definidas por TIC.

- Los funcionarios, contratistas y terceros solo podrán acceder a los activos de información previa autorización del propietario del activo y conforme a los procedimientos institucionales de control de acceso.

**Respaldo y continuidad**

- Todos los colaboradores deberán realizar copias de seguridad de la información clasificada como Pública Clasificada o Pública Reservada, según las políticas establecidas en el Manual de Backup y Plan de Continuidad del Negocio.

- Toda modificación, actualización o reemplazo de activos tecnológicos deberá cumplir con el procedimiento de Gestión de Cambios definido por la entidad.

**Gestión de riesgos y reporte de incidentes**

- Los funcionarios, contratistas y terceros deberán aplicar la metodología institucional de gestión de riesgos, identificando y tratando los riesgos de seguridad de la información y privacidad de datos personales que afecten los activos bajo su custodia.

VIGILADO Supersalud

- Todo evento o incidente de seguridad que afecte los activos de información deberá ser reportado de manera inmediata al proceso de Seguridad y Privacidad de la Información.

**Usos inapropiados de los activos de información**

Se consideran usos indebidos de los activos de información, los siguientes:

- Incumplir las políticas de seguridad y privacidad de la información y datos personales.
- Hacer mal uso o abuso de los activos bajo custodia.
- Modificar información sin autorización.
- Divulgar información de manera no autorizada.
- Impedir el acceso a información sin justificación válida.
- Alterar, desactivar o eliminar controles de seguridad.
- Realizar cualquier acción ilegal o no autorizada sobre la información.
- Usar los activos institucionales para fines personales o distintos a los autorizados.
- Instalar o usar software ilegal o sin licencia.

### 5.5.1. Clasificación y niveles de protección

La Red de Salud Ladera E.S.E. establecerá niveles de protección de la información de acuerdo con:

- Su importancia estratégica
- Los requisitos legales y normativos (Ley 1581 de 2012, Ley 23 de 1982, Resolución 3100 de 2019, entre otras).
- Las necesidades administrativas y operativas de la entidad

VIGILADO Supersalud

### 5.5.2. Manejo de Activos de Información

La Red de Salud Ladera E.S.E. debe garantizar el uso adecuado, seguro y responsable de los activos de información institucional, incluyendo los datos personales y sensibles que son procesados, almacenados, transmitidos o transportados, de acuerdo con la clasificación de la información establecida en las políticas institucionales.

**Lineamientos principales:**

- El acceso a la información se restringirá estrictamente conforme al nivel de clasificación asignado (pública, reservada, clasificada o sensible).
- Cada proceso deberá mantener un registro actualizado de las autorizaciones de acceso a los activos de información bajo su responsabilidad.
- La asignación, modificación o revocación de permisos de acceso deberá estar documentada y aprobada por el propietario del activo.

**Responsabilidad de las copias de respaldo:**

- El proceso de Gestión de Tecnologías de la Información (TIC) es responsable de garantizar la confidencialidad, integridad y disponibilidad (CID) de las copias de seguridad de la información institucional y los datos personales.

- Dicho proceso debe asegurar el cumplimiento del Manual de Backup y del Plan de Continuidad de Negocio y Recuperación ante Desastres, implementando medidas de seguridad para el almacenamiento y restauración de copias de respaldo.

- El acceso a las copias de seguridad estará limitado únicamente a personal autorizado, debidamente registrado y capacitado.

VIGILADO Supersalud

**Protección y uso adecuado de la información**

- La información institucional deberá utilizarse únicamente para el cumplimiento de las funciones laborales o contractuales autorizadas.
- Queda prohibida la divulgación, alteración, eliminación o copia no autorizada de la información institucional.
- En caso de pérdida, sustracción, alteración o divulgación no autorizada de información, los colaboradores deberán reportarlo inmediatamente al proceso de Seguridad y Privacidad de la Información para activar el plan de gestión de incidentes.

### 5.5.3. Disposición de los Medios Físicos y Digitales (Hardware y Software)

La Red de Salud Ladera E.S.E. debe garantizar que la disposición de los medios de almacenamiento (físicos o digitales) se realice de forma segura, controlada y documentada, cuando estos ya no sean requeridos para las operaciones institucionales o se encuentren en estado de obsolescencia tecnológica.

**Custodia y responsabilidad**

- La Subgerencia Administrativa y Financiera será responsable de la custodia segura de los medios de almacenamiento cuando deban ser retirados, reemplazados, almacenados, reutilizados o destruidos.

- Los medios retirados de circulación deberán mantenerse bajo condiciones seguras de almacenamiento, hasta su disposición final.

VIGILADO Supersalud

**Registro y trazabilidad**

- Todos los medios en proceso de disposición deberán ser registrados en el inventario institucional, garantizando la trazabilidad de su ciclo de vida (estado, fecha de retiro, responsable, motivo de disposición y método de eliminación).

- La disposición deberá realizarse mediante métodos que aseguren la eliminación definitiva de la información, como el borrado seguro certificado, la destrucción física o técnicas equivalentes, de acuerdo con los lineamientos de seguridad establecidos.

**Autorización y control de adquisiciones**

- Todas las adquisiciones de hardware y software tecnológico y de seguridad deberán contar con la autorización previa del proceso de Gestión de Tecnologías de la Información (TIC) y de las partes interesadas correspondientes.
- Las adquisiciones deberán cumplir con los criterios de interoperabilidad, licenciamiento, seguridad y sostenibilidad tecnológica, en concordancia con las políticas institucionales y la normatividad vigente.

### 5.5.4. Transferencia de Medios

La Red de Salud Ladera E.S.E. debe garantizar que toda información transportada mediante medios físicos (USB, discos externos, portátiles, CD/DVD, cintas de respaldo u otros) esté debidamente protegida contra accesos no autorizados, pérdidas, alteraciones o manipulaciones indebidas.

VIGILADO Supersalud

- **Lineamientos de transferencia segura**

- El transporte y disposición de medios físicos deberá realizarse siguiendo los lineamientos institucionales de seguridad y trazabilidad.
- Se deberá garantizar que la información contenida en dichos medios se encuentre cifrada o protegida mediante controles de seguridad, reduciendo el riesgo de divulgación o manipulación.
- Todo proceso de transferencia de medios deberá quedar registrado (responsable de entrega y recepción, fecha, tipo de medio, contenido clasificado, autorización correspondiente).
- En los casos que lo ameriten, deberá existir un Acuerdo de Confidencialidad y Transferencia de Información y Medios, firmado por las partes responsables de la custodia.
- La responsabilidad de la seguridad de los medios durante su transporte recaerá en el propietario del activo y en el área que autoriza la transferencia.

## 5.6. ETIQUETADO DE LA INFORMACIÓN

Con el fin de garantizar la correcta identificación, clasificación y protección de la información, la Red de Salud Ladera E.S.E. establece un sistema de etiquetado físico, electrónico y digital para todos los documentos y archivos institucionales.

**Lineamientos generales**

Todos los funcionarios, contratistas y terceros deben mantener organizados los archivos físicos y digitales conforme a los lineamientos de gestión documental institucional y de acuerdo con el esquema de clasificación de la información.

VIGILADO Supersalud

La plataforma tecnológica institucional destinada al almacenamiento de información (servidores, File Server, RFAST, SICODA y demás aplicativos) debe garantizar los principios de confidencialidad, integridad, disponibilidad, usabilidad y acceso controlado.

El etiquetado de la información deberá realizarse según la clasificación institucional definida, la cual contempla:

- Información Pública.
- Información Pública Clasificada.
- Información Pública Reservada.
- Información Sensible (ejemplo: historia clínica, datos financieros y contractuales).
- Las etiquetas deberán estar claramente visibles e identificables, facilitando su correcta gestión y tratamiento.

El etiquetado aplicará de manera obligatoria tanto a documentos físicos como electrónicos y digitales, manteniendo homogeneidad en toda la Red.

### 5.6.1. Lineamientos para el control de accesos lógico:

La Red de Salud Ladera E.S.E. establece políticas y procedimientos formales de control de acceso físico y lógico a los activos de información (sistemas de información, aplicaciones, instalaciones, correo electrónico, redes, servidores, historia clínica electrónica, etc.), con el

VIGILADO Supersalud

fin de garantizar los principios de confidencialidad, integridad y disponibilidad (CID) de la información institucional.

**Lineamientos generales**

- El acceso a los activos de información será limitado al personal autorizado y en función de sus responsabilidades laborales o contractuales.

- Los privilegios de acceso deberán cumplir con el principio de mínimo privilegio necesario, es decir, otorgar únicamente los permisos indispensables para el desempeño de las funciones asignadas.

- Todo acceso físico o lógico deberá ser revocado, modificado o desactivado inmediatamente después de la finalización del vínculo laboral o contractual.

- Cada funcionario, contratista o tercero deberá contar con un identificador único (ID de usuario), personal e intransferible, para el acceso a los sistemas.

**Gestión de roles y permisos**

La matriz de roles y permisos de acceso será administrada por los procesos de Gestión de TIC, Gestión de Talento Humano y Seguridad de la Información, manteniéndose actualizada de forma continua.

Las revisiones periódicas de usuarios, roles y permisos se realizarán como mínimo cada 6 meses.
Los usuarios inactivos durante 45 días o más serán suspendidos temporalmente por 15 días y, de no reactivarse mediante solicitud formal, la cuenta será respaldada y eliminada.

VIGILADO Supersalud

**Gestión de credenciales de acceso**

- Los usuarios y contraseñas son personales e intransferibles. En caso de que, por fuerza mayor, deban compartirse, el incidente deberá notificarse de inmediato a Seguridad de la Información, para su registro y posterior cambio de clave.
- Se prohíbe la creación de sesiones simultáneas con un mismo usuario.
- Se deberá implementar doble factor de autenticación (2FA) para usuarios administradores o con privilegios elevados.
- Toda asignación de credenciales deberá realizarse mediante canales seguros de comunicación.
- La información de accesos privilegiados deberá ser almacenada de manera segura, bajo las políticas de cifrado institucional.
- Las contraseñas deberán cumplir con la política institucional de contraseñas seguras, incluyendo longitud mínima, uso de caracteres especiales, caducidad periódica y renovación obligatoria.

**Integración con procesos administrativos**

- El proceso de Gestión de Talento Humano deberá enviar mensualmente al área de Seguridad de la Información las novedades administrativas (ingresos, retiros, traslados, vacaciones, incapacidades, suspensiones, etc.), con el fin de garantizar la cancelación, activación o modificación de accesos.
- El área de Seguridad de la Información deberá contar con acceso de lectura al sistema de contratación para validar en tiempo real terminaciones, suspensiones o modificaciones contractuales.
- En caso de cambio de proveedores de servicios tecnológicos o de terminación de vínculo laboral de un colaborador, se deberán realizar de manera inmediata los cambios de credenciales de acceso asociados.

VIGILADO Supersalud

### 5.6.2. Responsabilidades de los Usuarios en Control de Acceso

Todos los Empleados de Planta, Contratistas y Terceros de la Red de Salud Ladera E.S.E. son responsables de garantizar el uso seguro de sus credenciales de acceso y de proteger la información institucional bajo los siguientes lineamientos:

- Hacer uso adecuado de los usuarios y contraseñas asignados, evitando cualquier práctica que ponga en riesgo la seguridad.
- Almacenar las credenciales de acceso en medios seguros, evitando su registro en papel, dispositivos no cifrados o repositorios personales.
- Mantener la confidencialidad de la información a la que tienen acceso, de acuerdo con su rol y responsabilidades.
- Cambiar las contraseñas como mínimo cada 30 días y crear claves fuertes, fáciles de recordar pero difíciles de adivinar.
- Cambiar inmediatamente las contraseñas genéricas entregadas al momento de la asignación inicial.

- No reutilizar contraseñas personales en sistemas institucionales, ni contraseñas institucionales en cuentas externas.
- No utilizar la misma contraseña para diferentes sistemas institucionales.
- Implementar doble factor de autenticación (2FA) en el caso de usuarios administradores o privilegiados.

**Los administradores de activos de información deberán:**

- Cambiar las claves de acceso cuando haya cambio de proveedores o finalización de un contrato.
- Cambiar las contraseñas administrativas de los sistemas que gestionan mínimo cada 4 meses.

VIGILADO Supersalud

### 5.6.3. Acceso y Servicios a Redes

La Red de Salud Ladera E.S.E. establece lineamientos de seguridad para el acceso a las redes institucionales:

- Los roles y perfiles de acceso deberán estar previamente definidos y parametrizados en las herramientas de red.
- Todo acceso deberá solicitarse y aprobarse a través del procedimiento formal de control de accesos.
- El acceso a las redes y servicios estará limitado únicamente a personal autorizado, en concordancia con sus funciones.
- Para la conexión remota a la red institucional se deberá usar una conexión segura, como una VPN corporativa.
- Las redes estarán protegidas contra accesos no autorizados mediante sistemas de monitoreo, detección de intrusos y alertas tempranas.
- En infraestructura contratada con terceros (nube pública o privada), se garantizarán controles de acceso a través de cláusulas contractuales, acuerdos de confidencialidad y niveles de servicio (SLA).
- Las redes inalámbricas institucionales deberán contar con autenticación robusta y cifrado seguro (WPA2 o superior).
- Las redes de invitados estarán completamente separadas de la red institucional de empleados y de los sistemas críticos.
- La segmentación de red deberá garantizar la separación entre servidores, áreas administrativas y visitantes.

### 5.6.4. Claves de Acceso

La Red de Salud Ladera E.S.E. implementa políticas estrictas sobre la gestión de contraseñas para asegurar trazabilidad y protección de los activos de información:

VIGILADO Supersalud

- Requisitos de complejidad de contraseñas
- Longitud mínima de 9 caracteres.
- Incluir mayúsculas, minúsculas, números y al menos un carácter especial.
- Cambio obligatorio cada 30 días.
- No reutilizar las últimas 6 contraseñas.
- Evitar caracteres consecutivos o patrones predecibles.
- Configurar un tiempo de bloqueo automático (time out) de 3 minutos de inactividad.
- Las contraseñas deberán almacenarse cifradas bajo algoritmos seguros.

**Gestión de usuarios y contraseñas**

- Cada usuario debe ser personalizado e intransferible.
- En caso de usuarios genéricos, deberá existir un responsable designado de su administración.
- Todas las contraseñas predeterminadas por fabricantes de hardware o software (servidores, routers, switches, impresoras, appliances, herramientas de seguridad, etc.) deberán cambiarse inmediatamente después de la instalación.
- Los usuarios tienen prohibido prestar, divulgar o compartir sus credenciales.
- Cualquier sospecha o confirmación de uso indebido de una contraseña deberá reportarse de inmediato al proceso de Seguridad de la Información.
- Las contraseñas de servidores, sistemas de información y aplicaciones críticas deberán cambiarse como mínimo cada 4 meses.
- Requisitos técnicos para equipos con acceso a la red

**Todo equipo de cómputo que requiera conexión a la red interna deberá contar con**:

- Solución antimalware instalada y actualizada.

VIGILADO Supersalud

- Parches de seguridad vigentes.
- Mecanismos de autenticación habilitados.
- Aval de cumplimiento de seguridad por parte de los procesos de Gestión de TIC y Seguridad de la Información.

## 5.7. Lineamiento de Criptografía:

- Implementará herramientas de cifrado, con el fin de proteger la confidencialidad e integridad de la información. Así mismo, el Grupo/Oficina de Tecnológica de Información y las Comunicaciones determinara los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera.

## 5.8. Lineamiento de seguridad física y del entorno:

- La Red de Salud Ladera E.S.E adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.

- La Red de Salud Ladera E.S.E definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.

- Todas las personas que ingresen a las instalaciones de La Red de Salud Ladera E.S.E deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

VIGILADO Supersalud

### 5.9. Lineamiento de seguridad en las operaciones:

Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. La Red de Salud Ladera E.S.E. planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

### 5.10. Lineamiento de seguridad de las comunicaciones:

- El Grupo de Tecnológica de la Información y las Comunicaciones, establecerá los controles para acceso lógico y protección de las redes de la Red de Salud Ladera E.S.E, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red y que deberán ser acordados con la alta dirección.

- La Red de Salud Ladera E.S.E definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.

### 5.11. Lineamientos de Adquisición, desarrollo y mantenimiento de sistemas:

- El Grupo/Oficina de Tecnológica y Comunicaciones, velara que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.

- Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.

VIGILADO Supersalud

- Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

## 5.12. Lineamientos de relaciones con los proveedores:

- La Red de Salud Ladera E.S.E. 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.

## 5.13. Lineamiento de seguridad de la información en la continuidad del negocio:

- La Red de Salud Ladera E.S.E. establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.

- El Grupo/Oficina de TIC generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

VIGILADO Supersalud

### 5.14. Lineamientos de gestión de incidentes:

- Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar al Grupo/Proceso de TICS por cualquiera de los medios dispuestos para tal fin.

- Sera responsabilidad del Grupo de Tecnología y las Comunicaciones seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.

### 5.15. Lineamientos de cumplimiento:

La Red de Salud Ladera E.S.E. velara por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

### 5.16. Lineamiento de escritorio limpio:

- No deberán dejarse documentos críticos en el “Escritorio” tanto físico como el Escritorio virtual (se denomina “Escritorio” al espacio digital en los equipos de cómputo).

- Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.

- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.

VIGILADO Supersalud

### 5.17. Lineamiento de uso adecuado del internet:

- El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Estará limitado el acceso a redes sociales en general.

- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).

- El grupo/oficina de TIC podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

### 5.18. Lineamiento de uso de correo electrónico:

- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a la Red de Salud Ladera E.S.E, por lo tanto, su contenido también es propiedad de la Entidad.

- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.

VIGILADO Supersalud

- La oficina/grupo de tecnología podrá verificar el contenido de los buzones de los correos telefónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

### 5.19. Lineamiento de uso de usuarios y contraseñas:

- Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.

- Las credenciales son personales e intransferibles.

- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

## 6. SENSIBILIZACION Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACION:

### 6.1. SENSIBILIZACIÓN Y COMUNICACIÓN:

La Red de Salud Ladera E.S.E, definirá un “Plan de Comunicación en Seguridad de la Información” a través de su oficina de comunicación interna y externa y el Grupo/Oficina TIC, donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones o tips de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo de la oficina TIC y/o el Oficial de Seguridad de la información.

VIGILADO Supersalud

## 6.2. CAPACITACIONES EN SEGURIDAD:

La Red de Salud Ladera E.S.E, a través de sus áreas/procesos de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, el grupo TIC y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones.

## 7. PROBACION Y REVISION:

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de la Red de Salud Ladera E.S.E.

## 8. SANCIONES:

La falta de conocimiento de los presentes lineamientos no libera al personal de la Red de Salud Ladera E.S.E de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

a) Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.

b) Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

VIGILADO Supersalud

c) El Grupo TIC será el encargado de recopilar y entregar a la Oficina de Control Disciplinario las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el grupo TIC será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

## 9. BIBLIOGRAFIA.


- Congreso de Colombia. (1991). Constitución Política de Colombia. https://www.constitucioncolombia.com/

- Congreso de Colombia. (2009). Ley 1273 de 2009 – Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado: la protección de la información y los datos. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35227

- Congreso de Colombia. (2009). Ley 1341 de 2009 – Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=37818

- Congreso de Colombia. (2012). Ley 1581 de 2012 – Por la cual se dictan disposiciones generales para la protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

- Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013 – Reglamenta parcialmente la Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53644


VIGILADO Supersalud

- Presidencia de la República de Colombia. (2014). Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57332

- Presidencia de la República de Colombia. (2015). Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=72588

- Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). Decreto 1008 de 2018 – Por el cual se adopta la Política de Gobierno Digital. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=87211

- Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). Manual de Gobierno Digital. https://gobiernodigital.mintic.gov.co/679/w3-propertyvalue-11085.html

- Ministerio de Tecnologías de la Información y las Comunicaciones. (s.f.). Modelo de Seguridad y Privacidad de la Información – MSPI. https://gobiernodigital.mintic.gov.co/679/w3-article-101911.html

- Congreso de Colombia. (2019). Ley 1952 de 2019 – Por la cual se expide el Código General Disciplinario. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=102273

- ICONTEC. (2013). NTC ISO/IEC 27001:2013 – Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. (Disponible para compra): https://tienda.icontec.org/

VIGILADO Supersalud

| ELABORADO POR | REVISADO POR | APROBADO POR |
|---|---|---|
| Apoyo Gestión de las Tics | Jefe Oficina Gestión de las Tics | Julio Cesar Cuero Ponce<br>Jefe Oficina Tics |

| REGISTRO DE CAMBIOS Y REVISIONES | | | | |
|---|---|---|---|---|
| **REVISIÓN No.** | **FECHA** | **PÁGINAS** | **SOLICITANTE** | **OBSERVACIONES** |
| 0 | 21/11/2025 | 45 | Apoyo a las TIC | Creacion de documento por Daniela Estefanía Soto – Apoyo Gestión de las TICS |

VIGILADO Supersalud



icontec ISO 9001 co-sc 7215-1
IQNET CERTIFIED MANAGEMENT SYSTEM