MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

INTRODUCCIÓN

En un entorno cada vez más digitalizado, donde las tecnologías de la información se han convertido en el soporte esencial de los procesos institucionales, la seguridad y la privacidad de la información, representan un desafío estratégico y permanente. La ESE IMSALUD reconoce que la información es uno de sus activos más valiosos y, por tanto, requiere de políticas, procedimientos y controles que garanticen su confidencialidad, integridad y disponibilidad, en cumplimiento de la normatividad colombiana y de estándares internacionales como la familia ISO 27000.

La experiencia reciente, marcada por la acelerada transformación digital y los riesgos derivados de la pandemia, ha evidenciado la aparición de nuevas amenazas que ponen en riesgo la continuidad de los servicios y la confianza de los usuarios. En este contexto, el presente manual se constituye como una herramienta de apoyo para funcionarios, colaboradores, contratistas y terceros, orientando el uso responsable de los recursos tecnológicos y la protección de la información crítica de la institución.

Estos lineamientos buscan no solo prevenir el uso indebido de los activos de información, sino también fortalecer la cultura organizacional en torno a la seguridad digital, promoviendo prácticas que permitan mitigar riesgos, garantizar el cumplimiento normativo y asegurar la resiliencia institucional frente a incidentes. Asimismo, el manual deberá ser objeto de actualización periódica, respondiendo a cambios organizacionales, avances tecnológicos y nuevas disposiciones regulatorias, con el fin de mantener su vigencia y eficacia en la protección de la información.

JUSTIFICACIÓN

La ESE IMSALUD cuenta con la Política de Seguridad y Privacidad de la Información, la cual está aprobada por resolución y define los lineamientos en el manejo adecuado de la seguridad de la información a nivel institucional. En consecuencia, se desarrolla el presente manual de seguridad y privacidad de la información, como instrumento de apoyo en el alcance de los objetivos propuestos en la mencionada política brindando instrucciones claras sobre las acciones que se deben llevar a cabo a través de los diferentes controles sugeridos en el modelo de seguridad y privacidad de la información y que a su vez se encuentran alineados con el compendio de normas NTC ISO 27000

1. OBJETIVO

Establecer las acciones, criterios y comportamientos que deben observarse en el uso de los recursos tecnológicos y en el manejo de la información institucional, con el fin de garantizar su confidencialidad, integridad y disponibilidad, para prevenir los riesgos asociados a amenazas internas y externas, y asegurar el cumplimiento de la normatividad colombiana en materia de seguridad digital y protección de datos personales.

1.1 OBJETIVOS ESPECÍFICOS

- Proteger los activos de información de la ESE IMSALUD.
- Promover el uso responsable y seguro de los equipos, sistemas y servicios informáticos.
- Fortalecer la cultura organizacional en torno a la seguridad y privacidad de la información.
- Asegurar la continuidad de los procesos misionales y la confianza de los usuarios.

2. ALCANCE

El presente manual aplica para todos los procesos, áreas y/o dependencias de la ESE IMSALUD, así como a los funcionarios, colaboradores, contratistas, proveedores y terceros que, de manera directa o indirecta, tengan acceso o hagan uso de los activos de información de la institución.

Su alcance comprende:

- **Recursos tecnológicos:** hardware, software, redes, sistemas de información, dispositivos móviles y servicios digitales utilizados en la operación institucional.
- **Información crítica:** datos personales, sensibles, públicos, clasificados o reservados, en cualquier formato o soporte, desde su creación hasta su eliminación segura.
- **Procesos operativos:** acceso, almacenamiento, transmisión, intercambio y disposición final de la información, incluyendo teletrabajo y servicios en la nube.
- **Seguridad física y lógica:** instalaciones, equipos, controles de acceso, videovigilancia y mecanismos de protección de la infraestructura tecnológica.

- **Relaciones externas:** proveedores, aliados estratégicos y terceros que presten servicios tecnológicos o que tengan acceso a información institucional.

3. RESPONSABILIDADES

La Política de Seguridad y Privacidad de la Información, junto con los procesos, procedimientos, estándares, controles y directrices derivados de este manual, son de obligatorio cumplimiento para todos los actores que interactúan con los activos de información de la ESE IMSALUD. Su incumplimiento dará lugar a las acciones disciplinarias, contractuales, administrativas o judiciales que correspondan, conforme a la normatividad vigente.

4. MARCO NORMATIVO

- 1982 – Ley 23 de 1982: Propiedad Intelectual – Derechos de Autor.
- 1991 – Constitución Política de Colombia: Art. 15: Derecho Fundamental al Habeas Data. Art. 20: Libertad de Información.
- 1993 – Ley 80 de 1993: Estatuto General de Contratación de la Administración Pública.
- 1993 – Ley 87 de 1993: Normas para el ejercicio de control interno en entidades del Estado.
- 2000 – Ley 594 de 2000: Ley General de Archivos.
- 2000 – Decreto 599 de 2000 / Ley 906 de 2004: Código de Procedimiento Penal.
- 2000 – Directiva Presidencial 02 de 2000: Gobierno en línea.
- 2002 - 2005 – Decreto 1599 de 2005: Adopta el Modelo Estándar de Control Interno MECI.
- 2005 – Ley 962 de 2005: Simplificación y racionalización de trámites electrónicos.
- 2006 – Ley 1032 de 2006: Habeas Data y manejo de información en bases de datos personales.
- 2007 – Ley 1150 de 2007: Seguridad de la información electrónica en contratación en línea.
- 2007 – Ley 1266 de 2007: Régimen de Habeas Data financiero.
- 2008 – Ley 1266 de 2008: Protección de datos en centrales de riesgo.
- 2009 – Ley 1273 de 2009: Delitos informáticos.
- 2009 – Ley 1341 de 2009: Marco regulatorio de Tecnologías de la Información.
- 2010 – Decreto 2952 de 2010: Reglamenta artículos de la Ley 1266 de 2008.
- 2011 – Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- 2011 – CONPES 3701 de 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa. – Ley 734 de 2002: Código Disciplinario Único.
- 2012 – Ley 1581 de 2012: Protección de Datos Personales.

- 2012 – Decreto 2609 de 2012: Reglamenta la Ley 594 de 2000 y Ley 1437 de 2011.
- 2013 – Decreto 1377 de 2013: Reglamenta la Ley 1581 de 2012.
- 2014 – Ley 1712 de 2014: Transparencia y acceso a la información pública.
- 2014 – Decreto 886 de 2014: Reglamenta el artículo 25 de la Ley 1581 de 2012.
- 2015 – Decreto 1083 de 2015: Reglamenta el artículo 25 de la Ley 1581 de 2012.
- 2016 – CONPES 3854 de 2016: Política Nacional de Seguridad Digital.
- 2022 – Decreto 338 de 2022: Gobernanza de la Seguridad Digital en entidades públicas.

5. MARCO CONCEPTUAL

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC27000).
Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales:

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: 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 es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales 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. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de

riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones

que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. DESARROLLO DEL MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La entidad cuenta con la política de seguridad y privacidad de la información, aprobada por la alta dirección, actualizada, y publicada en su sitio web https://www.imsalud.gov.co/web/ la cual se difunde a todo el personal de la institución, en los espacios definidos por la oficina de Administración Laboral, para los procesos de inducción y reinducción de personal, así mismo se envía a cada uno de los correos electrónicos institucionales de los colaboradores.

La política de Seguridad y Privacidad de la Información es revisada periódicamente por la oficina de Información, Sistemas y procesos, para asegurar su conveniencia, actualización y eficacia, cada vez que se le genere una actualización debe ser presentada ante el comité de gestión y desempeño institucional para su aprobación, y para su adopción deberá contar con la respectiva resolución aprobada y firmada por el gerente de la entidad, presentada con el documento DIE-03-P-11-F-01 formato de resolución.

En lo pertinente al incumplimiento de la políticas de la seguridad de la información, se aplicará lo establecido en los procedimientos destinados para tal fin, enmarcados en la normatividad vigente.

6.2 ORGANIZACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La entidad cuenta con un Grupo de Trabajo de Gobierno Digital, encargado de abordar los temas relacionados con seguridad y privacidad de la información, así como la implementación y seguimiento de la Política de Gobierno Digital. Las decisiones y lineamientos de este grupo son revisados y aprobados por la Alta Dirección, garantizando su legitimidad y alineación con los objetivos institucionales.

La entidad cuenta con un profesional especializado en seguridad y privacidad de la información, encargado de dar cumplimiento a las acciones de la política de seguridad y privacidad de la información, definir los planes de trabajo, y dar tratamiento a los riesgos y aplicar los controles respectivos.

La entidad cuenta con cursos para la sensibilización en seguridad y privacidad de la información, orientados a la formación continua de los colaboradores alojados en un aula virtual, https://cursos.imsalud.gov.co/login/index.php accesible para todos los funcionarios de la entidad y terceros.

La entidad cuenta con el documento TIC-01-P-09 procedimiento de gestión de incidentes de seguridad digital, el cual define el protocolo para el reporte antes las entidades competentes del orden nacional como el Csirt gobierno y ColCert de MINTIC.

La entidad cuenta con el documento TIC-01-PL-03 plan de tratamiento de riesgo de seguridad y privacidad de la información, para atender los riesgos de seguridad digital y aplicar los controles respectivos antes incidentes.

La entidad cuenta con el documento TIC-01-PL-04 plan de seguridad y privacidad de la información, el cual define las acciones para implementar el MSPI en la ESE IMSALUD, propuesto por el Ministerio TIC.

La entidad en su sitio web https://www.imsalud.gov.co/web/ en su pie de página implementa el documento TIC-01-G-01 Guia aviso de privacidad garantizándole a los usuarios el uso adecuado de sus datos personales facultados en la misionalidad de la entidad y conforme a al documento DIE-01-PC-24 de la política de tratamiento de datos personales y el documento TIC-01-M-03 manual de tratamiento de datos de la entidad.

6.3 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

Los funcionarios, colaboradores, contratistas, clientes, practicantes y terceros en general, que requieran hacer uso de los activos de la información de la entidad, deberán conocer y apropiar el presente manual.

Los permisos de acceso a las diferentes fuentes y activos de información deben ser gestionados y autorizados por el coordinador de área y el jefe de la oficina de información, sistemas y procesos.

La información que le sea entregada o que tenga acceso el contratista en el desarrollo de la ejecución del contrato gozará de confidencialidad, y será incorporada en el clausulado del contrato de la obra o labor.

La Oficina de Servicios Generales – Proceso de Gestión Contractual, valida los antecedentes del personal a contratar por prestación de servicios de acuerdo con la normatividad vigente.

La Oficina de Administración Laboral y Gestión Contractual, cuenta mecanismos o controles apropiados para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales, y aplica el documento THM-01-P-02 procedimiento vinculación de personal, de acuerdo con la normatividad establecida para tal fin.

La Oficina Administración Laboral, es la instancia encargada de adelantar los procesos disciplinarios que correspondan, garantizando el debido proceso y la aplicación justa de las medidas establecidas en la normativa interna y en la legislación colombiana vigente, en caso de una posible violación a la seguridad de la información de la institución.

Todo servidor público, contratista, colaborador o tercero que preste sus servicios o que tenga algún tipo de relación con la empresa, al iniciar sus labores debe firmar el documento TIC-01-M-01-F-01 formato de acuerdo de confidencialidad, y el documento TIC-01-M-03-F-01 formato autorización tratamiento de datos personales, de acuerdo con la política de tratamiento de datos personales de la

empresa y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios. La copia de estos acuerdos debe ser archivada de forma segura por la oficina de Administración Laboral y Gestión Contractual.

La oficina de información, sistemas y procesos es la responsable de resguardar la reserva de las bases de datos que contengan información personal de funcionarios y terceros que laboran o laboraron en la entidad.

La oficina de información, sistemas y procesos y el personal de apoyo que se requiera, debe diseñar y ejecutar de manera permanente, un programa de concientización en seguridad de la información, con el fin de apoyar la protección adecuada de la información.

Al momento de la terminación de contrato o finalización de labores de un tercero, colaborador o funcionario, el acto debe ser informado por la oficina de personal, a la oficina de información, sistemas y procesos, para que sean inactivados los usuarios y credenciales de acceso a los aplicativos autorizados, así mismo le sean eliminados los accesos a la red, aplicando el documento TIC-01-P-12 procedimiento gestión de identidades y control de acceso.

6.4 GESTIÓN DE ACTIVOS

La oficina de archivo y gestión documental, el profesional especializado en seguridad y privacidad de la información, junto con los lideres de proceso son los responsables de la actualización, verificación y baja de inventario de los activos de información de la entidad, aplicando el documento TIC-01-G-03 guía para el levantamiento de inventario de activos de información.

La oficina de archivo y gestión documental, junto con el profesional especializado en seguridad y privacidad de la información, serán los responsables de asignar la propiedad de los activos de información definiendo sus propietarios y custodios, aplicando el documento TIC-01-M-02-F-05 formato para levantamiento de activos de información.

El propietario designado de los activos informáticos debe:

A. Asegurarse de que los activos están inventariados;
B. Asegurarse de que los activos están clasificados y protegidos apropiadamente;
C. Definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables;
D. Asegurarse del manejo apropiado del activo cuando es eliminado o destruido.

La oficina de información, sistemas y procesos es la responsable de definir el uso aceptable de los equipos informáticos y que sean conocidos por los miembros de la entidad.

El traslado o retiro de equipos de cómputo, periféricos, dispositivos de almacenamiento, software e información considerada crítica propiedad de la entidad, fuera de las instalaciones de la entidad es de responsabilidad del usuario que solicita el traslado.

Los servidores públicos, contratistas, colaboradores o terceros, no podrán instalar, usar o replicar software no autorizado por la oficina de Información, sistemas y procesos.

Clasificación de la Información

La empresa define los niveles más adecuados para clasificar su información, de acuerdo con su sensibilidad a través documento TIC-01-G-04 guía para la rotulación de la información, para que los propietarios de esta la cataloguen y determinen los controles requeridos para su protección.

La oficina de Archivo y Gestión Documental de la entidad diseña los lineamientos para la administración de los archivos aplicando el documento TIC-04-PL-01 plan institucional de archivos - pinar de acuerdo con lo establecido en la normativa vigente.

Las Tablas de Retención Documental (TRD) deben indicar el tipo de clasificación de las series, subseries y documentos en ella contenidas, aplicando el documento TIC-04-P-02 procedimiento aplicación y seguimiento de las tablas de retención documental.

Los servidores públicos, contratistas, colaboradores o terceros de la empresa deben aplicar la clasificación de la información de la ESE IMSALUD, las TRD, el inventario de activos de información y los lineamientos para la administración de los archivos, plasmados en el documento DIE-01-PC-07 política de archivo y gestión documental.

Cada propietario del activo de Información debe velar por la custodia y cumplimiento de su clasificación de acuerdo con lo establecido en lineamientos para la administración de los archivos y activos de Información.

Para el intercambio de información se debe tener en cuenta su clasificación para su debida protección en términos de confidencialidad.

6.5 CONTROL DE ACCESO

La conexión remota a la red de área local de la empresa debe establecerse a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por la Oficina de información Sistemas y Procesos.

La oficina de información, sistemas y procesos debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servidores y servicios publicados.

La oficina de información, sistemas y procesos es responsable de asegurar que las redes de datos tanto físicas como inalámbricas de la entidad cuenten con métodos de autenticación que eviten accesos no autorizados.

La oficina de información, sistemas y procesos es responsable de gestionar los accesos a plataformas, servicios de red y sistemas de información de acuerdo a procesos formales de autorización definidos en el documento TIC-01-P-12 procedimiento de gestión de identidades y control de acceso.

Los usuarios que tienen acceso a las plataformas, servicios de red y sistemas de información son responsables de las acciones realizadas en los mismos.

El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible.

El usuario es responsable de asegurar la no divulgación de las contraseñas asignadas para acceder a los sistemas de información.

Cualquier actividad que se realice con el usuario y contraseña será responsabilidad del funcionario, colaborador, contratista, cliente, practicante y/o terceros en general al cual le fue asignado.

El usuario es responsable de establecer una contraseña segura, que cumpla con las siguientes características:

- La longitud de la contraseña debe ser mínimo de 8 caracteres. Las aplicaciones en las cuales la tecnología utilizada no contemple una longitud mínima de ocho caracteres, la longitud mínima deberá ser la máxima contemplada por el sistema.
- La contraseña debe estar compuesta por una combinación de letras Mayúsculas, minúsculas, caracteres numéricos y símbolos especiales como los siguientes: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /
- No debe usarse una palabra o nombre común que aparezca en un diccionario.
- No debe haber una relación obvia con el usuario, sus familiares, el grupo de trabajo u otras asociaciones parecidas.
- Debe ser cambiada con una periodicidad de 90 días.

Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente.

No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

No se debe escribir la contraseña en papeles y dejarla en sitios donde pueda ser encontrada por terceros.

No se debe almacenar la contraseña en la computadora. Algunos cuadros de diálogo presentan una opción para guardar o recordar la contraseña; no debe seleccionarse esta opción

Una vez finalizada la gestión de servicios prestados por terceras partes para la empresa, el supervisor de contrato debe garantizar que los accesos queden cerrados al finalizar el proceso o contrato, o realizando la devolución de identidades citado en el documento TIC-01-P-12 procedimiento de gestión de identidades y control de acceso. La cual se puede ser gestionada por el colaborador o el supervisor del contrato a través del aplicativo SARA.

La oficina de información, sistemas y procesos con el apoyo de mesa de servicios debe garantizar que los usuarios, realicen el cambio de contraseña de acceso a los servicios de la empresa, cada vez que sea requerido.

Los administradores de los servicios tecnológicos deben cumplir con los lineamientos de contraseñas seguras indicadas.

Los administradores de los servicios tecnológicos o sistemas de información deben entregar de manera adecuada las credenciales de acceso, la cuales serán gestionadas a través del aplicativo SARA y entregadas al correo electrónico asociado por el usuario.

La oficina de información, sistemas y procesos recomienda a los usuarios finales de los aplicativos la implementación del doble factor de autenticación, la cual permitirá significativamente reducir el riesgo de accesos no autorizados.

6.6 SEGURIDAD FÍSICA Y DEL ENTORNO

El usuario es responsable de cerrar la sesión del sistema o bloquear su equipo en el momento en que se retire de su puesto de trabajo a una zona donde pierda la visibilidad de este.

Los sistemas de lectura biométrica se encuentran en las entradas de cada una de las sedes de la institución. El dispositivo permite la identificación por medio de huella, facial o tarjeta de proximidad. Todos los colaboradores, independiente de su tipo de vinculación deben ser registrados en el sistema de control de acceso antes de iniciar sus labores. La recolección de datos personales que se genere a través de este mecanismo de identificación se encuentra amparada bajo el documento DIE-01-PC-24 política de tratamiento de datos personales, la cual se puede consultar en nuestra página web: https://www.imsalud.gov.co/web/ y serán usados para el control de acceso físico a cada una de las sedes.

El ingreso o retiro de todo activo de información de los visitantes, funcionarios, colaboradores y terceros en general que usen las instalaciones de la ESE IMSALUD (consultores, pasantes, visitantes, etc.) será registrado e inspeccionado en los

controles de accesos de la Entidad. El personal de seguridad y vigilancia en los controles de acceso verificarán y registrarán las características de identificación del activo de información en la Bitácora de seguridad o libro de novedades.

El personal de vigilancia debe registrar en una bitácora o sistema de información el ingreso y retiro de todo equipo cómputo elemento informático (pc o portátil, mouse, teclado, cargador, etc.) servidores, equipos activos de red o cualquier equipo electrónico diferentes a Smartphone; en caso de que estos equipos sean propiedad de la empresa deberán contar con autorización expresa del Almacenista para su salida.

La oficina de información, sistemas y procesos controla el ingreso a los centros de datos y centros de cableado de la empresa, mediante el sistema físico de control de acceso para ingresar a la entidad, garantizando que solo el personal autorizado tenga los privilegios necesarios para su ingreso.

El acceso a las áreas restringidas por parte del personal de soporte técnico, de proveedores se debe solicitar por medio de una autorización con el visto bueno del jefe de la Oficina de información, sistemas y procesos, con supervisión de un funcionario de la dependencia.

La oficina de información, sistemas y procesos es responsable de la identificación y organización del cableado estructurado desde los puestos de trabajo hasta los paneles de conexión de los centros de cableado.

La oficina de información, sistemas y procesos debe velar por que los recursos de la plataforma tecnológica de la empresa ubicada en el centro de cómputo se encuentren protegidos contra fallas o interrupciones de las plantas eléctricas adoptando el documento TIC-03-P-01 procedimiento inspección y prueba de funcionamiento de plantas eléctricas.

La oficina de información, sistemas y procesos debe establecer los lineamientos para los controles contra amenazas externas y ambientales y quedarán enmarcadas en el documento TIC-01-PL-01 plan de contingencia de la operación tecnológica, y documento TIC-01-P-11 procedimiento plan pruebas de continuidad de las tic.

La oficina de información, sistemas y procesos debe realizar mantenimientos preventivos al centro de cómputo y centros de cableado que estén bajo su custodia.

En el centro de cómputo y centro de cableado está prohibido: fumar, Ingresar comidas o bebidas, el porte de armas de fuego, corto punzantes o similares, mover, desconectar y/o conectar equipos sin autorización, modificar la configuración del equipo o interconectarlo sin autorización, alterar software instalado en los equipos sin autorización, alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas, extraer información de los equipos en dispositivos externos sin previa autorización.

La Oficina de información, sistemas y procesos establece los mecanismos de soporte y mantenimiento a los equipos de cómputo, servidores y equipos activos de red, llevando la trazabilidad del servicio mediante el GLPI.

6.7 SEGURIDAD DE LAS OPERACIONES

Todos los colaboradores de la entidad son responsables de la administración de su escritorio físico y de la pantalla de su equipo de cómputo, para lo cual debe cumplir los siguientes lineamientos:

Almacenar de forma segura (con llave u otro control) medios de almacenamiento como (CD/DVD, dispositivos de almacenamiento masivo (memorias USB, discos extraíbles)), papelería y otros elementos que puedan contener información sensible o confidencial; mientras esté ausente de su puesto de trabajo y sin visibilidad de su escritorio.

Al imprimir documentos en impresoras de red que contengan información sensible o confidencial, el usuario responsable deberá retirarlos de manera inmediata y asegurarse de su resguardo adecuado, evitando que permanezcan desatendidos o accesibles a terceros.

No ingerir alimentos cerca del equipo de cómputo o de la documentación de la entidad. Al finalizar la jornada laboral o al ausentarse del puesto de trabajo se deben asegurar con llave los cajones, gabinetes o archivadores. Únicamente la información clasificada como pública o interna podrá estar en el escritorio sin custodia. En la pantalla no debe permanecer ningún icono que ejecute un programa que no sea nativo de la plataforma del sistema operativo o archivos o acceso directo a archivo. Para el personal operativo en la pantalla solo deben permanecer los iconos de acceso directo a las diferentes herramientas de gestión de la compañía.

Todo medio removible debe ser escaneado mediante las soluciones de seguridad, suministrado por La oficina de información, sistemas y procesos cada vez que se conecte a un equipo de la empresa.

Es responsabilidad de cada servidor público, contratista, colaborador o tercero tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío de este.

Cuando se requiera transferir un medio de almacenamiento de información de la ESE IMSALUD a otras entidades se debe establecer un acuerdo de confidencialidad, entre las partes. Dichos acuerdos deben dirigirse al mecanismo de transferencia segura de información de interés entre la empresa y las partes.

La oficina de información, sistemas y procesos autoriza el uso de periféricos o medios de almacenamiento externo, de acuerdo con las necesidades requeridas para el cumplimiento de las funciones y del perfil del cargo de los servidores públicos o contratistas

Los servidores públicos, contratistas o personal provisto por terceras partes deben acoger las condiciones de uso de periféricos y medios de almacenamiento establecidos por la Oficina de información Sistemas y Procesos.

Se deben emplear herramientas de borrado seguro como (KillDisk o HDDErase) y demás mecanismos de seguridad pertinentes en los medios de propiedad de la empresa que sean reutilizados o dados de baja, con el fin de controlar que la información de la ESE IMSALUD contenida en estos medios no se pueda recuperar.

Cuando se requiera transferir un medio de almacenamiento se debe tener en cuenta el registro de contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte y el recibido.

La entidad Implementa sistemas de monitoreo continuo de la infraestructura, aplicaciones y redes, y programa la notificación de alertas automáticas para detectar anomalías o fallos, implementando el software Zabbix.

La entidad aplica respaldo y/o recuperación de información programando respaldos periódicos, aplicando procedimientos de restauración para garantizar su efectividad e integridad, utilizando el software de Nakivo, aplicando el documento TIC-01-P-08 procedimiento copias de seguridad.

La entidad mantiene actualizados los sistemas de información, sistemas operativos, antivirus, así mismo aplica escaneos de vulnerabilidades de cada uno de los servicios tecnológicos conectado a la red, par identificar posibles brechas de seguridad.

6.8 SEGURIDAD DE LAS COMUNICACIONES

Firma Digital

La oficina de información, sistemas y procesos establece los lineamientos necesarios para el control y el uso de las firmas digitales para la empresa.

Toda solicitud de asignación de firma digital se realiza a través de la Oficina de información Sistemas y Procesos, para el caso de usuarios nuevos, esta debe ser solicitada a través de la mesa de ayuda de la entidad GLPI.

Los servidores públicos y contratistas, que realicen actividades para la empresa, y tengan a su cargo una firma digital, deben hacer buen uso de esta de acuerdo a lo establecido en este manual. El certificado asignado es personal e intransferible, por lo cual es responsabilidad del usuario los documentos que firme

Los servidores públicos y contratistas que se les haya asignado firma digital deben hacer uso de esta para el desarrollo de sus actividades, así mismo gestionar la renovación del certificado de la firma, cuando esté próxima a vencer.

Todos los documentos firmados digitalmente son auténticos se tomarán como originales y finales.

En caso de presentarse o identificarse algún incidente de seguridad de la información relacionado con el uso de la firma digital, el usuario debe reportarlo a la Oficina de información Sistemas y Procesos, a través de la mesa de ayuda o GLPI.

Es responsabilidad del usuario hacer buen uso de los servicios tecnológicos donde se pretenda usar la firma digital, en caso de que tenga dudas debe informar a la mesa de ayuda o GLPI de la entidad para realizar la respectiva revisión.

Los documentos que son firmados con la solución de firma digital de la empresa deben ser validados digitalmente y su custodia debe estar en un repositorio institucional destinado para tal fin, de acuerdo con la normatividad vigente.

El usuario debe comprobar la información que va a firmar, es decir, antes de realizar la firma el usuario debe comprobar que está de acuerdo con el contenido que va a firmar en las condiciones o contexto en el que se realiza la firma.

6.9 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

La oficina de información, sistemas y procesos aplica buenas prácticas de desarrollo seguro en los productos entregados, controlando el acceso lógico cuando estos estén en producción, aplicando documento TIC-01-P-06 procedimiento de creación y/o actualización de software.

La oficina de información, sistemas y procesos establece ambientes separados a nivel físico y lógico para el desarrollo-pruebas y producción; contando con su plataforma, servidores, aplicativos, dispositivos y versiones independientes de los otros ambientes, para evitar así que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad, confidencialidad y disponibilidad de la información de los servicios en producción.

Los desarrolladores deben garantizar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas y asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

Los desarrolladores deben, a nivel de los aplicativos, restringir el acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas para los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

6.10 RELACIÓN CON LOS PROVEEDORES

Gestión de Incidentes de Seguridad de la Información

La oficina de información, sistemas y procesos mantiene contacto continuo con las autoridades, con el fin de aplicar la trazabilidad en caso de que se presente un incidente de seguridad de la información que requiera de asesoría externa, el cual se registra mediante el documento TIC-01-P-09 Procedimiento De Gestión De Incidentes De Seguridad Digital.

La Empresa Social del Estado IMSALUD, a través de La oficina de información, sistemas y procesos cuenta con personal especializado en seguridad y privacidad de la información, que a su vez es el enlace con las entidades del orden nacional para compartir e intercambiar conocimientos, que permita la mejora continua del Sistema de Gestión de Seguridad de la Información de la empresa.

Es responsabilidad de los servidores públicos, contratistas, colaboradores y terceros que presten sus servicios o tengan algún tipo de relación con la empresa, informar de los incidentes de seguridad de la información a través de los medios dispuestos por la oficina de tecnologías y sistemas de información, como mesa de ayuda GLPI, correo electrónico, o comunicación directa con el personal de la dependencia.

Seguridad para la Gestión de la Continuidad del Negocio

Los proyectos que se desarrollen en la entidad deben contemplar una gestión de los riesgos de seguridad asociados a la información del proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados. En cualquier caso, los proyectos desarrollados por la empresa deben estar alineados a la presente política de seguridad y privacidad de la información, para el particular y con el ánimo de estar preparados ante cualquier eventualidad se aplica el documento TIC-01-P-11 Procedimiento plan pruebas de continuidad de las tic.

6.11 DISPOSITIVOS MÓVILES

La Empresa Social del Estado IMSALUD, se reserva el derecho de autorizar o denegar el acceso al servicio de acuerdo con las condiciones de seguridad que se detecten en el dispositivo.

La oficina de información, sistemas y procesos aplica control sobre los dispositivos móviles autorizados.

Los dispositivos móviles de propiedad de los servidores públicos, contratistas, o terceros, para conectarse a los servicios de la red de datos deberán realizar solicitud a La oficina de información, sistemas y procesos y cumplir con los lineamientos referentes a seguridad de la información.

Todos los dispositivos móviles que almacenen información de la empresa deben tener instalado un software antivirus, y sistema operativo actualizado.

Los dispositivos móviles entregados por la empresa, a los servidores públicos, o contratistas no tienen autorizado el cambio de la configuración, la desinstalación del software, el formateo o la restauración de fabrica del dispositivo.

En caso de pérdida o robo de un dispositivo móvil de propiedad de la empresa, los servidores públicos, o contratistas, tendrán que realizar la respectiva denuncia ante la entidad competente, y generar aviso inmediato al Jefe de la Oficina de Servicios Generales o al Almacenista, quienes deben realizar las acciones necesarias para la protección de la información.

6.12 TELETRABAJO - TRABAJO EN CASA

La oficina de información, sistemas y procesos establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las actividades que desarrollan los servidores públicos, contratistas, colaboradores y terceros que presten sus servicios o tengan algún tipo de relación con la empresa, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

Toda información gestionada por la empresa, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.

6.13 VIDEO VIGILANCIA

La ESE Imsalud implementa diferentes sistemas de videovigilancia como mecanismo de control de acceso físico, para minimizar los riesgos de seguridad de las usuarios y los bienes en las sedes de la institución mediante la monitorización constante e ininterrumpida de todas las actuaciones desplegadas por quienes, a causa de su labor o rol o acceso a los servicios, ingresan a nuestras sedes. Estos sistemas se componen de cámaras y dispositivos de almacenamiento ubicados en cada sede conforme el presupuesto lo permita. El sistema está centralizado en un servidor que gestiona todas las configuraciones y se encuentra en la sede administrativa.

La recopilación de imágenes y datos personales se realiza de conformidad con la ley 1581 de 2012, cumpliendo exegéticamente con las reservas de Ley, y la Política de Tratamiento de Datos de la entidad

Para los fines de publicidad y aceptación tácita de las videograbaciones que se hagan de sí,
se instalarán avisos de privacidad visibles para su lectura en entradas de cada una de nuestras sedes de atención y/o administración, de forma que su no objeción formal frente al manejo de imágenes, antes de ser grabadas, se entiende como aceptación tácita del tratamiento de datos y que el material videográfico obtenido de videovigilancia podrá ser usado para publicaciones informativas internas y/o externas, corporativas internas y externas, indagaciones, investigaciones y trámites administrativos o jurisdiccionales y todas aquellas que se requieran para

salvaguardar los intereses de la entidad, sus colaboradores y sus usuarios. Todo lo anterior conforme al manual de tratamiento de datos de la ESE Imsalud.

En todas las sedes de la ESE IMSALUD se encuentra desplegado y visible el documento TIC-01-G-01 Guia aviso de privacidad, el cual debe:

- Incluir información sobre quién es el Responsable del Tratamiento y sus datos de contacto.
- Indicar el Tratamiento que se dará a los datos y la finalidad de este.
- Incluir los derechos de los Titulares.
- Indicar dónde está publicada la Política de Tratamiento de la Información.

Los titulares de datos podrán ejercer sus derechos en cualquier momento, a través de las herramientas habilitadas para tal fin, tal y como se consigna en el documento TIC-01-M-03 Manual de Tratamiento de Datos.

Las credenciales de administración estarán a cargo del jefe de información, sistemas y procesos, quien puede delegarlas a un tercero mediante el procedimiento vigente referido en el documento TIC-01-P-12 gestión de identidades y control de acceso, y que incluya documento TIC-01-M-01-F-01 formato de acuerdo de confidencialidad firmado. Para la visualización de estas, en las diferentes sedes se le asignarán credenciales individuales al coordinador de la unidad básica de atención y al servicio de vigilancia mediante el procedimiento vigente de gestión de identidades, que incluya el acuerdo de confidencialidad firmado. El permiso incluye visualización en tiempo real y de fechas almacenadas, sin posibilidad de descarga de los videos o fotos, y además no se deberán realizar capturas por cualquier otro medio, ya sea mediante fotos o videos de la información que se pueda visualizar en el sistema. Para esto el coordinador será el único responsable de la custodia de los videos obtenidos con o sin autorización de las diferentes sedes que coordinan.

Si un cliente interno o externo desea visualizar las cámaras, debe radicar la solicitud formal por el medio adecuado (ventanilla única), siendo la mesa de ayuda GLPI el canal para el cliente interno. Al momento de dicha Visualización y ante la vulneración de la PROHIBICIÓN EXPRESA de que habla el párrafo anterior, respecto de la toma o conservación de fijaciones fotográficas y/o videográficas, quien dio el acceso a las grabaciones deberá (so pena de sufrir las sanciones de ley) reportar inmediatamente al jefe de información, sistemas y procesos para levantar los registros, reportes y denuncias correspondientes.

En el caso de que una autoridad judicial requiera una copia de los videos almacenados, si existen, el jefe de la oficina de información, sistemas y procesos o su delegado procederán a descargarlos y entregarlos mediante comunicación externa, y manteniendo la debida cadena de custodia hasta ser entregada a la autoridad correspondiente.

El mantenimiento preventivo y correctivo del sistema, así como su monitoreo diario del estado de los componentes y grabaciones, está a cargo de la oficina de información, sistemas y procesos.

La grabación se almacenará en cada sede por el periodo que permita la tecnología instalada, siendo veinte (20) días lo mínimo que se debe asegurar. Los sistemas se configurarán para que reescriban y se activarán los sensores de movimiento para maximizar la capacidad de almacenamiento.

6.14 INDICADORES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La entidad define y aplica indicadores que permitan evaluar de manera periódica la eficacia de las políticas, controles y procedimientos de seguridad y privacidad de la información en la ESE IMSALUD, asegurando el cumplimiento normativo, la protección de los activos de información y la confianza institucional.
Los indicadores deben ir asociados a cada uno de los pilares de seguridad privacidad de la información, según corresponda estableciendo la meta, frecuencia de medición, y unidad de medida:

- Confidencialidad: Indicador: INF - Índice de Cuentas con Gestión de Identidades Activas en SARA (SPI)

• **Meta**	95,00 %	**Semáforo**		(Lineal)	**Tendencia**		**Finalidad**	Maximizar

>= -∞ < 90	**>= 90 < 95**	**>= 95 < +∞**

  - ✓ Formula: (Sumatoria de usuarios con identidad vigente en SARA. / Sumatoria de Usuarios en KUBAPP.)*100

- Disponibilidad: Indicador: INF - Índice de Disponibilidad de Servicios Tecnológicos (SPI)

• **Meta**	100,00 %	**Semáforo**		(Lineal)	**Tendencia**		**Finalidad**	Maximizar

>= -∞ < 90	**>= 90 < 99**	**>= 99 < +∞**

  - ✓ Formula: (Horas en que el servicio estuvo disponible sin interrupciones / Horas en que el servicio debía estar disponible según el calendario institucional.)*100

- Integridad: Indicador: INF - Índice de Verificación de Integridad de las Copias de Seguridad (SPI)

• **Meta**	100,00 %	**Semáforo**		(Lineal)	**Tendencia**		**Finalidad**	Maximizar
	>= -∞ < 90	**>= 90 < 99**	**>= 99 < +∞**					

- ✓ Formula: (Respaldos que cumplieron las pruebas de restauración o validación / Número total de respaldos generados en el periodo.)*100

Dichos indicadores deben cumplir con los soportes específicos para su medición.

7 CONCLUSIÓN Y RECOMENDACIONES

La ESE IMSALUD reafirma su compromiso con la seguridad y privacidad de la información como un eje fundamental para la confianza de los usuarios y la continuidad de sus procesos misionales. Este manual establece lineamientos claros para proteger los activos de información, cumplir con la normatividad colombiana y adoptar buenas prácticas internacionales.

Su aplicación fortalece la cultura organizacional en torno a la seguridad digital y exige una actualización periódica, que permita responder a cambios tecnológicos, regulatorios y organizacionales. Con ello, IMSALUD avanza hacia una gestión integral, transparente y resiliente de la información, orientada a la mejora continua.

8 REFERENCIAS BIBLIOGRÁFICAS

- Modelo de Seguridad y Privacidad de la Información. MINTIC Versión 3.0.2.
- Elaboración de la política general de seguridad y privacidad de la información. MINTIC Versión 1.0.0
- ISO IEC 27001 ICONTEC Sistemas de Gestión de seguridad de la información

9 HISTORIAL DE CONTROL DE CAMBIOS

VERSIÓN	MOTIVO	FECHA

01	Elaboración del documento	30/11/2021
02	Se añaden los puntos 8.6. Seguridad física y del entorno y 8.13. Video vigilancia	30/10/2023
03	Actualización del manual por Modificación del nombre del documento, texto de la introducción, objetivo, y se agregan objetivos específicos, alcance, responsabilidades, organización cronológica marco normativo, adición de normas, numeración de capítulos, capítulo de indicadores, mejora textos, conclusión	24/03/2026
04		

Elaboró:	Revisó:	Aprobó:
Profesional Especializado en Seguridad y Privacidad de la Información	Jefe de Información, Sistemas y Procesos	Comité Institucional de Gestión y Desempeño