MANUAL DE SEGURIDAD INFORMÁTICA

TABLA DE CONTENIDO

INTRODUCCIÓN

En Jersalud S.A.S., reconocemos que la información constituye un activo estratégico de alta prioridad, indispensable para el desarrollo y ejecución de nuestra plataforma estratégica. Por ello, surge la necesidad de establecer reglas y medidas que garanticen la protección de la confidencialidad, integridad, custodia y disponibilidad de la información a lo largo de todo su ciclo de vida.

Este Manual de Seguridad Informática reúne los lineamientos, políticas, procedimientos, tecnologías efectivas y controles necesarios para definir las responsabilidades de colaboradores, contratistas, proveedores, visitantes y cualquier persona con vínculo laboral o contractual con la organización. Su enfoque está alineado con el cumplimiento de la normatividad legal vigente y las buenas prácticas internacionales en materia de seguridad de datos e información.

En un sector tan dinámico como el de la atención médica, donde la tecnología desempeña un papel cada vez más crucial, la seguridad de la información es esencial para salvar tanto la privacidad de los pacientes como la integridad operativa de la institución. La digitalización de los registros médicos, el uso extendido de las comunicaciones electrónicas y la creciente sofisticación de las amenazas cibernéticas exigen la implementación de medidas de protección, con herramientas prácticas para la gestión de amenazas, la capacitación del personal y la respuesta eficiente ante incidentes de seguridad, consolidando así un marco de protección integral.

Al adoptar los lineamientos descritos en este manual, la institución refuerza su postura de seguridad de la información, garantizando la protección de los datos de pacientes, médicos y empleados frente a amenazas en constante evolución.

1. GENERALIDADES

1.1.OBJETIVOS

1.1.1. Objetivo general

Establecer los lineamientos, políticas, procedimientos, tecnologías efectivas y controles de seguridad de la información necesarios para garantizar la protección de la confidencialidad, integridad y disponibilidad de los datos e información, así como posibles sanciones por su desacato.

1.1.2. Objetivo especifico

- Promover una cultura orientada a la seguridad de la información al interior de Jersalud S.A.S.
- Mantener altos niveles de confidencialidad, integridad y disponibilidad de los activos de información críticos de Jersalud S.A.S.
- Concientizar y sensibilizar a todos los colaboradores internos, proveedores y personal de interés general, acerca del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.
- Dar cumplimiento a la legislación vigente asociada a la seguridad de la información.
- Mejorar y optimizar la infraestructura de seguridad informática de la organización, incluyendo firewalls, sistemas de detección de intrusiones, y cifrado de datos, para garantizar una protección robusta contra amenazas cibernéticas y asegurar la integridad de la información confidencial.
- Optimizar los procesos, estableciendo directrices que ayuden a garantizar el mejoramiento continuo.
- Establecer los lineamientos que aseguren el proceso de los hallazgos de auditoría a través de identificación y controles de los planes de acción

1.2.ALCANCE

Las políticas y directrices incluidas en el presente Manual serán de aplicabilidad y cumplimiento por todos los colaboradores internos, contratistas, proveedores, terceros y en general a toda persona que tenga algún tipo de relación con la institución y cuenten con acceso a los sistemas y activos de información de Jersalud S.A.S, en cumplimiento de sus funciones y para conseguir un adecuado nivel de protección y seguridad de la información.

2. MARCO CONCEPTUAL

2.1. DEFINICIONES

ACCIÓN CORRECTIVA: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.
ACCIÓN PREVENTIVA: Medida de tipo proactivo orientada a prevenir potencialmente no conformidades asociadas a la implementación y operación del SGSI.
ACEPTACIÓN DEL RIESGO: Decisión de aceptar el riesgo.
ACTIVO DE INFORMACIÓN: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para organización. (Cualquier elemento que tiene valor para la organización, ya sea información o los sistemas relacionados con su tratamiento, almacenamiento y transmisión).
AMENAZAS: Cualquier circunstancia o evento con potencial para causar daño a un activo de información, como ciberataques, fallos humanos o desastres naturales.
APLICACIONES: Todo el software que se utiliza para la gestión de la información. Por ejemplo, VIE Cloud, Daruma, Meta 4, Moodle, Isismaweb, etc.
BACKUP: En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida de información. Forma parte esencial de las medidas de protección de la información.
CIFRADO: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad, permitiendo el acceso solo a usuarios autorizados con la clave correspondiente**.**
CLIENTE EXTERNO: Toda persona o entidad que, sin ser empleado directo, requiere acceso a ciertos recursos de la información para cumplir una función específica. Incluye a contratistas, proveedores, auditores médicos externos, estudiantes.
CLIENTE INTERNO: Todo colaborador que tiene un vínculo laboral directo con Jersalud S.A.S., que utiliza recursos informáticos para el desempeño de sus funciones laborales.
CONFIDENCIALIDAD: Principio de la seguridad que garantiza que la información sea accesible únicamente por el personal autorizado.

CPU: Central Processing Unit (CPU/Unidad Central de Procesamiento) también llamado microprocesador o simplemente procesador, es el componente principal del ordenador y otros dispositivos programables, que interpreta las instrucciones

contenidas en los programas y procesa los datos.
CREDENCIALES DE ACCESO: Usuario y contraseña asignados al cliente interno/externo que permiten el acceso de forma segura a un sistema o plataforma de la organización.
CUENTA DE USUARIO: Identidad digital única asignada a una persona para acceder a los sistemas y recursos informáticos de la organización.
DATOS: Todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen. Por ejemplo: Archivos de diferentes formatos.
DISPONIBILIDAD: Principio de la seguridad que garantiza que los sistemas de información y los datos estén operativos y accesibles para los usuarios autorizados cuando estos los requieran.
ENDPOINT: Sistema de seguridad que protege dispositivos finales (como PCs, servidores o móviles) contra amenazas como malware, ransomware y exploits, mediante antivirus, firewalls y detección de intrusiones.
FIREWALL: Dispositivo o software que monitorea y controla el tráfico de red entrante y saliente basado en reglas de seguridad predefinidas, previniendo accesos no autorizados.
GLPI: Plataforma de código abierto para la gestión de activos y servicios de Tecnología de la Información TI.
HACKING: Acceso no autorizado o manipulación de sistemas informáticos con fines maliciosos, como robo de datos o interrupción de servicios. Incluye técnicas como explotación de vulnerabilidades.
LAN: local área network o red de área local, es la interconexión de una o varias computadoras y periféricos.

MALWARE: Software malicioso diseñado para causar daño, interrumpir operaciones o acceder de forma no autorizada a los sistemas de información (virus, troyanos, ransomware, spyware).
MFA (Múltiple Factor de Autenticación): Método de control de acceso adicional para el inicio de sesión que requiere que el usuario proporcione dos o más pruebas de su identidad. (ej. contraseña + token o biometría).
OFFICE 365 o O365: Plataforma en la nube de Microsoft que incluye herramientas de productividad como correo electrónico (Outlook), mensajería instantánea y reuniones (Teams) y almacenamiento (OneDrive), con énfasis en seguridad y cumplimiento normativo.
PHISHING: Ataque cibernético que utiliza correos electrónicos o mensajes fraudulentos para engañar a usuarios y obtener información sensible, como credenciales o datos financieros.
SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información.
SGSI (Sistema de Gestión de Seguridad de la Información): Conjunto de políticas, procesos, procedimientos, roles y tecnologías que se implementan en una organización para gestionar, proteger y mejorar continuamente la seguridad de la información.
SOFTWARE: Conjunto de programas, instrucciones y datos que permiten operar computadoras y dispositivos electrónicos para realizar tareas específicas.

SPAM: Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. Correo no deseado o no solicitado que se distribuye masivamente, y que puede saturar los sistemas, afectar la productividad, ser usado como medio para propagar malware o realizar ataques informáticos.

TIC (Tecnologías de la Información y la Comunicación): Conjunto de herramientas, sistemas y procesos para gestionar información y comunicaciones, incluyendo hardware, software y redes.

USB: Es un tipo de conexión estándar que permite la transferencia de datos y energía entre dispositivos, como computadoras, memorias externas, teclados o periféricos.
VOUCHER: Es un comprobante, constancia o documento que respalda una transacción, servicio o derecho adquirido.

VPN (Virtual Private Network): Red privada virtual de las siglas en inglés, es una tecnología que crea una conexión segura y cifrada desde Internet dando acceso a recursos en la red LAN. Su objetivo es proteger la transmisión de datos, garantizar la confidencialidad de la información y permitir el acceso remoto seguro a los recursos institucionales.

WAN: Es una red de comunicaciones que abarca grandes distancias geográficas, conectando múltiples redes locales (LAN) ubicadas en distintas ciudades, regiones o países. Este tipo de red permite que organizaciones distribuidas geográficamente se comuniquen y compartan información de manera segura y eficiente.

3. CONTROLES ORGANIZACIONALES

3.1. CUMPLIMIENTO NORMATIVO LEY 23 DE 1982 SOBRE DERECHOS DE AUTOR

En Jersalud S.A.S. se da cumplimiento normativo a la Ley 23 de 1982 sobre derechos de autor y la Ley 603 de 2000, en lo referente al uso legal y licenciamiento del software, promoviendo así el respeto por los derechos de autor y la utilización responsable de las tecnologías de la información.

Únicamente el personal autorizado del Área de Tecnologías de la Información y las Comunicaciones (TIC) está facultado para realizar la instalación de software y/o hardware en los equipos informáticos y de telecomunicaciones de la organización. Esta medida garantiza el

cumplimiento de la normativa de propiedad intelectual y asegura el uso legal del software adquirido por la institución.

3.2. BUEN MANEJO DEL INSUMO INFORMÁTICO

Todo usuario es responsable del uso adecuado de los recursos informáticos asignados (computadoras, periféricos, aplicaciones, entre otros), así como del acceso a la red institucional e Internet a través de la infraestructura tecnológica dispuesta para los servicios administrativos y asistenciales de Jersalud S.A.S.

A continuación, se detallan las directrices para el correcto uso de estos insumos:

3.2.1. Mantenimiento y Limpieza.

a. Realizar limpieza diaria del equipo asignado (teclado, mouse, pantalla) en cumplimiento del **M-GC-006 MODELO DE LIMPIEZA Y DESINFECCIÓN,** numeral 16. Área de Tecnología de la Información y Equipos de Cómputo.
b. Evitar el consumo de alimentos o bebidas en las áreas de trabajo para prevenir daños en los dispositivos electrónicos.

3.2.2. Uso adecuado del Hardware.

a. El uso de impresoras y demás equipos tecnológicos está restringido exclusivamente a actividades laborales, no se permite el uso de impresoras con propósitos personales.
b. Apagar el computador al finalizar la jornada laboral.
c. No conectar equipos o dispositivos personales a la red sin la autorización del área de tecnología de la información TI.

3.2.3. Navegación Segura.

a. Abstenerse de acceder a sitios web de ocio, pornografía, contenido inapropiado, juegos en línea o redes sociales no autorizadas.
b. No descargar ni instalar software, aplicaciones o herramientas informáticas sin la previa aprobación del área de tecnología de la información TI.
c. Escanear con el software de seguridad todos los dispositivos de almacenamiento externo (USB, discos duros, entre otros.) antes de su uso para evitar la propagación de malware.

3.2.4. Seguridad de la Información.

a. Bloquear el equipo al ausentarse del puesto de trabajo con el fin de evitar que terceros accedan de forma no autorizada a la información o al sistema.
b. No almacenar archivos personales (fotografías, música, videos) en repositorios compartidos y definidos por el área de tecnología de la información TI.
c. Respetar las políticas de confidencialidad, evitando divulgar información sensible o institucional por canales no autorizados.
d. No compartir ni facilitar las credenciales de acceso (usuario y contraseña) a terceros, bajo ninguna circunstancia.

3.2.5. Cumplimiento del Programa para la Socialización, manejo y seguridad de las tecnologías en salud.

a. Asistir a todas las capacitaciones desplegadas al cliente interno de Jersalud S.A.S. respecto al uso y manejo seguro de las tecnologías informáticas.
b. Participar en la verificación del uso correcto de las tecnologías informáticas, tener disposición al cambio y retroalimentación por parte del personal de TI frente a las buenas prácticas en el manejo del software o hardware.
c. Acatar el control de las tecnologías informáticas externas que ingresen a Jersalud S.A.S.
d. Participar y contribuir a la mitigación de daños de las tecnologías informáticas de la institución.

3.2.6. Uso responsable y cumplimiento normativo.

a. Cumplir con todas las políticas y directrices emitidas por el área de tecnología de la información TI.
b. Reportar inmediatamente cualquier anomalía, daño o comportamiento sospechoso en el equipo informático o en las conexiones de la red.
c. Participar activamente en las capacitaciones de ciberseguridad y uso de herramientas tecnológicas, aplicando los refuerzos necesarios y corrigiendo las vulnerabilidades detectadas en caso de no aprobación.
d. Los recursos informáticos de Jersalud S.A.S. deben utilizarse exclusivamente para el cumplimiento de funciones institucionales o actividades relacionadas con el cargo.
e. Está prohibido el uso de equipos tecnológicos o conexiones a redes de la Institución para fines personales, negocios particulares, actividades ajenas a la institución o en beneficio propio, de terceros o de entidades que no cuenten con autorización expresa o convenio formal con la organización.

3.3. CONTROL DE IMPRESIÓN Y RACIONALIZACIÓN DEL COSTO DE IMPRESIÓN.

Todo colaborador tiene derecho a utilizar los servicios de impresión, siempre que sea para fines estrictamente laborales y estén relacionados con las funciones asignadas o con las responsabilidades definidas en su contrato con la Institución.

Como parte de la estrategia institucional para la optimización de recursos y la reducción de costos de impresión, cada usuario es responsable de garantizar el uso adecuado del servicio de impresión. Esto incluye:

- Imprimir únicamente documentos que sean necesarios y relevantes para el cumplimiento de sus funciones.
- Utilizar preferiblemente configuraciones de impresión en baja calidad (borrador) para documentos internos o de uso temporal.
- Evitar impresiones innecesarias, personales o no autorizadas.
- Respetar las campañas y políticas de control y seguimiento implementadas por la institución para la gestión eficiente del servicio de impresión.

El uso responsable de los recursos contribuye a la sostenibilidad financiera y ambiental de la Institución.

3.4.ASIGNACIÓN DE RECURSOS INFORMÁTICOS A TERCEROS.

Jersalud S.A.S podrá autorizar el uso de recursos tecnológicos a terceros, servicios de impresión, conectividad en red LAN, WiFi, acceso a Internet, correo electrónico institucional, entre otros, únicamente bajo orden expresa y documentada de la Dirección TI.

Dicha asignación deberá estar sujeta a controles, restricciones y seguimiento por parte del Área de Tecnologías de la Información, con el fin de garantizar el cumplimiento de las políticas institucionales de seguridad, uso responsable y protección de la información.

3.5. REPORTE DE MAL USO DE RECURSOS INFORMÁTICOS.

Todos los colaboradores son responsables de reportar de manera inmediata cualquier anomalía, daño o incidente relacionado con el mal uso de los recursos informáticos, especialmente en equipos de cómputo, escáner, tablets, impresoras, teléfonos, sistemas de videoconferencia, sistema de turnos, controles de acceso, monitores industriales y cableado estructurado (Datos, Voz y CCTV).

En casos como derrames de líquidos, alimentos u objetos extraños (clips, grapas, entre otros) sobre los equipos y dispositivos, el usuario deberá:

1. Desconectar inmediatamente el dispositivo afectado para prevenir mayores daños o riesgos eléctricos.
2. Informar de forma inmediata al área de Tecnologías de la Información - TI.
3. Generar una solicitud a través de la plataforma de soporte GLPI, como respaldo formal del incidente reportado.

El cumplimiento de este procedimiento es fundamental para garantizar la trazabilidad de los eventos, la atención oportuna y la conservación adecuada de los activos tecnológicos de la institución.

3.6. CLAVE PERSONAL E INSTRANSFERIBLE.

Las credenciales de acceso (usuario y contraseña) asignadas por el área de Tecnología de la Información TI, son estrictamente personales e intransferibles. Cada colaborador o cliente externo es responsable de:

- Garantizar la privacidad de sus credenciales de acceso.
- No compartir, divulgar, ni permitir el uso de su cuenta por otros usuarios o terceros.

El incumplimiento de esta directriz representa una vulneración a las normas de seguridad de la información. En caso de detectarse el uso indebido, se procederá con el conducto regular para la aplicación de las medidas disciplinarias o contractuales correspondientes.

3.7. RESPONSABILIDAD DE USO DE EQUIPOS INFORMÁTICOS.

Es responsabilidad de cada colaborador proteger el equipo informático asignado bajo su custodia para el desempeño de sus funciones. Mientras el usuario está haciendo uso del equipo, es completamente responsable del mismo. En caso de cualquier falla o desperfecto, debe reportarlo de inmediato al personal encargado de Tecnología de la Información TI.

Todo colaborador debe bloquear su sesión en el momento de retirarse del computador, los usuarios administrativos deben apagar su equipo de cómputo al finalizar su jornada laboral y los asistenciales que usan equipos de cómputo compartidos deberán cerrar sesión al momento de finalizar su jornada laboral.

El incumplimiento de estas disposiciones será reportado a la jefatura correspondiente y podrá generar acciones correctivas según los lineamientos internos de Jersalud S.A.S.

3.8. DIRECTRICES DEL USO DE CORREO ELECTRÓNICO Y MENSAJERÍA INSTANTÁNEA.

a. **Cambio de contraseña y seguridad de acceso:** El colaborador deberá cambiar su contraseña al primer acceso. Por seguridad, se recomienda actualizarla al menos cada tres meses. Toda cuenta debe estar protegida mediante métodos de autenticación multifactor (MFA), según las políticas de seguridad institucional.
b. **Conducta y comunicación institucional:** El lenguaje utilizado en los correos y mensajes debe ser apropiado, respetuoso y

alineado con el **M-GTH-041 MANUAL DE COMUNICACIÓN ESTRATÉGICA.** Se debe observar siempre la cortesía y profesionalismo en las comunicaciones.

c. **Confidencialidad e integridad de la información:** La información relacionada con la misión institucional transmitida por correo electrónico debe mantenerse íntegra y sin alteraciones, salvo autorización expresa del responsable de dicha información.
d. **Gestión del buzón:** Es responsabilidad del usuario mantener su bandeja de entrada organizada y libre de información irrelevante. Si el buzón se satura, no será posible recibir nuevos mensajes hasta liberar espacio.
e. **Incidentes de Seguridad:** Ante cualquier acceso no autorizado, intento de suplantación o vulneración de seguridad, el usuario debe notificar de inmediato al administrador del correo institucional y cerrar la sesión activamente.
f. **Prevención de amenazas y uso seguro:** No se deben abrir archivos adjuntos ni enlaces provenientes de remitentes desconocidos o sospechosos, para evitar infecciones por malware, ransomware o ataques de phishing. No está permitido enviar contenido malicioso, como virus, códigos dañinos o archivos diseñados para afectar el funcionamiento de los sistemas.
g. **Protección de datos y privacidad:** El usuario no debe divulgar su dirección de correo en sitios web públicos, formularios no autorizados o listas de distribución abiertas, para reducir la exposición a spam y amenazas informáticas. Se prohíbe compartir listas de correos institucionales sin la autorización del Director TI.
h. **Responsabilidad del usuario:** Cada colaborador es responsable del uso adecuado de su cuenta institucional de correo electrónico y mensajería. Toda actividad realizada desde su cuenta será atribuida exclusivamente al titular.
i. **Restricción del uso de WhatsApp:** WhatsApp no es un canal de comunicación oficial de la Institución. Su uso para temas institucionales implica riesgos como pérdida de trazabilidad, filtración de información, falta de respaldo, y vulneración de la confidencialidad. Toda comunicación formal debe realizarse exclusivamente por los medios autorizados por la institución.
j. **Uso de Microsoft Teams:** Su uso está autorizado únicamente para roles definidos por la institución, según el perfil funcional de cada colaborador. Debe utilizarse exclusivamente como canal oficial de comunicación.
k. **Uso exclusivo para fines institucionales:** El correo electrónico (Outlook) y el canal de comunicaciones (Microsoft Teams) son herramientas de trabajo de uso exclusivo para actividades propias de la Institución. Está prohibido su uso para fines personales, fraudulentos, inapropiados o como medio de difusión masiva no autorizada.

3.9. GARANTIZAR LEGALIDAD DEL SOFTWARE EN EL EQUIPO ASIGNADO.

Todo el software instalado en los equipos de cómputo de Jersalud S.A.S debe estar debidamente licenciado, autorizado y destinado exclusivamente para uso institucional.

Cada usuario es responsable del correcto uso y conservación del equipo asignado, así como de los recursos de software y hardware que le hayan sido entregados, de acuerdo con el inventario formalmente aceptado.

En caso de detectar la presencia de software no autorizado, no licenciado o ajeno a la Institución, el usuario debe reportarlo de inmediato al área de Tecnología de la Información TI. La instalación o uso de software ilegal será considerado una falta grave, y el usuario será responsable ante la Dirección de Jersalud S.A.S. y, si aplica, ante las autoridades competentes.

Cuando un equipo sea de uso compartido, todos los usuarios que accedan a él serán responsables solidarios del cumplimiento de esta política, independientemente de quién haya realizado la instalación indebida.

3.10. RESPONSABILIDAD SOBRE LOS RECURSOS TECNOLÓGICOS INFORMÁTICOS

Los recursos tecnológicos de Jersalud S.A.S. son bienes institucionales destinados exclusivamente para soportar la operación asistencial, administrativa y de investigación, y deben ser utilizados de manera responsable, segura y conforme a las políticas internas. El área de Tecnologías de la Información TI es responsable de la planeación, adquisición, implementación, mantenimiento y disposición final de los equipos informáticos, sistemas, aplicaciones y redes institucionales, garantizando su disponibilidad, seguridad y continuidad.

En Jersalud S.A.S., cada colaborador es responsable del uso adecuado de los recursos tecnológicos que se le asignen, velando por su conservación, custodia y correcto funcionamiento. El uso de estos recursos debe realizarse conforme a las políticas institucionales y los lineamientos definidos por el área de Tecnología de la Información TI. La responsabilidad sobre los recursos de tecnología asignados aplica a todos los colaboradores, contratistas y personal autorizado que haga uso de estos.

Está estrictamente prohibido atentar contra los recursos tecnológicos informáticos, incluyendo acciones como desarmar, instalar software no autorizado o realizar cualquier acción que afecte la operatividad o integridad de los dispositivos; en caso de que se determine que un daño fue ocasionado por negligencia, mal uso o manipulación indebida del usuario, este deberá asumir los costos de reparación o reposición de los equipos, conforme a lo establecido por el área de la Tecnología de la Información TI y/o el incumplimiento de estas responsabilidades será gestionado bajo los lineamientos de control interno y las disposiciones legales vigentes en materia de protección de datos y seguridad digital.

3.11. RED EXCLUSIVA PARA PROPÓSITOS LABORALES.

En Jersalud S.A.S., está prohibido prestar la estación de trabajo o el punto de red a terceros no autorizados, así como conectar equipos personales o externos sin aprobación del área de Tecnología de la Información TI.

La red institucional debe utilizarse exclusivamente para fines laborales. No está permitido su uso con fines personales, comerciales, publicitarios o fraudulentos.

3.12. PERDIDA DE ACCESO A LOS SERVICIOS INFORMÁTICOS.

El acceso a los servicios informáticos de Jersalud S.A.S. cesa de manera inmediata en los siguientes casos:

a. Empleados retirados voluntaria e involuntariamente.
b. Al terminar el convenio o prácticas en la institución.
c. Al terminar Outsourcing u ofertas mercantil de servicios con terceros.
d. Aplicación de sanciones disciplinarias o apertura de investigaciones que impliquen suspensión del acceso
e. Por terminación de cualquier vínculo con Jersalud S.A.S.

3.13. FALLAS CON TRÁMITE DISCIPLINARIO.

a. Usar y acceder a cuentas de usuario que no le corresponden o ajenas.
b. Compartir la información de credenciales (usuario/contraseña) con terceros.
c. Utilizar técnicas, herramientas de hacking o malware con el objetivo de escanear, vulnerar o corromper los sistemas de información sin autorización firmada por el representante legal de Jersalud S.A.S.
d. Hackear, escuchar o decodificar el tráfico de la red interna o externa o cualquier otro intento de obtención de información confidencial que se transmita a través de la red.
e. Realizar labores propias de los administradores del sistema sin permiso por escrito de la dirección de operaciones de TI.
f. Manipular, desarmar o intentar reparar equipos de cómputo, periféricos, dispositivos electrónicos, infraestructura de red o servidores de Jersalud S.A.S. Estas labores solo pueden ser realizadas por el personal del área TI o contratistas autorizados por la Dirección TI.
g. La instalación de software en equipos de cómputo es responsabilidad del área de Tecnología de Información TI, ningún usuario está autorizado para instalar, ejecutar o almacenar software no autorizado por la dirección TI.
h. El personal de soporte TI de Jersalud S.A.S no está autorizado para recibir, diagnosticar ni realizar intervenciones en equipos de cómputo que no pertenezcan a la institución, incluyendo aquellos de uso personal de empleados, contratistas o personas externas, dentro de las instalaciones de Jersalud S.A.S.
i. Está estrictamente prohibido consultar, modificar, copiar, grabar, suprimir o agregar información en archivos, carpetas o sistemas de información que no sean de uso propio, sin la autorización expresa del propietario de la información. Esta conducta aplica tanto a recursos almacenados localmente como en redes institucionales, y constituye una violación a la confidencialidad y a las políticas de seguridad de la información de Jersalud S.A.S.

3.14. RESPONSABILIDAD DEL PROVEEDOR DE OUTSOURCING DE TECNOLOGÍA DE LA INFORMACIÓN TI

El proveedor de Outsourcing de TI debe velar por el cumplimiento del Manual de Seguridad Informática, el incumplimiento de este incurrirá a sanciones o terminación anticipada de contratos si así lo define la dirección de TI.

3.15. SANCIONES

Las sanciones acerca del incumplimiento de este documento sobre el uso de tecnología se realizan según el vínculo de trabajo que se tenga con la persona que realiza la sanción.

3.15.1. Colaboradores

Se notificará a la oficina de Talento Humano para que se realice la respectiva investigación y descargos a los que haya lugar.

3.15.2. Contratistas

La notificación de la sanción es reportada al interventor del contrato.

3.15.3. Auditores médicos externos

La falta al cumplimiento de este reglamento manual se reportará al Director Médico, Gerente o Sede de sucursal para reporte oficial a la EPS correspondiente.

3.15.4. Docentes y estudiantes

La falta al cumplimiento de este reglamento será notificada al Coordinador del Programa Educativo, y se llevará a comité Docencia servicio.

3.16. POLITICA DE TRATAMIENTO DE DATOS PERSONALES

a. Tanto los usuarios, colaboradores, contratistas y proveedores deben dar su aprobación para el tratamiento de sus datos personales de acuerdo con lo descrito en la Política de Tratamiento de Datos de la Compañía, el art. 6º del Decreto 1377 de 2013 y el art. 5º de la Ley 1581 de 2012. De igual forma, de conformidad con el art. 26 de la Ley 1581 de 2012, según **F-GTH-113 FORMATO DE AUTORIZACIÓN PARA TRATAMIENTO DE DATOS**, lo anterior también se verá reflejado en las cláusulas contractuales y en las aplicaciones corporativas que soliciten información de datos personales.
b. La cuenta corporativa asignada de Office 365 y sus aplicaciones como Microsoft Teams tiene permiso de cambio de fotografía, al realizar la inclusión o cambio será considerado un dato sensible y el titular está dando su aprobación de acuerdo con lo descrito en la Política de Tratamiento de Datos de la Compañía, el art. 6º del Decreto 1377 de 2013 y el art. 5º de la Ley 1581 de 2012. De igual forma, de conformidad con el art. 26 de la Ley 1581 de 2012.
c. El colaborador o contratista que requiera realizar la entrega del grafo de su firma al área tecnología de la información TI para ser

incluida en los sistemas de información será considerado un dato sensible y el titular está dando su aprobación de acuerdo con lo descrito en la Política de Tratamiento de Datos de la Compañía, el art. 6º del Decreto 1377 de 2013 y el art. 5º de la Ley 1581 de 2012. De igual forma, de conformidad con el art. 26 de la Ley 1581 de 2012.

d. El colaborador o contratista desvinculado-voluntaria o involuntariamente que debe entregar los activos de información, su visto bueno de aceptación será firmado por la Dirección TI en **F-GTH-041 FORMATO ACTA DE ENTREGA DE PUESTO DE TRABAJO .**
e. La información generada, almacenada y recibida en el activo de información serán propiedad de Jersalud S.A.S.

3.17. CONEXIÓN DE EQUIPOS EXTERNOS A LA RED LAN

En Jersalud S.A.S. queda estrictamente prohibida la conexión de equipos externos o de uso personal (computadores portátiles, dispositivos de escritorio, impresoras, servidores, dispositivos de IoT y otros periféricos de red) a la infraestructura LAN institucional sin la autorización expresa del área de Tecnología de la Información TI.

3.18. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON PROVEEDORES

Los procesos de contratación y adquisición de productos y/o servicios de tecnologías de la información deben incluir un análisis de riesgos en materia de seguridad de la información. Dicho análisis deberá orientarse al cumplimiento de la normatividad legal vigente y a los lineamientos internos de la organización, garantizando en todo momento los principios de confidencialidad, integridad y disponibilidad de la información, así como la adecuada protección de los activos que se compartan, procesen o gestionen con terceros.

3.19. DERECHOS DE ACCESO A LA INFORMACIÓN

Ningún usuario de Jersalud S.A.S., ya sea interno o externo, está autorizado a acceder, copiar, modificar o divulgar información confidencial o sensible cuando su rol, funciones o responsabilidades no estén directamente relacionadas con el proceso al que pertenece dicha información.

3.20. DISPOSICIÓN FINAL DE MEDIOS DE ALMACENAMIENTO DIGITAL

En Jersalud S.A.S. velando por la confidencialidad de la información se garantiza el proceso de destrucción o formateo a bajo nivel de discos duros, unidades de almacenamiento extraíbles, memorias USB u otros dispositivos de almacenamiento cuando estas ya sean dadas de baja por obsolescencia o diagnóstico técnico.

3.21. LINEAMIENTOS PARA LA CREACIÓN Y USO DE CONTRASEÑAS SEGURAS.

Las contraseñas constituyen un mecanismo esencial para garantizar la protección de los sistemas de información de Jersalud S.A.S. En consecuencia, todos los usuarios están obligados a cumplir con las siguientes disposiciones:

a. **Carácter personal e intransferible:** Las contraseñas son únicas, confidenciales y de uso exclusivo del propietario de la cuenta.
b. **Restricciones de uso:** Queda prohibido utilizar en las contraseñas el nombre de la institución, áreas, fechas de nacimiento, números secuenciales, años o cualquier información que pueda ser fácilmente deducible.
c. **Requisitos de complejidad mínima**:
    - Longitud mínima de 8 caracteres.
    - Uso combinado de letras mayúsculas y minúsculas.
    - Inclusión de números y caracteres especiales
d. **Periodicidad de cambio:** Todas las contraseñas deberán renovarse con una periodicidad de tres meses.

Lo anterior esta articulado y se garantiza con el **I-GI-014 INSTRUCTIVO PARA LA CREACIÓN E INACTIVACIÓN DE USUARIO EN LOS SISTEMAS DE INFORMACIÓN**, el cual inicia con la recepción de solicitud de creación de usuario, novedad de nómina de usuario y terminación de vínculo laboral con la institución y cuentas externas. Asimismo, contempla la asignación, custodia y fortalecimiento de credenciales de acceso, garantizando el uso de contraseñas seguras para todos los diferentes sistemas de información, en concordancia con las políticas institucionales de seguridad. Finalizando con la entrega de la configuración de acceso correcto a las aplicaciones al responsable.

4. CONTROL DE PERSONAS

4.1. REPORTE NOVEDAD INGRESO/ RETIRO USUARIOS/ VACACIONES

Al momento del ingreso, retiro o suspensión temporal de un usuario de la institución, el área de Talento Humano de cada sucursal o nacional deberá notificar de forma inmediata al área de Tecnología de la Información mediante la creación de un caso a través de la plataforma GLPI, adjuntando el formato **F-GI- 081 FORMATO PARA CREACIÓN E INACTIVACIÓN DE USUARIOS EN LOS SISTEMAS DE INFORMACIÓN**. En el caso de estudiantes, internos y docentes, la responsabilidad de diligenciar y remitir el formato corresponde a la Coordinación de Docencia y Servicio, siguiendo el mismo procedimiento establecido.

Esta notificación permitirá crear, modificar, bloquear o desactivar las cuentas y credenciales asignadas, garantizando que el acceso a la red, sistemas y aplicaciones institucionales se mantenga conforme a los principios de seguridad de la información y a la normativa interna vigente.

4.2. MANIPULACIÓN DE INFORMACIÓN

En Jersalud S.A.S, ningún usuario, ya sea interno o externo, está autorizado a consultar, agregar, modificar o eliminar información

contenida en carpetas, archivos o sistemas que no le correspondan, o sin la autorización expresa del propietario de dicha información.

En el caso de información sensible, protegida por la legislación colombiana en materia de protección de datos personales, su tratamiento deberá cumplir estrictamente con lo establecido en el **M-GD-003 MANUAL DE POLÍTICAS INSTITUCIONALES**, sección 7.2. – Política de Tratamiento de Datos Sensibles.

5. CONTROLES FÍSICOS

5.1. RESTRICCIÓN AL USO DE DISPOSITIVOS USB DENTRO DE LA RED.

En Jersalud S.A.S. no se permite el uso de dispositivos USB, discos duros externos o tarjetas de memoria personales en equipos de cómputo corporativos, la dirección de Tecnología de la Información TI de cada sucursal definirá los permisos de uso específicos.

5.2. INGRESO PERSONAL NO AUTORIZADO A LA OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN TI, CENTRO DE CÓMPUTO Y/O CABLEADO

En Jersalud S.A.S., el acceso físico a los Centros de Cableado estructurado, de cómputo y data center estarán estrictamente restringido. El personal interno del área de Tecnologia de la Información TI podrá ingresar únicamente durante el horario laboral establecido, previa validación de su credencial vigente. Para ingresos fuera de este horario o durante fines de semana, se requerirá autorización por escrito del director TI y/o Dirección de Operaciones de TI.

El ingreso a centros de cableado estructurado y data center por parte de proveedores, contratistas y cliente interno requerirán acompañamiento de personal del área de Tecnología de la Información TI y autorización por escrito del director TI de sucursal y/o Dirección de Operaciones de TI.

5.3. MOVER FÍSICAMENTE LOS RECURSOS INFORMÁTICOS DEL PUESTO DE TRABAJO

En Jersalud S.A.S. no está autorizado al usuario el mover físicamente los equipos de cómputo, impresoras, equipos de red, servidores, periféricos y otros. Las actividades de movimiento y/o traslado de insumos de informático son labores exclusivas del área Tecnología de la Información TI, cualquier otra persona que lo haga sin la autorización pertinente será directamente responsable de la integridad de los equipos transportados.

5.4. USO DE OBJETOS NO ACORDES A LA FUNCIÓN DEL RECURSO INFORMÁTICO

En Jersalud S.A.S., no está permitido colocar líquidos, alimentos, objetos pesados, ni ningún elemento que pueda obstruir la ventilación cerca o sobre los equipos de cómputo. Asimismo, está prohibido ubicar insumos o dispositivos informáticos en el piso u otros lugares que puedan generar riesgo de daño por golpes, derrames, caídas o por interferir con el tránsito de personas.

5.5. INTERCAMBIO DE RECURSOS INFORMÁTICOS QUE ALTEREN EL INVENTARIO DE HARDWARE

En Jersalud S.A.S. no está autorizado intercambiar teclados, computadores de escritorio o de torre, monitores, reguladores, UPS o impresoras sin la autorización personal de Tecnología de la Información TI y el personal de Activos Fijos de la Institución, estos movimientos alteran el inventario de hardware.

6. CONTROLES TECNOLÓGICOS

6.1. PROTECCIÓN ENDPOINT

Jersalud S.A.S. debe garantizar que el 100% de los servidores y equipos de cómputo conectados a la red LAN institucional cuenten con protección de EndPoint Protection, centralizada, administrada y monitoreada por el área de Tecnologías de la Información.

No está permitido que equipos internos, de proveedores o externos se conecten a la red institucional o VPN, sin contar con un sistema de protección EndPoint licenciado y actualizado.

6.2. PERMISOS CONEXIÓN VIRTUAL PRIVATE NETWORK (VPN)

Jersalud S.A.S garantizará el adecuado manejo de acceso de Virtual Private Network (VPN), con el fin de proteger la información institucional y reducir los riesgos de perdida, manipulación o accesos no autorizados.

6.2.1. Autorización de acceso

a. Los permisos de acceso al recurso de Virtual Private Network (VPN) solo están sujetos a la autorización dada por las Gerencias, Vicepresidencias ó Presidencia y será autorizado a través del formato **F-GI-028 FORMATO DE AUTORIZACIÓN PARA ACCESO VPN.**
b. El formato deberá ser presentado por el jefe de área (Director ó líder nacional) de quien requiere el acceso al recurso Virtual Private Network (VPN) y autorizado o denegado por el Director de Operaciones TI.
c. En el caso de personal externo, la solicitud deberá ser escalada por el jefe de área responsable.
d. Cuando el colaborador finalice su vínculo laboral, talento humano notificará a la Dirección de Tecnología de la Información TI, para la correspondiente desactivación de manera inmediata, mediante el **I-GI-014 INSTRUCTIVO PARA LA CREACIÓN E INACTIVACIÓN DE USUARIO EN LOS SISTEMAS DE INFORMACIÓN.**

6.2.2. Lineamientos de seguridad para el uso de la Virtual Private Network (VPN)

Todo usuario con acceso autorizado a la Virtual Private Network (VPN) debe cumplir con los siguientes lineamientos:

a. Equipos permitidos: Solo se podrán conectar equipos corporativos o aquellos expresamente autorizados por Tecnología de la Información TI, los cuales deberán tener:

*Sistema operativo actualizado.

*Software de protección EndPoint licenciado y vigente.

b. Uso responsable: La VPN se usará únicamente para actividades laborales y con fines institucionales.

*Está prohibido compartir credenciales de acceso o permitir que otra persona utilice la sesión asignada.

*Solo se permite una sesión VPN activa por usuario.

c. Seguridad en la conexión: Se utilizará autenticación multifactor (MFA) para reforzar la protecció.

*Toda la información transmitida será cifrada para evitar accesos indebidos

*Se deben reportar de inmediato a Tecnología de la Información TI los intentos de acceso sospechoso o fallidos.

d. Uso aceptable: Están permitidas únicamente las actividades relacionadas con la labor en Jersalud S.A.S.

*Queda prohibido el uso de la VPN para fines personales o actividades no autorizadas

*El incumplimiento de estas disposiciones puede generar la suspensión del acceso, perdida de privilegios e incluso sansiones legales.

e. Monitoreo y capacitación: El área de Tecnología de la Información y Comunicaciones TIC realizará monitoreo y auditorias periódicas para garantizar el uso correcto de la VPN. Los usuarios recibirán capacitación para conocer las reglas de seguridad y el uso adecuado de la VPN.

6.3. RESPONSABILIDAD DE LAS COPIAS DE SEGURIDAD

El área de Tecnologías de la Información es responsable de planificar, ejecutar, monitorear y verificar las copias de seguridad de los servidores, así como de los archivos institucionales almacenados en las unidades de red o plataformas designadas oficialmente para el almacenamiento centralizado de información.

Por su parte, cada colaborador es responsable de proteger y respaldar la información que gestiona directamente desde su estación de trabajo, utilizando exclusivamente las herramientas autorizadas por la Institución, como OneDrive, SharePoint o la carpeta compartida de red cuando aplique. En caso de no contar con una licencia de Office 365, el área de Tecnología de la Información TI indicará el medio autorizado correspondiente.

El uso de estas plataformas garantiza que la información se respalde de forma segura y centralizada, en cumplimiento de las políticas de protección de datos de la Institución. Esto evita la pérdida de información, el acceso no autorizado o el uso de medios de almacenamiento no aprobados.

6.4. EXCEDER CUOTA BUZÓN DE MENSAJES

En Jersalud S.A.S no está autorizado al usuario exceder la cuota de envió de mensajes con archivos adjuntos que excedan los 10 Megas por email, las políticas de tamaño de los correos y el buzón de mensajes garantizan el correcto funcionamiento del servicio de mensajera.

6.5. CAMBIO CONFIGURACIÓN ESTACIÓN DE TRABAJO

En Jersalud S.A.S no está autorizado al usuario modificar la configuración de los equipos, adicionar o cambiar puertos, modificar configuraciones, cambiar papel tapiz, descansa pantallas o cualquier otro ítem de configuración sin el consentimiento del personal de soporte técnico de TI.

6.6. ASIGNACIÓN DE ROLES Y PRIVILEGIOS DE ACCESO

La asignación de roles y permisos de ingreso a Internet, Sistemas misionales, Office 365 y demás sistemas de información de Jersalud S.A.S. serán definidos de acuerdo con los perfiles establecidos en el formato F-GI-080 FORMATO ROLES Y ACCESO SISTEMAS DE INFORMACIÓN y serán habilitados de acuerdo a lineamientos del director de Tecnología de la Información TI.

6.7. CIFRADO DE DISCOS Y UNIDADES DE ALMACENAMIENTO

Con el fin de garantizar la confidencialidad e integridad de la información institucional, todos los equipos de cómputo y dispositivos de almacenamiento asignados por Jersalud S.A.S. deberán contar con cifrado de disco.

7. EVALUACIÓN

- Aplicación de cronograma de auditoría por parte del departamento TIC el cual se realizará cada seis meses evaluando los criterios establecidos en el **F-GI-068 FORMATO LISTA DE VERIFICACIÓN PARA LA AUDITORÍA DEL MANUAL DE SEGURIDAD INFORMÁTICA**

- Control del ingreso al cuarto de servidores a través del **F-GI-030 ORMATO DE INGRESO A CUARTO DE SERVIDORES.**

- Seguimiento a los indicadores:

7.1. INDICADORES

CODIGO DEL INDICADOR	INDICADOR	FÓRMULA	PERIOCIDAD
N.A.	Índice de eventos de vulneración de seguridad informática	Número de eventos de Vulneración de seguridad informática X 1000 Número de Usuarios del Sistema	**Mensual**

8. REFERENCIAS DOCUMENTALES

8.1. DOCUMENTOS INTERNOS

M-GC-006 MODELO DE LIMPIEZA Y DESINFECCIÓN

M-GTH-041 MANUAL DE COMUNICACIÓN ESTRATÉGICA

F-GTH-113 FORMATO DE AUTORIZACIÓN PARA TRATAMIENTO DE DATOS

F-GTH-041 FORMATO ACTA DE ENTREGA DE PUESTO DE TRABAJO .

I-GI-014 INSTRUCTIVO PARA LA CREACIÓN E INACTIVACIÓN DE USUARIO EN LOS SISTEMAS DE INFORMACIÓN

F-GI- 081 FORMATO PARA CREACIÓN E INACTIVACIÓN DE USUARIOS EN LOS SISTEMAS DE INFORMACIÓN

M-GD-003 MANUAL DE POLÍTICAS INSTITUCIONALES

F-GI-028 FORMATO DE AUTORIZACIÓN PARA ACCESO VPN.

F-GI-068 FORMATO LISTA DE VERIFICACIÓN PARA LA AUDITORÍA DEL MANUAL DE SEGURIDAD INFORMÁTICA

F-GI-030 ORMATO DE INGRESO A CUARTO DE SERVIDORES.

F-FI-080 FORMATO DE ROLES Y ACCESO SISTEMAS DE INFORMACIÓN

ANEXOS

Control de cambios		
Versión	**Fecha**	**Descripción**
1	11-10-2019	Creación del documento
2	01-08-2022	Se modifica el diseño de la plantilla, se cambia el nombre del documento reemplazando modelo por manual, se elimina la restricción al uso de dispositivos de almacenamiento de la Red, se elimina permisos para VPN, Se agrega creación y conexión centros de cableado, se agrega custodia insumos informáticos para uso exclusivo de actividades laborales, se agrega garantizar la legalidad del software en el equipo asignado.
3	30-09-2025	Como oportunidad de mejora detectada se realiza actualización y modificación del documento. Se divide por Controles de Seguridad de la Información: Controles Organizacionales, Controles de Personas, Controles Físicos, Controles Tecnológicos.

Elaborador por:	Revisado por:	Aprobado por:

Johnatan Steven Palomá Gutiérrez Profesional de Tecnología de la Información Diana Patricia Camargo Niño Profesional Especializado de Procesos	Sandra Patricia Peñaloza Líder de Garantía de la Calidad Luz Angela Acosta Urrego Profesional de Calidad Yolvi Amileth Rodríguez Navas Líder de Garantía de la Calidad Ever Danny Peña Rojas Director nacional de tecnología	Francia Viviana Devia López Director Médico Renso Eduardo Amaya Sánchez Director Médico Norvey Fernando Rodríguez Guevara Director Médico
Fecha: 2025-09-30	Fecha: 2025-09-30	Fecha: 2025-09-30