ÍNDICE

1. INTRODUCCIÓN

Servinformación determina la información como un activo de alta importancia, que permite el desarrollo continuo de la misión, visión y cumplimiento de los objetivos, por lo cual se genera la necesidad de implementar medidas que permitan proteger la confidencialidad, integridad y disponibilidad dentro del ciclo de vida de la información.

En el presente manual se establecen las Políticas Específicas del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) definidas por **Servinformación**, con las cuales se busca garantizar confidencialidad, integridad y disponibilidad de la información y deben ser adoptadas por los colaboradores, contratistas, visitantes y terceros que prestan servicios o tengan algún tipo de relación con **Servinformación**, y que están enfocadas al cumplimiento de la normatividad legal y a las buenas prácticas de seguridad de la información basadas en la Norma ISO/IEC 27001: 2022 y demás requisitos aplicables al contexto de la Organización.

2. OBJETIVO DEL MANUAL

Describir las Políticas Específicas de Seguridad de la Información a seguir por todo el personal de **Servinformación** (colaboradores, contratistas, visitantes y todos aquellos con acceso a la información), con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y de sus activos relacionados. Con lo anterior se busca fortalecer la gestión de seguridad y privacidad de la información de **Servinformación**.

3. ALCANCE DEL MANUAL

Este manual define las Políticas Específicas de Seguridad de la Información aplicables a **Servinformación**, las cuales son de obligatorio cumplimiento para todos los colaboradores, contratistas, visitantes y terceros que mantengan alguna relación con la Organización. El fundamento de estas políticas se encuentra en las directrices establecidas por la Norma ISO/IEC 27001:2022. Además, se complementan con los elementos pertinentes según lo definido en el numeral **5.7 Marco Normativo** del documento "**M-SI-02 Manual Seguridad de la Información**".

4. DEFINICIONES

Se establece el documento **"D-SI-07 Términos y Definiciones del Sistema de Gestión de Seguridad de la Información",** el cual desempeña un papel fundamental al ser una base clara y uniforme para el entendimiento del SGSI de Servinformación.

5. RESPONSABILIDADES GENERALES

Servinformación establece una serie de responsabilidades generales en relación con las políticas de seguridad del a información de la Organización:

Líder de Seguridad de la Información:

- Desarrollar y mantener las políticas de seguridad de la información.
- Asegurarse de que las políticas de seguridad de la información cumplan con los requisitos legales y regulatorios, así como los objetivos de seguridad de la Información de la Organización.
- Supervisar la implementación y el cumplimiento de las políticas de seguridad de la información.
- Brindar a los colaboradores la información y capacitación necesaria para cumplir las políticas de seguridad.

Comité de Seguridad:

- Revisar y aprobar las políticas de seguridad de la información.
- Supervisar el rendimiento y la eficacia de las políticas de seguridad de seguridad de la información.
- Asegurarse de que los recursos necesarios estén asignados para la implementación de políticas de seguridad.
- Revisar informes de incidentes y los incumplimientos a las políticas de seguridad de la información.

Gestión de IT:

- Implementar medidas técnicas para garantizar la seguridad de la información.
- Realizar el monitoreo y evaluaciones pertinentes a las medidas técnicas implementadas.

Responsables de Procesos:

- Integrar las políticas de seguridad de la información en sus procesos.
- Garantizar que los colaboradores a su cargo estén informados y conscientes sobre las políticas de seguridad de la información.
- Garantizar el cumplimiento de las políticas de seguridad de la información en sus procesos.
- Conocer y controlar las excepciones a las políticas que se deban mantener dentro de sus procesos.

Colaboradores:

- Conocer y cumplir las políticas de seguridad de la información y procedimientos relacionados.
- Participar activamente en las capacitaciones que apoyen el cumplimiento de las políticas de seguridad.

- Informar de cualquier incumplimiento a las políticas, incidentes, eventos, amenazas y demás situaciones que sean relevantes para la seguridad de la información de la Organización, al Líder de Seguridad de la Información.

6. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE SERVINFORMACIÓN

6.1. POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

Servinformación, para evitar la pérdida, robo o exposición al peligro de los recursos de la Organización que se encuentren dentro o fuera de sus instalaciones, provee los recursos que garanticen la mitigación de riesgos sobre la plataforma tecnológica.

6.1.1. OBJETIVO DE LA POLÍTICA

Garantizar la seguridad física y ambiental de los recursos de la Organización, tanto dentro como fuera de sus instalaciones, mediante la implementación de medidas y controles que minimicen los riesgos y aseguren la integridad de la plataforma tecnológica.

6.1.2. ALCANCE DE LA POLÍTICA

Aplica a todas las instalaciones, equipos, y recursos de Servinformación, así como a todo el personal interno y externo que tenga acceso a dichos recursos.

6.1.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Coordinar pruebas y actualizaciones del Plan de Continuidad del Negocio.
- Liderar la gestión de riesgos físicos y ambientales que puedan comprometer la seguridad de la información.

Comité de Seguridad:

- Revisar y aprobar el Plan de Continuidad del Negocio.
- Evaluar y mitigar los riesgos físicos y ambientales identificados.

Gestión IT:

- Implementar y mantener medidas de control de acceso físico y lógico.
- Supervisar el funcionamiento del Centro de Redes y garantizar los requisitos ambientales.
- Gestionar el control de acceso a áreas restringidas.
- Coordinar movimientos y reasignaciones de recursos tecnológicos.
- Gestionar problemas de hardware o software, y demás novedades reportados por los colaboradores.

Responsables de Procesos:

- Hacer cumplir los controles físicos implementados en las áreas de trabajo.
- Registrar ingresos y egresos de personal y terceros.
- Participar en la implementación y mantenimiento de medidas de seguridad física en sus procesos.

Colaboradores:

- Cumplir con las medidas de control de acceso e identificarse debidamente.
- Mantener los escritorios físicos y lógicos libres de información confidencial.
- Bloquear la pantalla del computador al ausentarse del puesto de trabajo.
- No almacenar información personal en los computadores de la organización.
- Informar inmediatamente sobre pérdida o robo de equipos.

6.1.4. GENERALIDADES

Directrices Relacionadas con el Trabajo en Áreas Seguras

- Servinformación establece el procedimiento "**P-SI-06 Trabajo en Áreas Seguras**" con el fin de establecer un entorno físico de trabajo acorde con los requerimientos de Confidencialidad, Integridad y Disponibilidad.
- Servinformación en sus instalaciones tiene implementado un sistema de control de acceso físico mediante huella dactilar. Adicionalmente, cuenta con una recepción donde se controla el ingreso y salida de terceros, el ingreso y salida de elementos, tanto de colaboradores como de terceros.
- La carga se recibe y despacha por el garaje de la casa. La recepción y despacho de carga es controlada por el Proceso Administrativo de la Organización y se tienen horarios específicos para la realización de estas actividades.
- Los ingresos y egresos de personal a las instalaciones de Servinformación deben ser registrados; por consiguiente, los colaboradores, visitantes y personal provisto por terceras partes deben cumplir completamente con los controles físicos implementados e identificarse debidamente.
- Se exige a todas las personas dentro de las instalaciones de Servinformación portar su carné de colaborador en un lugar visible. Todos los colaboradores tienen la responsabilidad de asegurarse de que toda persona lo lleve consigo y, en caso de no obtener una respuesta satisfactoria, deben reportar el evento de seguridad según lo establecido en el procedimiento "**P-SI-02 Gestión de Incidentes de Seguridad de la Información**".

Directrices Relacionadas con las Áreas de Acceso Restringido

- En Servinformación existen áreas donde se procesa o almacena información clasificada en los niveles más altos de confidencialidad, integridad o disponibilidad.

Estas **áreas de acceso restringido** requieren un nivel adicional de protección, que incluye:

- Perímetro adicional de seguridad (puertas con acceso bloqueado, accesos biométricos).
- Acompañamiento de un colaborador de Servinformación a los visitantes.
- Registro en bitácoras de visita.
- Circuito cerrado de TV (CCTV).
- Prohibición de entrada de equipos de video, fotografía o grabación.
- Demarcación o identificación de que el área es restringida.

- El Centro de Redes debe contar con mecanismos que permitan garantizar que se cumplen los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga.
- El Centro de Redes estará ubicado de tal forma que el acceso físico sea controlado exclusivamente por la Coordinación de Informática. Se realiza seguimiento a las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) que pueden llegar a afectar esta locación.
- La información sobre la naturaleza y localización de los sistemas de procesamiento y almacenamiento de Servinformación es de carácter reservado y solo debe ser divulgada a quienes demuestren la necesidad de conocer y sean autorizados por el Líder de Seguridad de la Información.
- Servinformación cuenta con un "**P-SI-17 Plan de Continuidad del Negocio**" que es probado periódicamente, con el fin de garantizar el correcto funcionamiento de la infraestructura de cara a mantener las operaciones de la Organización.
- Servinformación cuenta con aire acondicionado de contingencia, un sistema de alimentación ininterrumpida (UPS) que asegura el tiempo necesario para apagar adecuadamente los servidores ante una falla en el suministro de energía, y un enlace de red redundante.
- El ingreso de personas externas al Centro de Redes debe ser registrado en el formato para tal fin.
- Servinformación cuenta con un sistema de seguridad CCTV dentro de las instalaciones y adicionalmente, tiene contratado el servicio de vigilancia y monitoreo de las áreas externas de la Organización mediante vigilancia, durante las 24 horas del día. Por lo tanto, se debe tener en cuenta lo siguiente:
  - Está prohibido generar una copia de video sin previa autorización del Comité de Seguridad.
  - Toda solicitud de copias de video debe hacerse por escrito al Comité de Seguridad.
  - Las grabaciones realizadas por el NVR tienen una duración de 15 días.
  - Está prohibido dar información de especificaciones técnicas y ubicaciones de cámaras.

- Toda copia de video generada debe ser entregada mediante oficio o mediante cadena de custodia.

Directrices Relacionadas con el Equipo Desatendido, Escritorio Limpio y Pantalla Limpia

- Los colaboradores de Servinformación deben conservar su escritorio libre de información propia de la Organización, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento, cada vez que se vayan a retirar de sus puestos de trabajo.
- Al imprimir documentos de carácter confidencial, éstos deben ser retirados de la impresora inmediatamente.
- Los computadores cargarán por defecto el fondo de pantalla de Servinformación; este no debe ser modificado y debe permanecer activo.
- Los colaboradores de Servinformación deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo.
- Los usuarios son responsables y asumen las consecuencias por la pérdida de información que esté bajo su custodia.
- Se prohíbe el almacenamiento de información personal en los computadores de Servinformación.
- El escritorio lógico debe estar libre de información interna e información confidencial.

Directrices Relacionadas con la Seguridad Física de los Equipos

- La Coordinación de Informática es el único proceso autorizado para realizar movimientos y reasignaciones de recursos tecnológicos.
- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de Servinformación el usuario responsable debe informar a la Coordinación de Informática, mediante correo electrónico a servicedesk@servinformacion.com, quien debe hacer la gestión pertinente sobre la falla.
- Teniendo en cuenta el proceso y/o el cargo, los equipos portátiles pueden ser retirados de las instalaciones, efecto para el cual no requerirán permiso específico, no obstante el responsable debe velar por la seguridad del mismo y de la información que repose en él.
- En caso de pérdida o robo de un equipo portátil, el colaborador debe informar de inmediato por correo electrónico al jefe inmediato, a Gestión IT y a Gestión Humana. El colaborador debe presentar la denuncia correspondiente ante la autoridad competente.

6.2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA INFRAESTRUCTURA TECNOLÓGICA

Servinformación establece las directrices necesarias para asegurar la infraestructura tecnológica de la Organización, con el fin de garantizar la protección de la información generada, procesada o resguardada por la Organización. Por medio de tales directrices se orienta el uso, la configuración, la capacidad y el monitoreo de la infraestructura tecnológica en Servinformación partiendo de la necesidad de asegurar un uso apropiado y eficiente de los recursos. Esto se aplica a todos los activos tecnológicos, sistemas y componentes relacionados utilizados en la organización.

6.2.1. OBJETIVO DE LA POLÍTICA

Establecer los lineamientos para garantizar la integridad de los activos tecnológicos que conforman la infraestructura de Servinformación, con el fin de mantener un entorno seguro y confiable.

6.2.2. ALCANCE DE LA POLÍTICA

Esta política aplica a todos los usuarios que acceden, utilizan o administran los activos tecnológicos que conforman la infraestructura de Servinformación.

6.2.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Colaborar con Gestión IT en la implementación de medidas de seguridad en la infraestructura tecnológica.
- Asegurar que se realicen revisiones periódicas de la configuración y se tomen medidas correctivas cuando sea necesario.
- Participar en la elaboración de informes de seguridad relacionados con el uso de la infraestructura tecnológica.

Comité de Seguridad:

- Evaluar los riesgos en la infraestructura tecnológica y revisar incidentes de seguridad.
- Evaluar periódicamente la eficacia de las medidas de seguridad implementadas.
- Asesorar en decisiones estratégicas relacionadas con la infraestructura tecnológica.

Gestión IT:

- Gestionar el acceso a los recursos tecnológicos según las directrices establecidas.
- Administrar la instalación y configuración de equipos y software.
- Controlar, registrar, autorizar o denegar los cambios en la configuración de la infraestructura tecnológica de acuerdo con las políticas establecidas.

- Garantizar que se establezca y mantenga una línea base de la configuración clara y bien documentada.
- Garantizar las buenas prácticas en el monitoreo de la infraestructura tecnológica de la Organización.
- Mantener el inventario de activos tecnológicos actualizado.
- Gestionar el retiro de activos por obsolescencia u otros motivos.

Responsables de Procesos:

- Colaborar con Gestión IT para garantizar el uso eficiente de los recursos.
- Colaborar con Gestión IT para identificar y mantener una línea base de configuración actualizada.
- Notificar los cambios importantes en los procesos que afecten la configuración de la infraestructura tecnológica.

Colaboradores:

- Seguir los procedimientos establecidos al interactuar con los activos tecnológicos y sistemas.
- Colaborar con los responsables de procesos para implementar medidas de seguridad en su proceso.

6.2.4. GENERALIDADES

Directrices relacionadas con el Uso de la Infraestructura Tecnológica

- La infraestructura tecnológica de Servinformación no debe ser utilizada para actividades comerciales ajenas a la Organización; o para propósitos de entretenimiento, diversión o acceso a material no autorizado.
- Se prohíbe el uso de la infraestructura tecnológica de la Organización para cualquier tipo de actuación que vaya en contra de la ley y normatividad vigente.
- Los activos tecnológicos deben ser utilizados de manera eficiente, evitando su uso para el almacenamiento de información personal, material no autorizado o cualquier otro tipo de información que no sea necesario para el desarrollo de las funciones, actividades y obligaciones contractuales.
- Los usuarios deben utilizar las herramientas tecnológicas propias de Servinformación o licenciadas o aprobadas por Gestión IT, y deben abstenerse de utilizar aquellas aplicaciones que no hayan sido explícitamente aprobadas.
- Los usuarios deben abstenerse de copiar software licenciado o adquirido por Servinformación, usar herramientas portables no licenciadas para uso personal o beneficio de terceros, e instalar en los equipos de cómputo software no autorizado por la Organización.
- Los usuarios deben abstenerse de introducir software malicioso en la infraestructura tecnológica de Servinformación, así como monitorear, capturar, manipular o destruir la información que circula por la red de datos o voz.

- Los usuarios deben abstenerse de conectar dispositivos activos de red, o cualquier otro hardware, a la red de datos o voz sin la autorización de Gestión IT.
- Cualquier activo tecnológico adquirido por la organización, debe ser registrado de manera oportuna en GLPI y gestionados por Gestión IT. Además, se asignará un propietario a cada activo tecnológico, quien debe ser responsable de asegurar su correcto uso, así como de proporcionar la protección adecuada.
- Gestión IT puede utilizar herramientas tecnológicas o procedimientos manuales para monitorear el uso de la infraestructura tecnológica y aquel material almacenado, publicado, enviado, recibido o creado a través de estos recursos. Para el monitoreo o captura de tráfico por la red de datos, Gestión IT debe hacer uso de esta información únicamente con fines de detección y gestión de anomalías, alertas de seguridad o problemas en la red.
- Gestión IT puede otorgar o denegar el acceso a los activos tecnológicos a los usuarios que lo soliciten, según los lineamientos establecidos para tal fin.
- Ningún proceso de la Organización está autorizado para instalar equipos de cómputo, servidores, redes o cualquier otro componente tecnológico dentro de las instalaciones de la Organización, esta actividad es responsabilidad única de Gestión IT.

Directrices relacionadas con la Configuración de la Infraestructura Tecnológica

- Servinformación establece el procedimiento "**P-SI-11 Gestión de la Configuración**", con el cual se mantiene la gestión de la configuración que abarca todos los activos tecnológicos y componentes del SGSI.
- Gestión IT debe mantener una estructura de configuración clara y bien documentada.
- Todos los activos tecnológicos y componentes de la infraestructura de la Organización deben ser identificados y etiquetados de manera única para su fácil identificación y seguimiento.
- Gestión IT debe controlar y registrar todos los cambios realizados en los activos de tecnologías de la Organización.
- Gestión IT debe realizar revisiones periódicas de la configuración para garantizar su integridad y coherencia.
- Gestión IT debe mantener registros precisos de la configuración y los cambios realizados, incluyendo la documentación asociada.
- Se deben realizar revisiones de la configuración después de cualquier incidente o cambio importante para identificar y corregir cualquier desviación o violación de la política.
- La organización debe contar en todo momento con un inventario actualizado del software de su propiedad, aquel adquirido a terceros, bajo licenciamiento, entregado o recibido en comodato. Las licencias se almacenarán con los niveles de

seguridad adecuados y se registran en el inventario, indicando el número de usuarios permitidos por licencia y la fecha de renovación.

Directrices relacionadas con la Capacidad de la Infraestructura Tecnológica

- Servinformación gestiona la capacidad de su plataforma tecnológica crítica por medio de las herramientas brindadas por el proveedor de servicios en la nube.
- Se debe mantener un control constante sobre la demanda de capacidad de los sistemas de Servinformación. Además, se deben realizar proyecciones periódicas de los requisitos futuros de capacidad para garantizar que los recursos sean adecuados y puedan satisfacer la creciente demanda de almacenamiento de información.
- Los recursos críticos del sistema deben ser objeto de un control riguroso para asegurar la disponibilidad de capacidad adicional cuando sea necesario. Esto garantizará un rendimiento óptimo y una respuesta eficiente a situaciones de carga intensiva.
- El Centro de Redes debe estar conectado al proveedor de servicios de internet a través de al menos dos rutas distintas. Esta medida busca prevenir que una falla en una conexión afecte el desempeño de los servicios de voz e internet. Se debe contar con un proveedor de telecomunicaciones de contingencia en caso de que falle el proveedor principal. Esta redundancia en los servicios de telecomunicaciones garantiza la continuidad operativa incluso en situaciones de emergencia, evitando interrupciones críticas en la conectividad y comunicación.
- La infraestructura tecnológica debe ser diseñada con una arquitectura escalable y flexible, permitiendo la fácil adaptación a cambios en la demanda. Esto asegura que la capacidad pueda ser ajustada de manera eficiente para satisfacer las necesidades en constante evolución de la organización.
- Gestión IT debe implementar un programa de mantenimiento preventivo regular para todos los componentes de la infraestructura tecnológica. Esto incluye actualizaciones de software, revisiones de seguridad y la sustitución oportuna de hardware obsoleto para mantener un ambiente tecnológico robusto y actualizado.
- Se debe mantener una documentación completa y actualizada de la infraestructura tecnológica, incluyendo configuraciones, topologías de red y procedimientos de recuperación.

Directrices relacionadas con el Monitoreo de la Infraestructura Tecnológica

- Gestión IT debe utilizar herramientas de monitoreo avanzadas y actualizadas para supervisar de manera continua el rendimiento de la infraestructura tecnológica. Estas herramientas deben ofrecer capacidades integrales para la detección

temprana de problemas, análisis de tendencias y generación de informes detallados.

- Se deben configurar alertas proactivas basadas en umbrales predefinidos para recibir notificaciones inmediatas en caso de desviaciones significativas o problemas potenciales. Esto permite abordar los problemas antes de que afecten el rendimiento o generen interrupciones en los servicios.
- Se debe llevar un registro de eventos que capture y almacene de forma detallada todas las actividades y cambios en la infraestructura. Este registro es esencial para la identificación retrospectiva de problemas, análisis post-evento y cumplimiento de normativas.
- Gestión IT debe garantizar la seguridad de las herramientas de monitoreo mediante la implementación de prácticas de autenticación robustas, cifrado de datos y acceso restringido. Esto protege la integridad de la información sensible y evita posibles amenazas a la infraestructura.
- Gestión IT debe realizar revisiones periódicas para evaluar la efectividad del sistema de monitoreo. Ajustar las configuraciones y procedimientos según sea necesario para garantizar que el monitoreo continúe cumpliendo con los requisitos operativos y de seguridad.
- Para el manejo adecuado de eventos no deseados y para la investigación efectiva de incidentes de seguridad de la información, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por Servinformación, deben estar sincronizados. La implementación de dicha sincronización se debe realizar bajo el protocolo NTP.

Directrices relacionadas con el uso de Equipos de Computo

- Los colaboradores de Servinformación deben utilizar únicamente el equipo de cómputo asignado por la Organización, para la ejecución de las actividades.
- En consecuencia a lo anterior, el uso de computadores de propiedad de los colaboradores, para la ejecución de las actividades encomendadas por Servinformación, se encuentra restringido.
- Todos los computadores asignados a los colaboradores deben contar con el antivirus autorizado por Servinformación, así como el registro de eventos y logs generados por el software de monitoreo y de red provisto por la Organización.
- Los colaboradores no deben realizar cambios a nivel de hardware o software. Únicamente el proceso de Gestión IT está en la potestad de realizar este tipo de cambios.
- Los colaboradores no deben hacer uso de software no autorizado explícitamente por Gestión IT.
- La Coordinación Informática debe controlar y asignar los activos tecnológicos que se requieran para el desempeño de las actividades en Servinformación.

- Cuando un colaborador devuelve el equipo asignado, por terminación, cambio de cargo o se va a dar de baja, Coordinación Informática revisará que no se encuentre información almacenada localmente, y procederá a disponer de esa información según indicaciones del Responsable de Proceso relacionado.

Directrices relacionadas con el Mantenimiento de Equipos

Servinformación establece que, para el buen funcionamiento de las herramientas tecnológicas, se requiere realizar anualmente el mantenimiento preventivo de los equipos de cómputo e infraestructura tecnológica, tarea que debe ser canalizada a través del Proceso de Gestión IT, de acuerdo con el procedimiento "**P-IT-01 Gestión Soporte IT**".

- Al inicio del año, el Coordinador Informático se reunirá con los Responsables de Procesos para que de mutuo acuerdo se establezcan las fechas del mantenimiento, con el fin de no afectar las actividades habituales.
- El mantenimiento se realizará en jornada laboral.
- La Coordinación Informática, recordará las fechas presupuestadas por si hay alguna incidencia, si un proceso no pudiese atender la fecha programada la actividad debe ser reprogramada en el cronograma respectivo.
- Si el mantenimiento es correctivo, el colaborador afectado debe informar mediante envío de un correo electrónico a servicedesk@servinformacion.com, y con base al impacto de la falla, el colaborador de Coordinación Informática procede a brindar una solución oportuna al requerimiento.

Directrices Relacionadas con la Seguridad de la Información en la Nube

Servinformación, dentro de su interés por la adopción de Cloud Computing para el desarrollo de servicios y soluciones empresariales, es consciente de la necesidad de establecer medidas de seguridad en la nube en el marco del SGSI. Por tanto, acepta la implementación de controles y buenas prácticas relacionadas con seguridad en la nube, basadas en la documentación de Google Cloud Platform (GCP), recomendaciones aplicables del estándar ISO/IEC 27017: 2015 y demás entes y organizaciones que sean referente en el mercado, buscando siempre el cumplimiento de la norma ISO/IEC 27001: 2022. Lo anterior aplica a los servicios y soluciones empresariales desarrollados usando Cloud Computing.

- Las normas y buenas prácticas de Seguridad de la información sobre Cloud Computing deben adaptarse continuamente a las necesidades y cambios de la Organización por lo que no pueden permanecer estáticas, por tanto se debe velar por su actualización y revisión periódica.

- Aquellas políticas, planes y procedimientos establecidos dentro del SGSI de **Servinformación** y que sean aplicables en el contexto de Cloud Computing, son de obligatorio cumplimiento.
- Las buenas prácticas y recomendaciones de Seguridad de la Información provenientes de Google Cloud Platform deben ser tenidas en cuenta dentro de la prestación de los servicios.
- Las diferentes categorías de servicio en la nube utilizadas por un cliente deben tener diferentes niveles de responsabilidades entre el cliente, el supplier y el proveedor. Por lo tanto, para cada tipo de servicio en la nube utilizado por un cliente, la división de responsabilidades debe definirse y documentarse para garantizar que los controles apropiados se identifiquen e implementen.
- Se deben segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos en la nube contratada por la organización.
- Cuando corresponda, y como parte de la documentación de los proyectos, se deben emitir manuales de usuario y buenas prácticas con respecto al servicio en la nube con el propósito de educar, capacitar y concientizar en seguridad de la información relativa a dicho servicio.

6.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL CONTROL DE ACCESO

Servinformación implementa medidas para restringir el acceso a la información y a las instalaciones de procesamiento correspondientes. Con este propósito, establece los lineamientos para regular el acceso a las redes, servicios, uso de Internet y correo institucional. La Organización ejerce un estricto control sobre el acceso a toda su información, garantizando la seguridad y el nivel de protección necesario.

Se deben definir los requisitos de seguridad específicos para cada aplicación, con el objetivo de salvaguardar la integridad de los datos. El otorgamiento de acceso a la información se lleva a cabo considerando el principio de "necesidad de saber" (need-to-know), garantizando que solo aquellos con una necesidad legítima tengan acceso. De igual manera, cualquier acceso otorgado queda registrado para fines de auditoría y seguimiento.

6.3.1. OBJETIVO DE LA POLÍTICA

Garantizar la protección de la información y las instalaciones de procesamiento de información mediante el establecimiento de políticas, normas y controles de acceso a las redes y servicios, el uso de internet y el correo institucional.

6.3.2. ALCANCE DE LA POLÍTICA

Aplica a todos los colaboradores de Servinformación y abarca el control de acceso lógico a las redes, servicios de red, internet y correo institucional.

6.3.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Supervisar la implementación de medidas para restringir el acceso a la información.
- Verificar la aplicación del principio de "necesidad de saber" en el otorgamiento de acceso.
- Supervisar la gestión de eventos y auditorías para el seguimiento de accesos.

Comité de Seguridad:

- Evaluar periódicamente la efectividad de las medidas de control de acceso.
- Revisar y aprobar los perfiles de acceso para cada cargo.
- Participar en la revisión anual de derechos de acceso de usuarios.
- Colaborar en la gestión de eventos que amenacen la integridad de la información.

Gestión IT:

- Establecer perfiles de acceso para cada cargo.
- Administrar el Directorio Activo y llevar a cabo revisiones periódicas.
- Asegurarse de que se registren y gestionen adecuadamente los usuarios.
- Validar la aplicación de la autenticación de múltiples factores (MFA).

Responsables de Procesos:

- Autorizar accesos a activos de información bajo su responsabilidad.
- Revisar anualmente los derechos de acceso de cada perfil.
- Colaborar en la gestión de eventos que afecten la integridad de la información.

Colaboradores:

- Respetar los perfiles de acceso establecidos y las políticas de seguridad.
- Acatar las recomendaciones en cuanto a la gestión de contraseñas, cambios periódicos y seguridad de sus cuentas.
- Informar de inmediato sobre pérdida u olvido de contraseñas, o cualquier otro evento que interfiera en el acceso a los servicios.

6.3.4. GENERALIDADES

Directrices relacionadas con el Acceso a Sistemas y Aplicaciones

- Los propietarios de los activos de información deben autorizar los accesos a sus activos o aplicativos, siguiendo los perfiles establecidos y las necesidades de uso.

- Los usuarios de los recursos tecnológicos y sistemas de información de Servinformación se comprometen a realizar un uso adecuado y responsable, preservando la información a la cual tienen acceso permitido. El control de acceso a sistemas y aplicaciones se guía con el Procedimiento "**P-SI-04 Gestión de Usuarios**".
- Las aplicaciones críticas de Servinformación deben obligatoriamente implementar la autenticación a través del protocolo HTTPS y contar con mecanismos de protección contra intentos de ingreso. Con el objetivo de prevenir accesos no autorizados, se prohíben cuentas de administración genéricas o usuarios por defecto (root, admin, administrador, etc.).
- El uso de programas utilitarios con capacidad de anular sistemas y controles de aplicaciones no está permitido, a menos que sea necesario para actividades específicas de la Coordinación de Informática, siendo este uso estrictamente controlado por Servinformación.
- El control de acceso a los sistemas de procesamiento y almacenamiento de información se realiza mediante cuentas de usuario únicas para cada usuario. Se establece la revisión anual de las políticas de seguridad del Directorio Activo.
- Las cuentas de usuario y claves de acceso son personales e intransferibles. Servinformación ha implementado sistemas para detectar y bloquear accesos no autorizados.
- El personal de Servinformación y/o terceros autorizados solo deben tener acceso a la información necesaria para el desarrollo de sus actividades, garantizando el acceso únicamente a usuarios autorizados, en horarios preestablecidos y conforme a perfiles de acceso por cargo.

Directrices relacionadas con la Gestión de Privilegios

- Se ha establecido un perfil de acceso para cada cargo en Servinformación, que especifica el tipo de información al que el usuario tiene derecho. Para otorgar acceso, se considerará la clasificación interna de la información en la Organización y el perfil de acceso asociado al cargo.
- El propietario del activo de información revisará anualmente, o cuando sea necesario, los derechos de acceso de cada perfil. Los derechos de acceso de los usuarios pueden ser revocados total o parcialmente en caso de una administración inadecuada de la información por parte del usuario.
- A través del registro de eventos en los diversos recursos informáticos de la plataforma tecnológica, se realiza un seguimiento a los accesos de los usuarios a la información de la Organización. Esto tiene como objetivo minimizar el riesgo de pérdida de integridad de la información.

- Cada sistema de información debe contar con un administrador del sistema asignado, cuya responsabilidad debe ser garantizar el buen uso del sistema y administrar el acceso de manera adecuada.

Directrices relacionadas con la Administración de Acceso de Usuarios

- Servinformación establece el procedimiento "**P-SI-04 Gestión de Usuarios**", en cual se disponen las actividades para el registro, modificación y cancelación de usuarios; el suministro de acceso a usuarios, la gestión de derechos de acceso privilegiado, la gestión de información de autenticación secreta, y la revisión, retiro o ajuste de los derechos de acceso.
- La Coordinación Informática debe controlar el acceso mediante el enfoque basado en roles, aplicando los siguientes principios:
    - Lo que necesita conocer: solamente se concede acceso a la información que la persona necesita para la realización de sus tareas.
    - Lo que necesita usar: solamente se concede acceso a los equipos de cómputo, aplicaciones, procedimientos y áreas que la persona necesita para la realización de su tarea/trabajo/rol.
- La Coordinación Informática debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.
- Los usuarios autorizados a acceder a los sistemas de información de Servinformación, son responsables de la seguridad de las contraseñas y cuentas de usuario.
- En todos los sistemas o servicios en donde aplique, la autenticación de múltiples factores (MFA) es de uso obligatorio.
- La contraseña escogida para el acceso a cada uno de los sistemas de información de Servinformación debe corresponder a los lineamientos descritos en el apartado de "**Directrices Relacionadas con la Gestión de Contraseñas**".
- Está prohibido facilitar o proporcionar acceso a las aplicaciones e información a usuarios o a terceros no autorizados.
- Para desbloquear el acceso de Workspace o del Directorio Activo, el usuario debe realizar la solicitud mediante el correo electrónico servicedesk@servinformacion.com.

Directrices relacionadas con el Acceso a Redes

- El acceso a redes wireless se controla con autenticación por contraseña utilizando el protocolo WPA2.

- Coordinación Informática provee un servicio de conectividad a todos los colaboradores de Servinformación para la navegación en internet, dicho acceso se controla para equipos corporativos mediante segmentación de la red lógica.
- Se dispondrá de una red de invitados para la conexión de los equipos personales, tanto laptop como dispositivos móviles; esta red permitirá la salida hacia Internet, pero no permitirá la conexión con equipos de cómputo o servidores de Servinformación.

Directrices Relacionadas con la Gestión de Contraseñas

Para garantizar la seguridad en el manejo de contraseñas, Servinformación establece rigurosas directrices que abordan diversos aspectos:

- Cada contraseña debe ser única para cada aplicación o sistema de información.
- Las contraseñas deben cumplir con los siguientes requisitos: contener mayúsculas, minúsculas, números, caracteres especiales y tener una longitud mínima de ocho (8) caracteres (recomendable entre diez (10) y quince (15) caracteres).
- Los usuarios no deben crear contraseñas idénticas o muy similares a las que han tenido anteriormente.
- Para la construcción de una contraseña segura, se recomienda aplicar lo indicado en el instructivo "**I-SI-02 Buenas Prácticas para la Gestión de Contraseñas**".
- Las aplicaciones controladas mediante el directorio activo requieren cambios de contraseñas cada 30 días, y en Workspace, cada 90 días.
- Toda contraseña entregada por el Administrador de un Sistema debe ser cambiada de inmediato por el usuario.
- Las contraseñas pre-establecidas por proveedores deben cambiarse inmediatamente después de que el sistema se despliegue en producción.
- Después de tres intentos consecutivos fallidos de ingreso, el acceso de la cuenta debe ser bloqueado por un tiempo predeterminado.
- Los usuarios son responsables de todas las actividades realizadas con su identificación de usuario y sus claves personales.
- Se prohíbe comunicar las contraseñas a personas no autorizadas, y los usuarios deben mantener la confidencialidad de las mismas.
- Las contraseñas no deben ser almacenadas en computadoras sin formato protegido, libretas, cuadernos ni otros medios físicos.
- Al ingresar la contraseña, se debe tener cuidado para evitar que terceros no autorizados observen la misma. En caso de sospecha, se debe cambiar la contraseña y notificar al administrador de la aplicación.
- Queda estrictamente prohibido comunicar contraseñas a los clientes por correo electrónico sin cifrar o proteger. Se prefiere la comunicación telefónica.

- En caso de pérdida u olvido de la contraseña, se establecerá una nueva, y ninguna debe ser guardada por colaboradores de Servinformación.

Directrices relacionadas con el Uso de Dispositivos Móviles

- Servinformación limita la conexión de dispositivos móviles personales tales como smartphones y tablets a la red de invitados, a excepción de los dispositivos que sean propiedad de Servinformación, con el fin de minimizar los riesgos de seguridad de la información que implica el uso de dispositivos móviles. Así mismo, debe velar porque los colaboradores hagan un uso responsable de los servicios y equipos proporcionados por la Organización.
- Para los dispositivos móviles corporativos su conexión se debe controlar por medio del registro previo de la dirección MAC en el programa controlador de las antenas (UniFi Control Access).
- El colaborador que por algún evento específico utilice dispositivos móviles de su propiedad para el desarrollo de sus funciones, además de contar con la autorización previa para su uso, se debe alinear con las políticas establecidas para este tipo de activo de información.

Directrices relacionadas con el uso de altos Privilegios y Utilitarios

- Servinformación debe velar porque los recursos de la plataforma tecnológica y los servicios de red sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre las plataforma y servicios.
- Solo se debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos colaboradores designados para dichas funciones.
- Se debe validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a los usuarios administradores.
- Se debe revisar periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoría de la plataforma tecnológica y los sistemas de información.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ACTIVOS DE INFORMACIÓN

Servinformación reconoce la importancia de los activos de información, por esta razón establece que se deben identificar, clasificar, etiquetar y manejar los activos asociados con

la información y las instalaciones de procesamiento de información, para lo cual se debe elaborar un inventario de activos de información, el cual debe ser actualizado al menos una vez al año por el propietario del activo de información con la asesoría del Líder de Seguridad de la Información.

6.4.1. OBJETIVO DE LA POLÍTICA

Garantizar la protección de los activos de información de Servinformación, preservando la confidencialidad, integridad y disponibilidad de la información generada, procesada, almacenada y transmitida en la plataforma tecnológica de la organización.

6.4.2. ALCANCE DE LA POLÍTICA

Esta política se aplica a todos los activos de información relacionados con las operaciones de Servinformación, incluyendo la información confidencial, instalaciones de procesamiento de información y recursos tecnológicos proporcionados por la organización.

6.4.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Asegurar que las directrices de gestión de activos de información, clasificación y etiquetado de información, gestión de medios removibles, y disposición final de medios se implementen adecuadamente.
- Participar en la elaboración y actualización del inventario de activos de información de los Procesos.

Comité de Seguridad de la Información:

- Recomendar niveles de clasificación de la información.
- Revisar y aprobar los procedimientos relacionados con la gestión de activos.

Gestión IT:

- Colaborar en la identificación y clasificación de activos de información.
- Suministrar las herramientas de protección que requieran los activos de información de la Organización.
- Supervisar y documentar el proceso de destrucción de información confidencial.

Responsables de Procesos:

- Identificar y mantener actualizado el inventario de activos de información de su proceso.
- Clasificar la información de acuerdo con los niveles establecidos.
- Revisar anualmente el inventario de activos de su proceso.

Colaboradores:

- Compartir la responsabilidad de proteger y usar adecuadamente los activos de información.

- Etiquetar la información acorde con las políticas establecidas.

6.4.4. GENERALIDADES

Directrices relacionadas con la Gestión de Activos de Información

- En calidad de propietario de la información generada, procesada, almacenada y transmitida a través de la infraestructura tecnológica, **Servinformación** asignará responsabilidades a los diferentes procesos respecto a sus activos de información. Este enfoque garantiza el cumplimiento de directrices diseñadas para preservar la confidencialidad, integridad y disponibilidad de la información.
- La totalidad de la información confidencial de Servinformación, así como los activos que la almacenan y procesan, deben ser asignados a un responsable, debidamente inventariados y posteriormente clasificados. Estos procesos se llevarán a cabo de acuerdo con los requerimientos y criterios establecidos por la Organización.
- La protección y uso adecuado de los activos de información asignados es una responsabilidad compartida por todos los colaboradores y partes interesadas, sin importar el medio o la procedencia de dichos activos. Asimismo, se espera que se controle el uso de estos activos por parte de externos cuando estén bajo responsabilidad de algún colaborador de la Compañía.
- El almacenamiento local de información solo está permitido para el proceso de Actualización Cartográfica, y exclusivamente durante la ejecución de cada orden de trabajo.
- La identificación y control de activos de información es esencial para prevenir pérdidas o usos inadecuados. Los Responsables de Procesos asumen la responsabilidad de identificar los activos de información y de mantener actualizado el inventario correspondiente.
- Con el objetivo de garantizar la efectividad de estas directrices, se establece la revisión anual del Inventario de activos por parte de los Responsables de Procesos.
- Para la gestión de los activos de información se establece el Procedimiento "**P-SI-01 Gestión de Activos**".

Directrices relacionadas con la Clasificación y Etiquetado de Información

- El Comité de Seguridad de la Información debe recomendar los niveles de clasificación de la información, los cuales se establecen en el Procedimiento "**P-SI-01 Gestión de Activos**".
- La información debe ser protegida dependiendo del nivel de confidencialidad, integridad y disponibilidad asignado.
- Cada Responsable de Proceso, es el encargado de clasificar la información de acuerdo con los niveles establecidos por Servinformación.

- El Comité de Seguridad debe proveer los métodos de cifrado de la información de nivel “Confidencial”, así como debe administrar el software o herramienta utilizado para tal fin.
- Se aplican técnicas de enmascaramiento a todos los datos sensibles y confidenciales que se encuentran en posesión o bajo el control de la organización, independientemente de la forma en que se almacenen o procesen, incluyendo bases de datos, sistemas de archivos, copias de seguridad y entornos de desarrollo y prueba.
- La Coordinación Informática debe efectuar la eliminación segura de la información, acorde con el procedimiento “**P-SI-01 Gestión de Activos**”.
- Dentro del cumplimiento de los requisitos de confidencialidad de información, todos los colaboradores deben asegurarse de cumplir la “Directrices Relacionadas con el Equipo Desatendido, Escritorio Limpio y Pantalla Limpia” de este documento.

Directrices relacionadas con la Gestión de Medios Removibles

Servinformación prohíbe el uso no autorizado de medios removibles para los colaboradores, con el fin de evitar pérdida, fuga o robo de información, así mismo dispone de normas para la disposición de medios y la transferencia medios físicos, para lo cual establece:

- Servinformación promoverá el uso de carpetas compartidas en Drive en lugar de medios removibles para el intercambio de información al interior de la Organización.
- Las unidades o puertos de medios removibles de las estaciones de trabajo, equipos portátiles y servidores se bloquearán mediante directorio activo o antivirus.
- Cuando sea necesario, los dispositivos portátiles proporcionados deben contar con cifrado de discos.
- La verificación de posibles excepciones se debe realizar según lo establecido en el procedimiento “**P-SI-05 Gestión de Medios Removibles**”

Directrices relacionadas con la Disposición Final de los Medios

- Quien autoriza el retiro de activos por obsolescencia, daño o cualquier otro motivo es Gestión IT.
- Los medios físicos que contienen información confidencial se deben disponer en forma segura, mediante incineración, destrucción o el borrado de datos.
- La información almacenada en medios removibles debe ser transferida a la nube antes de la debida destrucción, de acuerdo con el tiempo de vida útil de los mismos.
- La actividad de Destrucción de Información debe ser documentada acorde con el procedimiento, y en el registro “**P-SI-01-R02 Acta Destrucción de Información**”.

- Se deben guardar varias copias, en medios separados, de los datos sensibles, con el fin de evitar la pérdida de información por daño o robo de los medios removibles.

6.5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LAS OPERACIONES

Servinformación establece los principios, directrices y procedimientos para garantizar la protección adecuada de la información durante todas las fases de sus operaciones. Esta política es esencial para gestionar y mitigar los riesgos asociados con la seguridad de la información en el entorno operativo de la empresa.

6.5.1. OBJETIVO DE LA POLÍTICA

Garantizar la protección de la información y recursos utilizados durante todas las fases de las operaciones de la Organización.

6.5.2. ALCANCE DE LA POLÍTICA

Aplica a todas las instalaciones, equipos, y recursos de Servinformación, así como a todo el personal interno y externo que intervenga en la operación de la Organización.

6.5.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:
- Coordinar la implementación de controles de seguridad en las operaciones.
- Coordinar la revisión y corrección de vulnerabilidades técnicas.

Comité de Seguridad:
- Revisar informes de incidentes de seguridad y su manejo.
- Revisar informes de incidentes de códigos maliciosos y definir acciones correctivas.

Gestión IT:
- Identificar y evaluar parches de seguridad para dispositivos tecnológicos.
- Mantener un registro actualizado de los parches aplicados.
- Revisar información sobre nuevas vulnerabilidades y coordinar su corrección.

Responsables de Procesos:
- Participar en la revisión y corrección de vulnerabilidades técnicas que afecten el proceso o producto a cargo.

Colaboradores:
- No propiciar el intercambio de archivos infectados o sospechosos.
- No instalar o emplear programas no autorizados para el manejo de antivirus.

6.5.4. GENERALIDADES

Directrices Relacionadas con Códigos Maliciosos

- **Servinformación** proporciona los mecanismos necesarios que garanticen la protección de la información y los recursos utilizados para su procesamiento y almacenamiento, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por software malicioso.
- Está prohibido escribir, generar, recopilar, difundir, copiar, ejecutar o intentar introducir cualquier código diseñado para autoreplicarse, dañar o entorpecer el acceso a cualquier equipo de Servinformación, red o información.
- Se deben proteger las estaciones de trabajo, equipos portátiles y servidores de Servinformación contra códigos maliciosos.
- El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos deben tener el antivirus instalado y activo.
- El único servicio de antivirus autorizado en Servinformación es el proporcionado directamente por el Comité de Seguridad, el cual cumple con todos los requisitos técnicos y de seguridad.
- El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados con códigos maliciosos o sean sospechosos de estarlo.
- El usuario no debe instalar o emplear programas no autorizados para manejo de antivirus.
- Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa de antivirus y que han sido instalados por la Coordinación de Informática.
- El programa de antivirus debe ser instalado única y exclusivamente por la Coordinación de Informática en los servidores y estaciones de trabajo.

Directrices Relacionadas con las Copias de Respaldo

- Servinformación establece el procedimiento “**P-SI-10 Procedimiento Copias de Respaldo**”.
- Se deben realizar copias de respaldo de la información y pruebas periódicas a las mismas. Servinformación se acoge a los controles implementados por Google Cloud Platform.
- Las copias de respaldo se guardarán únicamente con el objetivo de restaurarse en situaciones como: Borrado y corrupción de datos, incidente de seguridad de la información, falla en el almacenamiento, borrado de información accidental.
- Las copias de respaldo deben realizarse con una frecuencia suficiente para garantizar que la información más reciente esté disponible en caso de una interrupción o pérdida de datos.
- La frecuencia de las copias de respaldo debe determinarse en función del riesgo y la criticidad de los datos.

- Las copias de respaldo deben retenerse durante un período de tiempo suficiente para garantizar que la información pueda recuperarse en caso de una interrupción o pérdida de datos.
- El período de retención debe determinarse en función del riesgo y la criticidad de los datos.
- Las copias de respaldo deben almacenarse en un lugar seguro y protegido contra el acceso no autorizado, el daño físico y el riesgo de desastres naturales, priorizando el uso de los recursos suministrados por Google Cloud Platform. El almacenamiento debe garantizar que las copias de respaldo no estén expuestas a peligros que puedan afectar su integridad o disponibilidad.

Directrices Relacionadas con el Control de Software Operacional

- El proceso de instalación y desinstalación de software está autorizado exclusivamente al personal de Informática. Por lo tanto, a cualquier otro colaborador o contratista no le es permitido realizar esta labor.
- No se pueden instalar en los equipos de Servinformación hardware, ni software sin previa autorización del responsable del proceso de Gestión de TI y ticket de solicitud, con el propósito de garantizar trazabilidad de los cambios.
- El software propietario debe contar con su respectiva licencia y en el caso del software libre debe estar permitido el uso comercial.
- El instalador debe ser descargado de la página oficial del fabricante.
- Debe verificarse la integridad del archivo por medio de la comprobación de códigos hash.
- Se debe proporcionar capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de los nuevos sistemas de información o mejoras a sistemas de información existentes.
- Todos los sistemas nuevos y mejorados deben estar completamente soportados por documentación actualizada.

Directrices Relacionadas con las Actualizaciones de Parches de Seguridad

- Servinformación establece las directrices y procedimientos para garantizar la actualización oportuna y efectiva de parches de seguridad en todos los dispositivos tecnológicos utilizados en la infraestructura, con el fin de mitigar riesgos de seguridad y proteger la integridad, confidencialidad y disponibilidad de los datos y sistemas.
- La Coordinación Informática es responsable de identificar y evaluar los parches de seguridad disponibles para los dispositivos tecnológicos en uso.
- La Coordinación Informática realizará pruebas de parches antes de la implementación para garantizar su compatibilidad y funcionalidad adecuada.

- Las actualizaciones de parches deben ser programadas de manera regular, para garantizar que se implementen en un plazo adecuado.
- Se debe mantener un registro actualizado de los parches aplicados, incluyendo fechas, dispositivos afectados, descripción de los parches y personas responsables de su implementación.

Directrices Relacionadas con la Gestión de la Vulnerabilidad Técnica

- **Servinformación**, a través del Comité de Seguridad y Gestión IT, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas, acorde con el procedimiento de Gestión de Vulnerabilidades Técnicas.
- Servinformación establece el procedimiento "**P-SI-09 Gestión de Vulnerabilidades Técnicas**".
- Gestión IT, es responsable de verificar de manera permanente la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la organización.
- Se debe programar y ejecutar por lo menos una vez al año el plan de análisis de vulnerabilidades y/o hacking ético para las plataformas críticas de la Organización.
- Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad del dueño del Activo de Información, siguiendo las directrices del Procedimiento de Gestión de Cambios.

6.6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LAS COMUNICACIONES

Servinformación define e implementa los mecanismos de control que considere apropiados para proteger la confidencialidad, integridad y disponibilidad de las redes, los servicios en red y la información por allí transmitida.

6.6.1. OBJETIVO DE LA POLÍTICA

Asegurar la confidencialidad, integridad y disponibilidad de las redes, servicios en red y la información transmitida por Servinformación.

6.6.2. ALCANCE DE LA POLÍTICA

Se aplica a todas las actividades de comunicación, redes y servicios en red de Servinformación.

6.6.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Supervisar la implementación de controles para asegurar la disponibilidad y seguridad de Internet y el correo electrónico.

Comité de Seguridad:

- Revisar y aprobar los mecanismos de control propuestos por el Líder de Seguridad de la Información.
- Evaluar la eficacia de los acuerdos de confidencialidad.
- Supervisar la implementación de controles relacionados con Internet y el correo electrónico.

Gestión IT:

- Liderar la definición e implementación de mecanismos de segmentación de redes.
- Supervisar la continuidad y restablecimiento del servicio de Internet en casos de contingencia.
- Liderar la implementación de firewalls y mecanismos de seguridad perimetral.
- Asegurarse de que la arquitectura de red esté documentada y actualizada.
- Establecer procedimientos y controles para evitar amenazas provenientes de Internet.

Responsables de Procesos:

- Autorizar los requerimientos de solicitud/envío de información a terceras partes.
- Asegurar que el intercambio de información se realice cumpliendo con las políticas de administración de redes y protección de datos.

Colaboradores:

- Firmar acuerdos de confidencialidad y cumplir con las condiciones contractuales para el intercambio de información.
- Utilizar recursos de Internet de manera responsable y cumplir con las restricciones establecidas.
- Informar cualquier correo electrónico sospechoso y seguir las indicaciones de Coordinación Informática.
- Utilizar el correo institucional de manera responsable y segura.

6.6.4. GENERALIDADES

Directrices Relacionadas con la Gestión de la Seguridad en las Redes

- La Coordinación de Informática define e implementa los mecanismos de segmentación de las redes de Servinformación con base en los niveles de confianza, por dependencias o alguna combinación de las anteriores.
- La Coordinación de Informática debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación.
- Toda conexión a la red de Servinformación, debe tener mecanismos de autenticación para verificar la validez del usuario que se conecta.
- Las redes de Servinformación deben ser monitoreadas para prevenir accesos no autorizados o detectar cualquier violación a las políticas de seguridad de la información.
- Todas las conexiones desde las redes de Servinformación, con las redes externas deben estar protegidas por un firewall y se deben establecer reglas apropiadas para filtrar el tráfico permitido entre las mismas. Igualmente deben tener mecanismos de seguridad perimetral.
- La arquitectura de red de Servinformación y sus componentes deben mantenerse documentados y actualizados.
- La información sobre las direcciones lógicas internas, configuraciones e información de los sistemas de comunicación y cómputo de Servinformación, son de carácter confidencial al igual que la arquitectura y topología de red.

Directrices Relacionadas con la Transferencia de Información

- Servinformación asegura la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establece los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecen Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice el intercambio.
- Servinformación firmará acuerdos de confidencialidad con los colaboradores e incluirá una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información interna y confidencial. En este acuerdo quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se firmarán antes de permitir el acceso o uso de dicha información.
- Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se especificará el grado de sensibilidad de la información de Servinformación y las consideraciones de seguridad sobre la misma, así como los controles a implementar.

- Los colaboradores y contratistas deben seguir las indicaciones del Procedimiento "**P-SI-01 Gestión de Activos**" sobre Clasificación, Etiquetado y Manejo de la Información, para la transferencia de información de acuerdo con su clasificación.
- Los propietarios de los activos de información deben autorizar los requerimientos de solicitud/envío de información de Servinformación, por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.
- Los propietarios de los activos de información deben asegurarse que el intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de seguridad y de protección de datos personales de Servinformación.
- Los terceros con quienes se intercambia información de Servinformación deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad de la Organización, y de las condiciones contractuales establecidas.
- Los terceros con quienes se intercambia información de la Organización, deben destruir de manera segura la información suministrada, una vez ésta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.
- Restricciones específicas de divulgación de Información:
    - **Divulgación información del cliente**: está totalmente prohibido la divulgación de la información de los clientes a terceros, a menos que sea autorizada por la alta Dirección de la organización o requerida por autoridades judiciales.
    - **Divulgación de sistemas específicos de información**: los colaboradores no pueden divulgar a personas externas a Servinformación información sobre los sistemas usados o la forma como estos son implementados.
    - **Divulgación de información sobre vulnerabilidades del sistema**: la información específica sobre las vulnerabilidades del sistema, como los detalles de una reciente brecha, no deben ser divulgados a personas no autorizadas.

Directrices Relacionadas con el Uso de Internet

- Servinformación, consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporciona los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en Servinformación.
- El Comité de Seguridad debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

- La Coordinación de Informática debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- La Coordinación de Informática debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.
- Está prohibido conectar módems o celulares para acceder a Internet, dentro de la red LAN de Servinformación.
- Queda prohibido a todos los colaboradores y terceros acceder a cualquier página o dirección que contenga material pornográfico en cualquiera de sus variantes, o bien páginas que promuevan cualquier tipo de ideas que puedan ser consideradas ofensivas para las normas de Servinformación como violencia, terrorismo, grupos al margen de la ley, discriminación, entre otras.
- Se prohíbe el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal o institucional.
- Todo usuario es responsable del contenido de la comunicación e información que se envíe o descargue desde su cuenta de acceso.
- Todas las actividades realizadas en los sistemas de información de Servinformación, pueden ser monitoreadas con el fin de preservar la seguridad de la información de la Organización.

Directrices Relacionadas con el uso del Correo Institucional

- **Servinformación**, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre colaboradores y terceras partes, proporciona un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.
- **Servinformación** proveerá a todos los colaboradores un correo electrónico empresarial en el dominio servinformacion.com.
- La cuenta de correo electrónico institucional es personal e intransferible, los Colaboradores son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y el buzón asociado a la Organización.
- El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de Servinformación; esto es para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo.
- El correo electrónico institucional es una herramienta para el intercambio de información necesaria, que permite el cumplimiento de las funciones propias de cada cargo, no es una herramienta de difusión masiva de información y no debe ser

utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, software pirata, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso.

- No se pueden usar cuentas de correo electrónico diferentes a la asignada por la organización, para enviar o recibir mensajes de la organización.
- El envío de información masiva a los grupos generados para divulgación es limitado y es de uso exclusivo de los Procesos de Mercadeo, Gestión Humana, Gestión de Calidad y Gestión IT.
- El servidor de correo bloqueará archivos adjuntos o información nociva como archivos .ade, .adp, .apk, .appx, .appxbundle, .bat, .cab, .chm, .cmd, .com, .cpl, .diagcab, .diagcfg, .diagpack, .dll, .dmg, .ex, .ex_, .exe, .hta, .img, .ins, .iso, .isp, .jar, .jnlp, .js, .jse, .lib, .lnk, .mde, .msc, .msi, .msix, .msixbundle, .msp, .mst, .nsh, .pif, .ps1, .scr, .sct, .shb, .sys, .vb, .vbe, .vbs, .vhd, .vxd, .wsc, .wsf, .wsh y .xll o de ejecución de comandos que se vean perjudiciales.
- Bajo ningún motivo se debe abrir o ejecutar un correo de origen desconocido, debido a que podría tener código malicioso (virus, troyanos, keyloggers, gusanos, etc.), lo cual podría atentar contra los sistemas, programas y datos de la Organización.
- El usuario debe reportar cualquier recibo de correo sospechoso, mediante el módulo MGMT Incidentes de TI de Odoo, el correo sospechoso no debe ser abierto ni reenviado a ningún usuario. El usuario debe proceder según las indicaciones de Coordinación Informática.
- La cuenta de correo electrónico solo se puede utilizar para enviar y recibir información de la organización. La organización se reserva el derecho de acceder a la información que contengan las cuentas de correo asignadas al personal; si la misma puede representar una brecha de seguridad, un incidente de seguridad o una violación a las políticas de seguridad.
- Si se necesita enviar por correo electrónico contraseñas y claves de acceso las mismas deben estar cifradas o deben ser notificadas por un medio diferente.
- Información confidencial enviada por correo electrónico siempre se debe enviar en archivo cifrado, la contraseña para descifrar el archivo tiene que entregárselo al receptor vía telefónica o usando la herramienta de correo cifrado.

6.7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LOS CONTROLES CRIPTOGRÁFICOS

Servinformación establece un conjunto de directrices y procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información sensible a través de la implementación y gestión adecuada de técnicas criptográficas.

6.7.1. OBJETIVO DE LA POLÍTICA

Garantizar la confidencialidad, integridad y disponibilidad de la información, con un enfoque especial en la protección de datos personales y la privacidad. Para lograrlo, se establecen controles criptográficos eficaces que protejan la información confidencial y minimicen los riesgos asociados con su tratamiento.

6.7.2. ALCANCE DE LA POLÍTICA

Esta política se aplica a todos los empleados, contratistas, proveedores y cualquier entidad que maneje información dentro de la organización. Incluye, pero no se limita a, sistemas informáticos, dispositivos móviles, redes y cualquier otro medio que procese, almacene o transmita información. La política se extiende a todos los datos personales recopilados y procesados por la organización.

6.7.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Establecer procedimientos de gestión de claves que aseguren confidencialidad y disponibilidad.
- Garantizar que los controles criptográficos se actualicen de manera proactiva y continua.

Comité de Seguridad:

- Validar la implementación de algoritmos criptográficos y la gestión de certificados y claves.
- Determinar algoritmos criptográficos y protocolos autorizados.
- Supervisar la actualización y validez de las llaves criptográficas.

Gestión IT:

- Garantizar que los sistemas de información que requieran transmisión de información cuenten con mecanismos de cifrado.
- Proveer métodos de cifrado necesarios para garantizar la confidencialidad e integridad de la información.
- Desarrollar y establecer la gestión y administración de llaves de cifrado.
- Configurar los sistemas para admitir únicamente algoritmos criptográficos y protocolos autorizados.

Responsables de Procesos:

- Aplicar el cifrado de la información confidencial que manejan en sus actividades.
- Identificar sistemas de información que requieran cifrado para transmisión de información reservada.

Colaboradores:

- Aplicar el cifrado de la información confidencial que manejan en sus actividades.

- Administrar tokens y firmas digitales asignados para el desempeño de sus labores.

6.7.4. GENERALIDADES

- Los controles criptográficos deben seleccionarse de acuerdo con los riesgos de seguridad asociados a la información que se va a proteger.
- Los controles criptográficos deben mantenerse actualizados para garantizar que sigan siendo eficaces.
- Los controles criptográficos deben gestionarse de manera proactiva y continua para garantizar su seguridad.
- El Comité de Seguridad de Servinformación debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información confidencial cuente con mecanismos de cifrado de datos.
- El Comité de Seguridad de Servinformación debe desarrollar y establecer el manejo y la administración de llaves de cifrado.
- El Comité de Seguridad de Servinformación debe determinar los algoritmos criptográficos y protocolos autorizados para su uso en Servinformación y configurar los sistemas para admitir únicamente aquellos permitidos.
- El Comité de Seguridad de Servinformación debe descartar algoritmos de cifradas débiles tales como: DES, RC3, RC4 y protocolos débiles como; SSLv2 y SSLv3. Se debería considerar en su lugar el uso de algoritmos como: AES (cifrado simétrico), RSA (cifrado asimétrico) y los protocolos SSL/TLS 1.2 o 1.3 y tamaños de cifrado de 168 o 256 bits (cifrado simétrico) y 2048 bits (cifrado asimétrico) preferiblemente o en su defecto 128 bits (cifrado simétrico).
- Las llaves criptográficas deben ser actualizadas de acuerdo a su validez o cada vez que se sospeche que han perdido su confidencialidad.
- La administración de llaves criptográficas y certificados digitales estará a cargo del Gestión IT. Sin embargo, la administración de tokens y firmas digitales estarán a cargo de cada uno de los colaboradores a quienes les fueron asignados para el desempeño de sus labores.
- Los documentos que contengan contraseñas de usuario o claves para el control de acceso a los sistemas de información no pueden ser almacenados en texto plano y deben hacer uso de mecanismos de protección con contraseña.
- Todos los documentos que se han cifrado y descifrado, en caso de que se requiera, deben ser almacenados y tratados con las medidas de seguridad requeridas conforme al grado de clasificación de la información.
- Se deben proteger con contraseña todos los documentos al momento de ser compartidos, cuando contengan información confidencial.La entrega de la clave del documento debe realizarse a través de un medio diferente al que se envió el archivo.

6.8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA ADMINISTRACIÓN DE LOGS

Servinformación establece un conjunto de directrices para garantizar la seguridad de la información contenida en los registros de actividad o logs. Estos registros son esenciales para el monitoreo, la detección de amenazas y la auditoría de eventos en sistemas informáticos y redes.

6.8.1. OBJETIVO DE LA POLÍTICA

Proporcionar a Servinformación de pistas de auditoría y logs de los diferentes recursos de información permitiendo que la Organización pueda realizar investigaciones especiales, cumplir con regulaciones y verificar eventos de seguridad entre otros. La política regulará las actividades que permitan contar con estos rastros de auditoría y controlar su almacenamiento.

6.8.2. ALCANCE DE LA POLÍTICA

Esta política se aplica a todas las personas que realicen tareas de administración sobre los recursos informáticos de Servinformación, y a todos los recursos informáticos que brinden soporte al negocio de Servinformación.

6.8.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Revisar los logs relacionados con eventos o incidentes de seguridad de la información.
- Supervisar la correcta clasificación de los logs según su tipología.

Comité de Seguridad:

- Revisar informes periódicos sobre el cumplimiento de la política.
- Revisar los logs relacionados con eventos o incidentes de seguridad de la información.

Gestión IT:

- Garantizar que todos los recursos informáticos bajo su responsabilidad cuenten con pistas de auditoría y logs.
- Asegurar que los eventos de seguridad especificados dejen registros.
- Implementar y mantener la sincronización de relojes en los sistemas.

Responsables de Procesos:

- Asegurar que los eventos relevantes para el proceso sean debidamente registrados.
- Definir el período de retención de logs para los eventos específicos de su proceso.

- Colaborar en la auditoría regular de eventos anómalos o sospechosos.

Colaboradores:

- Cooperar con las revisiones y auditorías de logs según sea necesario.

6.8.4. GENERALIDADES

- La clasificación de los logs debe realizarse en el momento de su generación y en función de su uso o aplicabilidad, lo cual permite su interpretación para determinar qué datos deben o no contener. La tipología para clasificar son las siguientes:
    - **Trace**: Se utiliza para conocer el curso de una aplicación o proceso. Ejemplo: Partes específicas de los logs
    - **Info**: Se utiliza cuando se notifica alguna novedad o acción dentro de una aplicación o proceso. Ejemplo: Alta de un usuario.
    - **Warn**: Se utiliza cuando es necesario notificar algún comportamiento fuera de lo normal, pero sin afectar su funcionalidad de una aplicación o proceso.
    - **Error**: Se utiliza cuando ocurren fallas de funcionalidad, pero no genera indisponibilidad. Ejemplo: Al dar clic sobre un producto para agregarlo al carrito de compras y este no se agrega debido a un error.
    - **Fatal**: Se utiliza cuando ocurre un error que compromete el funcionamiento de la aplicación o el proceso. Ejemplo: Falla en la conexión a la base de datos.
    - **Debug**: Se utiliza cuando se requiere ver con mayor granularidad o a detalle un evento o conjunto de eventos.
- Todos los recursos informáticos (sistemas de información, aplicativos, sistemas operacionales, bases de datos, dispositivos de comunicación, dispositivos de seguridad y servidores, etc) deben contar con pistas de auditoría y logs que registren las actividades de los usuarios, las excepciones, las fallas y eventos de seguridad.
- Los siguientes eventos de seguridad deben dejar registro o pistas de auditoría para que puedan ser monitoreados:
    - Intentos de acceso a los sistemas incluyendo los exitosos y los fallidos.
    - Mecanismos de identificación y autenticación utilizados.
    - Uso y acciones realizadas con privilegios administrativos.
    - Aumento de privilegios.
    - Incorporaciones y eliminaciones de cualquier cuenta con privilegios administrativos.
    - Acceso y acciones sobre información con categoría confidencial.
    - Inicialización, acceso y acciones sobre los registros y bitácoras de auditoría.
    - Creación, modificación y eliminación de objetos a nivel sistema.
    - Acceso a información sensible.
    - Acceso a las bitácoras de auditoría o logs.

  - Inicialización de las bitácoras de auditoría o logs.
  - Cambio en los parámetros de adquisición, distribución y almacenamiento de tiempo (según configuración de relojes).
- La mínima información que debe contener un evento, siempre y cuando sea técnicamente posible es:
  - Identificación del usuario.
  - Tipo de evento.
  - Fecha y hora.
  - Indicación del éxito o fallo (de corresponder).
  - Origen y destino del evento (recurso informático).
  - Mensaje (donde se detalla la acción realizada).
  - Número de cuenta origen y destino (para las operaciones y servicios bancarios).
  - Los datos de identificación del dispositivo de acceso utilizado por el usuario (para las operaciones y servicios bancarios).
- Lo eventos no deben contener información o datos sensibles o confidenciales, entre estos:
  - Password.
  - Keys.
  - Tokens.
  - Datos financieros.
  - Datos personales.
- Adicionalmente, siempre que sea posible, se deben auditar los siguientes eventos generales:
  - Actividad de la administración de usuarios.
  - Cambios en la configuración de la seguridad, permisos y auditoría.
  - Actividad sobre la infraestructura tecnológica.
  - Protección perimetral.
  - Intentos de acceso fallidos.
  - Creación de cuentas por personal no habilitado.
- Todos los sistemas de la organización que lo permitan técnica y funcionalmente deben configurarse para utilizar la tecnología de sincronización de acuerdo con la zona regional definida (Sincronización de relojes), con el fin de generar sus pistas de auditoría sincronizadas a un mismo tiempo.
- Se debe elaborar un procedimiento en el cual sean definidos los lineamientos para la revisión de los logs, análisis, documentación e implementación de medidas de mitigación en caso de corresponder.
- Los registros que se originen por comportamiento anómalo o sospechoso (reversas, anulaciones, etcétera) y otros eventos de seguridad de la información pertinentes, deben ser auditados regularmente y guardados por el período definido por el dueño

del proceso o sistema, para ayudar en futuras investigaciones y monitoreo del control de acceso.

- Las redes, los sistemas y las aplicaciones computacionales de Servinformación deben ser monitoreados en forma regular, vía consulta de logs, para asegurar su conformidad con las políticas de acceso.
- Los archivos de Logs deben ser almacenados en medios que estén protegidos de toda intervención, externa o interna, que pueda modificarlos o alterarlos, incluyendo la intervención de usuarios con derechos de accesos privilegiados o especiales.
- Los archivos de Logs deben ser guardados por períodos suficientes para cumplir con los criterios de auditabilidad definidos por la organización.
- El Responsable de Cloud Engineering puede acceder a los registros de eventos de seguridad y en el caso de que fuera necesario, es el responsable de autorizar al personal el acceso a este registro, teniendo en cuenta:
    - Limitar la visualización de pistas de auditoría a quienes lo necesiten por motivos laborales.
    - Proteger los archivos de las pistas de auditoría contra modificaciones no autorizadas.
- Todo recurso informático debe contar con un plan de respaldo de las pistas de auditoría y logs por medio de la herramienta con que se cuente, teniendo en cuenta todos los componentes de la plataforma tecnológica de producción.
- Se deben conservar los logs y registros de auditorías de los componentes de la plataforma tecnológica, durante el tiempo definido en los marcos o normativas de seguridad de la información, requisitos legales y contractuales vigentes y aplicables.
- Se debe elaborar un procedimiento en el cual sean definidos los lineamientos para el respaldo y la restauración de los logs y/o pistas de auditoría.

6.9. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO

Servinformación implementa un proceso integral de monitoreo y análisis de incidentes de seguridad de la información para identificar causas, tomar acciones correctivas y preventivas, con el objetivo de reducir la incidencia y garantizar la disponibilidad, confidencialidad e integridad de la información. Además, establece un plan de continuidad del negocio para asegurar la disponibilidad de servicios críticos durante interrupciones o desastres, minimizando el impacto en la operación y manteniendo la satisfacción del cliente.

6.9.1. OBJETIVO DE LA POLÍTICA

Garantizar una respuesta eficaz y ordenada frente a los incidentes y eventos de seguridad de la información en Servinformación, y de aquellas situaciones que puedan comprometer la continuidad del negocio.

6.9.2. ALCANCE DE LA POLÍTICA

Aplica a todos los colaboradores de Servinformación y al personal proporcionado por terceras partes, así como a los sistemas de información críticos y la plataforma tecnológica que los respalda.

6.9.3. RESPONSABILIDADES ESPECÍFICAS

Lider de Seguridad de la Información:

- Coordinar y supervisar la gestión de incidentes de seguridad de la información.
- Ser el punto de contacto principal para la notificación inmediata de violaciones a las normas y políticas.
- Ser informado de todas las violaciones y eventos relacionados con la información y los recursos tecnológicos.
- Actualizar el análisis de riesgos, impacto al negocio y estrategias de continuidad anualmente o cuando sea necesario debido a cambios significativos.
- Coordinar la identificación de procesos críticos y su integración con los requisitos de continuidad de la seguridad de la información.
- Supervisar la implementación de actividades para garantizar la continuidad del negocio y minimizar impactos.

Comité de Seguridad de la Información:

- Reconocer situaciones de emergencia o desastre.
- Liderar temas relacionados con la continuidad del negocio y recuperación ante desastres.
- Validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- Analizar y establecer requerimientos de redundancia para sistemas críticos y la plataforma tecnológica.
- Participar en la elaboración del plan de recuperación ante desastres y procedimientos de contingencia.

Gestión IT:

- Participar en la gestión de los incidentes de seguridad de la información cuando le corresponda.
- Realizar pruebas periódicas para asegurar el cumplimiento de los requerimientos de disponibilidad.

- Asegurar que todos los sistemas de información que respaldan operaciones críticas tengan planes de reanudación y recuperación.
- Supervisar la implementación de estrategias del plan de continuidad del negocio, tiempos estimados de recuperación y procedimientos alternos.

Líderes de proceso:

- Participar en la gestión de los incidentes de seguridad de la información cuando le corresponda.
- Participar en la identificación e implementación de actividades para garantizar la continuidad del negocio.
- Colaborar en la elaboración y prueba de planes de reanudación y recuperación.

Colaboradores:

- Reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos de manera inmediata.
- Participar en entrenamientos y capacitaciones sobre las actividades del plan de continuidad del negocio.
- Seguir los procedimientos alternos o de contingencia durante la activación del plan de continuidad.

6.9.4. GENERALIDADES

Directrices Relacionadas con la Gestión de Incidentes

- Servinformación gestiona los incidentes de seguridad de la información aplicando la "**M-SI-05 Metodología de Gestión de Incidentes de Seguridad de la Información**" y aplicando el Procedimiento "**P-SI-02 Gestión de incidentes de Seguridad de la Información**".
- Servinformación debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- Gestión IT debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad de la Información o líderes de productos o procesos, según sea necesario.
- Es responsabilidad de los colaboradores de Servinformación y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.
- Toda violación a las normas y politicas descritas en este documento, se deben notificar inmediatamente al módulo MGMT Incidentes de TI de Odoo o directtamente al Lider de Seguridad de la Información.

Directrices Relacionadas con la Continuidad del Negocio

- Servinformación planifica e implementa el PCN teniendo en cuenta no sólo los recursos tecnológicos, sino también los demás activos de información y los procesos críticos de la Organización, además de la continuidad de la seguridad de la información. Servinformación se compromete a realizar pruebas periódicas a la continuidad del negocio y a la continuidad de la seguridad de la información implementada, con el fin de asegurar que son válidas y eficaces durante situaciones adversas. Esta estrategia se encuentra detallada en los documentos **"PL-SI-01 Plan de Continuidad de Negocio"**, "**PL-SI-02 Plan de Recuperación de Desastres**" y "**P-SI-07 Gestión de Riesgos Catastróficos y Estrategias de Recuperación**"..
- El Comité de Seguridad de la Información debe reconocer las situaciones que pueden ser identificadas como emergencia o desastre para Servinformación o los procesos.
- El Comité de Seguridad de la Información debe liderar los temas relacionados con continuidad del negocio y recuperación ante desastres.
- El Comité de Seguridad de la Información debe realizar análisis de impacto al negocio y análisis de riesgos de continuidad para, proponer estrategias de recuperación en caso de activarse el plan de contingencia, con las consideraciones de seguridad de la información a que haya lugar.
- El Comité de Seguridad de la Información debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- Gestión IT, en conjunto con el Comité de Seguridad de la Información, deben elaborar un plan de recuperación ante desastres para el Centro de Redes y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.
- El Comité de Seguridad de la Información y Gestión IT deben analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para Servinformación y la plataforma tecnológica que los apoya.
- Gestión IT debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de Servinformación.
- Gestión IT debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de Servinformación

6.10. POLÍTICA DE CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

Servinformación se compromete a garantizar la identificación, documentación y cumplimiento de la legislación asociada a la seguridad de la información, incluyendo aquella relacionada con los derechos de autor y la propiedad intelectual. Con este propósito, se procurará que el software instalado en los recursos de la plataforma tecnológica cumpla con los requisitos legales y de licenciamiento aplicables.

6.10.1. OBJETIVO DE LA POLÍTICA

Garantizar el cumplimiento de los requisitos legales y contractuales relacionados con la seguridad de la información, con un enfoque especial en derechos de autor, propiedad intelectual y licenciamiento de software.

6.10.2. ALCANCE DE LA POLÍTICA

Esta política se aplica a todos los aspectos de Servinformación que involucren seguridad de la información, abarcando la identificación, documentación y cumplimiento de la legislación vigente, así como la protección de derechos de autor y licenciamiento de software.

6.10.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Coordinar con la Oficina Asesora Jurídica y el Comité de Seguridad para garantizar la identificación, documentación y actualización de los requisitos legales, reglamentarios o contractuales aplicables.
- Colaborar con Gestión IT para asegurarse de que todo el software en la plataforma cumpla con los requisitos legales y de licenciamiento.

Comité de Seguridad:

- Colaborar con Gestión IT en la revisión periódica de los sistemas de información.

Gestión IT:

- Asegurarse de que todo el software en Servinformación esté protegido por derechos de autor y cuente con la licencia correspondiente.
- Coordinar la revisión periódica de los sistemas de información para garantizar el cumplimiento de las políticas y procedimientos de seguridad.

Responsables de Procesos:

- Colaborar con Gestión IT en la revisión periódica de los sistemas de información.

Colaboradores:

- Cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software.
- Abstenerse de duplicar software o su documentación sin autorización.
- No descargar materiales sujetos a propiedad intelectual en los equipos de la organización.

6.10.4. GENERALIDADES

- La Oficina Asesora Jurídica y el Comité de Seguridad tienen la responsabilidad de identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a Servinformación en relación con la seguridad de la información. Además, Servinformación se compromete a proteger todos los registros que evidencien el cumplimiento de los requisitos normativos.
- Gestión IT y el Comité de Seguridad deben asegurarse de que todo el software en Servinformación esté protegido por derechos de autor y cuente con la licencia correspondiente.
- Los usuarios, por su parte, deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software, evitando la duplicación no autorizada. La Organización debe incluir cláusulas de propiedad intelectual y derechos de autor en contratos con terceros.
- Servinformación se regirá por la Ley 527 de 1999 y sus decretos reglamentarios. Los Responsables de Procesos deben revisar regularmente el cumplimiento de las políticas y procedimientos de seguridad de la información en sus procesos y reportar cualquier hallazgo al Líder de Seguridad de la Información.
- Gestión IT coordinará la revisión periódica de los sistemas de información para garantizar el cumplimiento de las políticas y procedimientos de seguridad.
- La adquisición de software debe realizarse a proveedores legalmente constituidos y acreditados para evitar violaciones de derechos de autor.
- No se pueden instalar o usar programas propiedad de terceros sin la autorización explícita del propietario, y no se deben descargar materiales sujetos a propiedad intelectual en los equipos de la organización.
- El Líder de Seguridad de la Información y el responsable del proceso de Gestión IT deben implementar los controles necesarios para garantizar la integridad, confidencialidad y disponibilidad de la información clasificada como sensible.
- Los registros de información deben manipularse de acuerdo con la Política de Gestión de Activos, y los registros clasificados como confidenciales no deben extraerse de la organización sin la aprobación del Líder de Seguridad de la Información.
- Las acciones en caso de incumplimiento de las políticas y normas de seguridad estarán basadas en lo indicado en la sección **19.SANCIONES** del "**M-SI-02 Manual Seguridad de la Información**".

6.11. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES

Servinformación, en estricto cumplimiento del artículo 15 de la Constitución Política de Colombia, así como de la Ley Estatutaria 1581 de 2012 y sus normativas reglamentarias y complementarias, se compromete a salvaguardar de manera integral (desde el ámbito jurídico, técnico y organizativo) el derecho fundamental de Habeas Data de todos los Titulares de información personal, ya sea en calidad de Responsable o Encargado de su Tratamiento. Asimismo, garantizamos en todo momento los derechos fundamentales a la intimidad, buen nombre y privacidad de las personas naturales.

6.11.1. OBJETIVO DE LA POLÍTICA

Garantizar de manera integral (jurídica, técnica y organizativa) la protección y el ejercicio del derecho fundamental de Habeas Data, así como velar por los derechos fundamentales a la intimidad, el buen nombre y la privacidad de las personas naturales. Además, busca establecer los términos, condiciones y finalidades para el tratamiento de datos personales por parte de Servinformación, ya sea obtenidos a través de sus canales de atención o procesados por terceros.

6.11.2. ALCANCE DE LA POLÍTICA

La política se aplica a todas las personas cuyos datos personales son tratados por Servinformación, ya sean colaboradores, proveedores u otras terceras partes. Se extiende a todos los canales de atención de la organización y abarca el tratamiento de datos personales tanto de titulares de información como de colaboradores de Servinformación.

6.11.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Velar por el cumplimiento de las normativas legales relacionadas con la privacidad y protección de datos personales.
- Coordinar la aplicación de controles y procedimientos de seguridad de la información.

Comité de Seguridad:

- Colaborar en la identificación de riesgos y la implementación de medidas de seguridad.
- Evaluar periódicamente la efectividad de las prácticas de protección de datos.

Gestión IT:

- Implementar medidas técnicas para garantizar la seguridad de los datos personales.
- Colaborar en la auditoría y monitoreo de sistemas para prevenir posibles brechas de seguridad.
- Asegurar la confidencialidad, integridad y disponibilidad de la información.

Responsables de Procesos:

- Colaborar en la aplicación de controles específicos para la protección de datos en sus procesos.

Colaboradores:

- Guardar discreción y reserva absoluta con respecto a la información de Servinformación.
- Cumplir con las condiciones contractuales y de seguridad establecidas en relación con el tratamiento de datos personales.
- Participar en programas de formación y concientización sobre seguridad de la información.

6.11.4. GENERALIDADES

Servinformación en cumplimiento con lo dispuesto en el artículo 15 de la Constitución Política de Colombia y la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias y complementarias, garantiza de forma integral (jurídica, técnica y organizativa) la protección y el ejercicio del derecho fundamental de Habeas Data (conocer, rectificar y actualizar) de todos los Titulares de la información de carácter personal, de la cual sea Responsable o Encargada de su Tratamiento, asimismo, garantizará en todo momento los derechos fundamentales a la intimidad, el buen nombre y la privacidad de las personas naturales, razón por la cual adopta y aplica el manual "**M-SI-01 Manual de Políticas de Tratamiento de Datos Personales**".

Se establecen los términos, condiciones y finalidades para las cuales Servinformación, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla Servinformación, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, Servinformación exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus colaboradores, estableciendo los controles necesarios para preservar aquella información que Servinformación conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de Servinformación y no sea publicada, revelada o entregada a colaboradores o terceras partes sin autorización.

- Los procesos que procesan datos personales de colaboradores, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de Servinformación.
- Los procesos que gestionan datos personales de colaboradores, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales
- Los colaboradores deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de Servinformación o de sus integrantes de los cuales tengan conocimiento en el ejercicio de sus funciones.
- En busca de mantener la seguridad de la información en actividades relacionadas con Protección de Datos Personales, se establece el "**D-SI-01 Documento de Seguridad para la Protección de Datos**".

6.12. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN EL USO DE INTELIGENCIA ARTIFICIAL

Servinformación establece un conjunto de directrices y medidas diseñadas para garantizar la confidencialidad, integridad y disponibilidad de la información cuando se emplea tecnología de inteligencia artificial. Esta política tiene como objetivo principal proteger los datos sensibles y la infraestructura asociada con las aplicaciones de IA, minimizando los riesgos de ciberseguridad y asegurando el cumplimiento de normativas y estándares.

6.12.1. OBJETIVO DE LA POLÍTICA

Garantizar la seguridad, confidencialidad e integridad de la información tratada mediante el uso de inteligencia artificial. Se busca proteger especialmente los datos personales y la privacidad de los individuos, mitigando riesgos y asegurando el cumplimiento de normativas legales y éticas.

6.12.2. ALCANCE DE LA POLÍTICA

Esta política se aplica a todas las actividades que involucren el uso de inteligencia artificial dentro de la organización, independientemente de la forma en que se implemente la tecnología (algoritmos, aprendizaje automático, procesamiento de lenguaje natural, etc.). Se extiende a todos los empleados y terceros que interactúen con los sistemas de inteligencia artificial de la organización.

6.12.3. RESPONSABILIDADES

Líder de Seguridad de la Información:

- Colaborar con otros líderes para establecer medidas de seguridad para minimizar la recopilación y retención de datos personales.
- Asegurarse de que se obtenga el consentimiento informado antes de utilizar datos personales para entrenar modelos de inteligencia artificial.
- Supervisar la transparencia en la comunicación sobre el uso de la inteligencia artificial.

Comité de Seguridad:

- Evaluar y aprobar medidas específicas de seguridad para minimizar la recopilación y retención de datos personales.
- Monitorear la implementación de controles de seguridad en el contexto de la inteligencia artificial.

Gestión IT:

- Implementar y mantener medidas técnicas de seguridad para proteger la información tratada mediante inteligencia artificial.

Responsables de Procesos:

- Integrar consideraciones de seguridad desde las etapas iniciales del desarrollo de la inteligencia artificial en los procesos correspondientes.
- Asegurar la transparencia en la comunicación interna y externa sobre el uso de la inteligencia artificial en los procesos específicos.
- Colaborar con el Líder de Seguridad de la Información para implementar medidas específicas para minimizar la recopilación y retención de datos personales.

Colaboradores:

- Participar en programas de capacitación relacionados con la seguridad de la información y el uso de inteligencia artificial.

6.12.4. GENERALIDADES

- La implementación responsable de sistemas de inteligencia artificial exige una cuidadosa selección y utilización, prestando atención a los riesgos de seguridad inherentes. Los datos empleados en estos sistemas deben ser resguardados contra accesos no autorizados, uso indebido, divulgación no autorizada, alteración o destrucción.
- Desde las fases iniciales de la implementación de la inteligencia artificial, es imperativo considerar la privacidad de la información. Se deben establecer medidas para minimizar la recopilación y retención de datos personales, así como obtener el consentimiento informado antes de emplear datos personales en el entrenamiento de modelos de inteligencia artificial.

- La seguridad de los sistemas de inteligencia artificial debe ser gestionada de manera proactiva y continua, asegurando una salvaguarda constante frente a posibles amenazas y vulnerabilidades.

6.13. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DEL RECURSO HUMANO

Toda vinculación laboral realizada por **Servinformación** se rige por las leyes de la República de Colombia y por lo dispuesto en el Código Sustantivo del Trabajo. El proceso de selección se ejecutará de acuerdo a los manuales y procedimientos establecidos por la Organización.

6.13.1. OBJETIVO DE LA POLÍTICA

Garantizar la seguridad de la información en todas las etapas de la vinculación, ejecución y desvinculación laboral en Servinformación, en cumplimiento de las leyes de la República de Colombia y el Código Sustantivo del Trabajo.

6.13.2. ALCANCE DE LA POLÍTICA

Esta política se aplica a todo el personal de Servinformación desde el proceso de selección hasta la desvinculación, abarcando la gestión de información y la seguridad de la información.

6.13.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Coordinar con Gestión Humana la elaboración y ejecución del Programa de Capacitación en Seguridad de la Información.
- Garantizar que los colaboradores reciban información sobre la importancia de la seguridad de la información.
- Coordinar con Gestión Humana las acciones disciplinarias relacionadas con incumplimiento de los lineamientos de Seguridad de la Información, de acuerdo con la norma ISO/IEC 27001: 2022, los documentos "**P-GH-07 Procedimiento Disciplinario**" y "**M-SI-02 Manual Seguridad de la Información**" y la legislación aplicable.

Comité de Seguridad:

- Supervisar el cumplimiento de la política y proponer ajustes si es necesario.

Gestión IT:

- Participar en la entrega y recogida de activos respectivos durante la vinculación, desvinculación o cambio de empleo.

- Asegurarse de la eliminación de accesos lógicos y la transferencia de información según los procedimientos establecidos.
- Asegurar que los colaboradores de Servinformación, cuentan con los elementos y herramientas necesarias para la correcta ejecución de sus funciones.

Responsables de Procesos:

- Asegurar la entrega y recogida de activos respectivos durante la vinculación, desvinculación o cambio de empleo.
- Colaborar con Gestión Humana y Gestión IT para garantizar una transición segura de la información y activos.

Gestión Humana:

- Realizar las validaciones necesarias de la información suministrada por el candidato antes de la vinculación definitiva.
- Velar para que los colaboradores firmen un acuerdo de confidencialidad y no divulgación durante la contratación.
- Velar porque los colaboradores conozcan y acepten las políticas de seguridad de la información de la Organización.
- Determinar la competencia necesaria de los colaboradores en relación con la seguridad de la información.
- Coordinar con el Líder de Seguridad de la Información la elaboración y ejecución del Programa de Capacitación en Seguridad de la Información.
- Velar por que los colaboradores de Servinformación, cuentan con los elementos y herramientas necesarias para la correcta ejecución de sus funciones.
- Iniciar acciones para la devolución de activos, eliminación de accesos lógicos y transferencia de información en caso de desvinculación.
- Iniciar las acciones disciplinarias relacionadas con incumplimiento de los lineamientos de Seguridad de la Información, de acuerdo con la norma ISO/IEC 27001: 2022, los documentos “**P-GH-07 Procedimiento Disciplinario**” y “**M-SI-02 Manual Seguridad de la Información**” y la legislación aplicable.

Colaboradores:

- Firmar un acuerdo de confidencialidad y no divulgación durante la contratación.
- Ser conscientes de la política de seguridad de la información y su contribución a la eficacia del sistema de gestión de la seguridad de la información.
- Reportar al Líder de Seguridad de la Información cualquier incidente o evento de seguridad de la información del que tengan conocimiento.
- Participar activamente en las capacitaciones relacionadas con la seguridad de la información.

6.13.4. GENERALIDADES

Directrices relacionadas con la Vinculación Laboral

- Gestión Humana realizará las validaciones necesarias de la información suministrada por el candidato antes de su vinculación definitiva.
- Gestión Humana debe velar para que todos los colaboradores firmen durante la contratación un acuerdo de confidencialidad y no divulgación, en el que se especifique el período por el cual se debe mantener el acuerdo y las acciones que se toman cuando se incumpla este requisito.
- Gestión Humana debe velar para que todos los colaboradores conozcan y acepten las políticas de seguridad de la Información de Servinformación.
- Gestión Humana debe determinar la competencia necesaria de los colaboradores para realizar el trabajo bajo su control y que afecte su desempeño en la seguridad de la información.
- Gestión Humana debe garantizar que estas personas sean competentes sobre la base de una educación, formación o experiencia, siguiendo los procedimientos e instructivos propios del proceso de selección.

Directrices relacionadas con la Ejecución del Empleo

- Las personas que realicen trabajos bajo el control de la Organización deben ser conscientes de:
    - La política de seguridad de la información.
    - Su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios de un mejor desempeño de la seguridad de la información; y
    - Las implicaciones de no cumplir con el SGSI.
- Para lograr lo anterior, Gestión Humana y el Líder de Seguridad de la Información elaboran anualmente el Programa de Capacitación, según los indicado en el plan "**PL-SI-08 Plan de Capacitación y Sensibilización de Seguridad en la Información**" y los procedimientos "**P-SI-12 Procedimiento de Capacitación y Sensibilización de Seguridad en la Información**" y "**P-GH-Capacitación y Plan Carrera**". Se debe garantizar que los colaboradores reciban inducción relacionada con la importancia de la seguridad de la información y participen de las capacitaciones a las que haya lugar. Es obligación del Líder de Seguridad de la Información coordinar con Gestión Humana las fechas, canales de comunicación y temas de capacitación, tipo de formación entre otros aspectos.
- Cada colaborador está comprometido a reportar al Líder de Seguridad de la Información cualquier incidente o evento de seguridad de la información del que

tenga conocimiento, por los medios y formas establecidos para ello en el procedimiento "**P-SI-02 Gestión de incidentes de Seguridad de la Información**".
- En atención a los requisitos de la norma ISO/IEC 27001: 2022 y demás legislación aplicable con relación a los procesos disciplinarios, Servinformación sigue los lineamientos de acuerdo al Reglamento Interno de Trabajo.

Directrices relacionadas con la Desvinculación y Cambio de Empleo

- Servinformación establece el cumplimiento de las Leyes Colombianas vigentes con relación a la vinculación laboral, desvinculación laboral y el cambio de cargo según lo descrito en el documento "**P-GH-03 Procedimiento de desvinculación**".
- En caso de terminación del contrato, Gestión Humana iniciará oportunamente las acciones para la devolución de activos de información, eliminación de los accesos lógicos y transferencia de información de acuerdo con los procedimientos establecidos.
- En caso de que un colaborador obtenga un cambio de funciones, se debe seguir los mismos procedimientos donde se asegure la entrega de activos, actualización de los accesos lógicos, transferencia de información y la posterior entrega de los mismos de acuerdo a su nuevo rol.
- Cada líder de proceso, con el acompañamiento de Gestión Humana y Gestión IT, debe asegurarse de la entrega de los activos al proceso encargado.

6.14. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN EL RELACIONAMIENTO CON PROVEEDORES Y CONTRATISTAS

Servinformación establece mecanismos de control en sus relaciones con proveedores o contratistas, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas y procedimientos de seguridad de la información de la Organización.

6.14.1. OBJETIVO DE LA POLÍTICA

Garantizar la confidencialidad, integridad y disponibilidad de la información compartida con proveedores y contratistas.

6.14.2. ALCANCE DE LA POLÍTICA

Esta política se aplica a todas las relaciones con proveedores y contratistas que involucren acceso a la información o servicios de Servinformación.

6.14.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Supervisar la implementación de requisitos de seguridad en los contratos y acuerdos con proveedores y contratistas.
- Participar en las inducciones de seguridad de la información con de contratistas, garantizando que sean conscientes de sus responsabilidades de Seguridad durante la ejecución de sus labores.

Comité de Seguridad:

- Establecer condiciones de comunicación segura, cifrado y transmisión de información con proveedores y contratistas.
- Colaborar en la respuesta a incidentes de seguridad junto con el equipo de respuesta a incidentes de ciberseguridad.

Gestión IT:

- Coordinar la solicitud formal de accesos a sistemas de información y equipos de cómputo por parte de proveedores y contratistas.

Responsables de Procesos:

- Colaborar en la comunicación de políticas y procedimientos de seguridad de la información a contratistas bajo su responsabilidad.
- Participar en la evaluación del cumplimiento de requisitos de seguridad por parte de proveedores y contratistas en el contexto de los procesos.

6.14.4. GENERALIDADES

Directrices Relacionadas con la relación con los Proveedores

- La vinculación de proveedores debe guiarse por lo establecido en el documento "**P-ADM-01 Procedimiento de Compras**".
- En los contratos con proveedores se deben incluir cláusulas que definan los requisitos mínimos de seguridad de la información y protección de datos personales con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información, tanto de la Organización como de sus Clientes y demás partes interesadas.
- De igual forma, debe asegurarse la inclusión de cláusulas de confidencialidad, propiedad intelectual y derechos de autor en contratos con proveedores.
- Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal a la Coordinación de Informática vía correo electrónico.
- El Comité de Seguridad debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios.

- Los proveedores deben garantizar la protección y confidencialidad de toda la información que le sea entregada por Servinformación, para el desarrollo del objeto contratado.
- Los proveedores deben notificar inmediatamente cualquier incidente de seguridad de la información o ciberseguridad que afecte a la información o activos tecnológicos de Servinformación y/o sus clientes directa o indirectamente. De igual manera, debe tener la capacidad de responder y contener de manera oportuna y coordinada con el equipo de respuesta a incidentes de ciberseguridad de Servinformación.
- Los proveedores deben capacitar al personal que está vinculado para el desarrollo del objeto contractual cuando así sea solicitado por Servinformación.

Directrices Relacionadas con la relación con Contratistas

- Los contratistas deben conocer las políticas de seguridad de Servinformación descritas en el presente manual, y comprometerse a dar cumplimiento de dichas políticas dentro de la ejecución del contrato. Por tanto, los supervisores de contratos deben asegurar que se comunican dichas políticas y procedimientos de seguridad de la información a los contratistas.
- En los contratos con contratistas se deben incluir cláusulas que definan los requisitos mínimos de seguridad de la información y protección de datos personales con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información, tanto de la Organización como de sus Clientes y demás partes interesadas.
- De igual forma, debe asegurarse la inclusión de cláusulas de confidencialidad, propiedad intelectual y derechos de autor en contratos con contratistas.
- Los accesos a los sistemas de información y equipos de cómputo requeridos por los contratistas deben ser solicitados de manera formal a la Coordinación de Informática vía correo electrónico.
- El Comité de Seguridad debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los contratistas.
- Los contratistas deben garantizar la protección y confidencialidad de toda la información que le sea entregada por Servinformación, para el desarrollo del objeto contratado.
- Los contratistas deben notificar inmediatamente cualquier incidente de seguridad de la información o ciberseguridad que afecte a la información o activos tecnológicos de Servinformación y/o sus clientes directa o indirectamente. De igual manera, debe tener la capacidad de responder y contener de manera oportuna y coordinada con el equipo de respuesta a incidentes de ciberseguridad de Servinformación.

- Los contratistas deben proteger sus estaciones de trabajo de manera anticipada y proactiva contra amenazas y/o riesgos que puedan llegar a afectar la información que le ha entregado Servinformación.
- Los contratistas durante las etapas de desarrollo y pruebas deben establecer e informar al Servinformación los controles, herramientas y/o mecanismos para el borrado seguro y destrucción de la información en su estación de trabajo. conforme a las mejores prácticas de la industria.

6.15. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN DISEÑO Y DESARROLLO

Servinformación, define los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, desarrollados en Servinformación.

6.15.1. OBJETIVO DE LA POLÍTICA

Garantizar la seguridad de la información en los procesos de diseño y desarrollo de sistemas de información en Servinformación.

6.15.2. ALCANCE DE LA POLÍTICA

Se aplica a sistemas nuevos o mejoras a sistemas existentes desarrollados en Servinformación.

6.15.3. RESPONSABILIDADES ESPECÍFICAS

Lider de Seguridad de la Información:

- Revisar el cumplimiento de los requisitos de seguridad de la información acordados con el Cliente.
- Colabora con el Comité de Seguridad y Gestión IT en la definición de requisitos de seguridad para procesos de desarrollo de software contratados.

Comité de Seguridad:

- Revisa y aprueba los lineamientos de desarrollo seguro definidos.

Gestión IT:

- Apoya los procesos que contraten el desarrollo de software en la definición de requisitos de seguridad de la información.

Responsables de Procesos:

- Definen requisitos de seguridad de la información para sistemas de información nuevos o mejoras.

- Velan por el cumplimiento de los requisitos de seguridad esperados en el desarrollo de sistemas de información.
- Aseguran que los sistemas de información desarrollados por terceros cuenten con acuerdos de licenciamiento y cumplan con las leyes aplicables.

Colaboradores:

- Aplicar los lineamientos de seguridad en el desarrollo de software.

6.15.4. GENERALIDADES

Directrices Relacionadas con la Seguridad de los Sistemas de Información

- Garantizar la autenticación segura de los usuarios para proteger los sistemas y datos de la organización, mediante la implementación de mecanismos de autenticación fuertes en todos los sistemas y aplicaciones críticas desarrolladas por Servinformación.
- Salvaguardar la confidencialidad y seguridad de las contraseñas utilizadas para acceder a los sistemas y aplicaciones de la organización, evitando su entrega a través de medios inseguros.
- Garantizar la protección adecuada de los activos de información de la organización, asegurando la disponibilidad, confidencialidad e integridad de dichos activos, aplicando medidas de cifrado de información y recursos en múltiples regiones, durante las distintas fases de desarrollo de software.
- Cumplir los requisitos de Seguridad de la Información acordados con el Cliente durante los procesos de negociación.
- Implementar mecanismos de monitoreo y registro de eventos de las actividades de los usuarios.
- Implementar metodologías de desarrollo seguro.
- Los procesos que contraten el desarrollo de software, deben apoyarse en el Comité de Seguridad y Gestión IT para definir los requisitos de seguridad de la información de los mismos.
- Servinformación cuenta con ambientes de desarrollo, pruebas y producción separados.
- Servinformación controla el acceso a los ambientes de desarrollo y pruebas de la misma forma que controla el acceso al ambiente de producción.

Directrices Relacionadas con la Seguridad en los Procesos de Diseño y Desarrollo

- Servinformación debe velar porque el desarrollo de los sistemas de información cumpla con los requisitos de seguridad esperados, así como con pruebas de aceptación y seguridad al software desarrollado. Además, Servinformación

asegurará que todo software desarrollado, cuenta con el nivel de soporte requerido por la Organización.

- Los cambios en sistemas, plataforma tecnológica o paquetes de software, deben realizarse de acuerdo con el "**P-SI-03 Procedimiento Gestión de Cambios**".
- El Comité de Seguridad debe definir los lineamientos de desarrollo seguro, los cuales deben ser revisados periódicamente para asegurar que permanezcan actualizados en términos de combatir nuevas amenazas y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.
- El Comité de Seguridad aplicará los mismos controles aplicados al ambiente de producción en el ambiente de desarrollo y QA, tales como, control de acceso, copias de respaldo, registro de eventos, etc.
- El Comité de Seguridad debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas.
- El Comité de Seguridad debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de Servinformación.
- Los procesos deben asegurarse que los sistemas de información desarrollados por terceros, cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.
- Los procesos deben tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes aplicables.
- Cuando se contrata desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por Servinformación. Se debe acordar la entrega de manuales técnicos que describen la estructura del sistema, así como el diccionario de datos, librerías y archivos que lo conforman; y manuales funcionales, que describen las funcionalidades de la aplicación.
- Se deben realizar pruebas de aceptación del software, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros (en donde sea aplicable). En estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debería verificar que se han corregido los defectos relacionados con la seguridad.
- Las actividades relacionadas con pruebas se deben alinear con el procedimiento "**P-SI-08 Procedimiento de Pruebas de Seguridad en Desarrollo**".

Directrices Relacionadas con el uso de Datos de Prueba

- El líder de proyecto debe certificar que la información a ser entregada a los desarrolladores (tanto internos como externos) para sus pruebas debe ser enmascarada o que los datos sensibles deben ser eliminados con el fin de no revelar información confidencial de los ambientes de producción y por ende, dar

cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

- El líder de proyecto debe certificar que la información a ser entregada a los desarrolladores para sus pruebas debe ser enmascarada y no revelar información confidencial de los ambientes de producción.
- Se aplican técnicas de enmascaramiento a todos los datos sensibles y confidenciales que se encuentran en entornos de desarrollo y prueba.
- El líder de proyecto debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

6.16. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DEL CAMBIO

Servinformación establece los principios y directrices para la gestión de cambios en la organización. La gestión de cambios garantiza que todos los cambios realizados en el SGSI y en la infraestructura tecnológica se planifiquen, evalúen, aprueben, implementen y documenten de manera controlada, minimizando los riesgos y maximizando los beneficios para la seguridad de la información. Esta política se aplica a todos los cambios que afecten al SGSI, incluyendo cambios en la infraestructura tecnológica, procesos, políticas, procedimientos y controles de seguridad de la información.

6.16.1. OBJETIVO DE LA POLÍTICA

Garantizar la gestión controlada de cambios en la infraestructura tecnológica y en los elementos del SGSI, minimizando los riesgos y maximizando los beneficios para la seguridad de la información.

6.16.2. ALCANCE DE LA POLÍTICA

Esta política se aplica a todos los cambios que afecten al SGSI, abarcando la infraestructura tecnológica, procesos, políticas, procedimientos y controles de seguridad de la información.

6.16.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Proponer los cambios que sean pertinentes para garantizar que el SGSI siga siendo efectivo y se ajuste a las necesidades cambiantes de la organización.
- Participar en la revisión de los cambios implementados para evaluar su efectividad y abordar problemas identificados.

Comité de Seguridad:

- Revisar y aprobar los criterios y procedimientos para la evaluación, aprobación, programación e implementación de cambios.
- Revisar y aprobar la evaluación de viabilidad, impacto y riesgos potenciales de las solicitudes de cambios.
- Participar en el seguimiento de los cambios implementados para evaluar su efectividad y abordar problemas identificados.

Gestión IT:

- Programar y planificar cambios aprobados considerando la disponibilidad de recursos y los impactos en las operaciones del SGSI.
- Monitorear y revisar los cambios implementados para evaluar su efectividad y abordar problemas identificados.

Responsables de Procesos:

- Colaborar en la implementación adecuada y controlada de los cambios en los procesos que supervisan.

Colaboradores:

- Colaborar en la implementación adecuada y controlada de los cambios según las instrucciones y procedimientos establecidos.

6.16.4. GENERALIDADES

- La Gestión del Cambio es un aspecto crucial en cualquier organización, y para garantizar su eficacia, es imperativo establecer roles y responsabilidades claramente definidos. Además, se deben establecer criterios y procedimientos para la evaluación, aprobación, programación e implementación de cambios.
- Es esencial mantener registros precisos de todos los cambios realizados, incluyendo información detallada sobre el cambio, su justificación, impacto y los recursos necesarios. Todas las solicitudes de cambios deben ser evaluadas por el respectivo comité para determinar su viabilidad, impacto y riesgos potenciales.
- Los cambios aprobados deben ser programados y planificados adecuadamente, teniendo en cuenta la disponibilidad de recursos y los impactos en las operaciones del SGSI.
- Servinformación cuenta con el procedimiento "**P-SI-03 Gestión de Cambios**" para guiar esta actividad. De igual forma, cualquier cambio que implique la modificación de los documentos rectores del SGSI, deben ser implementados acorde con los procedimientos "**P-CA-01 Elaboración de Documentos**" y "**P-CA-02 Control de Información Documentada**".
- En el caso específico de cambios en los sistemas de información, se deben realizar pruebas mínimas para garantizar la integridad de la información en producción. Estas pruebas deben ser planificadas, ejecutadas, documentadas y controladas, con el ambiente de pruebas siendo lo más idéntico posible al ambiente real de producción.

- Los cambios deben reflejar detalles de actividades previas, durante y después del cambio, así como procedimientos en caso de regreso del cambio (rollback). Además, cualquier cambio relacionado con el mantenimiento de software o modificación de parámetros debe realizarse sin comprometer la seguridad existente.
- Antes de la implementación de un nuevo sistema, se deben especificar claramente los requerimientos importantes de seguridad. También, se deben realizar pruebas exhaustivas sobre el software a adquirir, contemplando aspectos funcionales, de seguridad y técnicos, así como la revisión de procesos de retorno a la versión anterior.
- La necesidad de la implementación de un cambio puede surgir de:
    - **Cambios en el entorno de amenazas**: las amenazas a la seguridad de la información evolucionan constantemente, por lo que es importante que el SGSI se actualice para abordar nuevas amenazas y riesgos.
    - **Cambios en la legislación y regulación**: las leyes y regulaciones relacionadas con la seguridad de la información cambian con frecuencia,y el SGSI debe mantenerse al día para cumplir con los requisitos legales y regulatorios.
    - **Cambios en la estructura de la organización**: si la estructura de la Organización cambia significativamente, es posible que se deba actualizar el SGSI para reflejar estos cambios.
    - **Cambios en la tecnología:** la tecnología de la información y las comunicaciones cambian constantemente, y el SGSI debe actualizarse para reflejar estos cambios y asegurarse de que la Organización esté utilizando las mejores prácticas de seguridad.
    - **Resultados de evaluaciones y auditorías:** los resultados de las evaluaciones y auditorías del SGSI pueden revelar áreas que necesitan mejoras o actualizaciones en las políticas.

6.17. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

Servinformación se compromete a garantizar la seguridad de la información durante la gestión de proyectos, definiendo medidas para asegurar la identificación y gestión de objetivos y riesgos de seguridad de la información. Estas directrices se aplican a cualquier proyecto, independientemente de su naturaleza. Los líderes de proceso o proyecto deben seguir las directrices específicas, que incluyen la inclusión de objetivos de seguridad, valoración de riesgos y seguimiento de controles durante todas las fases del proyecto.

6.17.1. OBJETIVO DE LA POLÍTICA

Garantizar la seguridad de la información durante la gestión de proyectos, asegurando la identificación y gestión de objetivos y riesgos de seguridad de la información.

6.17.2. ALCANCE DE LA POLÍTICA

Esta política se aplica a cualquier proyecto, independientemente de su naturaleza o tamaño.

6.17.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Proporcionar orientación y asesoramiento sobre aspectos de seguridad de la información durante la ejecución de proyectos.
- Colaborar con los líderes de proceso o proyecto para garantizar la inclusión de objetivos de seguridad de la información en los objetivos del proyecto.
- Supervisar la realización de la valoración de riesgos de seguridad de la información durante el proyecto.

Comité de Seguridad:

- Evaluar periódicamente la efectividad de las medidas de seguridad implementadas en los proyectos.

Gestión IT:

- Colaborar con los líderes de proceso o proyecto para integrar medidas de seguridad de la información en la planificación y ejecución de proyectos.
- Proporcionar recursos y apoyo técnico necesario para implementar controles de seguridad.

Responsables de Procesos o Proyectos:

- Incluir objetivos de seguridad de la información en los objetivos del proyecto.
- Liderar la valoración de riesgos de seguridad de la información en el proyecto.
- Supervisar la implementación y el seguimiento de controles de seguridad durante todas las fases del proyecto.

Colaboradores:

- Colaborar en la implementación de los controles de seguridad dentro de los proyectos a los que son asignados.

6.17.4. GENERALIDADES

Servinformación, para garantizar la seguridad de la información durante la gestión de proyectos, define asegurar la identificación y gestión de objetivos y riesgos de seguridad de la información. Esto aplicará a cualquier proyecto, independientemente de su

naturaleza. Por lo tanto, es responsabilidad de los Líderes de Proceso o Proyecto asegurar que se sigan las siguientes directrices:

- Incluir objetivos de seguridad de la información en los objetivos del proyecto.
- Realizar valoración de los riesgos de seguridad de la información en la fase inicial del proyecto, para identificar los controles necesarios.
- Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.
- Cuando corresponda, y como parte de la documentación de los proyectos, se deben emitir manuales de usuario y buenas prácticas con respecto al servicio prestado con el propósito de educar, capacitar y concientizar en seguridad de la información relativa a dicho servicio.
- La gestión de riesgos de Seguridad de la Información en Servinformación se orientan según los documentos ”**M-SI-03 Metodología Gestión de riesgos**” y “**P-SI-13 Gestión del riesgo en los procesos y proyectos**”.

6.18. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL TRABAJO EN CASA

A partir del uso de tecnologías de la información y las telecomunicaciones TIC, se define que los colaboradores puedan desarrollar trabajo en casa por medio del uso de las TIC, sin que se constituya como modalidad de teletrabajo según lo descrito en el numeral 4 del artículo 6 de la Ley 1221 de 2008 “*por el cual se establecen normas para promover y regular el teletrabajo*”. Por lo tanto, para el caso de Servinformación se denomina **trabajo en casa**.

La totalidad de políticas, normas, procedimientos y guías de buenas prácticas descritas dentro del SGSI de **Servinformación** son de obligatorio cumplimiento, independientemente de que el colaborador trabaje desde casa o desde la oficina.

6.18.1. OBJETIVO DE LA POLÍTICA

Garantizar la seguridad de la información de Servinformación durante el trabajo en casa de los colaboradores, mediante el establecimiento de medidas y procedimientos específicos que mitiguen los riesgos asociados al uso de tecnologías de la información y las telecomunicaciones (TIC).

6.18.2. ALCANCE DE LA POLÍTICA

Esta política se aplica a todos los colaboradores autorizados por Servinformación que realicen trabajo en casa utilizando TIC para acceder a la información de la Organización desde redes externas.

6.18.3. RESPONSABILIDADES ESPECÍFICAS

Líder de Seguridad de la Información:

- Proponer la implementación de medidas de seguridad efectivas para garantizar la protección de la información cuando los colaboradores trabajan desde casa.
- Supervisar los procesos de auditoría, revisiones y seguimiento a la seguridad de la información, asegurando la participación de los colaboradores que trabajan desde casa cuando sea necesario.

Comité de Seguridad:

- Revisar los resultados de las auditorías y revisiones de seguridad de la información, evaluando la eficacia de las medidas implementadas para el trabajo en casa.

Gestión IT:

- Garantizar que el acceso remoto a la información de la organización sea seguro, estableciendo y manteniendo conexiones seguras y autenticación adecuada.
- Asegurarse de que los equipos de cómputo desde los cuales los colaboradores acceden remotamente cumplan con los requisitos de seguridad establecidos.

Responsables de Procesos:

- Asegurar que los colaboradores que trabajan desde casa participen activamente en auditorías y revisiones relacionadas con la seguridad de la información.

Colaboradores:

- Participar activamente en auditorías y revisiones relacionadas con la seguridad de la información.
- Cumplir con la totalidad de políticas y directrices establecidas, independiente de su lugar de trabajo.

6.18.4. GENERALIDADES

- Cualquier colaborador de **Servinformación** autorizado y que requiera tener acceso a la información de la Organización desde redes externas, pueden acceder remotamente mediante un proceso de autenticación, a través de conexiones seguras y garantizando el cumplimiento de requisitos de seguridad de los equipos de cómputo desde los que se accede.
- Los colaboradores que trabajen desde casa deben contar con un espacio de trabajo seguro, adecuado y alineado con las recomendaciones de Gestión Humana y el

consultor de Salud Ocupacional, libre de distracciones y ruido, y en el que puedan proteger la información de la Organización.

- Los colaboradores deben mantener una comunicación regular con sus compañeros de trabajo y supervisores utilizando las herramientas y plataformas de comunicación proporcionadas por la Organización.
- Los colaboradores que trabajen desde casa deben participar en capacitaciones y actividades de concienciación sobre seguridad de la información, proporcionadas por la Organización, para asegurar su conocimiento y cumplimiento de las políticas y procedimientos del SGSI.
- Los colaboradores deben participar en los procesos de auditoría, revisiones y seguimiento a la seguridad de la información, cuando así sea requerido.
- La gestión responsable del uso de equipos portátiles y teléfonos celulares asignados es esencial. Deben mantenerse los mismos estándares de seguridad que si los dispositivos estuvieran dentro de las instalaciones de la organización.
- Es crucial garantizar una protección adecuada durante la conexión a redes. Los equipos deben contar con la última versión de parches liberados por los fabricantes.
- El acceso remoto a la información de la Organización sólo debe ocurrir después de una identificación y autenticación exitosa, junto con el establecimiento de los mecanismos adecuados de control de acceso. Este enfoque garantiza la integridad y seguridad de la información corporativa.

7. EXCEPCIONES

Las excepciones al cumplimiento de las políticas de Seguridad de la Información o la aplicación de los controles técnicos relacionados no serán permitidas sin un análisis y autorización previo. Aprobar una excepción a una política implica cumplir con condiciones y requisitos específicos, así como obtener la debida autorización de las partes responsables de la Seguridad de la Información. Para aprobar una excepción se ha establecido el documento "**P-SI-14 Excepciones a las Políticas de Seguridad de la Información**". Este procedimiento no es válido en situaciones que puedan resultar en el incumplimiento de los requisitos directos de la norma ISO/IEC 27001:2022, ni de alguna ley o regulación aplicable.

8. INCUMPLIMIENTO

El incumplimiento de las anteriores Políticas de Seguridad de la Información puede resultar en acciones disciplinarias, conforme a lo descrito en el documento "**M-SI-02 Manual Seguridad de la Información**" en el apartado **19. SANCIONES**.

9. HISTORIAL DE CAMBIOS

HISTORIAL DE CAMBIOS		
Fecha	Revisión	Descripción
05/02/2024	00	Emisión del documento. Se reestructura el documento “M-SI-02 Manual Seguridad de la Información”, llevando las Políticas Específicas de Seguridad a un documento aparte con el fin de facilitar la comprensión y el control documental.