TABLA DE CONTENIDO

1. INTRODUCCIÓN

La tecnología, la investigación y el conocimiento, han logrado un gran avance, convirtiendo a la información en uno de los activos más valiosos de las empresas y a la seguridad de la información en una de las principales preocupaciones de éstas. De manera paralela, se han desarrollado diferentes tipos de amenazas que atentan contra el buen funcionamiento de los sistemas de información, como los virus, los malware, cibercriminales, spyware y un sin número de amenazas existentes.

La seguridad de la información se enfoca en cinco objetivos principales:

- **Integridad**, que garantiza que los datos sean los que se supone que son.
- **Confidencialidad**, que asegura que solo los individuos autorizados tengan acceso a los recursos que se intercambian.
- **Disponibilidad**, que garantiza el correcto funcionamiento de los sistemas de información.
- **Evitar el rechazo**, que garantiza que no se pueda negar una operación realizada.
- **Autenticación**, que asegura que solo los individuos autorizados tengan acceso a los recursos.

Para ello, las empresas diseñan procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.
La Clínica SOMA no es ajena a esta situación, y para desempeñar su misión, se ha venido apoyando de diversas tecnologías y sistemas de información en los que se almacenan datos de sus empleados, estados financieros, proveedores y de manera muy importante, los registros de la atención médica de los usuarios.

2. ALCANCE

Aplica a todos los colaboradores de la clínica Soma. Son responsables de su implementación los empleados, contratistas, personal en práctica formativa y demás clientes internos que recolectan, almacenan, gestionan y consultan información institucional. Este manual beneficia a la institución, clientes internos y externos, usuarios y su familia.

3. OBJETIVO GENERAL

Proveer condiciones seguras que garanticen la confidencialidad, integridad y disponibilidad de la información de la clínica Soma.

4. OBJETIVOS ESPECIFICOS

4.1. Proteger los activos de información con base en los criterios de confidencialidad, integridad y disponibilidad mediante la implementación de un sistema de Gestión de seguridad de la información.
4.2. Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
4.3. Sensibilizar y capacitar a los usuarios, en el sistema de Gestión de Seguridad de la Información, fortaleciendo el nivel de conciencia de estos.

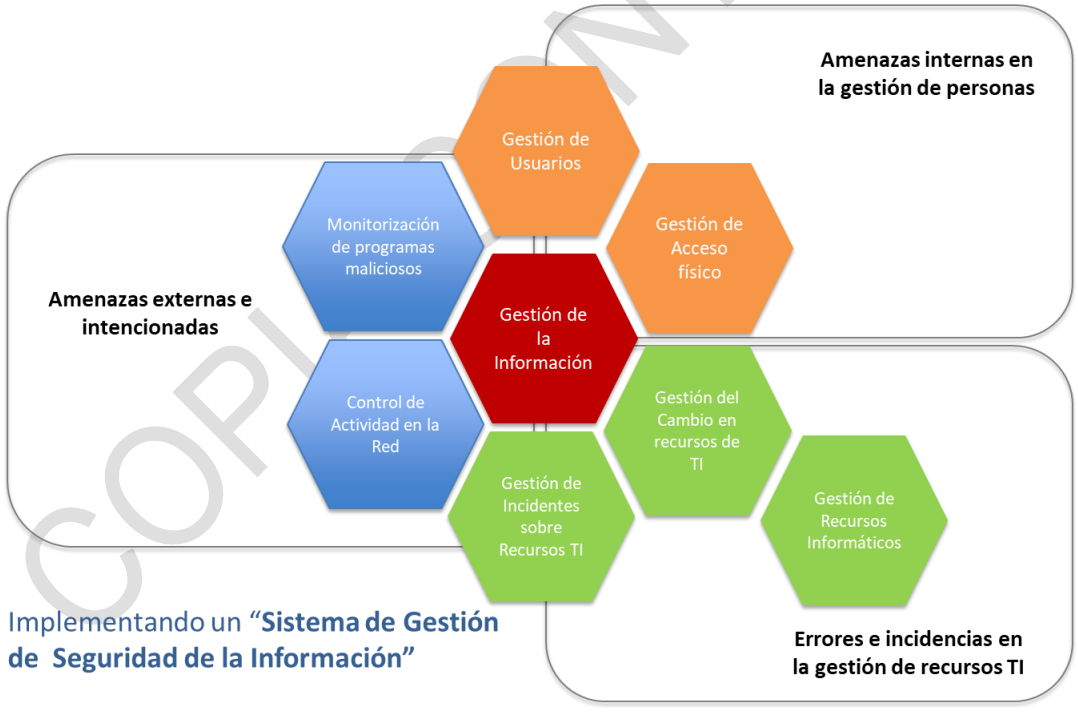
4.4. Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías internas planificadas a intervalos regulares.
4.5. Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información.

5. DESARROLLO DEL MANUAL

El ámbito de trabajo de la "Seguridad de la Información", aplica a:

- Gestión de usuarios y claves de acceso a los sistemas de información.
- Gestión de acceso físico.
- Gestión de recursos informáticos.
- Gestión del cambio de recursos de TI (Tecnología de la Información).
- Gestión de incidentes sobre recursos informáticos.
- Control de actividades en la red.
- Monitoreo de programas maliciosos y detección de intrusos

Para garantizar la seguridad de la información, se deben identificar, evaluar, analizar y gestionar las amenazas internas y externas, además de los errores e incidentes presentados en la gestión de recursos de TI como se ilustra en la siguiente imagen.



A continuación, se detalla la reglamentación emitida por la Clínica SOMA para el cuidado de cada uno de los elementos que componen un sistema de información, de modo se garantice la seguridad de esta.

5.1. GESTIÓN DE USUARIOS Y CLAVES DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

Los usuarios de los sistemas de información son todos aquellos que recolectan, almacenan, gestionan y consultan información. Corresponde al área de Informática, atender las solicitudes de creación, modificación e inactivación de las cuentas de usuario para la disponibilidad y uso de los recursos tecnológicos como archivos, directorios y aplicaciones, entre otros.

Para garantizar la seguridad de la información se debe tener en cuenta, entonces, los siguientes lineamientos institucionales para garantizar la conservación, seguridad, confidencialidad e integralidad de esta:

- **Creación de usuario:**
  - Dicho proceso inicia con la solicitud debidamente registrada en el aplicativo de la mesa de ayuda de Informática por el jefe o encargado del área, especificando claramente los sistemas en los que aplica la solicitud y sus tipos.
  - El estándar definido para crear los usuarios es con su número de identificación al igual que la clave asignada por primera vez (siempre y cuando los sistemas lo permitan). Corresponde al usuario cambiar la clave una vez ingrese por primera vez al sistema al que se le otorgó el acceso.
  - El usuario le será entregado al funcionario así:
    - ✓ Personal clínico: al momento de recibir la capacitación en el sistema clínico.
    - ✓ Personal administrativo: a través del jefe o encargado del área vía e-mail.
  - La capacitación en los diferentes sistemas de información para el nuevo usuario es responsabilidad del jefe o encargado del área.

- **Actualización de usuarios:**
  - Cuando por algún motivo, entre ellos cambio de cargo o funciones, se requiera actualizar los accesos a los sistemas de información, corresponde al jefe o encargado del área, registrar la solicitud en el software de mesa de ayuda de Informática.

- **Inactivación de usuarios:**
  - Todo empleado que se retire de la Clínica SOMA debe solicitar al área de Informática su paz y salvo. En este momento, el encargado de Informática debe registrar la solicitud de inactivación del usuario en la mesa de ayuda de Informática.
  - Cuando el retiro obedece a un despido, el área de Gestión Humana debe registrar la solicitud de inactivación del usuario en la mesa de ayuda de Informática, y en caso de requerirse inactivación inmediata, deberá informar a través de llamada telefónica.

- **Control actualización de usuarios:**
  - Mínimo una vez al mes, el analista designado por el área de Informática verificará con el sistema de Nómina que los usuarios que ya no trabajan en la Clínica tengan inactivo su usuario en los diferentes sistemas de información a los que tenía acceso.
- **Manejo de claves de acceso a los sistemas de información:**
  - Se recomienda que las claves de acceso a los sistemas de información sean mínimo de 8 caracteres, uno de ellos en mayúscula, al menos un número y un carácter especial.

- Las contraseñas son personales e intransferibles y deben cambiarse periódicamente por el usuario. Mientras los sistemas de información lo permitan, se configurarán para que el usuario deba cambiar su contraseña como mínimo cada 3 meses.
- Si al usuario se le olvida su clave o contraseña, deberá colocar una solicitud en la mesa de ayuda de Informática para poder cambiarla. Mientras los sistemas lo permitan, se colocará por default el número de identificación del usuario como contraseña. Corresponde al usuario cambiar la clave una vez ingrese al sistema.

5.2. GESTIÓN DE ACCESO FÍSICO

La información generada en la clínica Soma se encuentra almacenada en su mayoría en medios electrónicos, sin embargo, se dispone de información física en menor proporción, que igualmente debe ser custodiada.

A continuación, se describe las normas generales para el acceso físico de la información.

a) Archivo Clínico y Administrativo

El archivo clínico y administrativo, por ser un lugar dentro de la institución con unas características de infraestructura especial y diferente al resto de la empresa, requiere de unas disposiciones reglamentarias particulares, a saber:

- Se restringe la circulación de personal no autorizado por las instalaciones físicas del archivo, para garantizar la confidencialidad, seguridad y custodia de la información contenida en la historia clínica y demás registros almacenados.
- El acceso físico a las historias clínicas estará permitido solo al personal autorizado según la Resolución 1995 de 1999 y demás normas que la regulen o modifiquen.
- La Dirección Administrativa y Financiera debe garantizar la infraestructura necesaria y acorde a los estándares de habilitación y los lineamientos del Archivo General de la Nación para que el archivo cumpla con las condiciones de almacenamiento, aireación, disposición y seguridad de la información.
- Las historias clínicas físicas son enviadas a un ente externo llamado Iron Mountain para su custodia y conservación, quienes recogen la información a necesidad de la Clínica (generalmente cuando se dispone de aproximadamente 30 cajas) para ser almacenada en sus bodegas. La información entregada al tercero se encuentra disponible para la clínica a través de una plataforma administrada por éste o mediante solicitud para que envíen a la Clínica, los documentos originales.

b) Cuarto de servidores y concentradores

- No se permite el acceso al centro de cómputo de personas ajenas a la institución, a no ser que sea para fines de revisión de infraestructura y deberá estar acompañado con un funcionario del área de Informática.
- Está estrictamente prohibido el ingreso de alimentos y/o bebidas al centro de cómputo.
- Cada equipo **de cómputo debe estar conectado a un regulador de voltaje para garantizar la estabilidad de la energía o a una UPS** para regular la energía y suprimir los picos de voltaje, así como garantizar la continuidad de la operación en caso de falla de energía
- Los servidores deberán estar en un lugar con temperatura entre 17 y 20 grados centígrados.
- El centro de cómputo debe encontrarse en un área cerrada donde no entre polvo ni humedad. Mínimo una vez al mes, deberá asearse el área y debe hacerse en compañía de uno de los funcionarios de Informática. Lo mismo aplica para los centros de cableado.
- Debe garantizarse que los servidores se encuentren instalados en muebles adecuados para ello.
- La iluminación debe ser apropiada para evitar reflejos en las pantallas y se debe evitar la incidencia directa del sol sobre los equipos.
- La iluminación no debe alimentarse de la misma fuente que la de los equipos de cómputo.

c) Gestión Humana:

Al igual que el archivo clínico, se hace imprescindible la adecuación de un espacio físico para el almacenamiento y custodia en forma segura de las hojas de vida de los clientes internos y se debe garantizar el cumplimiento de las siguientes normas:

- Los tiempos de conservación de las hojas de vida quedarán estipulados por la normatividad vigente y por lo establecido en las Tablas de Retención Documental (TRD).
- Toda la información generada en esta dependencia debe ajustarse al nivel de restricción de la información que corresponda, según el caso.
- La solicitud de información por parte de los usuarios estará sujeta a los procesos y procedimientos diseñados para tal fin y se respetaran los plazos para la entrega de la misma.
- Las hojas de vida de los clientes internos deberán permanecer en lugar seguro y de acceso restringido, con la infraestructura necesaria para la conservación, almacenamiento y custodia.

5.3. GESTIÓN DE RECURSOS INFORMÁTICOS

Son considerados recursos informáticos, cualquier aplicación, herramienta, componente o dispositivo que se puede agregar a una computadora o sistema; por lo tanto, puede ser tanto un recurso de hardware (dispositivos) como de software (programas).

a) Hardware

El Hardware se refiere a las partes físicas, tangibles, de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como: monitor, CPU, teclado, mouse, parlantes, impresoras, escáner, lectores de códigos de barras, entre otros. Las siguientes son algunas consideraciones para tener en cuenta con el Hardware:

- Los computadores instalados en la institución son de uso exclusivo del personal de la Clínica para el desarrollo de sus funciones y, por tanto, no pueden ser usados para actividades diferentes.
- Se solicita a los empleados, abstenerse de alterar o dañar las etiquetas de identificación de cualquier equipo computacional y sus periféricos.
- Es responsabilidad de los colaboradores, velar porque los equipos de cómputo instalados en áreas comunes no sean utilizados por personal externo a la Clínica.
- Por protocolo se tiene establecido efectuarle mantenimiento preventivo 2 veces al año a los equipos propiedad de la Clínica, siempre y cuando su garantía no esté vigente.
- En los mantenimientos preventivos y correctivos de los equipos, se verifica la existencia de programas o información para adultos y de encontrarla, se elimina del equipo y se deja constancia de lo encontrado
- A efecto de evitar el deterioro de los equipos de cómputo, el cliente interno deberá tener en consideración las reglas básicas de su cuidado, las que se indican a continuación:

  - ✓ No ingerir, ni dejar alimentos y/o bebidas cerca y/o encima de los equipos.
  - ✓ Facilitar la ventilación del equipo, no colocar papeles u otros objetos cerca de las ranuras de ventilación del equipo.
  - ✓ No colocar objetos pesados, encima de la unidad central de proceso (CPU), a fin de evitar su deterioro o maltrato.
  - ✓ Mantener alejados de la CPU y monitor (pantalla) todo elemento electromagnético como imanes, teléfonos, radios, etc.
  - ✓ No colocar la Unidad Central de Proceso (CPU), en el piso o lugares inestables y/o expuestos a ser golpeados involuntariamente.
  - ✓ No trasladar ni mover los equipos y/o periféricos de un lugar a otro, de ser necesario, el traslado, deberá colocarse un requerimiento al área de Informática.
  - ✓ Está prohibido abrir los equipos de cómputo.
  - ✓ Conservar limpio el teclado, monitor y mouse mediante limpieza externa.
  - ✓ Conservar los cables en buen estado, ordenados y correctamente conectados; no debe existir ningún tipo de tensión y evitar doblarlos.
  - ✓ Tratar los teclados con cuidado y abstenerse de humedecerlos.
  - ✓ No colocar la punta de los dedos, lapiceros u objetos metálicos en el vidrio del monitor para señalar la pantalla.
  - ✓ Ubicar y mantener el equipo alejado del polvo y la luz solar directa.
  - ✓ No conectar ventiladores, cafeteras u otros aparatos con motor eléctrico en los mismos enchufes o líneas de los equipos de cómputo.
  - ✓ Se recomienda no sacar los portátiles de las oficinas de la Clínica SOMA, pero de ser absolutamente necesario, debe estar autorizado por el jefe inmediato y se recomienda llevar a cabo las siguientes acciones previo al retiro del equipo:
    - Analizar si realmente es necesario o existen otras alternativas.
    - Si realmente es necesario retirar el equipo de la oficina, asegúrate de tener copia de los datos más relevantes y guardarla en un lugar seguro.
    - Tomar nota del número de activo del equipo.
    - Verificar con el responsable de los activos fijos de SOMA que el equipo se encuentre debidamente asegurado.
    - Garantizar que el dispositivo se encuentre configurado con una contraseña de encendido.

- ✓ Cuando estés fuera de la oficina, es importante:
  - Portar el equipo en una mochila o bolso.
  - Ubicar el portátil o equipo en un lugar oculto, que no sea fácilmente visible.
  - Vigilar constantemente el portátil o componente tecnológico.
- ✓ En caso de hurto, se hace necesario llevar a cabo las siguientes acciones:
  - Notificar del robo al jefe inmediato, a Informática a través del celular de la disponibilidad y a Contabilidad mediante correo electrónico.
  - Si el equipo es alquilado o rentado, el personal de informática deberá notificar del suceso al proveedor.
  - El auxiliar de soporte técnico deberá cambiar las claves e inactivar todas las cuentas de usuario a que se diera lugar.
  - El usuario responsable del equipo deberá colocar el denuncio ante la autoridad competente y entregar una copia del denuncio al auxiliar de soporte técnico para que archive dicha copia del denuncio en la carpeta física destinada para ello
  - El área de Activos Fijos después de analizar si es favorable o no para la Clínica, deberá notificar del robo ante la aseguradora.
- ✓ No se autoriza la conexión de portátiles personales a la red de SOMA y mucho menos se garantiza su funcionamiento. De ser necesario y con la debida autorización, se hará uso de la red WI-FI de invitados disponible en algunas áreas de la Clínica.

b) Software

El software está compuesto por un conjunto de programas que son diseñados para cumplir una determinada función dentro de un sistema, ya sean estos realizados por parte de los usuarios o por las mismas corporaciones dedicadas a la informática.
El concepto de software compone la parte lógica de un sistema de computación, permitiéndole el funcionamiento. Esto quiere decir entonces que no solo los programas son y forman un software, sino que la información del usuario y los datos procesados integran el software, ya que forma parte de él todo componente intangible y no físico. Las siguientes son algunas consideraciones para tener en cuenta con el Software:

- La Coordinación de Informática, es la responsable de la instalación y/o desinstalación del software autorizado en la Institución.
- Se prohíbe la instalación de cualquier tipo de programas en los equipos de la institución por parte del colaborador de SOMA. De requerir un software en especial, deberá hacerse la respectiva solicitud a la Coordinación de Informática.
- La información obtenida y desarrollada en el cumplimiento de las funciones es propiedad intelectual de la institución, la cual no deberá ser distribuida, comercializada ni divulgada.
- No se permite en la institución, el ingreso de copias ilegales o piratas.
- Es de carácter obligatorio hacer una revisión de los medios extraíbles de almacenamiento, con el software antivirus que disponga la institución tales como: CD, DVD, memoria USB, antes de utilizarlos.
- Si el cliente interno detecta alguna anomalía o problema en su computador personal (Software y hardware), debe notificarlo al área de Informática a través de la mesa de ayuda o mediante una llamada telefónica.

- El área de almacén debe velar porque los computadores personales y periféricos asignados a su personal estén debidamente inventariados y con la firma del cliente interno respectivo.
- El cliente interno en ninguna circunstancia debe modificar la configuración de su computador, la dirección IP asignada, el nombre de su usuario y/o grupo de trabajo establecido.
- Está prohibido instalar Software no licenciado, chat (MSN Messenger, ICQ, Yahoo, Messenger, etc.), protectores de pantalla, juegos y otros de carácter similar.
- Está prohibido el uso de WhatsApp para enviar información personal, clínica o confidencial de los usuarios atendidos.

Teniendo en cuenta que la información del usuario y los datos procesados integran el software, ya que forma parte de él todo componente intangible y no físico, a continuación se describen las consideraciones a tener en cuenta con la información que se origina y custodia en la clínica Soma:

- La información almacenada en los equipos asignados a un único usuario deberá cumplir con las siguientes normas:

  - ✓ Los datos generados o procesados por el usuario que requieran ser almacenados por algún tiempo en especial, deberán estar ubicados en una carpeta llamada “SOMA”, ubicada en la raíz del disco “C”.
  - ✓ La información que repose en los equipos de cómputo es propiedad de la Clínica SOMA, motivo por el cual no está autorizado tener información personal almacenada en el dispositivo a cargo.
  - ✓ Toda información almacenada en los equipos de cómputo de la institución y no hecha explícitamente pública, será tratada como confidencial, y se harán todas las adecuaciones posibles por garantizar la privacidad de ésta.
  - ✓ Es responsabilidad del usuario, depurar periódicamente la información almacenada en el equipo.
  - ✓ Los equipos asignados a grupos de personas no deberán tener información almacenada en ellos y mucho menos información clínica de los pacientes, gráficos, imágenes y notas en WordPad.
  - ✓ La información contenida en el sistema no se podrá recolectar, almacenar, procesar ni divulgar de manera fraudulenta o ilegal, ni utilizarse para fines contrarios a los previstos en la Constitución Política y la ley.
  - ✓ La información reportada al sistema debe ser completa, veraz y actualizada, de manera que muestre la situación real del dato, lo que comprende no sólo su estado actual, sino los datos históricos.
  - ✓ La información contenida en el sistema se manejará con los controles técnicos y humanos tendientes a impedir su deterioro, pérdida, alteración, consulta o uso no autorizado o fraudulento.

c) Copias de respaldo

Es responsabilidad del área de informática, garantizar la copia de respaldo de la siguiente información:

Bases de datos

Correspondientes a los sistemas de información desarrollados por el área o adquiridos por la Clínica a través del área de Informática para el desempeño de las funciones del personal, entre ellos:

- ✓ Sistemas ERP (Hosvital y Servinte)
- ✓ Nómina
- ✓ Intranet
- ✓ Aviso
- ✓ Bitácora
- ✓ Pretriage
- ✓ Hoja de ruta
- ✓ Medicamentos de control
- ✓ Entre otros

Periodicidad: De acuerdo con la criticidad de la información

Rotación: Mensual

- **Programas**

  Se garantiza la copia de las dos últimas versiones de cada uno de los programas que se tienen en producción, esto es, la versión de producción y la versión que anteriormente se tenía en producción para los desarrollos realizados por el área de Informática y adquiridos a través de ella.

  Periodicidad: mínimo una vez al mes y cada que haya cambio de versión.

- **Servidores**

  Se dispone de servidores de contingencia para las aplicaciones más críticas, las cuales ponen en riesgo la continuidad operativa de la clínica. Son ellos:

  - ✓ Servidor de dominio
  - ✓ Servidor de aplicaciones y base de datos de ERPs y Nómina

  Periodicidad: Disponibilidad inmediata

- **Carpetas compartidas**

  Se generará una vez al mes, respaldo de la información contenida en las carpetas compartidas ofrecidas de manera oficial por el área de Informática.

  Rotación: bimensual

- **Información compartida en los portátiles y PC´s a cargo de los empleados de SOMA**

  La generación de la copia de respaldo (backup) de los PC o portátiles, debe tener una periodicidad, según la importancia de la información a respaldar y de la frecuencia con que

cambia. Esta función es responsabilidad del usuario a quien se le asigne el equipo de cómputo y no del área de Informática, por tal motivo, el área de Informática no se hace responsable de pérdida de datos. Para realizar la copia se debe tener en cuenta en **"Instructivo cómo realizar el backup a los equipos informáticos (IN-IC-02**)".

Rotación: Se recomienda semanal como mínimo

Se hace necesario, implementar procedimiento de restauración de datos, al menos dos veces al año, de manera tal que se garantice la disponibilidad de la información en el momento en que se requiera.

d) Planes de contingencia

El área de Informática ha implementado un plan de contingencia, con el fin de garantizar la continuidad en la operación de sus procesos cuando se presente un mal funcionamiento en los sistemas de información. Este plan de contingencia se encuentra detallado en el manual **"MN-IC-03 – Plan de contingencia de sistemas de información"**

5.4. GESTIÓN DEL CAMBIO DE RECURSOS DE TI Y CONTROL DE CAMBIOS EN APLICATIVOS

La gestión del cambio de recursos de TI busca facilitar y lograr la implementación exitosa de los procesos de transformación, trabajando con y para las personas en la aceptación y asimilación de los cambios para garantizar la continuidad del negocio. Cuando se aplica a los recursos de TI, implica cualquier cambio en los recursos de software y hardware. Es responsabilidad del área de Informática asegurar que todo cambio esté registrado, planificado, probado, socializado y evaluado antes de ser autorizado, según lo definido en el "**Manual de Gestión del Cambio (MN-PE-02)**".

Para garantizar el éxito, es necesario considerar lo siguiente:

- Todo cambio debe ser liderado por el integrante de Informática a cargo del sistema, equipo o dispositivo a cambiar.
- Se debe diligenciar el formato "**Gestión de Cambio (FO-GH-19)**" para evaluar y gestionar los riesgos que genera el cambio de recursos informáticos.
- Es crucial definir la priorización del cambio:
  - ✓ Estándar: propio del sistema, equipo o dispositivo; no es prioritario.
  - ✓ Urgente: resuelve un problema mayor que afecta la continuidad del negocio a nivel de seguridad o financiero.
  - ✓ Baja: cambio de bajo riesgo.
- Deben anexarse al formato mencionado los siguientes documentos:
  - ✓ Casos de prueba diligenciados y aprobados por los usuarios líderes, si aplica.
  - ✓ Listado de correcciones y mejoras implementadas en la nueva versión y que se espera poner en producción.
  - ✓ Listado de actividades a llevar a cabo en caso de requerir devolver la actualización.
  - ✓ Registro de capacitación, si es necesario.

- ✓ Recursos requeridos.
- ✓ Riesgos.

- El cambio debe ser aprobado mediante reunión con los involucrados.
- Solo si el cambio es aprobado, podrá ponerse en producción.
- Se debe notificar el cambio a los usuarios del sistema, equipo o dispositivo a través de todos los medios de comunicación disponibles.
- Después del cambio, se deben evaluar los resultados y extraer lecciones aprendidas.
- La información del cambio se almacenará en un directorio a cargo de Informática y será consultable por las personas relevantes.

Control de Cambios en Aplicativos

Este proceso estructurado se enfoca en la planificación, implementación y evaluación de cambios en aplicativos, asegurando la estabilidad y eficiencia operativa. Desde la solicitud inicial hasta el registro detallado, este enfoque integral garantiza una gestión efectiva de modificaciones, minimizando riesgos y asegurando la continuidad de los aplicativos en un entorno dinámico.

1. **Solicitud de Cambio:**
   a. Todos los cambios en aplicativos deben iniciarse mediante una solicitud formal en el aplicativo GLPI.
   b. La solicitud debe incluir detalles sobre el propósito, alcance, impacto potencial, recursos requeridos y cronograma esperado.
   c. La solicitud debe ser aprobada por el propietario del aplicativo y otras partes interesadas relevantes, cuando sea necesario.

2. **Evaluación de Impacto:**
   a. Se realiza una evaluación de impacto para determinar la complejidad y el alcance del cambio.
   b. Se identifican posibles riesgos y se desarrollan estrategias de mitigación.
   c. La evaluación incluye consideraciones de seguridad, rendimiento y compatibilidad con otros sistemas.

3. **Planificación del Cambio:**
   a. Se elabora un plan detallado que incluye todas las actividades necesarias para la implementación del cambio.
   b. Se designa un responsable del cambio y se establecen roles y responsabilidades claros.
   c. Se comunica el plan a todas las partes interesadas relevantes.

4. **Pruebas del Cambio:**
   a. Se realizan pruebas exhaustivas para garantizar que el cambio no afecte negativamente el funcionamiento del aplicativo.
   b. Las pruebas deben abarcar casos de uso normales y escenarios de uso inesperados.
   c. Se documentan los resultados de las pruebas y se obtiene la aprobación del equipo.

5. **Implementación del Cambio:**

a. La implementación se lleva a cabo según el plan previamente establecido.
b. Se realiza un seguimiento en tiempo real para detectar posibles problemas y garantizar una implementación sin contratiempos.
c. Se dispone de un mecanismo para revertir el cambio en caso de emergencia.

6. **Validación Post-Implementación:**
   a. Se realiza una validación post-implementación para confirmar que el cambio se ha realizado según lo previsto.
   b. Se evalúa la implementación del cambio con los usuarios finales y se abordan posibles problemas surgidos después de la implementación.

7. **Registro de Cambios:**
   a. Se mantiene un registro detallado de todos los cambios mediante el aplicativo GLPI, incluyendo información sobre la solicitud, evaluación de impacto, planificación, pruebas, implementación y validación post-implementación.
   b. El registro sirve como documentación para futuras referencias y auditorías.

5.5. GESTIÓN DE INCIDENTES SOBRE RECURSOS INFORMÁTICOS

Es normal que ocurran incidentes sobre recursos informáticos incluyendo incidentes en la seguridad de la información. Por lo anterior, es importante disponer de una buena gestión de incidentes y cuando ocurra algo, todos los departamentos deben saber cómo actuar.

Para la gestión de incidentes sobre los recursos informáticos, se deberá seguir el proceso definido en el **Manual Gestión del riesgo (MN-CI-01)**, el cual, en términos generales busca identificar la probabilidad de ocurrencia de un daño o pérdida como materialización de una amenaza.

5.6. CONTROL DE ACTIVIDADES EN LA RED

La información institucional puede ser trasmitida y almacenada a través de diferentes medios de comunicación y herramientas informáticas, las cuales deben ser adecuadamente controladas y manejadas para garantizar la confidencialidad y evitar la pérdida o fuga de información. Para esto, se debe tener en cuenta lo siguiente.

a) Uso de buzones de correo

- Los buzones de correo se crearán de manera genérica de acuerdo con el cargo desempeñado por el funcionario a quien estará destinado.
- Los buzones de correo serán asignados por la Clínica SOMA, a aquellos funcionarios que lo requieran para el desempeño de sus funciones y podrán ser asignados a un funcionario específico o a un grupo de personas dependiendo de la necesidad.
- El uso de correo personal para el manejo de información institucional está prohibido.
- Los usuarios y contraseñas de correo son personales y no deben compartirse con nadie, a menos que las funciones así lo ameriten y el buzón sea compartido por un grupo de trabajo.

- Se solicita no abrir correos electrónicos de dudosa procedencia, si recibe uno de estos correos debe notificarse al área de Informática.
- El servicio de correo electrónico es para uso exclusivo de envío y recepción de información concerniente a las funciones que el cliente interno cumple para la institución. Por lo tanto, esta información forma parte del activo de la institución.
- Está prohibido el envío de información personal y clínica de los usuarios a través de correos electrónicos personales. De ser necesario, deberá hacerse uso de los correos institucionales destinados y autorizados para tal fin.
- Cambia tu contraseña periódicamente y crea contraseñas difíciles de ser descifradas, es esencial cambiarlas periódicamente, cada tres meses por lo menos. Ya que, si alguien consigue descubrir la contraseña de tu e-mail, por ejemplo, podrá leer tus mensajes sin que lo sepas, sólo para espiarte. Al cambiar tu contraseña, el espía ya no podrá acceder a tu información personal.
- El tamaño de los buzones de correo institucionales es de poca capacidad (máximo 30 MB), motivo por el cual, para garantizar su correcto desempeño se hace necesario mantenerlo depurado, evitando que los mensajes reboten por falta de espacio en ellos, lo cual es responsabilidad del dueño del buzón.
- Ningún funcionario debe utilizar su correo personal para el envío y recibo de información relacionada con las funciones desempeñadas en su trabajo.
- Los funcionarios deben mantener sus buzones depurados.
- No se debe permitir la entrada ni salida de archivos ejecutables de aplicaciones, música, videos y presentaciones personales.
- Se prohíben las cadenas de mensajes de cualquier tipo y la propaganda de tipo comercial, político o religioso, entre otros y, cualquier contenido ofensivo para los empleados de la Clínica.
- Hacer un buen uso del correo corporativo puede traducirse en optimización del tiempo, control en el desarrollo de actividades y efectividad en las tareas, por lo anterior, es importante seguir las siguientes recomendaciones:
  - ✓ Darles a todos los correos la categoría de ‘urgente’ puede generar un efecto negativo; pues, cuando realmente se envía un correo con esta característica, nadie le va a prestar atención.
  - ✓ Si está respondiendo un correo, asegúrese de ‘responder a todos’, solo si la respuesta es necesaria para el grupo.
  - ✓ Cuando redactes un correo electrónico para ser enviado a varias personas, incluye en el campo” Para”, sólo a quienes quieres dirigirte directamente y a los demás que sólo lo van a recibir a modo informativo, agrégalos en el campo CC (con copia).
  - ✓ Si bien el tono de los mensajes muchas veces refleja la relación con el destinatario, no hay que ser demasiado informales, pues se puede pasar por poco profesional. También es importante ser directos y no “adornar” mucho la información.
  - ✓ Además del protocolo de envío o respuesta de un correo, proteger la seguridad es importante. Pensar en claves de acceso difíciles, activar la verificación en dos pasos y cualquier otro sistema de control de seguridad es clave para proteger la información corporativa.
  - ✓ Antes de pulsar “Enviar”, haz una revisión general del mensaje, verifica que no tenga faltas de ortografía, que el lenguaje sea el adecuado y que esté incluida tu firma. También, cerciórate de haber adjuntado los archivos correctos y si deseas enfatizar

alguna palabra o idea, no la escribas en mayúscula, utiliza la opción Subrayar o Negrita.

- ✓ Incluye siempre en el asunto una idea que resuma el tema del cual se va a hablar. Enviar un correo electrónico sin asunto o no especificado sólo le va a restar importancia al mensaje y es probable que el destinatario decida no abrirlo.
- ✓ Sé breve y da un amplio contexto al mensaje. Para que se lea y se entienda, es preferible usar oraciones cortas y precisas. Si el mensaje es largo, divídelo en muchos párrafos para que sea más fácil de leer. Un texto preciso, bien estructurado, ayuda a evitar malentendidos o confusiones. Se puede enviar un mensaje a otros usuarios rápida y fácilmente. Utiliza un lenguaje apropiado y evita el humor, el sarcasmo y los insultos fuera de lugar. Para beneficiar a los destinatarios profesionales, es útil comenzar un mensaje con una de las siguientes frases: Para su información, Para su aprobación, seguimiento, entre otros.
- ✓ Evita usar letras mayúsculas. El texto escrito en mayúscula es difícil de leer. Es más, usar palabras en letras mayúsculas en Internet sugiere que está expresando emociones fuertes (tales como alegría o enojo), lo que puede no ser bien visto por el destinatario. Para enfatizar un término, escríbelo entre comillas.
- ✓ Procura mantener limpia la bandeja de entrada organizando los mensajes por carpetas y utilizando filtros para evitar spam.
- ✓ Sí tardas más de media hora en redactar un correo para dar una información simple o hacer una pregunta, ten en cuenta que quizá sea más efectivo dirigirse directamente a la persona o hacerle una llamada y tener una conversación de 5 minutos.
- ✓ Revisa de forma periódica la bandeja de correo no deseado para que no pases por alto alguna información importante que se haya filtrado allí por error.
- ✓ Sé cuidadoso al iniciar sesión en computadores diferentes a los corporativos, algunos de ellos pueden estar infectados para almacenar los datos que se generan.
- ✓ Evita usar tu cuenta de correo corporativa para asuntos personales y no la publiques en foros o sitios web si no es necesario. Esto le facilita a los spammers capturar tu cuenta e incluirla en sus listas de envíos masivos de spam y correos maliciosos.
- ✓ Antes de enviar un mensaje asegúrate de que tenga el adjunto, si aplica.
- ✓ Agrega como máximo de dos a tres archivos cuyo tamaño no sea demasiado grande, ya que el mensaje podría no salir de tu bandeja o ser recibido por el destinatario si los buzones tienen un límite inferior de capacidad de lo que pesan los archivos.
- ✓ No abra correos electrónicos de dudosa procedencia o no deseados y mucho menos los contestes ni haz clic en ningún enlace incluido en el mensaje. Los correos electrónicos no deseados usan una gran variedad de títulos atractivos para conseguir que el destinatario los abra. Muchos usuarios a menudo cometen el error de abrir estos correos electrónicos o ejecutar un adjunto malicioso o hacer clic en el link incluido en el propio mensaje. Ten especial cuidado en **no abrirlos y de eliminar directamente** aquellos correos en los que:

    - Nos informen:
        - Que hemos ganado en cualquier tipo de lotería o sorteo o que vamos a recibir cualquier tipo de premio.
        - De reyes o príncipes de Nigeria tratando de enviarnos una enorme cantidad de dinero.
        - De algún tipo de herencia sin reclamar.

- Que hemos ganado cualquier tipo de dispositivo electrónico u oferta sospechosa.

- Cualquier otro tipo de correo que nos resulte altamente sospechoso y que provenga de remitentes desconocidos o en los que:
  - Se visualice un logotipo que parece distorsionado o estirado.
  - Tenga textos que se refieran a nosotros como “estimado cliente” o “estimado usuario” en lugar de incluir nuestro nombre real.
  - Se nos advierta que una cuenta nuestra se cerrará a menos que confirmemos nuestra información inmediatamente.
  - Aparezcan frases que vengan de una cuenta de correo similar, pero diferente a una que la compañía real que nos envía el correo usa normalmente.
  - Aparezcan mensajes que informan de “amenazas a la seguridad” y requieren que actuemos inmediatamente.

- ✓ Debes hacer tu mejor esfuerzo para responder tus mensajes de correo de trabajo lo más rápido posible, ya que esto refleja la actitud de servicio al cliente que existe en la compañía.
- ✓ Cuando hayas leído un mensaje, decide inmediatamente dónde guardarlo. Los correos electrónicos se pueden administrar de la misma manera que el correo tradicional. Para encontrar un mensaje fácilmente, acostúmbrate a colocar los mensajes recibidos en carpetas por temas. De esta manera, será más fácil encontrar un mensaje viejo o las partes de un debate. Algunos clientes de correo electrónico permiten asignar un color al mensaje. Puede ser útil asignar un código de color para identificar ciertas categorías de mensajes.
- ✓ Excepto que sea necesario, no imprimas los correos electrónicos. Cuando el correo electrónico está guardado correctamente, se podrá encontrar fácilmente si se lo necesitas. Por esta razón, es inútil imprimir todos los correos electrónicos. Esto evita desperdiciar papel y ayuda a preservar el ambiente.
- ✓ Respeta la privacidad de los mensajes que recibes. Nunca envíes o copies a otros un correo electrónico que te fue enviado sin el consentimiento del remitente original.
- ✓ Abstente de reenviar o compartir información confidencial como: reportes financieros, porcentajes de aumento de sueldos, bonos u otro tipo de compensaciones económicas, detalles altamente sensibles sobre negociaciones laborales o comerciales, y toda información que pueda generar especulaciones, incertidumbre o inclusive que pueda causar desestabilidad en tu entorno.
- ✓ Si un mensaje de correo de estas características cae en manos equivocadas, podrías enfrentar graves repercusiones, incluso problemas legales.
- ✓ Cuando se llega al límite de memoria del correo el sistema no permite ni enviar, ni recibir correos. Una sencilla solución para liberar espacio, en la Bandeja de Entrada, es crear archivos conocidos como .PST.
- ✓ Las carpetas .PST funcionan como un cajón adicional que almacena correos importantes en un espacio en el disco duro de los equipos. Básicamente, usted pasa mails que no quiere perder de la Bandeja de Entrada al nuevo espacio, liberando memoria para poder enviar y recibir correos.

b) Carpetas compartidas

Buscando facilitar el acceso a información general e importante para todos los funcionarios de la Clínica SOMA, se ha creado en uno de los servidores, un directorio específico para cada una de las coordinaciones y para el sistema de gestión de la calidad.

Dichas carpetas se caracterizan porque:

- Tienen asignado un espacio limitado de disco duro.
- Se identifican con el nombre de cada una de las áreas o de la función a realizar.
- Se les otorga acceso a los usuarios a cada una, dependiendo de la información en ellas consignada.
- Es responsabilidad del área de Informática generar las copias de la información almacenada en ellas.

c) Internet

- La asignación de acceso a Internet debe ser solicitada a la Coordinación de Informática con la debida autorización del jefe inmediato.
- Se restringirá automáticamente el acceso a Internet a los clientes internos que naveguen en páginas NO PRODUCTIVAS (Páginas de Adultos, Chat, etc.).
- Evita los enlaces sospechosos: uno de los medios más utilizados para direccionar a las víctimas a sitios maliciosos son los hipervínculos o enlaces. Los enlaces pueden estar presentes en un correo electrónico, una ventana de chat o un mensaje en una red social: la clave está en analizar si son ofrecidos en alguna situación sospechosa (una invitación a ver una foto en un idioma distinto al propio, por ejemplo), provienen de un remitente desconocido o remiten a un sitio web poco confiable.
- Acceder a sitios web de dudosa reputación: a través de técnicas de Ingeniería Social, muchos sitios web suelen promocionarse con datos que pueden llamar la atención del usuario como descuentos en la compra de productos (o incluso ofrecimientos gratuitos), primicias o materiales exclusivos de noticias de actualidad, material multimedia, etc. Es recomendable para una navegación segura que el usuario esté atento a estos mensajes y evite acceder a páginas web con estas características.
- Asegúrate de que el sistema operativo y aplicaciones estén actualizadas: Corresponde al área de Informática, mantener actualizados con los últimos parches de seguridad no sólo el sistema operativo, sino también el software instalado en el sistema a fin de evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema.
- No descargar aplicaciones desde sitios web no oficiales. Muchos sitios simulan ofrecer programas populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware y descargan el código malicioso al momento que el usuario lo instala en el sistema.
- Utilizar tecnologías de seguridad: las soluciones antivirus, firewall y antispam representan las aplicaciones más importantes para la protección del equipo ante la principales amenazas que se propagan por Internet. Utilizar estas tecnologías disminuye el riesgo y exposición ante amenazas.
- Evitar el ingreso de información personal en formularios dudosos: cuando el usuario se enfrente a un formulario web que contenga campos con información sensible (por ejemplo, usuario y contraseña), es recomendable verificar la legitimidad del sitio. Una buena estrategia

es corroborar el dominio y la utilización del protocolo HTTPS para garantizar la confidencialidad de la información. De esta forma, se pueden prevenir ataques de phishing que intentan obtener información sensible a través de la simulación de una entidad de confianza.

- Tener precaución con los resultados arrojados por buscadores web: a través de diferentes técnicas, los atacantes suelen posicionar sus sitios web entre los primeros lugares en los resultados de los buscadores, especialmente en los casos de búsquedas de palabras clave muy utilizadas por el público, como temas de actualidad, noticias extravagantes o temáticas populares (como, por ejemplo, el deporte y el sexo). Ante cualquiera de estas búsquedas, el usuario debe estar atento a los resultados y verificar a qué sitios web está siendo enlazado.
- Aceptar sólo contactos conocidos: tanto en los clientes de mensajería instantánea como en redes sociales, es recomendable aceptar e interactuar sólo con contactos conocidos. De esta manera se evita acceder a los perfiles creados por los atacantes para comunicarse con las víctimas y exponerlas a diversas amenazas como malware, phishing, cyberbullying u otras.
- Evitar la ejecución de archivos sospechosos: la propagación de malware suele realizarse a través de archivos ejecutables. Es recomendable evitar la ejecución de archivos a menos que se conozca la seguridad del mismo y su procedencia sea confiable (tanto si proviene de un contacto en la mensajería instantánea, un correo electrónico o un sitio web). Cuando se descargan archivos de redes, se sugiere analizarlos de modo previo a su ejecución con una solución de seguridad.
- Utilizar contraseñas fuertes: muchos servicios en Internet están protegidos con una clave de acceso, de forma de resguardar la privacidad de la información. Si esta contraseña fuera sencilla o común (muy utilizada entre los usuarios) un atacante podría adivinarla y por lo tanto acceder indebidamente como si fuera el usuario verdadero. Por este motivo se recomienda la utilización de contraseñas fuertes, con distintos tipos de caracteres y una longitud de al menos 8 caracteres.
- Como siempre, las buenas prácticas sirven para aumentar el nivel de protección y son el mejor acompañamiento para las tecnologías de seguridad. Mientras estas últimas se encargan de prevenir ante la probabilidad de algún tipo de incidente, la educación del usuario logrará que este se exponga menos a las amenazas existentes, algo que de seguro cualquier lector deseará en su uso cotidiano de Internet.
- Usa navegadores diferentes, si eres usuario de Windows, tal vez tengas el hábito de utilizar el navegador Internet Explorer. El problema es que existe una infinidad de plagas digitales (spywares, virus, etc.) que exploran problemas de seguridad de ese navegador. Por esto, una acción importante es utilizar navegadores como Chrome o Firefox, pues, aunque éstos también puedan ser atacados por plagas, sucede con una frecuencia menor que para el Internet Explorer.

d) Conexión VPN (Virtual Private Network)

Las conexiones VPN tienen como objetivo facilitar el acceso a los sistemas de información disponibles en la Clínica SOMA de manera oportuna y segura desde lugares externos a la Clínica a través de internet, evitando así, ampliar las instalaciones físicas o lugares de trabajo por parte de personal externo o el desplazamiento físico del personal de apoyo a los procesos.
Se tienen las siguientes restricciones, buscando garantizar la conexión:

- La conexión VPN se brindará a los usuarios por un tiempo máximo de 1 año.
- La empresa a la cual se le brinda el acceso VPN deberá entregarle a la Clínica una copia de la política de tratamiento y protección de datos personales emitida por ella.
- Cada uno de los usuarios a conectarse vía VPN e incluso el representante de la empresa a la que pertenece el usuario, deberá firmar el **"Acuerdo de confidencialidad y buen uso de la información diseñado por la Clínica (FO-IC-22)"**.
- Si se evidencia que el usuario está haciendo mal uso de la VPN, se le desactivará el servicio.
- El usuario a quien se le dará acceso vía VPN deberá diligenciar el acuerdo de confidencialidad.
- Todo cambio requerido por el usuario VPN, deberá ser tramitado por el coordinador del área responsable de la conexión, no por el proveedor o tercero contratado. La coordinación de informática no atenderá ninguna solicitud directa por parte del usuario.
- Cualquier cambio en el perfil del usuario al que se le dará el acceso VPN, requiere diligenciar el formato "**Solicitud conexión vpn usuarios externos (FO-IC-28)**".
- Se debe garantizar que todo contrato firmado tenga lo correspondiente a la confidencialidad, tratamiento y protección de datos personales.

Con las conexiones VPN, se presentan los siguientes riesgos:

- Que se le otorgue al usuario a conectarse por VPN mayores privilegios a los requeridos. Riesgo que pretende minimizar mediante el uso del formato diseñado para solicitar la conexión VPN y ser muy específicos en detallar los accesos a los aplicativos.
- Que el equipo desde el que se conecte el usuario de VPN esté infectado con virus.
- Que el usuario utilice incorrectamente los aplicativos a que tiene acceso.
- Que la conexión siga activada y el usuario ya no labore para SOMA, para lo cual se garantiza:
    - La vigencia de la conexión será máxima de un año
    - Instruir al coordinador del área para que le notifique al área de informática cuando finalice el contrato con el usuario al que se le brindó la VPN
    - Estar monitoreando la actividad de los usuarios en la VPN

Se implementan entonces, los siguientes mecanismos de prevención:

- Para evitar el contagio, se hace necesario garantizar que se tenga un fireware y antivirus instalado en el servidor donde se encuentran los aplicativos, así como exigirle al proveedor que tenga instalado en su computador un buen programa de antivirus.
- Debe garantizarse entonces que el coordinador del área quien solicita la conexión VPN haya capacitado al usuario quien la utilizará, en los aplicativos a acceder

El procedimiento para obtener una conexión VPN es el siguiente:

- El coordinador del área que requiere la conexión VPN deberá diligenciar el **"Solicitud conexión VPN usuarios externos (FO-IC-28)"**, según la cantidad de usuarios que requieran la conexión VPN.
- Debe registrar la solicitud en el aplicativo de la mesa de servicio del área de informática y anexar el formato.

- El auxiliar de soporte técnico deberá crear y configurar el perfil del nuevo usuario VPN en los servidores a que se diera lugar para garantizar el acceso de acuerdo con los estándares definidos por el área. Deberá colocar como fecha de inactivación: 1 año
- El auxiliar de información deberá crear el usuario en los diferentes aplicativos a que se diera lugar según la solicitud y asignarle los permisos respectivos.
- El auxiliar de soporte técnico deberá instalar o instruir al usuario para que instale y configure en el equipo desde el cual se conectará, los programas requeridos para ello según instructivo y hacer pruebas de conexión con el usuario.

5.7. MONITOREO DE PROGRAMAS MALICIOSOS Y DETECCIÓN DE INTRUSOS

Desafortunadamente, millones de computadoras se encuentran continuamente a la merced de individuos, también conocidos como “hackers”, que utilizan programas maliciosos diseñados específicamente para atacar, dañar y obtener información ilegalmente a través de la Internet. Una solución a este problema es la instalación de programas diseñados exclusivamente para proteger los sistemas de las computadoras en contra de estas amenazas. Una combinación de dichos programas acompañado de un buen uso de las computadoras ayuda a proteger, detectar y eliminar la mayoría de estas amenazas (virus informáticos, programas espías, etc.), entre ellos:

- Los programas antivirus, ofrecen detección y eliminación de los programas espías; monitoreo constante y la facilidad de mantener una lista al día de miles de estos programas en la Internet.
- Programas Cortafuegos que se ocupan de limitar, controlar o parar el tránsito de información entre la computadora en el cual residen y todas aquellas computadoras o equipos que se comunican con ella.

De esta manera no podría ser vista por aquellos que se dedican a rastrear la Internet en busca de computadoras a las cuales puedan tener acceso. Medidas de Seguridad en General es un constante trabajo para mantenerse libre de las amenazas de los programas e individuos maliciosos que constantemente azotan la Internet; nosotros mismos debemos de desarrollar y ejercer buen sentido común para prevenir y detectar el peligro.

Dos de los mejores consejos que se pueden seguir para evitar estas amenazas son:

- Nunca habrá un correo electrónico con enlaces a sitios en la Internet o archivo adjunto que provenga de personas que no conozca, lo que tiene que hacer es eliminarlo inmediatamente. Si conoce a la persona, pero no esperaba el mensaje o duda de su contenido, verifique la veracidad del mensaje contactando a la persona que se lo envió; más vale prevenir que tener que lamentarse.
- Mantenga al día su computadora con todos los parches nuevos tanto como para el sistema operativo, así como para los otros programas que residen en la computadora.

Para detectar, informar y bloquear intrusos en la red de la Clínica, se requiere de la implementación de los **IDS** (Sistema de detección de intrusiones), los cuales corresponden a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales

o sospechosas, y de este modo, reducir el riesgo de intrusión. Existen dos claras familias importantes de IDS: el grupo **N-IDS** (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red, y el grupo **H-IDS** (Sistema de detección de intrusiones en el *host*), que garantiza la seguridad en el *host*.

En los últimos tiempos, los **IPS** (Sistema de prevención de intrusiones) están sustituyendo los IDS. Los IPS es un sistema de prevención/protección para defenderse de las intrusiones y no solo para reconocerlas e informar sobre ellas, como hacen la mayoría de los IDS.

En la clínica SOMA, hacemos uso de programas que permiten bloquear el acceso a personas no autorizadas, servidores de dominio, antivirus, cortafuegos, entre otros, y permanentemente, se está monitoreando y ajustando direcciones IP para impedir así su acceso a los servidores.

5.8. AUDITORIAS DE SEGURIDAD DE LA INFORMACIÓN PERSONAL

Anualmente se realizará auditoria a lo definido en el presente documento, y a partir de los resultados obtenidos, se formulará e implementarán planes de mejoramiento por parte de los líderes de proceso, según lo establecido en el **"Modelo mejoramiento continuo de la calidad (MO-MC-01)"**.

Adicionalmente, desde el área de informática se realizarán auditorías para verificar la seguridad de las bases de datos.

6. DEFINICIONES

Backup: es una copia de seguridad a mayor o menor escala. Puede ser una versión reciente de la información contenida en todos los equipos de nuestra compañía, o puede tratarse de servidores completos con grandes cantidades de datos.

BD: Siglas que significan "Base de Datos" y corresponde a una colección de información organizada de manera tal que un programa de computador pueda seleccionar rápidamente los datos que necesite. Una base de datos es un sistema de archivos electrónico.

Conexión VPN: Por sus siglas, Virtual Private Network, es una privada virtual capaz de conectar varios dispositivos como si se encontrasen físicamente en el mismo lugar, emulando las conexiones de redes locales.

Confidencialidad: Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático.
Correo malicioso: Se refiere a cualquier tipo de correo maligno que trata de afectar a un ordenador, un teléfono celular u otro dispositivo. Suelen llegar acompañados con archivos adjuntos que si son descargados pueden hacer que el equipo resulte infectado. Es conocido también como spam, spoofing" (suplantación de identidad) o "password phishing" (suplantación de identidad para obtener contraseñas).

Crakers: Los crackers son personas con avanzados conocimientos técnicos en el área informática y que enfocan sus habilidades hacia la invasión de sistemas a los que no tienen acceso autorizado. En general, los crackers persiguen dos objetivos:

- Destruir parcial o totalmente el sistema.
- Obtener un beneficio personal (tangible o intangible) como consecuencia de sus actividades.

Cyberbullying: El ciberbullying es el uso de los medios telemáticos (Internet, telefonía móvil y videojuegos online principalmente) para ejercer el acoso psicológico entre iguales. No se trata aquí el acoso o abuso de índole estrictamente sexual ni los casos en los que personas adultas intervienen

Dirección IP: Conjunto de números que identifica, de manera lógica y jerárquica a un elemento de comunicación/conexión de un dispositivo (computadora, laptop , teléfono inteligente) que utilice el protocolo o (Internet Protocol).

Disponibilidad: Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.

ERP: El término ERP se refiere a “Enterprise Resource Planning”, que significa “Sistema de Planificación de Recursos Empresariales”. Estos programas se hacen cargo de distintas operaciones internas de una empresa, desde producción a distribución o incluso recursos humanos.

Firewall: Un firewall (llamado también «cortafuego»), es un sistema que permite proteger a una computadora o una red de computadoras de las intrusiones que provienen de una tercera red (expresamente de Internet).

Grupo de usuarios: conjunto de usuarios con visibilidad entre ellos.

Hacker: Los hackers son personas con avanzados conocimientos técnicos en el área informática y que enfocan sus habilidades hacia la invasión de sistemas a los que no tienen acceso autorizado.

HOST: Dispositivos monousuario o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores web, etc.
De forma genérica, podemos decir que un anfitrión es todo equipo informático que posee una dirección IP y que se encuentra interconectado con uno o más equipos y que funciona como el punto de inicio y final de las transferencias de datos.

Integridad: Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.

IT: Abreviación Tecnologías de la Información.

Mecanismo de seguridad informática: técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático.

Password o contraseña: Código secreto compuesto por caracteres numéricos, letras y caracteres especiales que le permiten al usuario generador del mismo, acceder a un archivo, programas o computadoras.

PC: Siglas para referirse al computador personal.

Perfil: nivel de permisos. Define una serie de privilegios, por ejemplo: acceso a la agenda, tener acceso para crear tickets, o ser gestor de proyecto.

Phishing: Consiste en un método fraudulento de capturar información sensible, como números y claves de cuentas bancarias o de tarjetas de crédito.

Protocolo: Un protocolo en informática se refiere a un conjunto de reglas predefinidas con el propósito de estandarizar el intercambio de información en actividades informáticas. Al seguir un mismo protocolo se garantiza que habrá compatibilidad entre los dispositivos en los distintos puntos de un sistema informático.

Servidor de dominio: es un servidor que se encarga de garantizar la autenticación del usuario que está intentando ingresar a la red. Efectúa el proceso de garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, normalmente a través del uso de una contraseña.

Servidor Forti: Es un servidor firewall que se actúa entre una aplicación del usuario y un servidor real. Este servidor intercepta todas las peticiones y lleva a cabo dos funciones: mejorar el rendimiento y servir de filtro para bloquear o denegar las solicitudes al servidor, evitando así que intrusos ingresen a la red.

Seguridad de la información: es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

Seguridad Informática: métodos que buscan procesar almacenar y transmitir la información.

Software malicioso: hace referencia a cualquier tipo de software maligno que trata de afectar a un ordenador, con programas tales como los virus.

SPAM: Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

SPAMMER: Persona o robot que se dedica a hacer spam en Internet. Puede hacerlo con diversos fines, pero su cometido es siempre el mismo: abusar del envío de comunicaciones de cualquier tipo en medios digitales para bombardear a un número concreto de usuarios o cualquiera al que pueda alcanzar.
Spywares: En el mundo de la informática a esto es lo que le llamamos software espía, estos se instalan en nuestro sistema con la finalidad de robar nuestros datos y espiar nuestros movimientos por la red. Luego envían esa información a empresas de publicidad de internet

para comercializar con nuestros datos. Trabajan en modo 'background' (segundo plano) para que no nos percatemos de que están hasta que empiecen a aparecer los primeros síntomas.

Usuario: identificador para acceder a la herramienta. Los usuarios tendrán asociados una o varias combinaciones de perfil + grupo, definiendo el nivel de privilegios que tendrán y para qué grupo, pudiendo ser, por ejemplo, gestor de proyectos en un grupo y operador de tickets en otro.

Virus informático: es un programa (código) que se replica, añadiendo una copia de sí mismo a otro(s) programa(s). Sus principales características son:

- Auto-reproducción: Es la capacidad que tiene el programa de replicarse (hacer copias de sí mismo), sin intervención o consentimiento del usuario.
- Infección: Es la capacidad que tiene el código de alojarse en otros programas, diferentes al portador original.

7. DOCUMENTOS DE REFERENCIA

CÓDIGO	NOMBRE
	No aplica.

8. ANEXOS

CÓDIGO	NOMBRE
	No aplica.

9. CONTROL DE CAMBIOS

VERSIÓN	FECHA	NATURALEZA DEL CAMBIO
01	19/03/2020	N.A
02	30/11/2023	Incluir los controles existentes para los cambios de aplicativos.

ELABORÓ	REVISÓ	APROBÓ
Mauricio Taborda Palacio Coordinador de Información	Gloria López Agudelo Dirección de Calidad y Planeación	Víctor Manuel Blair Llorens Gerente
Firma: 	**Firma:** 	**Firma:** 
Fecha: 30/11/2023	**Fecha:** 30/11/2023.	**Fecha:** 30/11/2023