POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1 Introducción

La información se ha convertido en el activo más importante para cualquier organización dada la rapidez con la que se genera y transmite al mundo, gracias a este comportamiento también se ha incrementado el número de ataques a las empresas sin importar su tamaño o actividad comercial, ocasionando pérdidas económicas y/o de imagen; es así como la seguridad de la información juega un papel importante incrementando las necesidades de crear un conjunto de medidas preventivas y reactivas en las organizaciones y los sistemas tecnológicos que permiten resguardar y proteger dicha información buscando mantener la confidencialidad, disponibilidad e integridad de la misma. Por esa razón Cafesalud EPS reconoce su importancia y comprometido con la protección de la información propia, de afiliados, colaboradores y terceras partes constituye el siguiente documento, teniendo en cuenta el marco legal aplicable de protección de datos personales, la clasificación del acceso a la información (confidencial, sensible, compartible, pública y privada), los servicios provistos por los proveedores de TIC y los análisis de riesgos realizados; define las políticas de seguridad de la información como un marco normativo garantizando la prestación del servicio y atención en salud a sus afiliados.

2 Objetivo

Establecer los lineamientos para proteger la información y los sistemas de información donde se produce y procesa la información de Cafesalud, ante cualquier amenaza que pueda comprometer la confidencialidad, disponibilidad e integridad de dicha información.

3 Alcance

Aplica para todos los colaboradores directos, contratistas y proveedores y su cumplimiento es de obligatoriedad.

4 Política General de Seguridad

CAFESALUD EPS manifiesta su compromiso con la protección de la información y la reconoce como uno activo de alto valor para la organización, y se compromete a la protección de la misma mediante la generación y publicación de sus políticas, procedimientos, documentación y la asignación de responsabilidades para la gestión de la seguridad de la información.

5 Normativa

Ley 1581 de 2012 por el cual se dictan disposiciones generales para la protección de datos personales.

Decreto 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1266 de 2008 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 527 de 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

6 Roles y Responsabilidades

Rol	Descripción	Responsabilidad
Comité Presidencia	Mesa directiva compuesta por el presidente y vicepresidentes de Cafesalud.	Aprobación, revisión y seguimiento del modelo de seguridad de la información.
Oficial de Seguridad Informática	Asegura el cumplimiento de las políticas de seguridad informática de la Organización.	Definir las políticas de Seguridad de la información en la Compañía. Implementar y mantener el modelo de seguridad de la información, junto con sus documentos. Realizar el Plan de seguridad contra las amenazas, vulnerabilidades y riesgos. Asegurar que la infraestructura de TI soporta Políticas de Seguridad. Responder a los incidentes de seguridad de la información. Ayudar en el plan de recuperación de desastres.
Jurídica	Revisar el marco normativo y legal.	Realizar la asesoría legal frente al cumplimiento de la normatividad relacionada con la seguridad de la información y protección de datos personales.

Rol	Descripción	Responsabilidad
Gerencia de TIC	Equipo encargado de la implementación de las políticas de seguridad definidas en los recursos tecnológicos de la organización.	Implementar y operar la seguridad de la Infraestructura tecnológica. Implementar los privilegios y derechos de acceso a los recursos. Crear y asignar los perfiles de los usuarios. Controlar la creación de roles y perfiles, a través de una matriz destinada a tal fin. Soportar Políticas de Seguridad.
Dueños de la información	Área, grupo o responsable de la creación o tratamiento de la información acorde a sus funciones.	Ayudar con los requisitos de seguridad para su área específica. Determinar los privilegios y derechos de acceso a los recursos dentro de sus áreas. Conocer y clasificar adecuadamente la información.
Usuarios	Encargados de hacer un buen uso de los sistemas existentes y de almacenar en ellos información confiable, precisa, coherente y completa.	Conocer las políticas de seguridad. Reportar cualquier falla de seguridad detectada.

7 Políticas Específicas de Seguridad de la Información

7.1 Control de Accesos

- Los accesos deben ser asignados acorde a los roles y responsabilidades de los colaboradores de Cafesalud que acceda a los sistemas de información.
- Los accesos a los sistemas de información y la red deben de estar debidamente autorizados por los vicepresidentes, gerentes y/o directores siguiendo los procedimientos formalmente establecidos.

- Los accesos con privilegios especiales deben contar con la aprobación de la Gerencia TIC y/o la dirección de infraestructura y deben de estar debidamente justificados.
- Los responsables del manejo de usuarios privilegiados deben de aceptar su responsabilidad frente al uso del usuario asignado.
- Los responsables funcionales de los sistemas de información, deben de realizar revisiones periódicas por lo menos una vez en el año de los usuarios activos en los diferentes sistemas de información asegurando que las cuentas activas se encuentran debidamente autorizadas y corresponde a personal de la organización.
- Es responsabilidad de los gerentes, directores y/o coordinadores, notificar la desvinculación de un colaborador para que sean retirados los accesos de todos los sistemas incluidos los accesos físicos.
- Los usuarios y contraseñas, son personales e intransferibles, estas no se debe compartir ni divulgar por ninguna razón.
- El uso de usuarios grupales solo se asignará con la respectiva autorización del vicepresidente del área y/o gerente de área y siguiendo los procedimientos establecidos para la creación de usuarios.
- Los usuarios grupales se asignaran a una única persona y ella será responsable de su uso y de las actividades que con este se desarrollen.
- Los usuarios deben contar con una única identificación en la red así:
    - Primera letra del primer nombre + primera letra del segundo nombre + primer apellido + primer letra segundo apellido.
- En caso de existir usuarios homónimos seguir las siguientes opciones de estructura:
    - Primera letra del primer nombre + primera letra del segundo nombre + primer apellido + primer letra segundo apellido + las letras del segundo apellido que sean necesarias.

- Las contraseñas de usuario final para el acceso a la red y a todos los sistemas de información deben contar con los siguientes requisitos mínimos de seguridad:
  - Las contraseñas deben ser alfanuméricas
  - Las contraseñas deben de tener mínimo 8 caracteres
  - Las contraseñas se deben cambiar en un periodo mínimo de 45 días
  - No se debe permitir la reutilización de contraseñas por lo menos en un histórico de 5 usos.
  - El usuario se debe bloquear al 5 intento de contraseña fallida
  - La contraseña no debe ser igual al usuario

7.2 Clasificación de la Información

- Se debe clasificar los activos de información con base en su importancia y grado de confidencialidad.

7.3 Seguridad Física

- El carnet es personal e intransferible y debe ser usado para el ingreso y salida de las instalaciones. El uso del carnet es de carácter obligatorio y todos los funcionarios y contratistas deben de portarlo en un lugar visible mientras permanecen en las instalaciones.
- Los visitantes deben registrarse a la entrada, ser autorizados por un colaborador para poder ingresar y durante su estancia debe estar acompañados por el colaborador con el cual están desarrollando su actividad.

7.4 Copias de Respaldo

- Las políticas de respaldo para todos los sistemas de información deben ser definidas y aprobadas por la Gerencia TIC y acorde a las necesidades funcionales de los procesos impactados.
- Está prohibido compartir carpetas con otros usuarios de sus unidades locales.
- Está prohibido el uso de dispositivos de almacenamiento externo como memorias USB, Discos Portátiles u otros medios para copiar o transportar información salvo la expresa autorización de la Gerencia TIC.

7.5 Transferencia de Información

- El servicio de correo electrónico de Cafesalud debe ser utilizado para aspectos relacionados con las funciones propias del cargo o las funciones para las cuales fueron contratados.
- El correo electrónico es personal, por lo cual no debe ser utilizado por un usuario diferente al que se le ha asignado.
- No se autoriza el uso del correo electrónico corporativo para el envío masivo de correos.
- El uso de mecanismos de envío masivo de correos debe ser avalado por la Gerencia TIC y únicamente será usado por las áreas autorizadas para tal fin.
- No usar adaptaciones digitalizadas de firmas mecánicas (hechas a mano) para dar la impresión que el correo electrónico ha sido firmado por quien envía el mensaje.
- No se debe iniciar cadenas de correo electrónico ni ser renviadas a otros destinatarios de Cafesalud.

- Los correos de dudosa procedencia no deben ser abiertos, ni tampoco ejecutar archivos anexos que contengan estos mensajes; estos pueden contener algún tipo de software malicioso que puede afectar la información de la organización. En caso de presentarse alguna anomalía notificar inmediatamente a la Gerencia TIC.
- No es permitido enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, o mensajes que vayan en contra de las leyes, o mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- El tamaño de los buzones de correo es determinado por la Gerencia de TIC, de acuerdo con las necesidades de cada usuario y previa autorización del Jefe de la dependencia correspondiente.

7.6 Protección Contra Código Malicioso

- Todos los equipos y dispositivos con acceso a la red de la organización deben tener un cliente antivirus instalado, con protección en tiempo real.

7.7 Gestión de Vulnerabilidades Técnicas

- La ejecución de programas que analicen vulnerabilidades de los sistemas de información y/o la red, solo pueden ser realizadas por el personal autorizado por la Gerencia TIC, está prohibido a los usuarios realizar o intentar realizar este tipo de procesos.
- La Gerencia TIC realizará los análisis de vulnerabilidades que crea conveniente a los diferentes sistemas de información que prestan servicios a la organización.

7.8 Controles Criptográficos

- El uso de firmas digitales o llaves criptográficas es personal y no se deben compartir.
- La transferencia de información en especial aquella clasificada como confidencial o reservada desde ser cifrada para su transmisión.
- En caso de no poder realizar ningún tipo de cifrado sobre la información clasificada como sensible o reservada, se debe solicitar la evaluación del riesgo por parte de la Gerencia TIC para considerar medidas adicionales para mitigar el riesgo de pérdida o fuga.

7.9 Seguridad de las Comunicaciones

- El acceso a Internet es limitado para todos los usuarios y su acceso debe ser solicitado acorde a los procedimientos de gestión de accesos establecidos.
- El uso de servicios de mensajería (como Skype), es permitido únicamente para propósitos específicos de la organización.
- No está permitido la instalación de ningún tipo módems ni cambiar la configuración de sus equipos de red esta actividad únicamente la debe desarrollar la Gerencia TIC o a quien delegue.
- La descarga de archivos ejecutables es exclusiva del equipo de seguridad Informática y a través de ellos se debe canalizar cualquier tipo de requerimiento de esta índole.
- Los funcionarios y contratistas no deben ingresar a páginas de internet que contengan contenidos sexuales, racistas, o cualquier otro tipo de contenido ofensivo que vaya en contra de la ética, las leyes gubernamentales o la normatividad vigente.
- El acceso a internet es controlado por la Gerencia de TIC.

- La información clasificada como confidencial o reservada no debe ser publicada en servidores de Internet, ni esta debe ser accedida por medio de buscadores de internet.
- Se realizara monitoreo del tráfico de la red por seguridad y disponibilidad del servicio y solo será realizada por el personal autorizado por la Gerencia TIC.

7.10 Privacidad y Protección de los Datos Personales

- Acorde a lo establecido en la ley 1581 de 2012 y el decreto 1377 de 2013 que la reglamente, toda información que genere o procese Cafesalud y que está catalogada como sensible o reservada debe ser tratada con los controles necesarios para la protección es por esos que:
  - No reutilizar papel como reciclable y a su vez debe garantizar la destrucción de estos documentos cuando ya no sean requeridos para ningún proceso y trámite.
  - No pueden compartir datos e información para la cual no cuente con la autorización expresa o sin el consentimiento del propietario.
  - Todos los sistemas de información que capturen datos personales de ciudadanos deben cumplir con los requerimientos establecidos en la Ley antes citada.
  - Los usuarios no deben dejar ningún documento en los equipos de impresión y escaneo, quien lo encuentre deberá proceder a eliminarla o destruirla.

7.11 Relación con los Proveedores

- Antes de la externalización de cualquier servicio, función o proceso, se debe seguir una cuidadosa estrategia para evaluar el riesgo y las consecuencias financieras.

- Se debe seguir un proceso de licitación y/o contratación para seleccionar entre varios proveedores de servicios acorde a los procedimientos establecidos por Cafesalud.
- En todo caso, el prestador de servicios debe ser seleccionado después de evaluar su reputación, experiencia en el tipo de servicio a prestar, las ofertas y las garantías.
- Se deben realizar auditorías planificadas con antelación, para evaluar el desempeño del proveedor de servicios durante la prestación del servicio externalizado, función o proceso.
- El contrato de servicio y los niveles de servicio definidos, deben acordarse entre Cafesalud y el proveedor de servicios.
- Se deben establecer acuerdos de confidencialidad de la información y cuando el servicio externalizado finalice, acuerdos de destrucción de esta información, suministrada para la realización de sus labores.
- Se debe especificar el tipo de licencias que manejará el contratista, para el desarrollo del contrato.
- El proveedor de servicios debe obtener la autorización de Cafesalud, si se propone contratar a un tercero para apoyar el servicio externalizado, función o proceso.
- Se debe respaldar el contrato de prestación de servicios, con las pólizas a las que haya lugar: Cumplimiento del contrato, pago de salarios y prestaciones sociales y responsabilidad civil extracontractual.
- Los proveedores deben de cumplir las políticas de seguridad de la información y están obligados a reportar fallas o incidentes que se presenten o evidencien en la ejecución de sus actividades.
- Los accesos a las instalaciones y/o sistemas de información únicamente serán entregados si son requeridos siguiendo los procedimientos establecidos para tal fin.

- El servicio externalizado se regirá e implementará las políticas que establezca la organización, en cuanto a estándares de desarrollo, pruebas, paso a producción, administración de la configuración, documentación y seguridad de la información.

7.12 Uso de los Activos

- Los recursos informáticos sólo deben ser utilizados para las actividades propias de la organización y para las funciones del usuario responsable del recurso.
- Las computadoras portátiles deberán estar aseguradas antes de ser entregadas al funcionario responsable para su uso.
- Cada usuario es responsable de la conservación y el uso correcto de los recursos que le han sido asignados.
- Después de cinco (5) minutos de inactividad sobre el equipo de trabajo, este se bloqueará automáticamente.
- El usuario o funcionario debe reportar de forma inmediata a la Gerencia de TIC, cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas, golpes y/o peligro de incendio.
- Los usuarios deberán mantener los activos que le sean asignados limpios y libres de accidentes o uso inapropiado.

7.13 Política de Escritorio y Pantalla Limpia

- Los usuarios deben de mantener la información confidencial almacenada en lugares seguros y no a la exposición de pérdida o robo, escritorio limpio.

7.14 Dispositivos Móviles

- Los dispositivos móviles no pueden ser conectados a la red corporativa.
- Si es necesario conectar un dispositivo móvil a la red, esta debe ser la de invitados y con una validación previa de la Gerencia TIC.
- Restricciones Sobre Instalación y Uso de Software.
- Está prohibido por los usuarios la instalación de Software en los equipos de trabajo sin previa autorización de la Gerencia TIC.
- La Gerencia TIC es el único responsable de mantener y actualizar las configuraciones de los recursos. Ningún otro usuario está autorizado a cambiar o actualizar la configuración de estos.
- La Gerencia TIC se reserva el derecho de velar por el uso adecuado del licenciamiento de software y de eliminar/desinstalar de las maquinas, el software que no se encuentre licenciado por la Cafesalud.
- El uso de software libre solo puede ser autorizado por la Gerencia TIC previo estudio de seguridad.

7.15 Adquisición, Desarrollo y Mantenimiento de Sistemas

- La Gerencia TIC es el área responsable de definir y establecer los estándares y procedimientos para el desarrollo, mantenimiento y adquisición de sistemas de información, incluyendo la custodia del código fuente, ambientes de prueba, control de cambios y toda la infraestructura tecnológica relacionada, de conformidad con las mejoras prácticas del mercado y reglas internacionales de seguridad de la información.

- La Gerencia TIC es responsable de recomendar, asesorar y avalar lo relativo a la adquisición y distribución de licencias de software, equipos de seguridad, comunicaciones y otros dispositivos que compongan la plataforma tecnológica.

Elaboró	Revisó	Aprobó
Ivan Avendaño Avendaño	Edisson Zarate Caro	Carlos Alberto Cardona Mejía
Oficial de Seguridad de la Información	Gerente TIC	Presidente Ejecutivo Cafesalud