MACROPROCESO Y/O PROCESO AL CUAL PERTENECE LA POLÍTICA	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**RESPONSABLE**	DIRECCION DE TECNOLOGÍA

DEFINICIONES		
No.	**TÉRMINO**	**DEFINICIÓN**
1	Activo	Todo lo que tiene valor para la organización, dentro de los cuales se incluyen: • Información • Software, como los sistemas de información • Físico, Como computadores y servidores • Servicios • Personas, sus calificaciones, habilidades y experiencia • Intangibles, como la reputación y la imagen institucional
2	Antivirus	Programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.
3	Backup o Copia de Seguridad	Copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida. Son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque
4	Clave	Contraseña, clave o password es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso. En ocasiones clave y contraseña se usan indistintamente. (Asimismo llamado PIN - Personal Identificación Nombre).
5	Control Informático	Son métodos y mecanismos técnicos o tecnológicos para reducir el riesgo frente a la posible materialización de incidentes y eventos de seguridad informática con el fin de mantener niveles apropiados de Integridad, Confidencialidad, Autenticidad y Disponibilidad de los datos contenidos en los sistemas informáticos.
6	Confidencialidad	Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados
7	Correo Electrónico Institucional	Es el servicio basado en el intercambio de información a través de la red y el cual es provisto por Capital Salud EPS-S, para los trabajadores, contratistas y practicantes autorizados para su acceso

DEFINICIONES		
No.	**TÉRMINO**	**DEFINICIÓN**
8	Delito Informático	Alterar, dañar, borra o utilizar datos electrónicos para ejecutar un esquema de fraude, engaño, extorsión u obtención de dinero, propiedades o datos, utilizando servicios de computadora sin autorización, interrumpiéndolos, asistiendo a otros en el acceso no autorizado a sistemas de cómputo o introduciendo contaminantes en un sistema informático o una red de comunicaciones.
9	Disponibilidad	Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran
10	Hardware	Se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado; contrariamente, el soporte lógico es intangible y es llamado software.
11	Información	Conjunto organizado de datos contenido en cualquier documento físico o electrónico que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.
12	Información pública	Hace referencia a la información institucional destinada al cumplimiento de los objetivos de la entidad.
13	Integridad	Propiedad de salvaguardar la exactitud y estado completo de los activos.
14	Malware	Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.
15	Phishing	Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándolas a que visiten páginas web falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás información confidencial
16	Propietario de la Información	Es el responsable de preservar y disponer de la información de acuerdo con los lineamientos de la Entidad
17	Software	Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación
18	Spam	También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. El malware se utiliza a menudo para propagar mensajes

DEFINICIONES		
No.	**TÉRMINO**	**DEFINICIÓN**
		de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing
19	Spyware	Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.
20	Virus	Un virus es un programa informático creado para producir algún daño en el equipo y que posee, además, dos características particulares: pretende actuar de forma transparente al usuario y tiene la capacidad de reproducirse a sí mismo. Los virus pueden ingresar en su equipo desde otras computadoras infectadas, a través de medios extraíbles (CD, DVD, etc.) o por medio de una red (local o internet).
21	Vulnerabilidad	Hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.
22	Seguridad de la Información	Consiste en proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización independientemente del formato que tengan, estos pueden ser: (Electrónicos, En papel, Audio y vídeo, etc.).
23	Software incorrecto	Son errores de programación (bugs) y los programas utilizados para aprovechar uno de estos fallos y atacar al sistema son los exploits. Es la amenaza más habitual, ya que es muy sencillo conseguir un exploit y utilizarlo sin tener grandes conocimientos.
24	Exploits	Son los programas que aprovechan una vulnerabilidad del sistema. Son específicos de cada sistema operativo, de la configuración del sistema y del tipo de red en la que se encuentren. Puede haber exploits diferentes en función del tipo de vulnerabilidad.
25	Herramientas de seguridad	Puede ser utilizada para detectar y solucionar fallos en el sistema o un intruso puede utilizarlas para detectar esos mismos fallos y aprovechar para atacar el sistema. Herramientas como Nessus o Satán puede ser útil pero también peligrosa si son utilizadas por crackers buscando información sobre las vulnerabilidades de un host o de una red completa.
26	Puertas traseras	Durante el desarrollo de aplicaciones los programadores pueden incluir 'atajos' en los sistemas de autenticación de la aplicación. Estos atajos se llaman puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos. Si estas puertas traseras, una vez la aplicación ha sido finalizada, no se destruyen, se está dejando abierta una puerta de entrada rápida.
27	Bombas lógicas	Son partes de código que no se ejecutan hasta que se cumple una condición. Al activarse, la función que realizan no está relacionada con el programa, su objetivo es completamente diferente.
28	Gusanos	Programa capaz de ejecutarse y propagarse por sí mismo a través de redes, y puede llevar virus o aprovechar bugs de los sistemas a los que conecta para dañarlos.

DEFINICIONES		
No.	**TÉRMINO**	**DEFINICIÓN**
29	Caballos de Troya	Los caballos de Troya son instrucciones incluidas en un programa que simulan realizar tareas que se esperan de ellas, pero en realidad ejecutan funciones con el objetivo de ocultar la presencia de un atacante o para asegurarse la entrada en caso de ser descubierto.
30	Adware	Programas que abren ventanas emergentes mostrando publicidad de productos y servicios. Se suele utilizar para subvencionar la aplicación y que el usuario pueda bajarla gratis u obtener un descuento. Normalmente el usuario es consciente de ello y da su permiso.
31	Spoofing	Técnicas de suplantación de identidad con fines dudosos.
32	Programas conejo o bacterias	Programas que no hacen nada, solo se reproducen rápidamente hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etc.).
33	Técnicas salami	Robo automatizado de pequeñas cantidades dinero de una gran cantidad origen. Es muy difícil su detección y se suelen utilizar para atacar en sistemas bancarios.

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVO DE LA POLITICA:

Establecer y difundir las políticas de Seguridad de la información a todos los trabajadores y colaboradores de Capital Salud EPS-S, para que sea de su conocimiento y cumplimiento en los recursos y elementos tecnológicos asignados, permitiendo proteger la información, teniendo en cuenta aspectos legales, operativos, tecnológicos y de la entidad.

2. DESCRIPCIÓN DE LA POLÍTICA:

2.1. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Capital Salud EPS-S, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido a establecer un marco de confianza en el ejercicio de sus deberes, enmarcado en el cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para Capital Salud EPS-S, la protección de la información busca disminuir el impacto generado sobre sus activos, con objeto de velar por la integridad, confidencialidad y la disponibilidad de esta.

Esta política aplica a la Entidad según como se defina en el alcance, sus trabajadores, colaboradores y terceros, tomando como base el desarrollo de las acciones o toma de decisiones, permitiendo:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus clientes, socios y trabajadores.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los trabajadores, colaboradores y terceros de Capital Salud EPS-S.
- Garantizar la continuidad del negocio frente a incidentes presentados.

Capital Salud EPS-S, se compromete a salvaguardar la información que genera en la ejecución de sus funciones o la que le es entregada en custodia por usuarios dentro de la ejecución de los trámites de la Entidad, identificando y mitigando los riesgos asociados mediante la definición de lineamientos y directrices a las áreas, trabajadores, colaboradores, terceros y todo aquel que tenga interacción con esta información y la utilización físicamente o a través de equipos, plataformas o sistemas de información dispuestos para su gestión y resguardo, los controles establecidos en las políticas de seguridad descritas en el presente documento se encuentran fundamentados en la norma técnica colombiana NTC-ISO-27001:2013.

Toda la información que es generada por los trabajadores, colaboradores y terceros de Capital Salud EPS-S en beneficio y desarrollo de las actividades propias de la entidad es propiedad de Capital Salud EPS-S, a menos que se acuerde lo contrario en los contratos escritos y autorizados. Esto también incluye la información que pueda ser adquirida o cedida a la Entidad de parte de entidades o fuentes externas de información que sean contratadas o que tengan alguna relación con la Entidad.

Capital Salud EPS-S protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

Capital Salud EPS-S protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en Outsourcing.

Capital Salud EPS-S protegerá su información de las amenazas originadas por parte del personal.

Capital Salud EPS-S protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

Capital Salud EPS-S controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

Capital Salud EPS-S garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

A este documento podrán integrarse en adelante lineamientos o políticas relativas a la seguridad de la información siempre y cuando no sea contrario a lo expresado en esta política.

2.2. RESPONSABILIDADES FRENTE A LA SEGURIDAD DE LA INFORMACIÓN

2.2.1. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Capital Salud EPS-S por medio del Oficial de Seguridad o Ingeniero de Seguridad Informatica debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

Adicional a esto debe:

Establecer un programa que permita el fomento continuo de la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores, personas, usuarios de los sistemas de información y telecomunicaciones de Capital Salud EPS-S.

2.2.2. PROPIETARIOS DE LA INFORMACIÓN

Son propietarios de la información la gerencia y cada uno de los Directores de Área, así como los Coordinadores de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.

2.2.2.1. RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN

- Valorar y clasificar la información que está bajo su administración y/o generación (Pública, reservada, Privada, entre otras según corresponda).
- Autorizar, restringir y delimitar a los demás trabajadores, colaboradores o terceros de la entidad el acceso a la información de acuerdo con los roles y responsabilidades de los diferentes trabajadores, empleados temporales, o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
- Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de esta.
- Acoger e informar los requisitos de esta política a todos los trabajadores, colaboradores y terceros en las diferentes áreas de la Entidad.
- Utilizar solamente la información necesaria para llevar a cabo las funciones contractuales que le fueron asignadas, de acuerdo con los permisos.
- Manejar la Información de la Entidad y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual accedan y procesen, para evitar su copia, pérdida, alteración, sustracción, destrucción o uso indebido
- Evitar la divulgación no autorizada o el uso indebido de la información.
- Cumplir con todos los controles establecidos por los propietarios de la información.
- Informar a sus jefes o a la Dirección de Tecnología sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
- Proteger los datos almacenados en los computadores y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
- Reportar a la Dirección de Tecnología los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico-científicos designados para el desarrollo de sus funciones. No está permitida la conexión a la red institucional de equipos de cómputo y de comunicaciones ajena a la Entidad, ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Dirección de Tecnología.
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Gerencia de la Entidad puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad de la Entidad, al igual que las

unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la Entidad.

Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos.

2.2.3. RESPONSABILIDADES DE LA DIRECCION DE TECNOLOGÍA

- Establecer, mantener y divulgar las políticas y procedimiento de los servicios tecnológicos en toda la Entidad.
- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Entidad.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Entidad a la Gerencia de Capital Salud EPS-S.
- Implementar, cumplir y verificar el procedimiento establecido sobre las copias de seguridad generadas, custodiadas por terceros.
- Aplicar y hacer cumplir la Política de Seguridad de la Información y todo lo que esta conlleve.
- Administrar las reglas y acceso a los componentes tecnológicos, sistemas de información, aplicativos y demás fuentes de información al servicio institucional.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar la información y data institucional.
- Gestionar y resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la entidad. Esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.
- Habilitar o Deshabilitar la operación de Dispositivos de Almacenamiento externo de acuerdo con los lineamientos emitidos.
- Implementar los controles necesarios para verificar el cumplimiento de la presente política.
- Realizar back-up de la información en el momento que un trabajador, director, empleado temporal se retire de la entidad.

2.2.4. RESPONSABILIDAD CONTROL INTERNO

- Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información -SGSI, estarán a cargo de la Oficina de Control Interno.

2.2.5. RESPONSABILIDADES GRUPO MESA DE SERVICIOS

- Garantizar la disponibilidad y el soporte de los servicios
- Programar e informar a todos los usuarios sobre cualquier problema o mantenimiento que pueda afectar la normal prestación de los servicios.
- Gestionar los accesos a los diferentes servicios de acuerdo con las solicitudes recibidas de las diferentes Direcciones o Coordinaciones siguiendo el procedimiento establecido.
- Divulgar y dar cumplimiento a las políticas y procedimientos de los servicios de tecnología, incluida la presente política y sus modificaciones.

- Brindar el soporte necesario a los trabajadores a través de los canales de comunicación establecidos para la mesa de servicios.

2.2.6. RESPONSABILIDADES DE LOS TRABAJADORES, COLABORADORES Y TERCEROS, USUARIOS DE LA INFORMACIÓN

- Utilizar la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en la Matriz de perfiles.
- Manejar la Información de la entidad y rendir cuentas por el uso y protección de esta, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio institucional.
- Proteger la información a la que accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Guardar la confidencialidad de la información que le sea entrega o a la que tenga acceso en el desarrollo de sus actividades institucionales.
- Informar a los jefes y/o a la Dirección de Tecnología sobre la violación de estas políticas o falta a alguna de ellas.
- Proteger los equipos tecnológicos y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
- Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos asignados para el desarrollo de sus funciones. No está permitida la conexión a la red institucional, de dispositivos tecnológicos y de comunicaciones ajenos la entidad, ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Dirección de Tecnología.
- Usar software autorizado que haya sido adquirido legalmente por la Entidad. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento y visto bueno escrito de la Dirección de Tecnología Divulgar, aplicar y el cumplir con la presente Política.
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Gerencia de la Entidad puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad de la entidad, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la entidad.
- Proteger y resguardar la información personal que no esté relacionada con sus funciones en la entidad. Capital Salud EPS-S no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito.
- No almacenar información institucional en equipos tecnológicos (Memorias, Computadores portátiles, tabletas, SD y demás dispositivos que no sean propiedad de la Entidad) propia de los trabajadores.
- Respaldar la información institucional de uso diario en el File Server dispuesto para tales fines.
- No sacar de la entidad la información electrónica y documentos físicos con información sensible, confidencial, reservada o aquella que contengan firmas.
- Almacenar y salvaguardar la información electrónica de acuerdo con los lineamientos que establezca la Dirección de Tecnología y de Gestión Documental con base en las Tablas de Retención Documental-TRD.

Si esto es requerido para el desempeño laboral, debe estar notificado por el jefe de área y bajo su responsabilidad asegurando la integridad, confidencialidad y no falsificación de la documentación.

Todos los usuarios de los sistemas de información y telecomunicaciones de Capital Salud EPS-S, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en la presente política de seguridad de la información.

2.2.7. EXCEPCIONES A LAS POLÍTICAS DE SEGURIDAD INFORMATICA

- Debido a las comunicaciones directas o indirectas con proveedores y clientes internos o externos se deberán permitir algunas excepciones garantizando la seguridad de la información, tales como:

  a. Autorización asignación equipos móviles (Portátiles - Tablets) mediante formato F33-TSI, deberá ser diligenciado con datos de usuario NT a autorizar, firmado por coordinador, jefe directo o director.
  b. Permisos puertos (USB y unidad de CD/DVD) F33-TSI, deberá ser diligenciado con datos de usuario NT a autorizar, firmado por coordinador o jefe directo, director nacional de área.

2.3. POLÍTICA DE CONTROL DE ACCESOS

- La Entidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática de Capital salud EPS-S, considerándolas como importantes para el SGSI.

- La conexión remota a la red de área local de Capital Salud EPS-S debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por la Dirección de Tecnología.
- Todo aplicativo informático o software debe ser comprado o aprobado por la Dirección de Tecnologia en concordancia con la política de adquisición de bienes de la entidad.
- La Dirección de Tecnología establecerá niveles de protección de la información institucional electrónica y digital, de acuerdo con su roles y responsabilidades asignados a los usuarios del sistema, permitiendo el acceso a los servicios y/o sistemas informáticos a través de la asignación de contraseñas previa autorización del jefe de la dependencia y/o área.

2.3.1. USO DE CONTRASEÑAS Y USUARIOS:

Objetivos específicos:

- Presentar a todos los trabajadores y colaboradores de Capital Salud EPS-S responsables de la asignación, creación y modificación de usuarios y contraseñas las directrices a seguir y verificar que se cumplan a cabalidad con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

- Concienciar a todos los trabajadores y colaboradores sobre los riesgos asociados con el uso de las credenciales de acceso (usuario y contraseña) y las consecuencias de exponer de manera inadecuada la identidad ante cualquier tercero, entendiendo que los usuarios y claves asignados

a cada funcionario o colaborador son personales e intransferibles, la cual no debe ser revelada o divulgada por el mismo.

- Asegurar el correcto manejo de la información privada de la Entidad.

2.3.1.1. Características de los usuarios:

Los Usuarios NT deberán ser creados mediante el uso del primer nombre seguido de las iniciales de los dos apellidos.

Ejemplo No. 1: Wilmar Fabian Villamil Beltrán
Usuario NT: wilmarvb

En caso de que ya exista una persona con el mismo usuario deberá tomar la inicial del segundo nombre de la persona seguido de las iniciales de los dos apellidos.

Ejemplo No. 2: Wilmar Javier Velásquez Bermúdez
Usuario NT: wilmarjvb

En caso dado la persona no cuente con segundo nombre y se duplica el usuario deberá tomar las dos letras iniciales del primer apellido y la inicial del segundo apellido.

Ejemplo No. 3: Wilmar Velásquez Bermúdez
Usuario NT: wilmarveb

En caso excepcional o cuando no aplique ninguno de los anteriores métodos deberá comunicarse con el Ingeniero de Seguridad Informática para indicar el usuario a crear.

Igualmente deberá diligenciar la siguiente información para su correcta creación:

- Nombres y Apellidos
- Cedula
- Cargo
- Descripción (Información adicional)
- Dirección (Dirección Nacional a la que pertenece)
- Jefe directo
- Ubicación
- Teléfono oficina
- Genero
- Tipo de Contrato (temporal o fijo)

2.3.1.2. Características de las contraseñas:

Las claves o contraseñas deben:

No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.

Tener mínimo diez (10) caracteres alfanuméricos.

Cada vez que se cambien estas deben ser distintas por lo menos de las últimas veinticuatro anteriores.

La contraseña debe cumplir con los siguientes requisitos:

- Mínimo 1 carácter en mayúsculas
- Mínimo 1 carácter en minúsculas
- Mínimo 1 dígito en base de 10 dígitos (0 a 9)
- Mínimo 1 carácter especial no alfabéticos (Ejemplo: $, %, &)

Estos requisitos de complejidad se exigen al cambiar o crear contraseñas.

La asignación de contraseñas para el acceso y uso de las aplicaciones estará a cargo de la Dirección de Tecnología, previa autorización formal del jefe de la dependencia. El usuario será el responsable por los cambios que generen la autenticación.

2.3.2. PARA LOS USUARIOS:

La asignación de credenciales: usuarios (Login o User Id) y contraseñas (Clave o Password) a los diferentes trabajadores o colaboradores, así como su desactivación de los sistemas se harán de acuerdo con los procedimientos establecidos y según sea solicitado por los directores, coordinadores de oficina o por Gestión Humana, mediante el diligenciamiento del formato F33-TSI.

Las cuentas de usuario son entera responsabilidad del funcionario o colaborador al que se le asigne.

Las cuentas de usuario (usuario y clave) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como se definan.

De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, debe solicitarlo por escrito el jefe del área con su respectiva justificación y dirigirlo a la Dirección de Tecnología.

Si se detecta o sospecha que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta puede ser suspendida temporalmente y es reactivada sólo después de haber tomado las medidas necesarias a consideración de la Dirección de Tecnologia.

Uso Apropiado:

- Usar las credenciales de acceso exclusivamente para fines laborales y cuando sea necesario en cumplimiento de las funciones asignadas.
- Cambiar las contraseñas al primer ingreso y con una periodicidad de 15 días calendario.

Uso Indebido y Prohibido:

Entregar las claves a tercero y compañero de trabajo.

- Almacenar las credenciales de acceso en libretas, agendas, post-it, hojas sueltas, entre otros visibles. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado deberá ser único y bajo resguardo.
- Almacenar las credenciales sin protección, en sistemas electrónicos personales (Tablets, memorias USB, teléfonos celulares, agendas electrónicas, etc.).
- Intentar acceder de forma no autorizada con otro usuario y clave diferente a la asignada en cualquier sistema de información o plataforma tecnológica.
- Suplantar usuarios.
- Ingresar con credenciales de usuarios que se encuentren retirados, en licencia de maternidad, permiso o en periodo de vacaciones.
- Captura de usuarios y contraseña por medio de grabación, programas tecnológicos y demás que permitan recolectar dicha información.
- Utilizar el usuario y contraseña para propósitos comerciales ajenos a la Entidad.
- Intentar o modificar los parámetros de la seguridad de los sistemas de la red de Capital Salud EPS-S.

Monitoreo:

- Los administradores de los sistemas de información, bases de datos y plataformas tecnológicas pueden efectuar una revisión periódica de los accesos exitosos, no exitosos y el número de intentos efectuados a dichos sistemas para determinar posibles accesos indebidos o no autorizados.

2.3.3. PARA SISTEMAS DE INFORMACIÓN:

Todos los sistemas de información tienen usuarios administradores (*usuarios Root*) tanto en procesos de desarrollo como en producción, estos últimos (*Usuarios Root en Producción*) serán entregados en sobre sellado a la Dirección de Tecnologia, la cual tendrá bajo su responsabilidad:

- Cambio de esta conservando su confidencialidad.

- Generar y entregar accesos con funcionalidades limitadas de acuerdo con los procesos de cada área.

"Por ningún motivo se entregarán usuarios administradores (Root) a ningún representante de área distinta a la Dirección de Tecnologia*"*.

La entrega de usuarios y contraseñas a las demás dependencias se realizará de igual manera a como se realiza por parte del área de desarrollo a la Dirección de Tecnología adicionando formato F21-TSI (Acta de entrega herramientas tecnológicas y sistemas de información) completamente diligenciados y firmados.

Uso Apropiado:

- Ante el recibo de usuarios y contraseñas administrativas y/o funcionales se realizará cambio de esta al primer ingreso ya que toda modificación o afectación realizada con los mismos será responsabilidad de su propietario.
- Utilizar los usuarios entregados exclusivamente para la ejecución de sus actividades laborales.
- Actualizar credenciales de red cada 30 días sin excepción.

Uso Indebido y Prohibido:

- Prestar usuarios y contraseñas de sistemas de información a iguales o subalternos, cada usuario tiene funciones específicas.
- Almacenar usuarios y contraseñas en lugares visibles o inseguros.

Monitoreo: Se mantendrá monitoreo continuo de los usuarios administradores.

2.3.4. DESACTIVACIÓN DE USUARIOS NT:

Alcance: Funcionarios, Directos y Temporales

Desactivación de usuarios NT por retiro, licencia de maternidad, vacaciones o incapacidad superior a 3 días.

a. Cuando sea presentada la novedad de retiro de funcionarios de Capital Salud EPS-S, la Dirección de Gestión Humana y/o jefes, directores o Coordinadores, deberá generar caso de desactivación de usuario NT a través de Aranda previo a la salida del funcionario garantizando así la confidencialidad y resguardo de la información manipulada por el mismo.

b. Cuando por novedad de vacaciones, licencia de maternidad o incapacidad mayor a (3) días sea necesaria la reasignación temporal de cargos, la Dirección de Gestión Humana y/o jefes, directores o Coordinadores deberá generar caso en Aranda con mínimo (1) días de anterioridad, solicitando:

   - ✓ Redireccionamiento temporal de correos entrantes de buzón asignado al funcionario (Usuario NT que presenta la novedad) con destino (Usuario NT encargado temporal), con fecha de inicio y fin de redireccionamiento, cuando sea estrictamente necesario debido a sus funciones.
   - ✓ Asignación temporal de los accesos asignados al funcionario (Usuario NT que presenta la novedad) con destino (Usuario NT encargado temporal), con fecha de inicio y fin de estos, cuando sea estrictamente necesario debido a sus funciones.
   - ✓ Desactivación inmediata del usuario NT con novedad (vacaciones, licencia de maternidad o incapacidad mayor a (3) días), con fecha de reactivación tentativa.

Nota: Todo usuario NT que allá sido desactivado por retiro perderá toda información de accesos, y si llegase a reingresar nuevamente a Capital Salud EPS-S deberá solicitarse creación de usuario mediante el formato designado para tal fin.

2.3.5. RE-ACTIVACIÓN DE USUARIOS NT

Alcance: Funcionarios Directos y Temporales

Para Funcionarios Directos: Usuarios que se encuentren en licencia de maternidad, vacaciones o incapacidad superior a 3 días.

- Cuando sea presentada la novedad de vacaciones, licencia de maternidad o incapacidad mayor a (3) días, el día anterior a la finalización de dicha novedad el jefe directo deberá solicitar la re activación de usuario NT del funcionario que retoma sus funciones laborales, sin dicho caso no se podrá re activar ningún usuario NT, no se podrá dejar para re activación automática ya que pueden presentarse casos de ausentismo o extensiones de incapacidad sin inmediato conocimiento para la entidad, lo cual dejaría accesos activos con usuario imposibilitado para ejercer sus funciones labores generando vulnerabilidad y una violación al reglamento de seguridad informática de Capital Salud EPS-S.

Para funcionarios con contrato temporal:

- Cuando sea presentada la novedad de licencia de maternidad o incapacidad mayor a (3) días, el día anterior a la finalización de dicha novedad el jefe directo deberá solicitar la re activación de usuario NT del funcionario que retoma sus funciones laborales, sin dicho caso no se podrá re activar ningún usuario NT, no se podrá dejar para re activación automática ya que pueden presentarse casos de ausentismo o extensiones de incapacidad sin inmediato conocimiento para la entidad, lo cual dejaría accesos activos con usuario imposibilitado para ejercer sus funciones labores generando vulnerabilidad y una violación al reglamento de seguridad informática de Capital Salud EPS-S.

- Cuando sea presentada la novedad de vacaciones para usuarios temporales no se podrá solicitar reactivación de usuario NT, esta deberá ser tratada como creación de usuario ya que la salida de un funcionario temporal a vacaciones significa dar por terminado su contrato anual y no se garantiza su reingreso a la entidad.

2.4. POLÍTICA DE USO DE LOS ACTIVOS

Objetivos específicos:

- Mantener la protección adecuada de los activos de información mediante la asignación de estos a los trabajadores y colaboradores que deban administrarlos de acuerdo con sus roles y funciones.

Uso Apropiado:

- Los activos pertenecen a Capital Salud EPS-S y el uso de estos debe emplearse exclusivamente con propósitos laborales.
- Los trabajadores y colaboradores deberán utilizar únicamente los programas y equipos autorizados por la Dirección de Tecnología, para el cumplimiento de labores institucionales.
- La información y/o datos creados, almacenados y recibidos, serán propiedad de Capital Salud EPS-S, los trabajadores solo podrán realizar backup de sus archivos personales o de

información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato.

- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados a través de la mesa de servicios con su correspondiente justificación.
- El usuario será responsable de todas las transacciones o acciones efectuadas con su "cuenta de usuario".
- Todo archivo o material recibido a través de medio magnético/electrónico, de descarga por Internet o de cualquier red externa, deberá ser revisado para detección de virus o de cualquier otro código malicioso antes de ser ejecutado en el recurso asignado.
- La mesa de servicios y/o quién designe la Dirección de Tecnología, puede realizar backups de la información contenida en los computadores institucionales y no necesita autorización del funcionario, debido que la información contenida allí pertenece a la entidad.
- Los Activos que contienen información institucional, tales como discos duros, computadores portátiles o cualquier otro medio tecnológico portable perteneciente a la entidad, que se requiera sacar de la sede de ubicación debe contar con previa autorización del director de área, siendo este el responsable de la información contenida allí.
- Los computadores portátiles solo serán asignados a los directores.
- Los usuarios que por sus funciones requieran de configuración de correo institucional en sus dispositivos móviles (Smartphone) deberán realizar dicha solicitud a sus jefes directos los cuales a su vez deberán proyectar dicha solicitud al director de área y este a la Dirección de Tecnología.

Uso Indebido y Prohibido:

- La copia, sustracción, daño intencional o utilización de la información para fines distintos a las labores propias de la Entidad serán sancionadas de acuerdo con las normas y legislación vigentes.
- Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Dirección de Tecnología:

  - Instalar software en cualquier equipo que Capital Salud EPS-S, ponga a disposición de los trabajadores o colaboradores para desempeñar sus actividades.
  - Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo bajo el dominio de Capital Salud EPS-S y/o asignado para las labores institucionales;
  - Modificar, revisar, transformar o adaptar cualquier software propiedad de la entidad.
  - Realizar descargas de software no institucional en los computadores portátiles asignados, bajo una red externa.
  - Descompilar o realizar ingeniería inversa en cualquier software propiedad de Capital Salud EPS-S.
  - Copiar o distribuir cualquier software propiedad de Capital Salud EPS-S.

- Ningún usuario deberá acceder a la red o a los servicios tecnológicos de la Entidad, utilizando una cuenta de usuario o clave de otro usuario.
- Almacenar música, fotos, videos y demás documentos personales que ocupen espacio de almacenamiento en los computadores o demás elementos tecnológicos asignados.

Monitoreo:

- Cuando lo disponga, la Dirección de Tecnología efectuará la revisión de los programas utilizados en cada área. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considera como una violación a las Políticas de Seguridad de la Información.

2.5. POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

Capital Salud EPS-S proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes, tabletas y equipos portátiles, entre otros) institucionales y personales que hagan uso de servicios de la institución. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

2.5.1. NORMAS PARA USO DE DISPOSITIVOS MÓVILES

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por la entidad.

- la Dirección de Tecnología debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por Capital Salud EPS-S.

- la Dirección de Tecnología debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

- la Dirección de Tecnología debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

- la Dirección de Tecnología debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

- la Dirección de Tecnología debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales de CAPITAL SALUD EPS-S; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.

- la Dirección de Tecnología debe instalar un software de antivirus tanto en los dispositivos móviles institucionales como en los personales que hagan uso de los servicios provistos por la entidad.

- la Dirección de Tecnología debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

- la Dirección de Tecnología no aceptará ningún dispositivo móvil con su sistema operativo modificado a través de herramientas de hacking (Jailbreack, rooting, etc).

Normas dirigidas a: **TODOS LOS USUARIOS**

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales aprobados por la Dirección de Tecnología.

- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

Los Equipos de Cómputo Portátiles solo serán asignados a directores de área, dos por cada Dirección, uno para uso personal y otro de backup para ser utilizado por los funcionarios de área que por sus actividades lo requieran de manera temporal.

2.6. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

Objetivos específicos:

- Incentivar el uso del servicio de correo electrónico para fines estrictamente laborales.

- Asegurar el correcto manejo de la información privada de la Entidad por parte de los trabajadores.

- Garantizar la confidencialidad, la privacidad, el uso adecuado y moderado de la información a través de este servicio.

- Reemplazar el uso de papel con correo electrónico para comunicaciones internas.

- El acceso al servicio de correo electrónico es otorgado por Capital Salud EPS-S a sus trabajadores y el mismo sobrelleva responsabilidades y compromisos para su uso.

- El acceso incluye la seguridad, transmisión, recepción y almacenamiento de mensajes de correo electrónico y sus adjuntos.

- Se encuentra disponible un acceso externo de la red corporativa a través del siguiente enlace: https://login.microsoftonline.com/, este acceso está disponible para aquellos trabajadores que por cualquier motivo no puedan hacer uso del cliente de correo electrónico.

En Capital Salud EPS-S él envió de correo electrónico se encuentra firmado digitalmente mediante certificado digital expedido por Certicámara, lo cual de acuerdo con el Parágrafo del Artículo 28 de la ley 527 de 1999 expone que:

El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, por consiguiente y amparándonos en dicha ley cualquier correo transmitido bajo dominio @capitalsalud.gov.co tendrá el mismo peso que una carta membretada y firmada a mano.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por Capital Salud EPS-S y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

Al momento de hacer uso del correo electrónico se debe evitar la divulgación de material sexista, racista, ofensivo o difamatorio.

El usuario del correo electrónico deberá elaborar carpetas electrónicas y almacenar la información que se relacione con la misionalidad de la entidad y las Tablas de Retención Documental de cada una de las dependencias y/o áreas, con el propósito de evitar la impresión de estos.

Cuentas de correo que no hayan enviado o recibidos mensajes y no hayan sido usadas para ningún fin durante los últimos 90 días serán deshabilitadas, economizando licencias de correo para Capital Salud EPS-S.

TIPOS DE CUENTAS DE CORREO ELECTRÓNICO

Todas las cuentas de correo electrónico creadas son de propiedad de Capital Salud EPS-S

a. Cuentas Genéricas:

De acuerdo a la matriz de perfiles, el funcionario o colaborador puede ser autorizado a obtener y operar una cuenta de correo institucional para el uso diario de sus actividades laborales, estas deben ser solicitadas directamente por Gestión humana al momento de creación del usuario NT, por directores de área o por coordinadores de área siempre y cuando se adjunte aval de su director

correspondiente, se hará a través de los medios ya establecidos de la entidad asignando a su vez el responsable de manejo de la misma.

El nombre de dicha cuenta de correo se creará con el formato xxxxx.yyyyy@capitalsalud.gov.co donde xxxxx. yyyyy corresponde al nombre del cargo de acuerdo con la tabla de cargos establecida por Gestión Humana, en los casos que el nombre del cargo este compuesto por más de una palabra deberá ir separado por un punto; en caso de que existan varios funcionarios con el mismo cargo, deberá colocarse un consecutivo después de los nombres del cargo así:

Ejm1:
Cargo: Ingeniero de Tecnología
Correo: ingniero.tecnologia@capitalsalud.gov.co

Ejm2
Cargo: abogado laboral 3ra persona con el mismo cargo
Correo: abogado.laboral3@capitalsalud.gov.co

Ejm3
Cargo: Epidemiólogo
Correo epidemiologo@capitalsalud.gov.co

Los conflictos no aclarados por las reglas anteriores serán resueltos a criterio propio, por el administrador del sistema de correo, o por la persona que solicita la cuenta.
En caso de combinaciones que deriven en palabras malsonantes podrá solicitarse el cambio de identificador de usuario.

Todo mensaje de correo electrónico que salga de una cuenta personal institucional debe llevar la respectiva firma, es responsabilidad del usuario su configuración y/o inclusión.

NOMBRE COMPLETO DEL FUNCIONARIO
Cargo (Sin abreviaturas y especificando si el cargo es nacional)
Dirección, Gerencia o Vicepresidencia de la que depende el cago
Dirección de la Oficina o Dependencia
Teléfono y Ext.
Celular Corporativo (Si aplica)
Email:

Te entiende. Te atiende.

b. Cuentas Grupales:

Estas cuentas son creadas para las necesidades de comunicación oficial, para las áreas. Deben ser solicitadas directamente por el director del área que corresponda, a través de los medios ya establecidos de la entidad asignando a su vez el responsable de manejo de esta.

El nombre de la cuenta de correo se definirá con el formato XXX@capitalsalud.gov.co, donde XXX es el área según la necesidad operativa. El titular será responsable del uso que se dé a dicha cuenta y del mantenimiento periódico de las claves de esta.

Todo mensaje de correo electrónico que salga de una cuenta de Grupo de Trabajo debe llevar por regla general la siguiente estructura de firma, es responsabilidad del usuario responsable de su administración su configuración y/o inclusión.

NOMBRE DEL GRUPO
Área a la cual pertenece
Dirección de la Oficina o Dependencia
Ciudad, Colombia
Email:

Uso Apropiado:

- Mantener normas de respeto, confidencialidad y criterio ético por parte de todos los trabajadores y colaboradores con acceso a este servicio.
- Usar el correo electrónico Institucional exclusivamente para fines laborales: para la difusión o el envío de circulares, memorandos, oficios y archivos de trabajo, cuando sea necesario en cumplimiento de las funciones asignadas.
- Ingresar a las cuentas de correo de cada usuario a través de los medios que la entidad destina, que en este caso son los clientes de correo electrónico instalado y configurado en cada máquina.

Uso Indebido y Prohibido:

- Participar en la difusión de “cartas en cadenas” o de propagandas dentro y fuera de la Entidad, esto incluye comunicaciones sindicales que perjudiquen a Capital Salud EPS-S.
- Realizar intentos no autorizados para acceder a otra cuenta de correo electrónico Institucional.
- Revelar o publicar cualquier información clasificada privada o reservada de Capital Salud EPS-S.
- Descargar cualquier software o archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.
- Utilizar expresiones difamatorias o groseras en contra de personas, clientes y entidades públicas o privadas. Los mensajes enviados a través de este servicio no pueden contener material insidioso, ofensivo, obsceno, vulgar, racista, pornográfico, subversivo u otro material no formal que atente contra el buen nombre.
- Enviar información institucional por medio de canales no seguros (no codificados) como es Internet y/o las cuentas de correo de uso público (gmail, hotmail, yahoo, etc.) a menos de tener autorización explícita escrita por el jefe. El correo electrónico está sujeto a las mismas leyes, políticas y prácticas que se aplican a la utilización de otros medios de comunicación, tales como servicios telefónicos y medios impresos.
- Participar en actividades que puedan causar congestión o interrupción en la normal operación de los servicios de comunicación y correo electrónico de la Entidad.
- Enviar correos SPAM de cualquier índole.
- Reenviar correos con contenido PHISING.
- Usar seudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales
- Utilizar el correo electrónico para propósitos comerciales ajenos a Capital Salud EPS-S.
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.
- Usar correos públicos para la recepción, envió o distribución de información privada o reservada propia de Capital Salud EPS-S.
- Distribuir listas de direcciones de correo personales sin expresa autorización de sus dueños.
- Enviar archivos con extensión .exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta, .tar, .dll debido a que este tipo de extensiones son propensas a ser utilizadas para propagación de virus. Este tipo de archivos serán eliminados automáticamente por el sistema de correo.
- Enviar contenidos multimedia (video o audio) con extensión .wav, .mp3, .mp4, .mpeg, .wma, .wmv, .mov, .asf, .flv ya que estos documentos son muy pesados y ralentizan la red de comunicaciones.
- El uso inapropiado o el abuso en el servicio de correo electrónico ocasionan la desactivación temporal o permanente de las cuentas. La desactivación de la cuenta lleva consigo la imposibilidad de acceder a los mensajes de correo que estén en ese momento en el servidor y la imposibilidad de recibir nuevos mientras no vuelva a ser activada.

Envío y transferencia sobre el servicio de correo electrónico:

- La capacidad máxima de los buzones de cuentas grupales es de 500 GB y para las cuentas VIP la capacidad de almacenamiento es 1TB, siendo esta última donde solo se encuentra Gerencia, directores y aquellos perfiles que la dirección haya autorizado. Una vez el buzón llegue al umbral de alerta, tanto el usuario como el administrador del servicio de correo serán notificados para mover los mensajes no necesarios al equipo local o a la opción “Archivo” de la plataforma de correos.
- Los buzones tienen un límite para el envío y recepción de mensajes y sus adjuntos. Dicho límite se establece para garantizar estabilidad en los canales de comunicación y tener un QoS (Quality of Service) aceptable, adicional a las limitaciones de almacenamiento en el servidor de correo de Capital Salud EPS-S.
- Por tal razón. Se establece que el tamaño máximo de los archivos adjuntos para envío y recepción es de 20MB. El máximo número de destinatarios es 500, en los campos Para: CC: (con copia) y CCO: (con copia oculta) para un mensaje de correo es de 40 usuarios. El área de Comunicaciones de Capital Salud es la única autorizada a realizar envíos masivos de mensajes.
- Se recomienda el uso del campo CCO: para mantener la privacidad de los correos electrónicos de los destinatarios. Este campo hace que los destinatarios reciban el mensaje sin aparecer en ninguna lista ni ser visibles a los demás.
- Los correos masivos institucionales que por necesidades específicas de un área requieran ser enviados a una parte o toda la entidad, deben ser enviados a través del correo de Comunicaciones. Igualmente se debe solicitar que estos correos no sean contestados por parte de los destinatarios debido a que puede provocar lentitud en el canal de comunicación o tergiversar el objetivo de la información con comentarios adicionales.
- Es una buena práctica compartir los archivos a través del servicio del File Share y/o a través de OneDrive, para disminuir las exigencias técnicas en su transmisión.
- Los mensajes destinados a dominios (cuentas) no válidas se rechazan inmediatamente para evitar que direcciones erróneas (por ejemplo, mal escrito) sean aceptadas por el servidor como válidas.
- Se aplican políticas de filtrado de mensajes para evitar en la medida de lo posible la llegada de correo no deseado (SPAM) a los buzones de los usuarios. Un mensaje no se acepta cuando provenga de un servidor identificado como fuente de SPAM o como un servidor no válido para el envío de correo electrónico por alguna de las listas de bloqueo, en caso de tener información de correos maliciosos el usuario está en obligación de notificar a la mesa de ayuda.
- Se aplican políticas de filtrado de mensajes entrantes y salientes, rechazando el envío/recepción de mensajes que contengan virus. Cuando un mensaje es rechazado se envía una notificación al destinatario del mensaje, salvo en el caso de virus que falsifique el emisor del mensaje.
- Un adjunto se borra cuando, a través de los procesos automáticos de evaluación, sea identificado como portador de virus o cualquier otra amenaza para el destinatario, comunicándole al mismo este hecho mediante un mensaje al pie del correo electrónico.

Responsabilidades de los trabajadores y Colaboradores:

- Cuidar y revisar el contenido de los correos electrónicos que se envíen a través de su cuenta. El uso no autorizado de una cuenta de correo electrónico es ilegal y constituye una violación de la Política de la Entidad.
- Usar correctamente las credenciales de ingreso (usuario y clave) asignadas. La cuenta de correo que proporciona la entidad es corporativa no debe asociarse con asuntos personales y es intransferible, por lo que no debe compartirse con otras personas.

- Cerrar totalmente la sesión de lectura y envío de correos para evitar el uso de su identidad, cuando se retire del equipo en que se encuentre configurada la cuenta de correo.
- Dar aviso al Grupo de Soporte Tecnológico, a través de los medios establecidos, de cualquier fallo de seguridad en su cuenta de correo, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.
- Responsabilizarse por la información o contenido que sea transmitido a través de la cuenta de correo asignada; Los usuarios del servicio deben considerar que los mensajes enviados a un destinatario pueden ser reenviados a cualquier número de cuentas de correo de otros individuos o grupos.
- Descargar, verificar y resguardar la información recibida a través de este servicio en su buzón local de correo electrónico, de ser este configurado, en el cliente de correo instalado en su equipo de cómputo.
- La información que sea almacenada en la nube (OneDrive) y sea compartida a agentes internos y externos será responsabilidad de cada trabajador.
- El uso de las herramientas de Office 365 es para uso exclusivo de labores corporativas el manejo de la información desde cualquier dispositivo será responsabilidad de cada trabajador.

Monitoreo:

- Capital Salud EPS-S tiene el derecho a acceder y revelar los contenidos electrónicos de los correos electrónicos institucionales de sus trabajadores y colaboradores, dando su consentimiento a la Entidad en caso de que algún ente fiscalizador a nivel interno o externo requiera esta información. Priman las exigencias de carácter legal o disciplinario.
- Revisión periódica del tráfico de mensajes sobre los canales de comunicación como prevención de ingreso de mensajes tipo SPAM o PHISING, ingreso de virus sobre las redes y equipos informáticos, verificación de volúmenes de archivos anexos que puedan afectar la operación del sistema.
- Monitoreo en línea del servicio institucional en cualquier momento para revisión de contenido o eventualidad
- La Dirección de Tecnología y/o el Grupo de Mesa de Servicios pueden monitorear el cumplimiento de las directrices institucionales en el momento que así lo considere o le sea requerido.

2.7. POLÍTICA DE USO DE SERVICIO DE INTERNET

Objetivos específicos:

- Incentivar el uso del servicio de Internet e Intranet para fines estrictamente laborales de Capital Salud EPS-S.
- Asegurar el correcto manejo de la información privada de la Entidad.
- Garantizar la confidencialidad, la privacidad y de uso adecuado de la información a través de este servicio.

Se espera que los usuarios de este servicio conserven normas de buen uso, confidencialidad y criterio ético.

Cada director o Coordinador de área tiene la autonomía de otorgar y solicitar el acceso de sus trabajadores y colaboradores este servicio, de acuerdo con el procedimiento vigente.

Uso Apropiado:

Todos los trabajadores y colaboradores con autorización al uso y acceso a estos servicios deben:

- Utilizar este servicio exclusivamente para fines laborales.
- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los trabajadores y colaboradores con acceso a este servicio.
- Descargar documentos tomando las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

Uso Indebido y Prohibido:

- Acceder a sitios de juegos o apuestas en línea.
- Acceder a sitios de divulgación, descarga o distribución de películas, videos, música, real audio, webcams, emisoras online, etc.
- Acceder y/o descargar material pornográfico, drogas, alcohol, webproxys o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes e institucionales o políticas establecidas en el presente documento.
- Utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados por el Grupo de Mesa de Servicios.
- Descargas de software, así como su instalación en las herramientas tecnológicas asignadas para el desempeño de sus labores
- Compartir en sitios web información propia Capital Salud EPS-S clasificada como reservada o privada, así como cualquier información de sus usuarios, trabajadores y colaboradores.
- Disponer este servicio para la recepción, envió o distribución de información clasificada o reservada de Capital Salud EPS-S a través de servicios de transferencia (Dropbox, Drive, wetransfer, entre otros que no sean establecidos institucionalmente) y cuentas de correo públicos (Gmail, Hotmail, Yahoo, entre otros que no estén bajo el dominio capitalsalud.gov.co) a menos que alguno de estos servicios sea autorizado y solicitado de manera escrita por el jefe.
- Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.
- Cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derecho de autor.
- Utilizar el servicio de Internet para propósitos comerciales no autorizados ajenos a Capital Salud EPS-S.
- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados por Capital Salud EPS-S.
- Interferir intencionalmente con la operación normal de cualquier sitio web o portal en Internet.
- Comprar o vender artículos personales a través de sitios web o de subastas en línea.
- Acceder a sitios de contenido multimedia (videos, música, emisoras online, redes sociales, páginas de deportes.) debido al alto consumo de canal de comunicaciones. Únicamente se autorizará el acceso a aquellos trabajadores y colaboradores que por sus actividades requieran acceso a estos sitios externos con previa aprobación de su jefe directo-justificada ante la Dirección de Tecnología.
- Publicar o enviar opiniones, declaraciones políticas y asuntos no propios de la Entidad, dirigidos a trabajadores, colaboradores y público en general, a través de este servicio.

Monitoreo:

- La Dirección de Tecnología validará el top de las páginas más visitadas con el fin de establecer los accesos efectuados y el consumo respectivo.
- Si se determina que alguna de las páginas previamente es requerida para el desempeño de funciones de algún funcionario o colaborador esta será habilitada únicamente con el consentimiento y solicitud justificada de su jefe directo.
- Los usuarios del servicio deben considerar que algunos sitios web no son seguros, especialmente los que hacen suplantación de entidades a los bancos y/o emisores de tarjetas de crédito (PHISING) por lo que se recomienda confirmar esta información directamente con las mismas entidades. Igualmente, no se debe proveer información personal ni laboral a sitios de dudosa validez.

Capital Salud EPS-S no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al acceder a sitios de suplantación o al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito al hacer el uso de este servicio.

2.8. POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN.

Capital Salud EPS-S consiente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo con el tipo de clasificación establecido por la ley, define reglas de como clasificar la información, liderado por el proceso de Gestión Documental de la Entidad.

- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la entidad como, por ejemplo:
- Formularios / comprobantes propios o de terceros.

- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.

- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.

Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.

- Los usuarios responsables de la información en Capital Salud EPS-S, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

- Un activo de información es un elemento identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como “Importante” para Capital salud EPS-S; Independiente del tipo de activo, se deben considerar las siguientes características:

a. El activo de información es reconocido como valioso para La entidad.

b. No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.

c. Los niveles de clasificación de la información valiosa que se ha establecido son: INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA (PRIVADA Y SEMI-PRIVADA) e INFORMACIÓN PÚBLICA.

2.9. POLÍTICA DE CONSERVACIÓN DE LA INFORMACIÓN

Capital Salud EPS-S deberá diseñar una estrategia para asegurar la conservación y disponibilidad de la información, en función de afrontar los riesgos de la obsolescencia tecnológica. Es imprescindible que dichos documentos estén organizados, clasificados de acuerdo con la Tabla de Retención Documental -TRD, descritos e indizados, para poder ser identificados y recuperados de la forma más pertinente en el momento en que se desee. Para asegurar la protección de los documentos electrónicos y su autenticidad, se recomienda que estos no sean dependientes del software que los creó y, además, que sean convertidos al formato .pdf, con la incorporación de metadatos que son los datos que describen el contexto, el contenido y la estructura de los documentos y su gestión a lo largo del tiempo (Norma ISO 25489-1 2016)

Mediante los metadatos insertados en los documentos digitales se asegura su identificación, por lo cual se debe incorporar información relacionada con la fecha y hora de creación, su creador, el calendario de conservación, su clasificación y relación con otros documentos, etc. Estos metadatos también se pueden almacenar en un repositorio y deberían poder extraerse de los formatos propietarios mediante el lenguaje de marcas .xml.

Según artículo 2.8.2.7.9 del Decreto 1080 de 2015, los metadatos mínimos de los documentos electrónicos de archivo son:

I. De Contenido
II. De Estructura
III. De Contexto

En cuanto al almacenamiento de los documentos digitales, se debe asegurar un soporte estable contra la obsolescencia tecnológica, forma documental fija y vínculo archivístico que, a su vez, permita las migraciones a nuevos soportes, con la completa garantía de que se protege la información contenida, asegurando disponibilidad, confidencialidad e integridad.

2.10. POLÍTICA DE USO DE PANTALLAS DESPEJADAS.

Objetivos específicos:

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al manejo de información tanto física como digital y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener las pantallas y escritorios organizados y controlando el reposo de información clasificada o reservada a la vista.
- Definir el uso adecuado y ordenado de las áreas de trabajo desde el punto de vista físico y tecnológico entendiéndose para tal fin como escritorio el espacio físico o puesto de trabajo asignado a cada funcionario o colaborador y pantalla, el área de trabajo virtual sobre el sistema

operativo de su computador, que contiene tanto sus carpetas electrónicas como los archivos y accesos a los diferentes aplicativos Institucionales.

- Clasificar las carpetas electrónicas con los documentos misionales del área de acuerdo con la Tabla de Retención Documental e identificar los documentos de apoyo.
- El uso y conservación de los puestos de trabajo (escritorios) y de los fondos de escritorio de sus computadores (pantallas) es una responsabilidad de cada uno de los trabajadores, contratistas y practicantes que tengan acceso a la información de la Entidad, sea de manera temporal o indefinida, en el normal desarrollo de sus actividades. Para su definición y aplicación se define de la siguiente manera:

Escritorios:

- Se deben dejar organizados los puestos y áreas de trabajo, entendiéndose por esto el resguardo de documentos con información clasificada o reservada evitando que queden a la vista o al alcance de la mano de personal ajeno a la misma.
- En la medida de lo posible los documentos con información clasificada o reservada debe quedar bajo llave o custodia.
- Se debe evitar el retiro de documentos clasificados o reservados de la entidad y en el caso de ser necesario se debe propender por su protección fuera y su pronta devolución al mismo.
- Se deben controlar la recepción, flujo envío de documentos físicos en la entidad desde el punto de correspondencia.
- Se debe restringir el fotocopiado de documentos fuera de las instalaciones de la entidad. De ser necesario el jefe debe autorizar el retiro de dichos documentos y garantizar su protección y confidencialidad fuera.
- Al imprimir o fotocopiar documentos con información clasificada o reservada, esta debe ser retirada inmediatamente de las impresoras o multifuncionales utilizadas para tal fin. Y no se debe dejar desatendida sobre los escritorios.
- No se debe reutilizar papel que contenga información clasificada o reservada.

Pantallas:

- Los computadores o estaciones de trabajo deben ser bloqueados por los usuarios al retirarse de los mismos y los mismos deben ser desbloqueados por medio del usuario y contraseña asignado para su acceso. Es responsabilidad del trabajador, asegurar que el equipo tenga la protección adecuada así contribuimos con el uso eficiente de la energía.
- Las áreas de trabajo virtuales “pantallas” del computador deben tener el mínimo de iconos visibles, limitándose estos a los accesos necesarios para la ejecución de la ofimática, accesos a sistemas de información y a carpetas y unidades de red necesarios para la ejecución de las actividades.
- Los documentos digitales deben ser organizados en carpetas y evitar dejarlos a la vista en las pantallas de los computadores.
- Los trabajadores y colaboradores al retirarse de la entidad deben apagar los computadores asignados.
- Al presentarse una inactividad de 5 minutos el sistema del computador se boqueará de manera automática. Estos pueden ser nuevamente utilizados por los usuarios al volver a realizar la autenticación por medio de los usuarios y contraseñas asignados.

Monitoreo:

La Dirección de Tecnología, realizará brigadas de monitoreo para verificar el estado de los computadores, monitores y escritorios virtuales, generando el respectivo informe de lo encontrado.

2.11. POLÍTICA DE USO PARA CONEXIONES REMOTAS.

Objetivos específicos:

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al acceso y gestión de información sobre las plataformas institucionales de manera remota y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener segura la información y los elementos utilizados para el acceso y operación remota de información.
- Dictar las pautas para mantener organizado y resguardado las credenciales de acceso, así como los elementos de protección para asegurar la conexión remota.

Responsabilidades de la Dirección de Tecnología:

- Establecer e implementar los métodos de conexión remota a la plataforma tecnológica de Capital Salud EPS-S.
- Implementar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica Institucional.
- Restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- Verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de manera permanente.

Monitoreo:

- Revisiones de ingresos fallidos.
- Validación de las conexiones entrantes.

2.12. POLÍTICA DE USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO.

Objetivos específicos

- Concienciar a los trabajadores y colaboradores de la Entidad sobre los riesgos asociados con el uso de los medios de almacenamiento externos, a los asignados por la Entidad.
- Asegurar el correcto manejo de la información digital que reposa en la Entidad.
- Delimitar el uso de estos medios de almacenamiento en las estaciones de trabajo, de acuerdo con el perfil de usuario.

El uso de dispositivos de almacenamiento externo no está permitido en Capital Salud EPS-S para los trabajadores y colaboradores, con el fin de facilitar el compartir y transportar información la Dirección de Tecnología pone a disposición el File Server, correo institucional, OneDrive Corporativo y carpetas compartidas localmente en los equipos.

La entidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por Capital Salud EPS-S, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran en los equipos de cómputo, servidores e infra estructura de la entidad.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la Dirección de Tecnología diligenciando el formato F16-TSI en su totalidad y será objeto de auditorías de seguridad con el fin de evitar pérdidas de datos en la información.

Dentro de los dispositivos de almacenamiento externo con restricción se incluyen, pero no se limitan:

- Memorias Flash USB
- Reproductores portátiles MP3/MP4
- Cámaras con conexión USB
- iPhone/Smartphones
- SD Cards/ Mini SD Cards/ Micro SD Cards.
- PDAS / Tablets
- Tarjetas Compact Flash
- Discos duros de uso externo.
- CD/DVD´S

Está prohibido el uso de almacenamiento en línea, es decir, aquellas unidades virtuales de almacenamiento personal por medio de internet, en las cuales se incluye, pero no se limitan los servicios de Google Drive, OneDrive, Dropbox, Rapidshare, GigaSize, MediaFire y 4shared.

Uso Indebido y Prohibido

- Almacenar o transportar información clasificada confidencial o reservada de Capital Salud EPS-S.
- Ejecutar cualquier tipo de programa no autorizado por la Entidad desde cualquiera de las unidades de almacenamiento en mención.
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del usuario de alguno de estos medios de almacenamiento.
- Emplear dispositivos de almacenamiento externo con el fin de almacenar o exponer información sensible o reservada de los trabajadores, colaboradores y usuarios de la Entidad.
- Queda RESTRINGIDO el uso de Dispositivos de Almacenamiento Externo.

Monitoreo:

- Todos los eventos realizados sobre los dispositivos de almacenamiento externo, conectados a cualquier equipo de cómputo de la entidad, pueden ser auditados con el ánimo de registrar y controlar las actividades realizadas sobre cada uno de estos, la ubicación y el usuario que los empleó.

- Las entradas de software malintencionado, de espionaje o virus podrán ser detectadas inmediatamente e informadas a la Mesa de servicios.
- Cada vez que la Dirección de Tecnología lo considere, generará informes sobre el uso de todos los dispositivos para permitir la evaluación del "uso racional de los dispositivos" y que estos sean permitidos, a fin de incrementar los niveles de seguridad para proteger la información de la Entidad.

2.13. POLÍTICA DE USO DE CARPETAS VIRTUALES (FILE SERVER)

Objetivos específicos:

- Garantizar el respaldo de la información institucional relevante.
- Proporcionar a los trabajadores y colaboradores un medio para compartir la información.
- Concienciar a los trabajadores y colaboradores sobre la importancia del uso de este recurso.

Uso Apropiado:

- Para que los usuarios tengan acceso a la información ubicada en los discos de red, se debe registrar la solicitud a través de servicios compartidos especificando el acceso y permisos, correspondientes al rol y funciones a desempeñar, a la mesa de servicios
- Los usuarios tendrán permisos de escritura y lectura de información en los discos de red, dependiendo de sus funciones y su rol.
- La información institucional de relevancia que se trabaje en las estaciones cliente de cada trabajador debe ser trasladada periódicamente a los discos de red por ser información institucional.
- La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.

Uso Indebido y Prohibido:

- Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, en los discos de red y demás recursos tecnológicos institucionales asignados.
- Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.
- Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

Monitoreo:

- La responsabilidad de generar las copias de respaldo de la información de los discos de red está a cargo de la Dirección de Tecnología.
- Revisión de los logs de auditoria de las carpetas

2.14. POLÍTICA DE USO DEL SERVICIO DE IMPRESIÓN.

Objetivos específicos:

- Concienciar a los trabajadores y colaboradores sobre el buen uso de las impresoras y el consumo de papel.

Uso Apropiado:

- Los documentos que se impriman en los recursos tecnológicos de Capital Salud EPS-S deben ser de carácter institucional.
- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

Uso Indebido y Prohibido:

- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la mesa de servicios.

Monitoreo:

- El área administrativa mediante la herramienta adquirida realizar la respectiva gestión sobre el consumo de impresiones

2.15. POLÍTICA PARA REALIZAR BACKUPS

Objetivos específicos:

- Establecer el procedimiento para realizar los respectivo backups.
- Concienciar a los trabajadores y colaboradores de almacenar información institucional y no personal en el recurso tecnológico asignado.

Uso Apropiado:

- En el evento de retiro de un funcionario o traslado de dependencia, previa notificación del Área de Gestión Humana, la Mesa de servicios generará una copia de la información contenida en el equipo asignado al perfil del usuario, a una unidad de almacenamiento.
- El backup solo debe contener archivos institucionales y se debe estructura el nombre de la carpeta de la siguiente manera:
    - Usuario NT – área, Ejemplo: MariaSR-Tecnología
- Una vez esta información se encuentre ubicada en la unidad de almacenamiento, se le realiza copia de seguridad en cinta magnética, para conservar esta información en el tiempo.
- Si el jefe del área de la cual se retira el usuario requiere copia de esta información, debe realizar solicitud a la Dirección de Tecnología.

- Para realizar los backups, la Dirección de Tecnología no requiere autorización previa de los trabajadores, esto debido a que los computadores y la información almacenada en ellos es de carácter institucional
- Se considera una buena práctica resguardar las copias de Seguridad en un sitio diferente

Uso Indebido y Prohibido:

- Ningún trabajador final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que cuenten con previa autorización del director de área y la Dirección de Tecnología.
- Tratar o acceder a la información sin previa autorización.

2.16. POLÍTICA DE REGISTRO Y SEGUIMIENTO DE EVENTOS (LOGS) EN SISTEMAS DE INFORMACIÓN Y COMUNICACIONES.

En toda entidad es importante preservar la integridad, confidencialidad y disponibilidad de los registros de eventos (logs) generados por los sistemas de información y comunicaciones con el fin de tener control total de las transacciones informáticas lo cual no es ajeno para Capital Salud EPS-S y por tal motivo se generó la presente política.

Objetivos Específicos:

Preservar la integridad, confidencialidad y disponibilidad de los registros de eventos (logs) tomas de los sistemas de información por la Dirección de tecnología.

Término y definición de LOG:

Log: Es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto .txt, al que se le van añadiendo líneas a medida que se van realizando acciones sobre los sistemas de información.

Alcance de la política:

Esta política deberá ser aplicada a todos los sistemas de comunicaciones y de la información.

2.17. POLÍTICA DE BORRADO SEGURO Y DESTRUCCIÓN DE LA INFORMACIÓN

Objetivos Específicos:

- Definir el estándar de borrado seguro de la información de los dispositivos de almacenamiento presentes en Capital Salud EPS-S.

Borrado Seguro y Destrucción de la Información

Toda organización debe contar con una política de borrado seguro de la información de los dispositivos de almacenamiento con los que trabaja, y esta debe implicar al menos los siguientes elementos:

- Gestión de soportes adecuada:
  - Realizar un seguimiento de los dispositivos que están en funcionamiento, las personas o departamentos responsables, la información contenida en ellos y su clasificación en función del grado de criticidad para el negocio.
  - Llevar a cabo la supervisión de los dispositivos que almacenan las copias de seguridad de estos datos.
  - Controlar cualquier operación realizada sobre un dispositivo: mantenimiento, reparación, sustitución, etc.
  - En los traslados de los dispositivos de almacenamiento a instalaciones externas a las de la empresa, hay que asegurar que se cumple la cadena de custodia de estos, para evitar fugas de información.
- Documentación de las operaciones de borrado realizadas:

Al seleccionar una herramienta de borrado, elegir aquella que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo ha sido realizado.

En el caso de que la destrucción lógica no se realice correctamente por fallo del dispositivo, este hecho debe documentarse claramente y utilizar métodos de destrucción física de dicho soporte, asegurando que se realice de forma respetuosa con el medio ambiente.

- Métodos de destrucción de la información:

Los medios eficaces que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento son:

La desmagnetización, la destrucción y sobre escritura en la totalidad del área de almacenamiento de la información.

Las formas utilizadas por capital salud son las siguientes:

- Destrucción física

El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena.

- ✓ Caso Información Sensible CD/DVD/BLUE RAY:

Cuando la información a destruir se encuentre almacenada en unidades de almacenamiento CD ROM, deberá destruirse mediante rayado del disco contenedor de información previo a su fragmentación la cual podrá realizarse a mano o mediante trituradora de papel/CD'S.

✓ Caso Información Sensible En Papel:

Cuando el material se desintegra o desmenuza, todos los residuos se reducen a cuadrados de por lo menos 1 cm para documentos de criticidad baja-media (comunicados, correos impresos), este proceso se realiza a mano y de cinco milímetros (5mm) de lado para criticidad media-alta (listados de clientes, listados de inventarios, facturas incorrectas, presupuestos, información contable, números de cuenta, informaciones de crédito, declaraciones, impuestos, informes médicos, nóminas, copias de Cédula de Ciudadanía, historiales de personal, historiales médicos, tarifas, cheques cancelados, tarjetas de crédito, contratos, registros de seguridad, hojas de vida), este proceso se realiza mediante trituradoras de papel.

Ningún empleado o trabajador de la entidad está autorizado a realizar destrucción de la documentación, esto se realizará siguiendo los parámetros establecidos por la Dirección Administrativa y Financiera-Área Administrativa-Gestión Documental.

- Sobreescritura

La destrucción de datos por sobreescritura consiste en la escritura de un patrón de datos (Binarios) sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento entre (3 – 35 Veces), para este caso hacemos uso de la herramienta de código abierto CBL Data Shredder.

2.18. POLÍTICA DE SEGURIDAD FÍSICA.

Objetivos específicos:

- Concienciar a los trabajadores y colaboradores de los riesgos físicos presentes.
- Establecer controles para impedir la violación, deterioro y la perturbación de las instalaciones y datos.

Seguridad Física

Cuando hablamos de seguridad física nos referimos a todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

A continuación, mencionaremos algunos de los problemas de seguridad física que podemos enfrentar y las medidas a tomar para evitarlos o al menos minimizar su impacto.

- **Protección del hardware:**

El hardware es frecuentemente el elemento más costoso de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

Problemas a los que nos enfrentamos:

- ✓ Acceso físico
- ✓ Desastres naturales
- ✓ Alteraciones del entorno

- **Acceso físico**: Para la detección de accesos se emplean medios técnicos, como cámaras de vigilancia de circuito cerrado y alarmas de seguridad.

- **Cuartos Técnicos**: En Capital Salud EPS-S, en especial para los cuartos técnicos existe el siguiente protocolo para los diferentes tipos de mantenimiento de estos.

✓ **Mantenimiento General**: Se programa una visita anual durante la cual se lleva a cabo un mantenimiento general y detallado (Peinado de rack de datos, validación de patch panel, re ponchado de pathcore o cambio dependiendo de su estado, identificación de puntos en patch panel con su correspondiente marquillado, certificación de puntos y mantenimiento básico).
✓ **Mantenimiento Preventivo**: Adicional al mantenimiento general se realiza un mantenimiento preventivo pasados seis meses del general, en el cual se realizan las siguientes actividades (limpiado de polvo, reemplazo de películas antiestática, monitoreo de ruido eléctrico y limpieza general del cuarto técnico).

Nota: Para la realización de los mantenimientos ya mencionados se debe acordar entre ambas partes (Capital Salud EPS-S y Proveedor de Servicio) el cronograma el cual será entregado y evaluado con mínimo un mes de anticipación, el proveedor remitirá los datos (Número de Identificación, Numero de contacto, Datos de EPS, ARL, certificado de Alturas “de ser necesario” y carnet) del personal autorizado y calificado para realizar tal labor.

Antes de ingresar a los cuartos técnicos se deberán realizar validación de antecedentes judiciales y relacionar los datos del personal prestador del servicio de mantenimiento en las bitácoras de ingreso a la entidad y la del cuarto técnico la cual se identifica como formato (F06-TSI) en la intranet, en ambas se relacionara (fecha y hora de ingreso, fecha y hora de salida y actividad realizada), este deberá estar siempre acompañado del **Analista de Infraestructura**, ya que es la persona designada por Capital Salud EPS-S para supervisar y monitorear los mantenimientos de los cuartos técnicos, a su vez ambas partes cliente y proveedor son monitoreados por el sistema de circuito cerrado de la organización.

Una vez terminado el Analista de Infraestructura analizará y emitirá dictamen de la actividad realizada.

- **Equipos de Cómputo y Oficina**: En Capital Salud EPS-S, para los equipos de cómputo se tiene la directriz de que los equipos de cómputo deben ser apagados todos los días evitando la degradación de estos, adicional a esto se contemplaron al igual que para los cuartos técnicos dos mantenimientos anuales.

- **Cámaras de Vigilancia de Circuito Cerrado y Alarmas de Seguridad:** En Capital Salud EPS-S se tienen administrados los sistemas de vigilancia de la siguiente manera:

✓ **Cámaras de Vigilancia de Circuito Cerrado:** El circuito cerrado de cámaras de vigilancia estará a cargo de la Dirección de Tecnología, la cual realizará monitoreo continuo del estado de funcionalidad de las cámaras de vigilancia contratadas con la empresa de vigilancia proveedora de servicios de seguridad.

La Dirección de Tecnología tiene las facultades de visualizar todas las sedes de la entidad, realizar solicitud de copia de las grabaciones de video realizadas por los CCTV a demanda en caso de ser requeridos para investigaciones de control interno, modificar la ubicación y solicitar cambio de cámaras de ser requerido para asegurar los activos de Capital salud EPS-S.

Adicional a esto cada una de las sucursales tendrá visual de las sedes donde tengan campo de acción de la siguiente manera:

- Sucursal Meta: Todos los PAU del Meta
- Sucursal Bogota: Todos los PAU de Bogota

Por otra parte, la Direccion Administrativa y Financiera tendrá la obligación de hacer cumplir el contrato establecido con la entidad prestadora de servicios de seguridad, deberá solicitar y validar previamente los datos de identificación del personal de seguridad que resguarda cada una de las sedes de Capital Salud EPS-S, consultando en las bases de datos estatales de Procuraduría y Policía Nacional.

✓ **Alarmas de Seguridad:** Los sistemas de alarmas de seguridad son una pieza fundamental para el resguardo de los activos de Capital salud EPS-S por ello es necesario establecer los roles de los funcionarios encargados de administrar las contraseñas de inicio y cierre de cada sede de la entidad.

Estos usuarios y contraseñas son de carácter único e intransferible por lo cual se sobre entiende que no podrán ser prestados y/o utilizados por ninguna persona que no sea a quien se le allá delegado mediante acta de entrega (F21-TSI) y acuerdo de confidencialidad (F28-TSI).

Asignación de Usuarios y Contraseñas Alarmas de Seguridad:

- Coordinadores PAU: Tendrán configurados usuarios y contraseñas para activación y desactivación de alarmas de sistema de seguridad únicamente de la sede asignada, cada coordinador de PAU podrá contar con 2 Backup (Personas de confianza designadas por el coordinador de PAU con accesos para activar y desactivar las alarmas de seguridad).
- Gerentes Administrativas de Sucursal: Tendrán configurados usuarios y contraseñas para activación y desactivación de alarmas de sistema de seguridad únicamente de la sede asignada, cada Gerente Administrativo de Sucursal podrá contar con 1 Backup (Persona de confianza designada por Gerente Administrativo de Sucursal con accesos para activar y desactivar las alarmas de seguridad).

Seguimiento y Monitoreo

La Dirección de Tecnología hará seguimiento a los sistemas de alarmas de seguridad por medio de mensajes de correo electrónico almacenados en el buzón especial (NotificacionAlarma@capitalsalud.gov.co) mediante el cual se confirmarán activaciones y desactivaciones de los sistemas de seguridad de la entidad.

Vigencia y Complejidad de las Contraseñas de Alarmas de Seguridad

Por seguridad de cada una de las sedes de Capital Salud EPS-S la duración de cada contraseña será de máximo 20 días calendario, mínimo 10 caracteres, debe incluir letras mayúsculas, minúsculas, números y símbolos, la suma de cambio de contraseñas deberá ser superior o igual a 18 contraseñas diferentes al año.

- Desastres naturales: Además de los posibles problemas causados por ataques realizados por personas, es importante tener en cuenta que también los desastres naturales pueden tener muy graves consecuencias, sobre toda la infraestructura tecnológica, por esta razón se tienen en cuenta los siguientes:
- Terremotos y vibraciones: Los terremotos son el desastre natural menos probable en la mayoría de los organismos ubicados en Colombia, por lo que no se harán grandes inversiones en prevenirlos, aunque hay varias cosas que se pueden hacer sin un desembolso elevado y que son útiles para prevenir problemas causados por pequeñas vibraciones, las empleadas en Capital Salud EPS-S son:

  ✓ No situar equipos en sitios altos para evitar caídas.

  ✓ No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos.

  ✓ Separar los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen.

  ✓ Utilizar fijaciones para elementos críticos.

  ✓ Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.

  ▪ Tormentas eléctricas: Riesgo natural especialmente frecuente en invierno, que genera subidas súbitas de tensión muy superiores a las que pueda generar un problema en la red eléctrica. A parte de la protección mediante el uso de pararrayos, las únicas soluciones a este tipo de problemas son: desconectar los equipos ante una tormenta y la implementación de UPS con energía regulada.

  ✓ En el caso de Capital Salud EPS-S se utilizan UPS en todas las sedes, garantizando energía a los equipos críticos y usando como guía la siguiente formula con la cual calculamos un tiempo de soporte aproximado, dependiendo de la carga en tiempo real sobre la UPS.

  N = número de baterías en el SAI = 2
  V = voltaje de las baterías = 12
  AH = Amperios-Hora de las baterías = 9

Eff = eficiencia del SAI (por norma, suele oscilar entre el 90% y el 98% dependiendo del SAI) = aproximadamente 95%
VA = Volti-Amperios del SAI = 1000
Duración del SAI a carga máxima = ((2 x 12 x 9 x0.95)) /1000) x 60 = 12.31 minutos.

Una vez que sabemos que dura 12.31 minutos, tenemos que entender que este tiempo es lo que duraría el SAI al 100% de su capacidad.

- Inundaciones y humedad:

  - ✓ Humedad: En entornos normales es recomendable que haya un cierto grado de humedad, ya que en si el ambiente es extremadamente seco hay mucha electricidad estática. No obstante, tampoco interesa tener un nivel de humedad demasiado elevado, ya que puede producirse condensación en los circuitos integrados que den origen a corrosión y posiblemente un cortocircuito. En general no es necesario emplear ningún tipo de aparato para controlar la humedad, pero no está de más disponer de alarmas que nos avisen cuando haya niveles anómalos.
  - ✓ Inundaciones: Se encuentran dentro de las amenazas destructivas ya que casi cualquier medio (máquinas, cintas, routers...) que entren en contacto con el agua quedan automáticamente inutilizados, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos. Contra ellas podemos instalar sistemas de detección que apaguen los sistemas si se detecta agua y corten la corriente en cuanto estén apagados. Hay que indicar que los equipos deben estar por encima del sistema de detección de agua, sino cuando se intente parar ya estará mojado.

- Incendios y humos: el fuego y los humos, que en general provendrían de incendio de equipos por sobrecarga eléctrica. Contra ellos emplearemos sistemas de extinción, que, aunque pueden dañar los equipos que apaguemos, nos evitarán males mayores. Además del fuego, también el humo es perjudicial para los equipos, al ser un abrasivo que ataca a todos los componentes electrónicos, en Capital Salud EPS-S las áreas seguras se deberán mantener fuera del alcance de humo y agentes corrosivos.

- Alteraciones del entorno: En nuestro entorno de trabajo hay factores que pueden sufrir variaciones que afecten a nuestros sistemas los cuales tendremos que conocer e intentar controlar.
  Deberemos contemplar problemas que pueden afectar el régimen de funcionamiento habitual de las máquinas como la alimentación eléctrica, el ruido eléctrico producido por los equipos o los cambios bruscos de temperatura.

- Electricidad: Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo. En Capital Salud EPS-S para corregir los problemas con las subidas de tensión tenemos instaladas tomas de tierra que en conjunto con las SAI (Sistemas de Alimentación Ininterrumpida), además de proteger ante cortes mantienen el flujo de corriente constante, evitando las subidas y bajadas de tensión. Estos equipos disponen de baterías que permiten mantener varios minutos los aparatos conectados a ellos, permitiendo que los sistemas se apaguen de forma correcta, además de los problemas del sistema eléctrico también debemos preocuparnos de la corriente estática, que puede dañar los equipos. Para evitar problemas se emplean espráis antiestáticos o ionizadores y se tiene cuidado de no tocar componentes

metálicos, mediante sensores de humedad se controla de que el ambiente esté excesivamente seco minimizando el riesgo.

- Ruido eléctrico: El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos, y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación.

  Para prevenir los problemas que puede causar el ruido eléctrico en Capital Salud EPS-S se ajustó de tal manera que el hardware no estuviera cerca de los elementos que pueden causar el ruido. En caso de que fuese necesario hacerlo se instalaran filtros o se apantallaran las cajas de los equipos.

- Temperaturas extremas: En Capital Salud EPS-S entendemos que ya sea un calor excesivo o un frio intenso, perjudican gravemente a todos los equipos. Por lo cual mantenemos monitoreados a los equipos operando entre 10 y 32 grados Celsius. Para controlar la temperatura hacemos uso de termómetros ambientales.

2.19. POLÍTICA PARA USO DE TOKENS DE SEGURIDAD.

Capital Salud EPS-S proveerá las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y velará porque los funcionarios hagan un uso responsable de estos.

2.19.1. NORMAS PARA USO DE TOKENS DE SEGURIDAD.

Normas dirigidas a: AREAS USUARIAS DE TOKENS DE SEGURIDAD.

- Cada área usuaria de tokens de seguridad debe asignar un funcionario administrador de los mismos con la potestad para autorizar las solicitudes de acceso.

Normas dirigidas a: ADMINISTRADOR DE LOS TOKENS DE SEGURIDAD.

- El Administrador de los tokens de seguridad debe procesar las solicitudes de dichos tokens según los requerimientos de cada entidad proveedora de éstos y adjuntar la documentación necesaria para su utilización.
- El Administrador de los tokens debe recibirlos y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos de acuerdo con el navegador web autorizado por el ingeniero de Seguridad Informatica, para Capital Salud EPS-S en navegador autorizado será Microsoft EDGE.
- El Administrador de los tokens debe crear o solicitar creación de los usuarios y perfiles en cada portal o sitio de uso, según las actividades a realizar por cada funcionario creado.
- El Administrador de los tokens debe entregar a los funcionarios designados los usuarios y seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de acta y tula (o sobre) de seguridad para custodia de estos.
- El Administrador de los tokens debe dar avisos a las entidades emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de estos.
- El Administrador de los tokens debe realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.

Normas dirigidas a: USUARIOS DE TOKENS DE SEGURIDAD

- Los usuarios que requieren utilizar los tokens de seguridad deben contar con una cuenta de usuario en los portales o sitios de uso de estos; dichos tokens harán parte del inventario físico de cada usuario a quien se haya asignado, esta asignación debe estar acompañada de acta de entrega y acuerdo de confidencialidad.
- Los usuarios deben devolver el token asignado en estado operativo al Administrador de los tokens cuando el vínculo laboral con Capital Salud EPS-S se dé por terminado o haya cambio de cargo, para obtener paz y salvo, el cual será requerido para legalizar la finalización del vínculo con Capital Salud EPS-S.
- Cada usuario de los portales o sitios de uso de los tokens debe tener su propio dispositivo, el cual es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.
- El almacenamiento de los tokens debe efectuarse bajo estrictas medidas de seguridad, en la tula o sobre asignado para cada token, dentro de caja fuerte o escritorios con llave al interior de las áreas usuarias, de tal forma que se mantengan fuera del alcance de terceros no autorizados.
- Los usuarios deben notificar al Administrador de los tokens en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comunique con las entidades emisoras de dichos tokens.
- Los usuarios no deben permitir que terceras personas observen la clave que genera el token, así como no deben aceptar ayuda de terceros para la utilización del token.
- Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como funcionarios de Capital Salud EPS-S. En caso de que suceda algún evento irregular con los tokens los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.
- Los usuarios deben mantener los tokens asignados en un lugar seco y no introducirlos en agua u otros líquidos.
- Los usuarios deben evitar exponer los tokens a campos magnéticos y a temperaturas extremas.
- Los usuarios deben evitar que los tokens sean golpeados o sometidos a esfuerzo físico.
- Los usuarios no deben abrir los tokens, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.
- Los usuarios no deben usar los tokens fuera de las instalaciones de Capital Salud EPS-S para evitar pérdida o robo de estos.

2.20. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Objetivo:

Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y limitar el impacto de estos.

Alcance:

La política de gestión de incidentes de seguridad de la información está dirigida a toda persona que tenga legítimo acceso a los sistemas informáticos de Capital Salud EPS-S, incluso aquellos gestionados mediante contratos con terceros y lugares relacionados.

Normas dirigidas a: Dirección de Tecnología

La Dirección de Tecnología es responsable de:

- Disponer de los recursos necesarios a fin de brindar una apropiada gestión de los incidentes de seguridad, mediante la designación de un equipo responsable por la gestión de incidentes de seguridad de la información.
- Difundir la presente política a todo el personal del Organismo, independiente del cargo que desempeñe y de su situación contractual.

Todo el personal que trabaje en Capital Salud EPS-S es responsable por:

- Dar cumplimiento a la presente política, independiente del cargo que desempeñe y de su situación contractual.
- Reportar los eventos de seguridad informática que sean detectados a mesa de servicio con el fin de que estos sean gestionados por los administradores de la infraestructura en conjunto con el oficial de seguridad informática, siguiendo los procedimientos operativos establecidos para tal fin.

Normas dirigidas a: El Oficial de Seguridad en Capital Salud EPS-S:

- Adoptar medidas de seguridad eficientes para proteger sus activos de información críticos de acuerdo con la NTC – ISO – IEC 27035 - 2013.
- Analizar los eventos de seguridad informática para determinar si se trata de un incidente de seguridad de la información.
- Informar de forma completa e inmediata sobre la existencia de un potencial incidente de seguridad informática que afecte a activos de información críticos del Estado.
- Ejecutar procedimientos de repuesta a incidentes para contener y mitigar los incidentes.

2.21. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Objetivo:

Formar al personal en temas relacionados con la seguridad de la información, cuya finalidad sea disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

Normas dirigidas a: Clientes Internos y Externos

- Es deber de clientes internos y externos de Capital salud EPS-S leer, entender y dar cumplimiento a la política de seguridad de la información de la entidad.

Normas dirigidas a: Dirección de Tecnología

- Concientizar a clientes internos y externos sobre las vulnerabilidades latentes mediante boletines de seguridad a través de correo electrónico, fondo de pantalla institucional e intranet.

Normas dirigidas a: Gestión Humana

- Generar espacios de capacitación con el fin de concienciar a los funcionarios sobre temas relacionados con riesgos informáticos (perdida de información, robo de información, piratería, virus informáticos, etc).

2.22 POLÍTICA DE GESTION DE PROVEEDORES.

Capital Salud EPS-S identificará pautas para establecer y mantener relaciones claras y fortalecidas con aquellos terceros con quien se establezca una relación contractual bien sea de servicios o de productos, que aseguren el adecuado cumplimiento de los acuerdos establecidos, donde se garantice la aplicación de medidas de seguridad de la información en cumplimiento de los objetivos de la Entidad.

2.23 POLÍTICA DE GESTIÓN DE SEGURIDAD EN LA CONTINUIDAD DEL NEGOCIO.

La Entidad identificará las necesidades y requisitos de seguridad de la información para su vinculación en el plan de continuidad de negocio, de modo que se asegure que, ante situaciones de crisis o desastres, no se descuide los niveles de seguridad y se incurra en impactos indeseados.

2.24 POLÍTICA DE GESTIÓN DE CUMPLIMIENTO.

Capital Salud EPS-S mantendrá estrategias para la identificación y actualización de información acerca de legislación, normatividad o regulación nacional relacionada con la protección de datos y/o seguridad de la información para las cuales se deba enfocar estricto cumplimiento.

La Entidad mantendrá el inventario y actividades de actualización de toda aquella legislación o regulación nacional relacionada con la protección de datos y/o seguridad de la información para las cuales se deba enfocar estricto cumplimiento.

2.25 POLÍTICA DE INCORPORACIÓN AL CUMPLIMIENTO REGULATORIO.

Toda solución de servicios o infraestructura tecnológica debe cumplir con las condiciones contractuales, de legislación y regulación externa o interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la Entidad.

2.26 POLÍTICA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

Capital Salud EPS-S en cumplimiento con lo exigido por el grupo de acceso a la información y protección de datos personales y lo establecido en los ítems de la NORMA ISO 27001, adopta las siguientes políticas en cuanto a la Adquisición, desarrollo y mantenimiento de los sistemas de información.

2.26.1 POLÍTICA PARA REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

La Dirección de Tecnología asegurará que el software adquirido y desarrollado tanto al interior del instituto, como por terceras partes cumplirá con los requisitos de seguridad y calidad establecidos.

Normas para los requerimientos de seguridad de los sistemas informáticos:

- Aprobar la adquisición y/o desarrollo de software, de tal forma que se garantice la compatibilidad, integración con las plataformas de Capital Salud.

- Establecer una metodología para el desarrollo de software, que incluya la definición de requerimientos de seguridad y las buenas prácticas para el desarrollo seguro, con el fin de proporcionar a los terceros (proveedores) de sistemas de información un punto de vista más claro, enmarcados dentro de la arquitectura de seguridad, software y hardware.
- Incluir en la definición de requerimientos de seguridad de los sistemas de información aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones entre otros.
- Los terceros proveedores de sistemas de información deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se desee desarrollar, de acuerdo con los parámetros de seguridad y controles deseados.
- Los terceros proveedores de sistemas de información deben garantizar que todo sistema de información adquirido o desarrollado debe usar herramientas de desarrollo licenciadas y reconocidas.
- Los terceros proveedores de sistemas de información deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los terceros proveedores de sistemas de información deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla el tiempo.
- Los terceros proveedores de sistemas de información deben garantizar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.

2.26.2 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS.

La Dirección de Tecnología, brindara por medio de solicitud herramientas de cifrado que permitan proteger la confidencialidad, integridad y disponibilidad de la información sensible o no pública.

- Velar porque la información digital clasificada como publica sea almacenada y/o transmitida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.
- Desarrollar y establecer mecanismos para el manejo y administración de llaves de cifrado.
- Verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información no publica, cuente con mecanismos de cifrado de datos.
- Corroborar los requisitos legales aplicables a la utilización de mecanismos de cifrado.
- Las llaves serán protegidas contra modificación y destrucción; las llaves privadas serán protegidas contra uso inapropiado.
- En caso de robo, pérdida o divulgación de las llaves de cifrado debe ser reportado a la Dirección de Tecnología.

2.26.3 POLÍTICA DE SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE.

Capital Salud asegurara que el software desarrollado internamente o adquirido a través de terceras partes debe cumplir con los requerimientos de seguridad resguardando la disponibilidad, integridad y confidencialidad de la información manteniendo mecanismos de seguridad en todo el ciclo de vida de desarrollo y mantenimiento; así mismo los desarrolladores revisaran y determinaran la acción a seguir para el tratamiento de las vulnerabilidades con el fin de cerrar brechas de seguridad.

Normas de Seguridad en los procesos de desarrollo y soporte:

- Identificar que los requisitos de seguridad en las fases del ciclo de vida de desarrollo de software y se deben justificar y documentar.
- Se deben realizar pruebas de seguridad en un ambiente de pruebas con el fin de identificar vulnerabilidades antes de realizar el paso a producción.
- Se deben tener ambiente de producción y ambiente de prueba cada uno de ellos debe estar separado.
- El ambiente de prueba debe ser igual al ambiente de producción.
- Realizar cambio de versión de aplicaciones implementadas en ambientes productivos debe realizarse bajo el procedimiento de control de cambios.
- Contar con controles de seguridad para mantener la integridad y disponibilidad de los datos y sistemas de información para ello debe hacer una copia de respaldo en caso de que se deba restablecer el servicio.
- La Dirección de Tecnología aplicará mecanismos de prueba de aceptación de nuevos sistemas de información, actualizaciones y versiones nuevas, así como supervisar, monitorear la actividad del desarrollo de los sistemas tercerizados y realizar pruebas de funcionalidad de la seguridad.
- Hardware o software que se vaya adquirir y/o conectar a la infraestructura debe ser adquirido por intermedio de la Dirección de Tecnología y gestionado por la misma Oficina para su correcta gestión y seguimiento.
- El software suministrado por Capital Salud no debe ser suministrado a terceros.
- El software que se adquiera en la entidad debe ser licenciado a nombre de Capital Salud.

2.26.4 POLÍTICA GESTIÓN DE LA VULNERABILIDAD TÉCNICA.

La Dirección de Tecnología realizara periódicamente (una vez al año) un análisis de vulnerabilidades a las plataformas tecnologías de la entidad con el fin de hallar vulnerabilidades que puedan afectar la operación interna y así mismo mitigarlas a través de estos análisis.

Normas de Gestión de la vulnerabilidad Técnica:

- Revisar periódicamente la aparición de nuevas vulnerabilidades técnicas estas serán reportadas a los administradores de las plataformas tecnológicas con el fin de mitigar las mismas.
- Verificar la información publicada por parte de los fabricantes y foros de seguridad en identificación de nuevas amenazas que puedan afectar los sistemas de Capital Salud.
- Generar los procedimientos a seguir para la configuración segura de las plataformas tecnológicas.
- Realizar al menos una vez al año un plan de análisis de vulnerabilidades y/o hacking ético a las plataformas tecnológicas, que cumplan con los estándares establecidos.

3. ALCANCE:

El documento define las Políticas que deberán ser aceptadas y aplicadas de manera obligatoria a todos los trabajadores, colaboradores y terceros que tengan acceso a información a través de documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la entidad.

4. ORIGEN: Interno.

5. PLAZO: Largo plazo.

6. RECURSOS NECESARIOS PARA EL DESARROLLO DE LA POLÍTICA: Recurso Humano y Tecnológico.

7. PERIODICIDAD: Trimestral.

8. ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN:

La información transmitida en el marco de colaboración, negociación, ejercicio de funciones y/o proyectos tiene carácter confidencial y, así, aceptan no divulgarla y mantener la más estricta confidencialidad respecto a dicha información, advirtiendo, en su caso, de dicho deber de confidencialidad y secreto a sus trabajadores, contratistas y a cualquier persona que, por su cargo o relación con la Entidad, deba tener acceso a dicha información.

Ninguno de los trabajadores podrá reproducir, modificar, hacer pública o divulgar a terceros la información, sin previa autorización escrita y expresa de la Entidad.

El empleado acepta y declara que se somete a las responsabilidades y sanciones que por omisión a este acuerdo le sean imputables, sin perjuicio de las responsabilidades civiles o penales a que hubiere lugar en virtud de la ley.

El presente Acuerdo de Confidencialidad de la Información, tendrá vigencia durante el tiempo que el empleado preste sus servicios a Capital Salud EPS-S; y, por ética profesional, posteriormente a su salida de la institución, sin perjuicio de que se vaya adoptando nuevas medidas de seguridad, las cuales serán parte de este acuerdo.

9. SANCIONES POR INCUMPLIMIENTO:

El incumplimiento a las políticas establecidas en el presente documento traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a seguridad y privacidad de la información se refiere.

10. REFERENCIAS

DOCUMENTOS DE REFERENCIA	
CÓDIGO	**NOMBRE DEL DOCUMENTO**
LEY 23 DE 1982	Sobre Derechos de Autor. Congreso de la República. Disponible en Línea http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431 [Consultado en junio de 2017]
CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15.	"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Disponible en Línea: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15 [Consultado en junio de 2017]
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. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276 [Consultado en junio de 2017]
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. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488 [Consultado en junio de 2017]
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. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492 [Consultado en junio de 2017]
DECRETO 4632 DE 2011	Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones. Disponible en Línea: http://wsp.presidencia.gov.co/Normativa/Decretos/2011/Documents/Diciembre/09/dec463209122011.pdf [Consultado en junio de 2017]
LEY ESTATUTARIA 1581 DE 2012,	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Consultado en junio de 2017]

DOCUMENTOS DE REFERENCIA	
CÓDIGO	**NOMBRE DEL DOCUMENTO**
MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	Modelo de Seguridad y Privacidad de la Información alineado con la Estrategia de Gobierno en línea para ser adoptado por todas las entidades estatales Disponible en Línea: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf [Consultado en octubre de 2018]
NORMA TECNICA COLOMBIANA ISO27000	Contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información, Disponible en Línea: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjlh8quoKDeAhWIzFMKHTspDIIQFjABegQIChAC&url=https%3A%2F%2Ftienda.icontec.org%2Fwp-content%2Fuploads%2Fpdfs%2FNTC-ISO-IEC27000.pdf&usg=AOvVaw3zcBlpFRBDilwc3ePlVyrr. [Consultado en octubre de 2018]
NORMA TECNICA COLOMBIANA ISO27001	Norma técnica colombiana que describe cómo gestionar la seguridad de la información en una empresa. Disponible en Línea: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwj2ypXloKDeAhWJ7FMKHYzaDUUQFjACegQICBAC&url=https%3A%2F%2Ftienda.icontec.org%2Fwp-content%2Fuploads%2Fpdfs%2FNTC-ISO-IEC27001.pdf&usg=AOvVaw1nA0ja885WYUobjeD28P8d. [Consultado en octubre de 2018]

11. ELABORACIÓN, REVISIÓN Y APROBACIÓN DE LA POLITICA:

NOMBRE RESPONSABLE DE LA ELABORACION	Fabian Villamil Beltrán	**CARGO**	Ingeniero de Seguridad Informática
FECHA DE MODIFICACIÓN	Enero 2022		
NOMBRE RESPONSABLE DE LA REVISION	Jhon Alexander Cepeda Zafra	**CARGO**	Director de Tecnología
FECHA DE REVISIÓN	Enero 2022		
NOMBRE RESPONSABLE DE LA APROBACION	Jhon Alexander Cepeda Zafra	**CARGO**	Director de Tecnología
FECHA DE APROBACION	Enero 2022		

JHON ALEXANDER CEPEDA ZAFRA
Director de Tecnología

FABIAN VILLAMIL BELTRÁN
Ingeniero de Seguridad Informática