TABLA DE CONTENIDO

INTRODUCCIÓN

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de las Políticas y Estándares adecuados con el objetivo de minimizar los riesgos. Hoy es imposible hablar de un sistema 100% seguro, sencillamente porque el costo de la seguridad total es muy alto.

Las Políticas de Seguridad de la Información son un plan de acción de las empresas para afrontar riesgos de seguridad, surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una compañía sobre la importancia y sensibilidad de la información. La creación de una política corporativa permite a la empresa desarrollarse y mantenerse en su sector de negocios. Esta política debe ser elaborada y aprobada desde la alta dirección de la empresa y debe considerar compromiso de todas las áreas, ya que es una actividad colectiva.

Sin embargo, es una ardua tarea homogenizar esta información, más aún cuando nuestra empresa posee distintas áreas que requieren un enfoque diferente sobre la seguridad, de aquí nace la necesidad de que sea de conocimiento general.

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la Red de Salud del Centro E.S.E en materia de seguridad.

1. OBJETIVO

Establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal de la Red de Salud del Centro E.S.E, para que sea de su conocimiento y obligatorio cumplimiento en la utilización los recursos informáticos asignados.

1.1. OBJETIVOS ESPECIFICOS

Se establecen el alcance a cada política como; seguridad del personal, seguridad física y ambiental, seguridad y administración de equipos de cómputo, controles de acceso lógico, cumplimiento de seguridad informática y políticas del teletrabajo.

2. ALCANCE

El documento define las Políticas y Estándares de Seguridad que deberán adoptar de manera obligatoria todos los usuarios (funcionarios, colaboradores, terceros, aprendices, practicantes) para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos de la Red de Salud del Centro E.S.E.

3. DEFINICIONES

Acceso Físico: Es la actividad de ingresar a un área.

Acceso Lógico: Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.

Acceso Remoto: Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación, ya sean telefónicas o por medio de redes de área amplia, que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.

Antivirus: Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.

Ataque: Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo.

Base de datos: Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.

Confidencialidad: Se refiere a la obligación de los servidores judiciales a no divulgar información a personal no autorizado para su conocimiento.

Contraseña: Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular.

Control de Acceso: Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.

Copyright: Derecho que tiene un autor, incluido el autor de un programa informático sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o generosa como el autor decida. Proceso de Gestión de Tecnologías y la Información: Se refiere al proceso de la Red de Salud del Centro E.S.E encargado de las Tecnologías de la Información y Comunicaciones. Disponibilidad: Se refiere a que la información esté disponible en el momento que se necesite.

Estándar: Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.

Falta administrativa: Acción u omisión contemplada por la normatividad aplicable a la actividad de un servidor judicial, mediante la cual se finca responsabilidad y se sanciona esa acción u omisión.

FTP: Protocolo de transferencia de archivos. Es un protocolo estándar de comunicación que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.

Gusano: Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el

gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.

Hardware: Se refiere a las características técnicas y físicas de las computadoras. Herramientas de seguridad: Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.

Identificador de Usuario: Nombre de usuario (también referido como UserID) único asignado a un servidor judicial para el acceso a equipos y sistemas desarrollados, permitiendo su identificación en los registros.

Impacto: Magnitud del daño ocasionado a un activo en caso de que se materialice.

Incidente de Seguridad: Cualquier evento que represente un riesgo para la adecuada conservación de confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.

Integridad: Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.

Internet: Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes (world wide web) en donde cualquier usuario consulta información de otra computadora conectada a esta red e incluso sin tener permisos.

Intrusión: Es la acción de introducirse o acceder sin autorización a un activo.

Maltrato: Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad del Supremo Tribunal de Justicia. Se contemplan dentro de éste al descuido y la negligencia.

Malware: Código malicioso desarrollado para causar daños en equipos informáticos, sin el consentimiento del propietario. Dentro de estos códigos se encuentran: virus, spyware, troyanos, rootkits, backdoors, adware y gusanos.

Mecanismos de seguridad o de control: Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir 34 la probabilidad de que una vulnerabilidad exista sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

Medios de almacenamiento magnéticos: Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CD's, DVD's, etc.)

Módem: Es un aparato electrónico que se adapta una terminal o computadora y se conecta a una red de. Los módems convierten los pulsos digitales de una computadora en frecuencias dentro de la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.

"Necesidad de saber" principio: Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades dentro de la Comisión.

Normatividad: Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.

Password: Véase Contraseña.

Respaldo: Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

Riesgo: Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene.

Servidor: Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

Sitio Web: El sitio web es un lugar virtual en el ambiente de internet, el cual proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a él.

Software: Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.

Spyware: Código malicioso desarrollado para infiltrar a la información de un equipo o sistema con la finalidad de extraer información sin la autorización del propietario.

UserID: Véase Identificador de Usuario.

Usuario: Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware). 35

Virus: Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o medios de almacenamiento magnético de computadoras.

Vulnerabilidad: Es una debilidad de seguridad o brecha de seguridad, la cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental.

4. MARCO LEGAL

ISO 27001, Ley 1273 de 2009

5. RESPONSABILIDADES

Gerente – Aprueba políticas y recursos

Directivos, Lideres, coordinadores, jefes, funcionarios – Realizan y cumplen lo establecido en el documento.

6. TALENTO HUMANO REQUERIDO

Ing. de Sistemas con conocimientos en seguridad informática

7. MATERIALES, INSUMOS Y EQUIPOS REQUERIDOS

Equipos de cómputo, red de datos, correo electrónico

8. MARCO TEORICO

La elaboración de esta política debe tener total aprobación por parte de la Gerencia y Directivos, dado que de aquí depende en el apoyo de que se cumpla lo aquí estipulado por todos los funcionarios y proveedores externos de la compañía, se debe tener una concientización del riesgo que corre nuestra información, hardware y software al pasar por alto alguna de estas políticas y es deber de todos cumplirla y hacerla cumplir, en este se informa los posibles fallos que se pueden llegar a tener y cuál es su parte preventiva y tips para que no se materialicen esos riesgos. Es por eso por lo que el capítulo de desarrollo del plan se clasifica en 6 políticas y se amplían el detalle de cada una.

9. DESARROLLO DEL PROGRAMA

9.1 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política Corporativa de seguridad de la información en la Red de Salud del Centro E.S.E la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Todos los usuarios de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de la Red de Salud del Centro E.S.E., así como el estricto cumplimiento al Manual de Políticas y Estándares de Seguridad Informática para usuarios.

9.1.1. Responsabilidades de los Usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática de la Red de Salud del Centro E.S.E. contenidas en el presente manual.

9.1.2 Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos de la Red de Salud del Centro E.S.E. deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información de la Red de Salud del Centro E.S.E

9.1.3. Entrenamiento en Seguridad Informática

Todo funcionario o colaborador que ingrese a la Red de Salud del Centro E.S.E deberá:
Leer el Manual de Políticas y Estándares de Seguridad Informática para Usuarios de la Red de Salud del Centro E.S.E, el cual se encuentra disponible la plataforma “Almera” en el proceso estratégico Gestión de Tecnologías y la Información y en los escritorios de todos los equipos de cómputo donde se dan a conocer las obligaciones para los usuarios y las sanciones que pueden aplicar en caso de incumplimiento.

9.1.4. Medidas disciplinarias

Cuando el Proceso de Gestión de Tecnologías y la Información identifique el incumplimiento al presente Manual emitirá el reporte o denuncia a quien corresponda, para los efectos de su competencia y atribuciones.

9.2 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Red de Salud del Centro E.S.E, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como a las instalaciones y los diferentes Centros de Cómputo la Red de Salud del Centro E.S.E

9.2.1 Resguardo y protección de la información

9.2.1.1 El usuario deberá reportar de forma inmediata al Proceso de Gestión de Tecnologías y la Información, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser robos, saboteos, fugas de agua, conatos de incendio u otros.

9.2.1.2 El usuario tiene la obligación de proteger los CDs, DVDs, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración y contengan información reservada o confidencial.

9.2.1.3 El uso de memoria estará restringido por medio de los puertos USB de los computadores en modo propiedad o alquiler a cargo de la Red de Salud Centro E.S.E y solo se harán las excepciones que la Gerencia y el proceso de Gestión de Tecnologías y la Información determinen con su respectiva información de responsabilidad aquel que tenga el acceso (Una vez introducida la memoria USB en un equipo de cómputo esta debe ser analizada por el antivirus el cual debe estar actualizado).

9.2.1.4 Es responsabilidad del usuario evitar en todo momento la fuga de la información de la Red de Salud del Centro E.S.E que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

9.2.2 Controles de acceso físico

9.2.2.1 Cualquier persona que tenga acceso a las instalaciones de la Red de Salud del Centro E.S.E, deberá registrar en las bitácoras de las personas de seguridad, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la Red de Salud del Centro E.S.E, el cual podrán retirar el mismo día, sin necesidad de trámite alguno.

En caso de que el equipo que no es propiedad de la Red de Salud del Centro E.S.E, permanezca dentro de la institución más de un día hábil, es necesaria la elaboración de una orden de salida.

9.2.3 Seguridad en áreas de trabajo

Los Centros de datos de la Red de Salud del Centro E.S.E son áreas restringidas, por lo que sólo el personal autorizado por el área de Gestión de Tecnologías y la Información puede acceder a ellos.

9.2.4 Copias de seguridad

La Red de Salud del Centro E.S.E debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por el Proceso de Gestión de Tecnologías y la Información y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

El Proceso de Gestión de Tecnologías y la Información tiene establecidos procedimientos explícitos de resguardo y recuperación de la información, especificaciones acerca del traslado, frecuencia, identificación y los períodos de retención de esta. Dispone de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios magnéticos que contienen la información crítica deben ser almacenados en la oficina que el proceso de Gestión Documental determine con la recomendación de establecer los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

9.2.4.1 Todo equipo de cómputo del área administrativa y quien lo requiera del área asistencial se le realizará copia de seguridad a las carpetas “Mis Documentos” y “Escritorio” según programación que realizará el Proceso de Gestión de Tecnologías y la Información. Toda información en otra ubicación y que no sea informada la necesidad de copia de seguridad, corre por cuenta y riesgo del usuario.

9.2.4.2 En caso de requerirse la recuperación de información resguardada, este procedimiento deberá requerirse por documento escrito al Proceso de Gestión de Tecnologías y la Información con el visto bueno del líder de proceso.

9.2.5 Energía regulada

9.2.5.1 La Red de Salud del Centro E.S.E dispone de alimentación de energía regulada exclusivamente para el soporte eléctrico a los equipos de cómputo y comunicaciones. En ningún caso se deben conectar en la energía regulada (toma de corriente anaranjado) celulares, ventiladores, radios, cafeteras, impresoras láser u otros dispositivos eléctricos o electrónicos.

9.2.5.2 Como medio de protección del medio ambiente, los equipos deberán permanecer encendidos solamente en horas laborables, para evitar el consumo innecesario de energía.

9.2.5.3 Asegúrese, antes de retirarse de su puesto de trabajo que todos los dispositivos se encuentren apagados: CPU, monitor e impresora. En los casos de cambio de turnos, el computador debe ser reiniciado en el momento de la entrega del turno.

9.2.6 Acceso remoto

9.2.6.1 La conexión desde redes externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de la Red de Salud del Centro E.S.E, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el Proceso de Gestión de Tecnologías y la Información.

9.2.6.2 No está permitida la conexión de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos a través de los cuales se puedan realizar intercambios de información con cualquier recurso de la Red de Salud del Centro E.S.E.

9.2.7 Redes inalámbricas - WiFi

La Red Inalámbrica es una extensión de la red local de la Red de Salud del Centro E.S.E que permite el acceso a Internet y otros servicios informáticos sin necesidad de disponer de una conexión por cable a la red.

La comunicación se realiza a través de radiofrecuencia entre el dispositivo móvil portátil, celular, tableta, etc. y los AP (Access Point) o puntos de acceso distribuidos en algunas de las IPSs.

Este servicio es para uso exclusivo de funcionarios o colaboradores y para fines exclusivamente relacionados con la actividad laboral. El funcionario que requiera de dicho servicio debe facilitar información propia del dispositivo (Mac Address) para ser registrado en la plataforma y luego reconocido por las redes inalámbricas.

El líder de proceso, comuna o área autorizará el registro de equipos de conexión inalámbrica de personal a su cargo y realizará la solicitud correspondiente a Gestión de Tecnologías y la Información.

El uso de los canales inalámbricos será exclusivo para facilitar las comunicaciones y queda expresamente prohibido utilizarlos para escuchar música, observar videos o descarga de material audiovisual.

9.2.8 Fondo de escritorio y protector de pantalla

La Red de Salud del Centro E.S.E utiliza fondos de escritorio y protectores de pantalla institucionales como un medio para difundir información de importancia que concierne a todos los usuarios, por lo tanto, es no está permitido realizar modificaciones a estos elementos en los equipos de cómputo.

9.2.9 Protección y ubicación de los equipos

9.2.9.1. Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de estos sin la autorización del Proceso de Gestión de Tecnologías y la Información, debiéndose solicitar a la misma en caso de requerir este servicio.

9.2.9.2. El proceso de activos fijos de la Red de Salud del Centro E.S.E será el encargado de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el departamento de Gestión de Tecnologías y la Información.

9.2.9.3. El equipo de cómputo asignado será para uso exclusivo de las funciones asignadas al usuario en la Red de Salud del Centro E.S.E. y sólo se grabará información propia del ejercicio de sus funciones.

9.2.9.4. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que utiliza en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

9.2.9.5. Es responsabilidad de los usuarios almacenar su información únicamente en las carpetas “Escritorio” y “Mis Documentos” que son los directorios de trabajo recomendados y a los que se les programa copia de seguridad.

9.2.9.6. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

9.2.9.7. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o de la CPU.

9.2.9.8. Se debe mantener el equipo informático en un entorno limpio y sin humedad.

9.2.9.9. El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

9.2.9.10. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una anticipación no inferior a tres días hábiles al Proceso de Gestión de Tecnologías y la Información a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.

9.2.9.11. Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello se hace responsable de cualquier daño que pueda derivar de esta acción.

9.2.10. Mantenimiento de equipo

9.2.10.1. Únicamente el personal perteneciente al Proceso de Gestión de Tecnologías y la Información y proveedores debidamente autorizados podrán llevar a cabo los servicios y reparaciones al equipo informático.

9.2.10.2. Ningún funcionario realizará tareas de instalación de equipo, de programas (software) o de reparación, así cuente con capacitación técnica o profesional para realizarlo, ya que debe contar con una cuenta de “administrador” y de obtenerla de manera irregular estará en falta grave; dicha actividad es responsabilidad del personal que se contrate para dicho mantenimiento.

9.2.10.3. Los usuarios deberán asegurarse de informar acerca de la información que considere relevante cuando el equipo sea enviado a reparación y asegurarse del respaldo de aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal del Proceso de Gestión de Tecnologías y la Información.

9.2.10.4 Cuando el funcionario responsable de un equipo de cómputo detecte problemas en el funcionamiento de este (parte lógica o física), está obligado a comunicar inmediatamente al líder de proceso para que se proceda a verificar el equipo y se emita un diagnóstico donde se determinará las pautas a corregir la falla o referir la reparación.

9.2.10.5 El Proceso de Gestión de Tecnologías y la Información programará el mantenimiento preventivo de los equipos de cómputo de la Red de Salud del Centro E.S.E dos veces al año, para tal fin elaborará y divulgará los cronogramas con suficiente anticipación. El usuario está en el deber de facilitar su equipo en la fecha y hora que aparecen en el cronograma.

9.2.11. Pérdida o transferencia de equipo

9.2.11.1. El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo con la normatividad vigente en los casos de robo, extravío o pérdida de este.

9.2.11.2. El resguardo para los equipos portátiles tiene el carácter de personal y será intransferible.

9.2.11.3. El usuario deberá dar aviso de inmediato al Proceso de Gestión de Tecnologías y la Información por la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

9.2.12. Uso de dispositivos especiales

9.2.12.1. El uso de los grabadores de discos compactos “Quemadores” es exclusivo para respaldos de información que por su volumen así lo justifiquen.

9.2.12.2. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

9.2.13. Daño del equipo

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna avería por maltrato, descuido o negligencia por parte del usuario, éste deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso la determinará la causa de dicha avería.

9.3 POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura de la Red de Salud del Centro E.S.E. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la Red de Salud del Centro E.S.E o hacia redes externas como internet.

Los usuarios de la Red de Salud del Centro E.S.E que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, malware o spyware. El usuario puede acudir al Proceso de Gestión de Tecnologías y la Información, o al representante de ésta en su comuna, para solicitar asesoría.

9.3.1. Uso de medios de almacenamiento

9.3.1.1. Toda solicitud para utilizar un medio de almacenamiento de información compartido deberá contar con la autorización del titular del área dueña de la información y ajustarse a las directrices que se manejan para este tipo de carpetas, en ningún momento podrán convertirse en depósitos archivos.

Dicha solicitud deberá explicar en forma clara y concisa los fines para los que se otorgará la autorización, ese documento se presentará con firma del líder del proceso involucrado y del líder del Proceso de Gestión de Tecnologías y la Información.

9.3.1.2. El Proceso de Gestión de Tecnologías y la Información respalda de manera periódica la información sensible y crítica que se encuentre en sus computadores, en las carpetas autorizadas.

9.3.1.3. En caso de que se requiera algún respaldo de información a algún medio externo, este servicio deberá solicitarse o autorizarse por escrito por el Proceso de Gestión de Tecnologías y la Información.

9.3.1.4. Los trabajadores o colaboradores de la Red de Salud del Centro E.S.E deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones propias para su cargo.

9.3.1.5. Las actividades que realicen los usuarios de la Red de Salud del Centro E.S.E en la infraestructura de Tecnología de la Información son registradas y susceptibles de auditoría.

9.3.2. Instalación de Software

9.3.2.1. Los usuarios que requieran la instalación de software que no sea propiedad de la Red de Salud del Centro E.S.E, deberán justificar su uso y solicitar autorización al Proceso de Gestión de Tecnologías y la Información, a través de un oficio firmado por su líder del proceso, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software presente la factura de compra de dicho software.

Si el dueño del software no presenta la factura de compra del software, el personal asignado por el Proceso de Gestión de Tecnologías y la Información de manera inmediata a desinstalar dicho software.

9.3.2.2. Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, así sea software libre (celulares, cámaras, etc.), servidores, o cualquier equipo conectado a la red de la Red de Salud del Centro E.S.E, que no esté autorizado por el Proceso de Gestión de Tecnologías y la Información.

9.3.3. Identificación del incidente

9.3.3.1. El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo al Proceso de Gestión de Tecnologías y la Información o al encargado de la comuna, lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

9.3.3.2. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar a su líder de proceso.

9.3.3.3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la Red de Salud del Centro E.S.E, debe ser reportado al Proceso de Gestión de Tecnologías y la Información.

9.3.4. Administración de la configuración

Los usuarios de las áreas de la Red de Salud del Centro E.S.E no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la Red de Salud del Centro E.S.E, sin la autorización por escrito del Proceso de Gestión de Tecnologías y la Información quien llevará los registros pertinentes.

9.3.5. Seguridad de la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Proceso de Gestión de Tecnologías y la Información en la cual los usuarios realicen la exploración de los recursos informáticos en la red de datos de la Red de Salud del Centro E.S.E, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

El Proceso de Gestión de Tecnologías y la Información se reserva el derecho de suspender o eliminar el acceso a cualquier equipo de cómputo a cualquier usuario, sin previo aviso al mismo, si el hacerlo es necesario para mantener la disponibilidad, seguridad e integridad de las operaciones para los demás usuarios de los recursos o de la Red de Salud del Centro E.S.E, o

cuando se presuma alguna falta o violación a este reglamento u otros pertinentes que amerite este tipo de acciones para el proceso de investigación.

9.3.6. Uso del correo electrónico institucional

9.3.6.1. Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentra fuera o ausente), el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la Red de Salud del Centro E.S.E, a menos que cuente con la autorización del líder del proceso al que pertenece.

9.3.6.2. Los mensajes y la información contenida en los buzones de correo son propiedad de la Red de Salud del Centro E.S.E y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

9.3.6.3. Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó el Proceso de Gestión de Tecnologías y la Información.

9.3.6.4. La Red de Salud del Centro E.S.E, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad violando políticas de Seguridad Informática de la Red de Salud del Centro E.S.E o realizado acciones no autorizadas.

Como la información del correo electrónico institucional de la Red de Salud del Centro E.S.E es privada, la única forma en la que puede ser revelada es mediante una orden judicial.

9.3.6.5. El usuario debe de utilizar el correo electrónico de la Red de Salud del Centro E.S.E, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto. El tamaño de los buzones de correo es determinado por el Proceso de Gestión de Tecnologías y la Información de acuerdo con las necesidades de cada usuario.

9.3.6.6. La asignación de una cuenta de correo electrónico externo deberá solicitarse por escrito al Proceso de Gestión de Tecnologías y la Información, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del líder del proceso que le corresponda.

9.3.6.7. Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

9.3.6.8 Expresamente No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico de la Red de Salud del Centro E.S.E como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, YouTube, WhatsApp, Instagram, TikTok, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales. Ni para realizar registros en plataformas externas.
- El envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia.

• El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por el Proceso de Gestión de Tecnologías y la Información.

9.3.6.9 El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que la Red de Salud del Centro E.S.E proporciona. De igual manera, las cuentas de correo personales no se deben emplear para uso institucional a no ser que se cuente con las respectivas autorizaciones del líder de proceso y visto bueno del líder de Gestión de Tecnologías y la Información.

9.3.6.10 El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación del Proceso de Gestión de Tecnologías y la Información. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre de la dependencia respectiva y/o servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.

9.3.6.11 Toda información de la Red de Salud del Centro E.S.E generada con los diferentes programas computacionales (Ej. Servinte, Rfast8, Office, Open Office, Access, WordPad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas de Tecnología. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

9.3.6.12 Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la Red de Salud del Centro E.S.E y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

9.3.7 Uso del programa de mensajería instantánea Spark

9.3.7.1 Los usuarios de los equipos de cómputo están en la obligación de mantener activo el programa de mensajería instantánea Spark, por ser un medio de comunicación institucional.

9.3.7.2 Los mensajes deben utilizarse para intercambiar comunicaciones sobres aspectos relacionados con el ejercicio de sus labores o que vayan en el beneficio de la comunidad de la Red de Salud del Centro E.S.E.

9.3.7.3 En la construcción de los mensajes se deben observar las normas mínimas de las relaciones humanas y la netiqueta.

9.3.7.4 Los usuarios tienen la potestad de crear tantos grupos de Spark como considere necesarios con el fin de focalizar sus mensajes de difusión y así evitar interferir en las actividades de otras personas.

9.3.7.5 El envío de zumbidos está expresamente prohibido y debe ser utilizado sólo en casos de urgencia.

9.3.8. Controles contra código malicioso

9.3.8.1 Para prevenir infecciones por virus informáticos, los usuarios de la Red de Salud del Centro E.S.E, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por el Proceso de Gestión de Tecnologías y la Información.

9.3.8.2 Los usuarios de la Red de Salud del Centro E.S.E, antes de utilizar cualquier información que esté almacena en memorias USB, discos externos, CD, etc., deben verificar mediante el antivirus que estén libres de cualquier tipo de código malicioso.

9.3.8.3 El usuario debe verificar mediante el software de antivirus instalado en su equipo que estén libres de virus todos los archivos: bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, considerando los que tengan que ser descomprimidos.

9.3.8.4 Ningún usuario de la Red de Salud del Centro E.S.E debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Tampoco debe probarlos en cualquiera de los ambientes o plataformas de la Red de Salud del Centro E.S.E. El incumplimiento de este estándar será considerado una falta grave.

9.3.8.5 Ningún usuario ni colaborador de la Red de Salud del Centro E.S.E o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Proceso de Gestión de Tecnologías y la Información.

9.3.8.6 Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y comunicarse inmediatamente con personal autorizado del Proceso de Gestión de Tecnologías y la Información para la toma de medidas pertinentes.

9.3.8.7 Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar de manera periódica al Proceso de Gestión de Tecnologías y la Información las actualizaciones del software de antivirus.

9.3.8.8 Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el Proceso de Gestión de Tecnologías y la Información en programas tales como: antivirus, correo electrónico, programas de ofimática y navegadores.

9.3.8.9 Debido a que algunos virus son extremadamente complejos, ningún usuario de la Red de Salud del Centro E.S.E debe intentar erradicarlos de los computadores, lo indicado es llamar al personal del Proceso de Gestión de Tecnologías y la Información para que sean ellos quienes lo solucionen.

9.3.9. Permisos de uso de internet

9.3.9.1 El acceso a internet provisto a los usuarios de la Red de Salud del Centro E.S.E es exclusivamente para las actividades relacionadas con las necesidades del cargo y función que desempeña.

9.3.9.2 La asignación del servicio de internet acorde a las labores a realizar se instalará previamente en todos los equipos de la Red de Salud del Centro E.S.E, cualquier adición deberá solicitarse por escrito al Proceso de Gestión de Tecnologías y la Información, señalando los motivos por los que se desea la ampliación del servicio. Esta solicitud deberá contar con el visto bueno del líder de proceso y el Subgerente Administrativo.

9.3.9.3 Todos los accesos a internet tienen que ser realizados a través de los canales provistos por la Red de Salud del Centro E.S.E.

9.3.9.4 Los usuarios con acceso a Internet de la Red de Salud del Centro E.S.E tienen que reportar todos los incidentes de seguridad informática inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

9.3.9.5 El acceso a internet a través de canales no convencionales tiene que ser previamente autorizado por el Proceso de Gestión de Tecnologías y la Información.

9.3.9.6 Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:

- Serán sujetos de monitoreo de las actividades que realizan en internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización del Proceso de Gestión de Tecnologías y la Información.

- La utilización de internet es para el desempeño de las funciones propias del cargo en la Red de Salud del Centro E.S.E y no podrá utilizarse para propósitos personales.

9.3.9.7. Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea son:

NIVEL 1: Sin restricciones: Los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea.

NIVEL 2: Internet restringido y mensajería instantánea: Los usuarios podrán hacer uso de internet y servicios de mensajería instantánea, aplicándose las políticas de seguridad y navegación.

NIVEL 3: Internet restringido: Los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación

NIVEL 4: El usuario no tendrá acceso a Internet.

9.3.9.8 No está permitido

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, WebProxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El acceso a páginas relacionadas compras, ventas, viajes y alojamientos.
- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, WhatsApp, Instagram, Twitter, LinkedIn, Pinterest y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de la Red de Salud del Centro E.S.E.

- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Proceso de Gestión de Tecnologías y la Información, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

9.4 POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es su nombre de usuario (userID) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica de la Red de Salud del Centro E.S.E, por lo cual deberá mantenerlo de forma confidencial.

El Proceso de Gestión de Tecnologías y la Información, es el único que puede otorgar la autorización a usuarios para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica de la Red de Salud del Centro E.S.E, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones, con apego al principio "Necesidad de saber".

9.4.1 Controles de acceso lógico

9.4.1.1 El acceso a la infraestructura tecnológica de la Red de Salud del Centro E.S.E para personal externo debe ser autorizado al menos por un líder de proceso o subgerente de la Red de Salud del Centro E.S.E, quien deberá notificarlo mediante oficio al Proceso de Gestión de Tecnologías y la Información, quien lo habilitará.

9.4.1.2 Está prohibido que los usuarios utilicen la infraestructura tecnológica de la Red de Salud del Centro E.S.E para obtener acceso no autorizado a la información u otros sistemas de información de la Red de Salud del Centro E.S.E.

9.4.1.3 Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

9.4.1.4 Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Proceso de Gestión de Tecnologías y la Información antes de poder usar la infraestructura tecnológica de la Red de Salud del Centro E.S.E.

9.4.1.5 Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la Red de Salud del Centro E.S.E, a menos que se tenga autorización del Proceso de Gestión de Tecnologías y la Información.

9.4.1.6 Cada usuario que accede a la infraestructura tecnológica de la Red de Salud del Centro E.S.E debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.

9.4.1.7 Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

9.4.1.8 Los usuarios tienen prohibido usar el nombre de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

9.4.2. Administración de privilegios

9.4.2.1 Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de la Red de Salud del Centro E.S.E, deberán ser notificados por escrito o vía correo electrónico al Proceso de Gestión de Tecnologías y la Información con el visto bueno del líder de proceso o subgerente, para realizar los cambios pertinentes.

9.4.3. Administración y uso de contraseñas

9.4.3.1 La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

9.4.3.2 Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por RING, indicando si es de acceso a la red o a módulos de sistemas de información, para que se le proporcione una nueva contraseña.

9.4.3.3 La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante el Proceso de Gestión de Tecnologías y la Información como colaborador de la Red de Salud del Centro E.S.E.

9.4.3.4 Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

9.4.3.5 Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos;
- Deben estar compuestos de al menos ocho (8) caracteres. Estos caracteres deben ser alfanuméricos, o sea, números y letras;

- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario;
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

9.4.3.6 La contraseña podrá ser cambiada únicamente por requerimiento del dueño de la cuenta.

9.4.3.7 Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de solicitar el cambio inmediatamente.

9.4.3.8 Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

9.4.3.9 Los cambios o desbloqueo de contraseñas solicitados por el usuario al Proceso de Gestión de Tecnologías y la Información serán solicitados mediante oficio firmado por el líder de proceso del usuario que lo requiere.

9.4.5. Control de accesos remotos

9.4.5.1 Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno de la Red de Salud del Centro E.S.E.

9.4.5.2 La administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por la Red de Salud del Centro E.S.E.

9.5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

9.5.1. Derechos de Propiedad Intelectual

9.5.1.1 Está prohibido por las leyes de derechos de autor y por la Red de Salud del Centro E.S.E, realizar copia no autorizadas de software, ya sea adquirido o desarrollado por la Red de Salud del Centro E.S.E.

9.5.1.2 Los sistemas desarrollados por personal, interno o externo, que sea parte del Proceso de Gestión de Tecnologías y la Información, o sea coordinado por ésta, son propiedad intelectual de la Red de Salud del Centro E.S.E.

9.5.2. Revisiones del cumplimiento

9.5.2.1 El Proceso de Gestión de Tecnologías y la Información realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para usuarios.

9.5.2.2 El Proceso de Gestión de Tecnologías y la Información podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado.

9.5.2.3 Dada la naturaleza del presente reglamento, su conocimiento y observancia son obligatorios para todos los usuarios equipos de cómputo de la Red de Salud del Centro E.S.E. Su desconocimiento nunca podrá ser invocado como excusa para evitar las sanciones correspondientes.

9.5.3. Violaciones de seguridad informática

9.5.3.1 Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el Proceso de Gestión de Tecnologías y la Información.

9.5.3.2 Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información. Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación del Proceso de Gestión de Tecnologías y la Información, con excepción de los Órganos Fiscalizadores.

9.5.3.3 Ningún usuario de la Red de Salud del Centro E.S.E debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por el Proceso de Gestión de Tecnologías y la Información.

9.5.3.4 No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, programa maligno, spyware, o similares diseñado para auto replicarse, dañar, afectar el desempeño, acceso a las computadoras, redes e información de la Red de Salud del Centro E.S.E.

9.6. POLÍTICAS Y ESTÁNDARES DEL TELETRABAJO

9.6.1. Generalidades

Las empresas lo han llamado trabajo en casa o trabajo flexible, pero en términos legales estamos hablando de teletrabajo, una modalidad para generar empleo que en Colombia empezó a promoverse desde 2008 con la Ley 1221 y que posteriormente se reglamentó con el Decreto 884 de 2012.

De acuerdo con esta Ley, el teletrabajo es una forma de organización laboral que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación (TIC), sin requerirse la presencia física del trabajador en un sitio específico de trabajo. El teletrabajo puede ser autónomo, móvil o suplementario.

El teletrabajo es muy diferente a trabajar en una oficina, y no sólo en temas de productividad. En cuanto a ciberseguridad, las empresas tienen todo un sistema para proteger su información, redes y dispositivos en la oficina; pero en tu casa y en tu computador personal, los estándares corporativos no serán los mismos. Así, uno de los mayores retos del teletrabajo es garantizar la confidencialidad, integridad y disponibilidad de los datos de las empresas. Las siguientes políticas ayudarán a protegerse de las ciberamenazas que conlleva el teletrabajo.

Los usuarios son uno de los principales riesgos en ciberseguridad, por lo que las medidas de seguridad informática deben extremarse cuando acceden a los sistemas y plataformas de la empresa para realizar su trabajo desde casa o de forma remota.

9.6.2. Políticas para el teletrabajo

Es necesario implementar reglas de seguridad informática para evitar colocar en riesgo la información personal o la de su empresa, ya que trabajar desde casa implica que sus datos no estén protegidos de la misma forma que sucede cuando está en una oficina.

9.6.3 Redes WiFi

Cuando esté trabajando y manejando información confidencial de la empresa, siempre debe asegurarse de estar conectado a una red segura, sea una red privada, como la de su casa, o la red privada corporativa (VPN).

Navegar en una red de wifi pública desde un parque o una cafetería puede ser un riesgo para su información privada, desde sus cuentas en el banco hasta las fotografías que envía a sus amigos. En este sentido, le resultará útil una Red Privada Virtual (VPN por sus siglas en inglés), que crea una red privada partiendo de una red pública. Cuando se usa una red privada, las actividades que realice en línea están encriptadas y así no expone ni su información personal ni la de la empresa.

9.6.4 Sistema operativo actualizado

Los ciberdelincuentes pueden aprovecharse de cualquier deficiencia de sus equipos para robar información. Es por ello por lo que debe tener en cuenta:

Actualice el sistema operativo de los equipos regularmente, pues estas actualizaciones ayudan a corregir errores en los dispositivos, agregan nuevas características y corrigen debilidades en la seguridad informática.

Proteja el computador con un antivirus que se encargue de identificar y evitar ataques de malware que puedan robar información.

Utilice contraseñas seguras de acceso a los dispositivos y cámbielas regularmente.

Evite enviar correos electrónicos relacionados con el trabajo desde su correo personal. En estos casos, sólo utilice el correo corporativo.

9.6.5 Pérdida o robo del dispositivo

Estas situaciones pueden colocar en riesgo su información y la de la empresa. Para empezar, debe denunciar el robo ante las autoridades policiales, ya que esto aumenta las posibilidades de que recupere lo perdido. Informe también, a su familia, a sus amigos y a la empresa sobre la pérdida.

Siempre que pueda hacerlo, trate de rastrear el dispositivo a través de las opciones que las diferentes marcas ofrecen. Esta información de seguimiento también es vital para la policía. En caso de que el ladrón burle el sistema de bloqueo del dispositivo, usted debe entrar a los sitios web de las aplicaciones que usa, para cerrar las sesiones y cambiar las contraseñas.

Finalmente, si el dispositivo es irrecuperable, desactívelo. Aunque perderá contacto con él, evitará que el ladrón pueda acceder a sus cuentas o reutilizarlo.

9.6.6 Virtualización de aplicaciones

Con la opción de la virtualización de aplicaciones usted como usuario será capaz de ejecutar en su computadora una aplicación que no está instalada en el equipo.
La aplicación será ejecutada gracias a un paquete que contendrá las configuraciones necesarias. Con esta opción, se reducirán algunas necesidades; Se desinstalarán aplicaciones que se vuelven inútiles; tendrá las herramientas disponibles en cualquier momento y el sistema operativo no será modificado.

9.6.7 Resguardo de documentos

Los documentos y archivos de trabajo deben ser almacenados en una nube y no en el dispositivo. De igual forma deben tomarse medidas de seguridad informática para que la información ahí almacenada permanezca segura.
Podemos empezar por utilizar contraseñas seguras intercalando letras mayúsculas, minúsculas y números. También, puede activar una verificación, para que cada vez que quiera acceder a la nube, sea enviado a su celular un mensaje de texto que contendrá un código que deberá ingresar en el acceso a la nube

9.6.8 Bloqueo de dispositivos

Alguien puede echar un vistazo a la correspondencia de tu trabajo cuando hagas una pausa para ir al baño. Por lo tanto, es importante que bloquees la pantalla siempre que te levantes. Piensa que esta pequeña molestia es un pequeño precio para pagar y mantener seguros los secretos corporativos.

Aunque estés trabajando en casa y no haya extraños en la habitación, vale la pena bloquear el dispositivo. Probablemente no te gustaría que tu hijo le enviara accidentalmente a tu jefe un mensaje con emoticonos de corazones. O que tu gato pise el teclado y envíe el borrador de un mensaje a la mesa directiva. Da igual donde vayas, bloquea la pantalla al levantarte. Y está de más decir que el computador deberá estar protegido con una contraseña.

9.6.9 Uso de servicios corporativos

La empresa no es responsable de las configuraciones de los equipos propios de los usuarios, por ejemplo, tu cuenta personal en Google Drive. ¿Estás completamente seguro de que tu compañero será el único que vea el enlace al archivo que has enviado? Si ese archivo es accesible para cualquiera que tenga el enlace, entonces los motores de búsqueda pueden indexarlo. Y si alguien busca en Google algo relacionado con tu documento, puede aparecerle en los resultados de búsqueda y llamar la atención de quien ni siquiera sabía de su existencia.

Por lo tanto, utiliza los recursos corporativos como el ONE DRIVE empresarial para el intercambio de documentos y demás información. Esos almacenamientos en la nube, pero configurados para empresas, son por lo general más fiables que sus versiones gratuitas para usuarios. El correo corporativo por lo general tiene menos spam que tu correo personal y es menor el riesgo de no leer un correo importante o enviar algo a la persona equivocada. Además, tus compañeros sabrán que se trata de usted y no de alguien que se hace pasar por usted.

9.6.10 Siempre atentos

Es posible que algún mensaje malicioso y muy convincente lograra infiltrarse hasta tu correo corporativo. Esto es especialmente relevante para quienes trabajan a distancia, porque la cantidad de comunicaciones digitales aumenta notablemente con el teletrabajo. Por lo tanto, lee con cuidado los mensajes y no te apresures a responderlos. Si alguien necesita con urgencia un documento importante o exige el pago inmediato de una factura, comprueba que sea quien dice ser. No temas en llamar a las otras partes involucradas para aclarar o confirmar una vez más esta orden con tu jefe.

Sospecha especialmente de los mensajes de correo con enlaces. Si un enlace a un supuesto documento no señala un recurso corporativo, mejor olvídese de él. Si todo parece correcto y el enlace abre un sitio parecido a, digamos, OneDrive, no introduzca sus credenciales de inicio de sesión en él. Lo mejor es teclear la dirección de OneDrive en el navegador, iniciar sesión e intentar abrir de nuevo el archivo.

9.6.11. Acceso mediante software

Es común utilizar software de acceso remoto para conectarse desde su computador personal en casa a tu computador de la oficina o el consultorio, entre ellos está el HopToDesk (gratuito).

9.6.11.1 HopToDesk

HopToDesk es una herramienta gratuita de escritorio remoto que permite a los usuarios compartir su pantalla y permitir el acceso de control remoto a sus computadoras y dispositivos. A diferencia de otras herramientas similares, como TeamViewer o AnyDesk, HopToDesk es gratuito tanto para uso personal como comercial, proporciona un verdadero cifrado de extremo a extremo para todas las comunicaciones entre pares y es de código abierto. Por esta razón es necesario que en el momento de la utilización se tenga la configuración correcta.

9.6.11.2 Configuración

El HopToDesk debe ser vez instalado en los dos equipos que requieren controlar el escritorio remoto, cada uno de ellos tendrá su propio ID y contraseña. Una vez establecida la comunicación tendrá opciones de configuración para iniciar chat, modo de la pantalla, ajustes de teclado, transferencia de archivos y modo privacidad.

9.6.11.3 Funciones de escritorio remoto

HopToDesk permite el acceso desatendido, lo que le permite conectarse a una máquina remota en la que esté instalado HopToDesk sin necesidad de estar físicamente en el dispositivo para aprobar las conexiones entrantes.

Para mejores prácticas de seguridad, el acceso desatendido está desactivado de forma predeterminada, pero puede activarlo configurando una contraseña permanente haciendo clic en el ícono de lápiz junto al cuadro de contraseña.

9.6.11.4 Autenticación

Si sospecha que la contraseña de acceso al equipo es de conocimiento no autorizado, HopToDesk ofrece la posibilidad de volver a generar la contraseña que se le ha asignado a un equipo. (área de contraseña, símbolo restablecer). Lo ideal es establecer una contraseña permanente y cambiarla regularmente.

9.6.11.5 Modo privacidad

El modo privacidad permite que no se aprecie actividad en el equipo remoto

9.6.11.6 Lista de dispositivos

HopToDesk proporciona tres apartados: Sesiones recientes (equipos a los que se ha conectado recientemente), Favoritos (equipos seleccionados por el usuario, por lo general los de uso frecuente) y Descubierto (equipos que se encuentran en la misma red del usuario)

9.6.11.7 Permisos

Queda a discreción de usuario conceder al remoto los siguientes permisos: (despliegue el menú - tres puntos en el área de ID)

Habilitar teclado y mouse

Habilitar porta papeles (copiar y pegar)

Habilitar transferencia de archivos

9.6.12 Autorizaciones para efectuar teletrabajo

Ningún funcionario debe accesar los equipos y/o sistemas de información empresariales sin llenar los requisitos correspondientes.

9.6.12.1 De las subgerencias y asesores.

Corresponde a las subgerencias y asesores autorizar mediante documento o correo electrónico al líder de Gestión de Tecnologías y la Información, la utilización de conexiones remotas a los equipos o sistemas de información empresariales.

9.6.12.2 De Gestión de Tecnologías y la Información

Corresponde al proceso de Gestión de Tecnologías y la Información:
a.- Diligenciar con el usuario los documentos a que dé lugar
b.- Verificar que el equipo que se utilizará para el acceso cumpla con las normas mínimas de seguridad informática.
c.- Firmar acuerdos de confidencialidad.

9.6.12.3 De los accesos no autorizados

Corresponde al proceso de Gestión de Tecnologías y la Información documentar los accesos no autorizados y notificar al área jurídica para que se tomen las medidas disciplinarias correspondientes.

9.6.13 VPN Virtual Private Network – Red Privada Virtual

Una VPN (red privada virtual) es un software diseñado para proteger la privacidad en Internet, es la forma más segura y rápida de conectarse remotamente a los servicios de la Plataforma tecnológica de la Red de Salud del Centro E.S.E.

Cuando un equipo se conecta mediante una VPN a la plataforma de la Red de Salud del Centro E.S.E ese equipo, desde el lugar del mundo donde esté, hará parte de la red de datos de la empresa así que puede asemejarse a estar conectado desde cualquiera de nuestras IPSs y por

lo tanto debe cumplir con todos los requisitos de cualquier equipo de cómputo conectado físicamente a la red.

Es absolutamente necesario que todo equipo que se conecte a través de una VPN tenga instalada una protección adecuada para prevenir ataques de virus y malware como mínimo, de preferencia tener instalada la misma protección de los equipos empresariales.

Crear VPNs y configurarla en los equipos de cómputo es competencia exclusiva del personal del proceso de Gestión de Tecnologías y la Información , previa verificación del cumplimiento de los requisitos, se manejarán horarios limitados y horarios 7x 24 para el personal que así lo requiere por las diferentes actividades que la Gerencia exponga y de acuerdo a sus responsabilidades.

9.7 DE LOS MEDIOS DE COMUNICACIÓN EMPRESARIALES – GERENCIA DE LA INFORMACIÓN

Los canales a través de los cuales los usuarios pueden comunicarse durante las jornadas laborales están legalmente establecidos y se utilizarán únicamente para fines laborales.

9.7.1 Mensajería Spark

Mencionado en el ítem 3.7 del presente Manual, es el medio de mensajería instantánea adoptado por la empresa.

9. 7.2 Telefonía IP

La telefonía IP que se realiza a través de teléfonos fijos y virtuales permite la comunicación interna mediante el uso de extensiones y la externa tanto a teléfonos fijos como celulares, a estos últimos mediante autorización de las subgerencias respectivas. Este medio de comunicación debe utilizarse sólo para fines que tengan que ver con su actividad laboral.

9.7.3 Correo institucional y Almacenamiento en red One Drive

El correo institucional bajo el dominio @saludcentro.gov.co es la única plataforma de correo que debe utilizarse para comunicación electrónica tanto interna como externa. Corresponde a Gestión de Tecnología y la Información otorgar permisos correspondientes para utilizar otro tipo de plataforma de correo con la anotación de que en un plazo no mayor a 180 días debe migrar a plataforma institucional.

La información perteneciente a la Red de Salud del Centro E.S.E que requiera almacenamiento externo, debe depositarse en repositorios de la empresa bajo el dominio @saludcentro.gov.co, por ningún motivo deberá almacenarse en repositorios de terceros.

La información contenida en repositorios bajo el dominio @saludcentro.gov.co podrá será compartida con fines exclusivamente de trabajo y no deberá ser sincronizada y/o descargada en ningún equipo de cómputo.

Nota: Está totalmente prohibido la utilización de correos personales para enviar cualquier tipo de comunicación empresarial interna o externa, por lo tanto, no aplica la solicitud de permisos para su utilización.

9.7.4 Mensajería instantánea

La Red de Salud del Centro acepta la utilización de la aplicación de mensajería instantánea WhatsApp y Telegram de acuerdo con la legislación colombiana que está vigente en este momento y las que de manera interna se detallan a continuación:

La utilización de la mensajería instantánea WhatsApp y Telegram dentro de las jornadas de trabajo se realizará únicamente para fines relacionados con la actividad laboral y ejecutados en el teléfono celular. La utilización de estas plataformas en la Web está prohibida y su utilización

en los equipos de cómputo requiere de la autorización del proceso de Gestión de Tecnologías y la Información.

9.7.4.1 Objetivo

Los grupos de mensajería instantánea se crean con un objetivo específico, es obligación de cada uno de sus miembros acogerse a dicho objetivo y abstenerse de enviar mensajes que no sean de interés del grupo en general.

9.7.4.2 Contenido de los mensajes

Los mensajes deben de ser claros y positivos redactados de forma respetuosa asegurándose de que estén libres de ambigüedades que puedan prestarse para malas interpretaciones. Deben estar libres de ironías y/o exageraciones al referirse a una situación específica, por tal motivo, se solicita que los inconvenientes que reporten por Telegram lo envíen en un solo párrafo para que sea más efectiva la respuesta, la solicitud debe ir acompañada con imagen completa de la pantalla del error, numero ip del equipo de cómputo (punteada del computador) y una breve descripción del problema para que la persona encargada de pronta respuesta.

9.7.4.3 Grupo de soporte de Gestión de Tecnologías y la Información

El grupo de soporte a usuarios en la plataforma Telegram del proceso de Gestión de Tecnologías y la Información tiene como objetivo brindar ayuda oportuna a los usuarios que así lo soliciten en todo el alcance de la plataforma tecnológica (equipos de cómputo y comunicaciones, redes de datos, software). Las solicitudes que se realizan a través del grupo de soporte son aquellas que revisten afectación alta al desempeño de las actividades laborales, las demás deberán ser reportadas a través de la plataforma de tickets (RING) que se detalla en el ítem 9.7.4.4. Antes de realizar la solicitud es deber del usuario asegurarse de que la falla requiere de la intervención del personal de soporte evitando la generación de falsos positivos.

9.7.4.3.1 La solicitud de soporte

Adicional a lo expresado en el ítem 9.7.4.2 Las solicitudes de soporte que se realizan a Gestión de Tecnologías y la Información deben contener datos precisos que permitan a los técnicos brindar una atención oportuna evitando contra mensajes solicitando información, los datos básicos son:

a.- Descripción clara de la falla y/o imagen.
b.- Ubicación del equipo afectado (IPS y área)
c.- Dirección IP y/o contraseña con la que ingresan al equipo.

Evite cualquier otra información que no contribuya al grupo de soporte a dar solución al inconveniente.

En lo posible condense la información en un solo párrafo o bloque, evite enviar información fraccionada, tenga en cuenta que en el grupo hay muchos usuarios y es posible que su información termine dispersa.

Dado el caso de haber informado de la falla a través del grupo y por alguna razón la falla se soluciona sin la intervención del grupo de soporte, el usuario está en la obligación de informarlo por el mismo medio.

9.7.4.4 Plataforma de solicitudes RING (Tickets) de Gestión de Tecnologías y la Información

Para acceder a la plataforma y gestionar casos es a través de la URL http://ring.saludcentro.gov.co/ esta plataforma tiene por objetivo en Gestión de Tecnologías y la Información atender todas las solicitudes no urgentes, que tengan baja afectación de la actividad laboral y que tengan relación con la plataforma tecnológica (equipos de cómputo y comunicaciones, redes de datos, software, sistemas de información).

Las solicitudes de adquisición de tecnología no son del ámbito de la plataforma, estas deben realizarse mediante correo electrónico al líder de Gestión de Tecnologías y la Información.

9.7.4.4.1 Contenido del Caso

Las solicitudes realizadas a través de la plataforma RING a Gestión de Tecnologías y la Información deben contener datos precisos que permitan a los técnicos brindar una atención oportuna, evitando pérdida de tiempo en la búsqueda de la información completa para poder dar solución al caso, los datos reglamentarios son:

a. Descripción detallada del inconveniente y/o solicitud.
b. IPS donde se encuentra el equipo afectado o se plantea la solución.
c. Área de la IPS donde se encuentra el equipo afectado o se plantea la solución.
d. Información del equipo afectado: Número de activo fijo y Dirección IP para equipos de cómputo, número de extensión para los teléfonos.
e. Nombre completo de la persona solicitante.
f. Teléfono de contacto

Evite cualquier otra información que no contribuya al grupo de soporte a dar solución al inconveniente

Nota: En un RING solo se podrá reportar uno y solo un caso.

Las solicitudes en lo posible deben ser colocadas por la persona afectada por la falla ya que su nombre y teléfono de contacto aparecen en el ticket, de hacerlo a través de un tercero debe hacerse claridad al respecto y colocar los datos de contacto de la persona afectada.

10. INDICADORES

Nombre: Plan de Sensibilización del MPESI

Definición: El indicador permite medir la aplicación de los temas sensibilizados en la política seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de la evaluación que se realiza de manera anual.

Formula: Numero de personal aprobado sensibilizado / Total de personal a sensibilizar

11. ANEXOS

No aplica

12. FORMATOS RELACIONADOS

Plataforma Moodle

13. BIBLIOGRAFIA

- HopToDesk. (16 de abril de 2024). Plataforma de acceso remoto. https://www.hoptodesk.com/
- Ministerio de Tecnologías y la Información (01 de agosto de 2023). Teletrabajo. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/126148:Todo-lo-que-se-debe-saber-sobre-el-teletrabajo
- RING (01 de febrero de 2023). Registro Integral de Novedades a Gestionar. http://ring.saludcentro.gov.co/

CONTROL DE CAMBIOS Y REVISIONES				
Revisión	**Fecha**	**Versión Anterior**	**Versión Actual**	**Cambio Realizado**
01	01/04/2021	01	02	Se incluyo el Teletrabajo
02	01/08/2023	02	03	Se incluyo Almera, nueva plataforma de Tickets RING, cambio del nombre del proceso adicionando TIC, restricciones de uso de memorias USB.
03	21/10/2024	03	04	Se cambio plataforma AnyDesk por HopToDesk, se cambio el nombre del proceso de Gestión de la Información a Gestión de Tecnologías y la Información, se adiciona indicador

Elaboró:	**Revisó:**	Aprobó:
Marneilde Londoño Ricaurte Líder de Gestión de Tecnologías y la Información	Marneilde Londoño Ricaurte Líder de Gestión de Tecnologías y la Información	Natali Mosquera Narváez Gerente General