Tabla de contenido

PROPOSITO

El presente documento tiene como finalidad dar a conocer las políticas y estándares de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de la Red de Salud del Centro E.S.E.

INTRODUCCION

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de políticas y estándares adecuados. 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.

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.

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 cumplimiento en los recursos informáticos asignados.

ALCANCE

El documento define las Políticas y Estándares de Seguridad que deberán observar 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.

SANCIONES POR INCUMPLIMIENTO

El incumplimiento al presente Manual podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

BENEFICIOS

Las Políticas y Estándares de Seguridad Informática establecidos dentro de este documento son la base para la protección de los activos tecnológicos e información de la Red de Salud del Centro E.S.E.

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.

Todo usuario 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 apego al Manual de Políticas y Estándares de Seguridad Informática para usuarios.

1.1.- Responsabilidades de los Usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente manual.

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., así como comprometerse a cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

1.3. Entrenamiento en Seguridad Informática

Todo empleado 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 en la intranet de la empresa intranet.esecentro.gov.co y 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.

1.4. Medidas disciplinarias

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

2.- POLITICAS Y ESTANDARES DE SEGURIDAD FISICA Y AMBIENTAL

Política

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 las instalaciones y los diferentes Centros de Cómputo la Red de Salud del Centro E.S.E

2.1 Resguardo y protección de la información

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

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, aun cuando no se utilicen y contengan información reservada o confidencial.

2.1.3 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.

2.2. Controles de acceso físico

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.

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 la Dirección puede acceder a ellos.

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 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 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 la misma. 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.

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 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.

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

2.5 Energía regulada

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) ventiladores, radios, cafeteras, impresoras láser.

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.

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.

2.6 Acceso remoto

2.6.1 La conexión a redes inalámbricas 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 la Información.

2.6.2 No está permitida la sincronización de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Red de Salud del Centro E.S.E.

2.7 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.

2.8 Protección y ubicación de los equipos

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

2.8.2. 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 sistemas.

2.8.3. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas al usuario de la Red de Salud del Centro E.S.E.

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

2.8.5. 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.

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

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

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

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

2.8.10. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con anticipación al Proceso de Gestión de la Información a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.

2.8.11. 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 ésta acción.

2.9. Mantenimiento de equipo

2.9.1. Únicamente el personal perteneciente al Proceso de Gestión de la Información podrá llevar a cabo los servicios y reparaciones al equipo informático.

2.9.2. Ningún funcionario realizara 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 informal estará en falta grave; dicha actividad es responsabilidad del personal que se contrate para dicho mantenimiento.

2.9.3. 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 la Información.

2.9.4 Cuando el funcionario responsable de un equipo de cómputo detecte problemas en el funcionamiento del mismo (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 determinara las pautas a corregir la falla o referir la reparación.

2.9.5 El Proceso de Gestión de 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.

2.10. Pérdida o transferencia de equipo

2.10.1. 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 a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

2.10.2. El resguardo para los portátiles, tiene el carácter de personal y será intransferible.

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

2.11. Uso de dispositivos especiales

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

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

2.12. 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.

3.- POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

POLITICA

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 la Información, o al líder de su comuna, para solicitar asesoría.

3.1. Uso de medios de almacenamiento

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.

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 afectado o del Proceso de Gestión de la Información.

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

3.1.3. En caso de que se requiera algún respaldo de información en CD, este servicio deberá solicitarse o autorizarse por escrito por el Proceso de Gestión de la Información.

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.
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.

3.2. Instalación de Software

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 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 la Información de manera inmediata a desinstalar dicho software.

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 la Información.

3.3. Identificación del incidente

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 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.

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.

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 la Información.

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 la Información quien llevará los registros pertinentes.

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 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 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.

3.6. Uso del correo electrónico institucional

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.

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.

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 la Información.

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.

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 la Información de acuerdo con las necesidades de cada usuario.

3.6.6. La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito al Proceso de Gestión de 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.

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

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 y/o myspace, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.
- El envío de archivos que contengan extensiones ejecutables, bajo 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 la Información.

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.

3.6.10 El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación del Proceso de Gestión de 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.

3.6.11 Toda información de la Red de Salud del Centro E.S.E generada con los diferentes programas computacionales (Ej. Rfast8, Office, Open Officet, 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.

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.

3.7 Uso del programa de mensajería instantánea Spark

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.

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.

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

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.

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

3.8. Controles contra código malicioso

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 la Información.

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's, etc, deben verificar mediante el antivirus que estén libres de cualquier tipo de código malicioso.

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.

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 autoreplicarse, 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.

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 la Información.

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 la Información para la toma de medidas pertinentes.

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 la Información las actualizaciones del software de antivirus.

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 la Información en programas tales como:

- Antivirus;
- Correo electrónico;
- Programas de ofimática;
- Navegadores;
- Otros programas.

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 la Información para que sean ellos quienes lo solucionen.

3.9. Permisos de uso de internet

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.

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 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.

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

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.

3.9.5. El acceso y uso de módem en la Red de Salud del Centro E.S.E tiene que ser previamente autorizado por el Proceso de Gestión de la Información.

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 la Información.
- La utilización de internet es para el desempeño de su función y puesto en la Red de Salud del Centro E.S.E y no para propósitos personales.

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.

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 y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN Messenger, Yahoo, Skype, Net2phone 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 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.

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, de su identificador o 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 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".

4.1. Controles de acceso lógico

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 la Información, quien lo habilitará.

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.

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.

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

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 la Información.

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.

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.

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

4.2. Administración de privilegios

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 la Información con el visto bueno del líder de proceso o subgerente, para realizar los cambios pertinentes.

4.3. Administración y uso de contraseñas

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.

4.3.2. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito al Proceso de Gestión de la Información, indicando si es de

acceso a la red o a módulos de sistemas de información, para que se le proporcione una nueva contraseña.

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 la Información como colaborador de la Red de Salud del Centro E.S.E.

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.

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.

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

4.3.7. Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarlo inmediatamente.

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

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

4.5. Control de accesos remotos

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.

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 el Red de Salud del Centro E.S.E.

5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

5.1. Derechos de Propiedad Intelectual

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.

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

5.2. Revisiones del cumplimiento

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

5.2.2. El Proceso de Gestión de 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.

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.

5.3. Violaciones de seguridad informática

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 la Información.

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 la Información, con excepción de los Órganos Fiscalizadores.

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 la Información.

5.3.4. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, malware, 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.

5. GLOSARIO

Acceso: Es el privilegio de una persona para utilizar un objeto o infraestructura.
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 colaboradores de la empresa 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 tan generosa como el autor decida.

Proceso de Gestión de 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 colaborador, 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 colaborador 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 ó deficiencia en la autorización, totalidad ó 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 de la Red de Salud del Centro. 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 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).

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.

Revisó:	Aprobó:
FIRMADO EN ORIGINAL Subgerente y/o Representante de la Dirección	***FIRMADO EN ORIGINAL*** Gerente y/o Subgerente