SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

E.S.E. IMSALUD

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Hoy día, las empresas se encuentran abocadas a un manejo más efectivo y seguro de la información, por la cantidad y la complejidad de los datos que se manejan, y que crecen de día en día exponencialmente, aunados a procesos e interrelaciones que hacen más eficaz y eficiente los procesos de gestión y administración. Uno de los activos más valiosos que tienen las empresas sean estas privadas o estatales, es su información, por eso, la protección de esta información es importante, como importante es la implementación de un **Sistema de Gestión de Seguridad de la Información (SGSI),** que como lo sugiere su nombre es un conjunto de políticas y estrategias de administración de la información.

La E.S.E IMSALUD, no es ajena a esta necesidad de un manejo cada vez más cualificado de su información, el diseño de ésta, su implementación, su implantación, la ejecución de un conjunto de procesos que facilitan la gestión y el acceso a la información, de manera segura, confidencial, integra y disponible, minimizando al máximo los riesgos y amenazas, que se puedan presentar de pérdida, suplantación e injerencia de personas u otras entidades ajenas a la E.S.E IMSALUD.

El presente documento, basado en la norma ISO / IEC 27001: 2013 pretende proporcionar a la E.S.E IMSALUD una serie de políticas que permitirán garantizar una seguridad razonable y reducir a un nivel aceptable los riesgos que puedan afectar en relación a seguridad de la información en el contexto de su organización. Las políticas de seguridad de la información expresadas en este documento son la base para la implantación de normas y procedimientos por parte de la Gerencia, Sistemas y áreas involucradas.

2. ¿QUÉ ES SGSI?

- Dentro del contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en

conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

- La Seguridad de la Información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

3. **OBJETIVOS**

- Proteger los recursos de información de la E.S.E IMSALUD, la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad.
- Definir las directrices de la E.S.E IMSALUD para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.
- Describir las políticas de seguridad de la información, basadas en la investigación del manejo de los sistemas de la información, en donde éstas garanticen la integridad, confidencialidad y la disponibilidad de la información en la E.S.E. IMSALUD. Además de controlar el manejo de la información e indicar la correcta utilización de herramientas tecnológicas, al personal de la institución que posean relación con los sistemas.

4. **NORMATIVIDAD DEL SGSI**

Las normas por las que se rige el SGSI se encuentran contempladas en el marco Legal que hace parte de cada uno de los procedimientos que integran el SGSI, la lista se presenta a continuación:

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

- Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

- Estatuto anticorrupción: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública

- Ley 1437 de 2011: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

- Ley 527 de agosto de 1999 Comercio electrónico: Define y reglamenta el acceso y uso de los mensajes de datos (probatoria), del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación (parte de una PKI) y se dictan otras disposiciones

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

- Ley 594 de 2000 Ley General de Archivos (Sector Público): Regula la obligación que tienen las entidades públicas y privadas que cumplen funciones públicas, de elaborar programas de gestión documental, independientemente del soporte en que se produzca la información para su cometido estatal, del objeto social para el que fueron creadas.

- Ley 603 de 2000: LA DIAN trabaja con entidades públicas y privadas que hacen parte del comité antipiratería del software y de la producción intelectual, con el fin de extender las auditorías que hace todos los días, al tema de la informática.

- Ley 794 de 2003: Actos de comunicación procesal por medios electrónicos

- Ley 962 de 2005: Actuaciones administrativas por medios electrónicos
- Ley 1150 de 2007: Contratación del Estado por medios electrónicos
- Ley 1273 del 5 de enero 2009: Delitos informáticos
- Ley 1581 de 2012: Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo. La ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante tratamiento) por parte de entidades de naturaleza pública y privada.
- Decreto 1377 del 27 de junio de 2013: El Decreto tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información.

5. CONTEXTO DE LA ORGANIZACIÓN

CREACIÓN: LA EMPRESA SOCIAL DEL ESTADO E.S.E. IMSALUD, fue creada mandato del Honorable Concejo el 29 de Enero de 1.999, abriendo sus puertas a partir del 1° de Enero del 2000, al servicio de la comunidad, dando así cumplimiento a lo normado en el Acuerdo 087 del 29 de Enero de 1.999, por medio del cual se crea la Empresa Social del Estado E.S.E. IMSALUD, constituida como entidad pública descentralizada con autonomía administrativa y presupuestal, personería jurídica y patrimonio propio, para que asuma la prestación de los servicios de salud en el primer nivel de atención en el Municipio de San José de Cúcuta.

NATURALEZA JURÍDICA: Es una entidad pública descentralizada del orden Municipal dotados personería jurídica, autonomía administrativa y patrimonio propio adscrito a la dirección local de salud, integrante del Sistema General de Seguridad Social en Salud sometido al régimen jurídico previsto en la ley 100 y sus decretos reglamentarios.

JURISDICCIÓN: La Empresa Social del Estado del Primer Nivel de Atención en Salud del Municipio de San José de Cúcuta, tiene jurisdicción en todo el territorio del Municipio de San José de Cúcuta, su domicilio y sede de sus organismos administrativos en la Ciudad de Cúcuta.

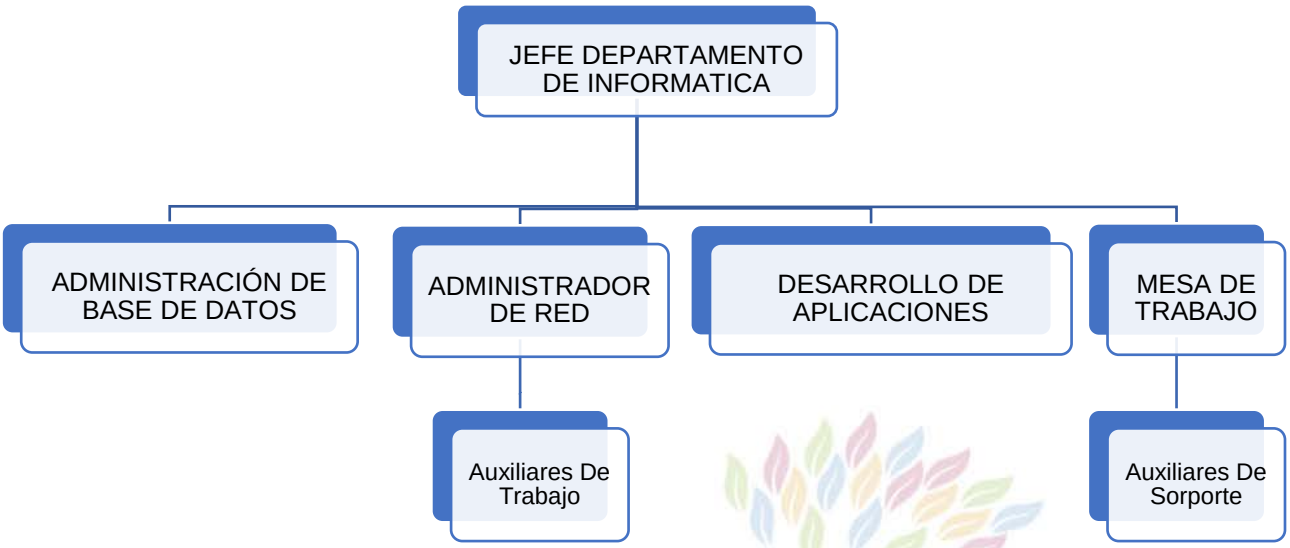
OBJETIVOS Y FUNCIONES: Contribuir al desarrollo social del municipio mejorando la calidad de vida y reduciendo la morbilidad, la mortalidad, la incapacidad, el dolor y la angustia evitables en la población usuaria, en la medida en que esto esté a su alcance. Producir servicios de salud eficientes y efectivos, que cumplan con las normas de calidad establecidas, de acuerdo con la reglamentación que se expida para tal propósito.

6. NECESIDADES DE LA ORGANIZACIÓN

Después de una etapa de diagnóstico a partir del cual se determinó que la E.S.E. "IMSALUD" no poseía los mecanismos, ni los procesos idóneos para proteger su información. Se vio la necesidad inmediata de crear el Departamento de Informática que gestionara el correcto funcionamiento y aplicación del sistema de gestión de seguridad de la información en la E.S.E IMSALUD.

Esta necesidad se hizo cada vez más palpable debido a que el manejo dado a la adquisición de recursos informáticos e infraestructura tecnológica, los servicios de soporte técnico, la administración de bases datos, el desarrollo y mantenimiento del software de la E.S.E, la cual carece de una organización adecuada. La tercerización de estos servicios otorgados a contratistas o personal ajeno a la institución, no sólo incrementa los costos, sino que dificulta la solución de problemas por la demora excesiva, la ralentización de los procesos, contribuyendo todo esto al mal funcionamiento en la prestación del servicio de salud.

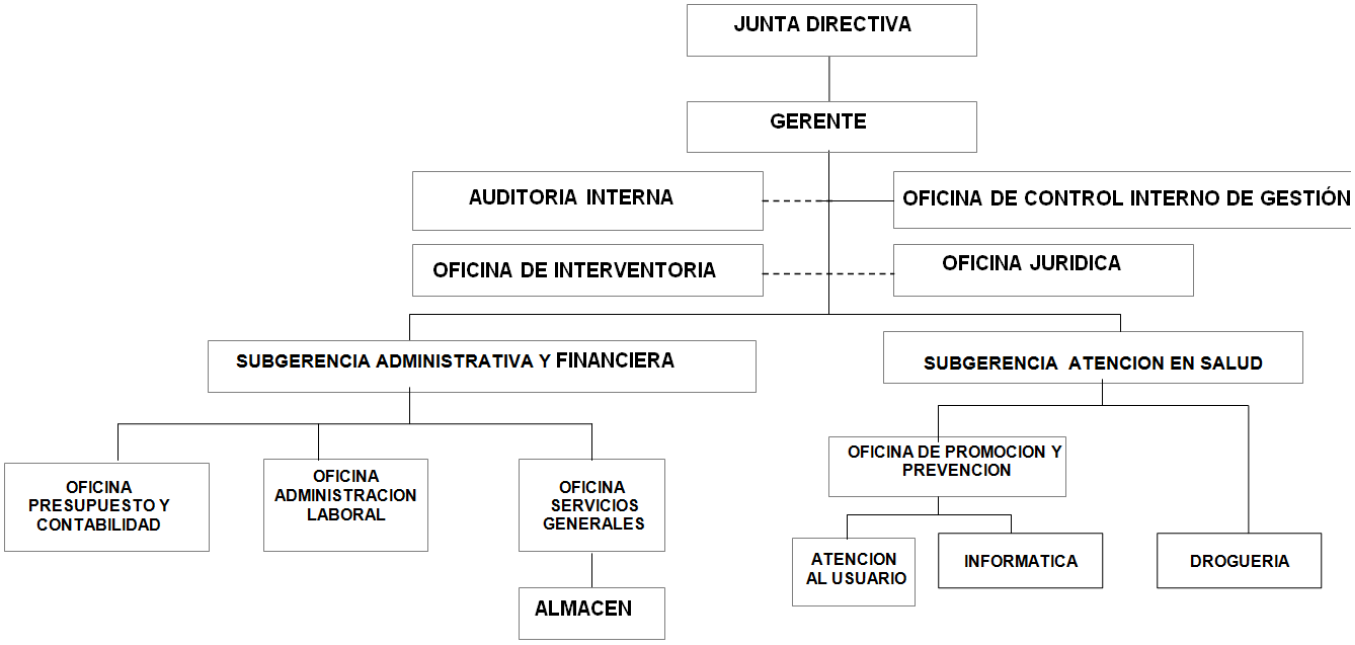
Organigrama Propuesta del Departamento de Informática



7. **ALCANCE DEL SGSI**

Las políticas de Seguridad de la Información son de aplicación en el conjunto de dependencias que componen la E.S.E IMSALUD, sus recursos, la totalidad de los procesos internos vinculados a la empresa a través de contratos o acuerdos con terceros y a todo el personal, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

ESTRUCTURA ORGANICA DE LA EMPRESA SOCIAL DEL ESTADO "IMSALUD"



Tomando en cuenta lo que engloba cada Sección del Sistema de Información de la E.S.E. IMSALUD, se ha determinado que el alcance de las Políticas de Seguridad para el diseño de un Sistema de Seguridad de la Información, será la subgerencia administrativa tal y como lo muestra a continuación la estructura organizacional.

Durante el periodo de tiempo que abarca este informe básicamente se presentaron las siguientes observaciones y/o acontecimientos generales:

El propósito de este procedimiento es proporcionar a la Junta Directiva las directrices básicas para que revise el SGSI de la organización y así asegurarse de su idoneidad, conveniencia, efectividad y mejoramiento continuo. La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información, así:

- Asegurando que se establezca la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la organización;
- Asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;
- Certificando que los recursos necesarios para el sistema de gestión de la seguridad de la información.
- Comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información;
- Asegurando que el sistema de gestión de la seguridad de la información logre los resultados previstos;
- Dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información;
- Promoviendo la mejora continua, y apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

8. RESPONSABILIDADES ANTE EL SGSI

La Junta Directiva de la E.S.E. IMSALUD es la responsable de desplegar los medios técnicos y humanos necesarios para garantizar la confidencialidad, integridad y disponibilidad de sus datos; Para ello instaurará las políticas, normativas, procesos y procedimientos que sean requeridos, y se compromete a distribuirlos entre todo el personal involucrado.

- Es responsabilidad del equipo de seguridad de la información de la E.S.E. IMSALUD establecer y revisar periódicamente los diferentes controles de acceso a los sistemas de

información que sostienen el negocio. Para ello, determinará perfiles de usuario y limitará los accesos al sistema en función de las necesidades requeridas por cada empleado, para el desarrollo de sus actividades laborales. Adicionalmente, siempre que sea de obligado cumplimiento, se tratará cualquier elemento introducido en los sistemas de información gestionados, según los requisitos establecidos por la legislación vigente sobre Propiedad Intelectual y Protección de Datos de Carácter Personal.

- El Equipo de Seguridad de la Información está compuesto por el Jefe del Departamento de Informática como por el Administrador de la Base de Datos, el Administrador de la Red y el abogado o representante legal de la E.S.E. IMSALUD. Este equipo de trabajo está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a la seguridad en la información y telecomunicaciones.
- También será responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones trimestrales, el Equipo de trabajo efectuará la evaluación y revisión de la situación de la Compañía en cuanto a seguridad de la información, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad.
- El equipo de la seguridad de la información es el responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Junta Directiva de la E.S.E. IMSALUD. También es responsable de evaluar, adquirir e implantar productos de seguridad de la información y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además, debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.
- El jefe del Departamento de informática, es el responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra.
- Así mismo debe reportar inmediatamente a su jefe inmediato o a un integrante del Departamento informática, cualquier evento que pueda comprometer la seguridad de la Junta Directiva de la E.S.E. IMSALUD y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

9. **OBSERVACIONES GENERALES**

A continuación, se informan las novedades encontradas en la visita a la Sede Administrativa, las Unidades Básicas de Atención, así como a la totalidad de las IPS´s de la E.S.E. Imsalud:

- En los centros de cableado las unidades básicas de Agua Clara, Comuneros, La Libertad, Loma de Bolívar, Policlínico Juan Atalaya y Puente Barco Leones, se encontraron muchos desperfectos como cables dañados, sin bota, otros cables que estaban ponchado tenían la pestaña partida, algunos cables que se utilizan para voz estaba siendo usados para datos y viceversa, los rack de algunas unidades básicas no contaban con aire acondicionado y falta de aseo ya que tenía mucho mugre y polvo, estos factores pueden afectar la conectividad de la red o en el peor de los casos dañar los equipos.
- Cabe mencionar que los centros de cableado de las unidades básicas se encuentran en mejor estado en cuanto a su organización, pero por la falta de identificación de los puntos se hace difícil su mantenimiento.
- Otra dificultad grave que se encontró es el control al acceso a los centros de cableado ya que los servicios de soporte los presta un contratista y no hay un registro de los cambios o fechas en las cuales se hicieron dichos cambios.
- Es preocupante encontrar oficinas donde la red eléctrica no cumple con las normas mínimas de seguridad, encontrando cables fuera de su respectiva canaleta, además, casos donde dos computadores comparten un regulador de voltaje o en su defecto, conectados directamente a los tomacorrientes directamente.
- Se evidenciaron numerosos puestos de trabajo sin acceso a internet; en algunos casos debido a daño en el punto de red y en otras por desperfecto en los cables UTP de conexión.
- En otros casos, se encuentran algunos puestos de trabajo con los cables de red sin uso de canaleta y en medio del camino en evidente exposición de daño.
- Se encontró oficinas que, a pesar de disponer de equipos de cómputo en condiciones favorables para conectarse a internet, no había en el recinto ningún punto de acceso a la red cableada.
- Un 80% de los computadores de no tiene clave de inicio lo cual permite que cualquier persona acceda a la información contenida en ellos.
- Hay unidades de computo que son manejadas por dos o más funcionarios sin tener cada uno su respectivo usuario y contraseña.
- En otros casos hay computadores donde no fue posible actualizarlos toda vez que cuentan con clave de administrador la cual es solicitada al intentar hacer cambios en la configuración de Windows pero ningún funcionario conoce dicha clave.

- Es evidente la falta de control de inventario ya que los equipos son cambiados de una dependencia a otra y son trasladados con la información que contienen aun así dichos datos no vayan a ser utilizados por el nuevo usuario.
- Ninguna estación de trabajo cuenta con una programación de copias de seguridad y en los únicos casos donde existe dicho proceso es porque el funcionario lo hace de manera personal, pero no como un plan de seguridad orientado por la institución.

10. POLITICAS DE SEGURIDAD

Para el desarrollo de las políticas de seguridad de la información se han propuesto 6 (seis) perfiles para el desarrollo de los controles y su fácil comprensión, estos perfiles se definen a continuación:

PERFIL ADMINISTRATIVO 1: En este perfil se encuentran la Gerencia y Sub Gerencia de la empresa.

PERFIL ADMINISTRATIVO 2: En este perfil se encuentran los jefes de departamento.

PERFIL OPERATIVO 1: En este perfil se encuentran los médicos, odontólogos, bacteriólogos, auxiliares de enfermería, auxiliares laboratorio, auxiliares de odontología, almacén.

PERFIL OPERATIVO 2: En este perfil se encuentran los digitadores.

PERFIL OPERATIVO 3: En este perfil se encuentran los cajeros.

PERFIL OPERATIVO 4: En este perfil se encuentran los auxiliares de secretaría, y de apoyo a la gestión.

Ya definido los perfiles a continuación se pasa a definir las políticas de seguridad que hacen referencia a:

Políticas de seguridad orientada a los usuarios finales (para los usuarios).
Políticas de seguridad de control de acceso (acceso a la información).
Política de seguridad física en las instalaciones.

Política de Seguridad para la Administración de Operaciones de Infraestructura de IT.
Política de Cumplimiento de Seguridad de la información.

11. POLÍTICA DE SEGURIDAD ORIENTADA A LOS USUARIOS FINALES

Objetivo

Obtener el compromiso por parte de los usuarios del Sistema de Gestión de Seguridad de la Información hacia el cumplimiento de las políticas de seguridad, planteadas en este documento.

Sanciones

El incumplimiento de estas normas, puede causar el despido inmediato y/o la nueva contratación, debido a la falta de compromiso de velar por la seguridad de la información de la E.S.E. IMSALUD. Además, se comunicará a la Junta Directiva de la E.S.E. IMSALUD, para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas.

Políticas.

- Todos los perfiles de usuario del sistema de información de la E.S.E. IMSALUD, deben aceptar los convenios de seguridad y confidencialidad de la información, así, como su uso adecuado, cumpliendo estrictamente con las normas descritas en el presente documento.
- Las políticas de seguridad de la información deben ser cumplidas, sin excepción por la totalidad de los perfiles de usuarios.

- Se considera una falta grave y causal de proceso disciplinario por parte de la oficina de unidad interna disciplinaria a los funcionarios de planta que sean sorprendidos cometiendo actividades graves como robo, daño o divulgación de información confidencial perteneciente a la E.S.E y las sanciones al personal de O.P.S serán dictadas por la Junta Directiva de la E.S.E IMSALUD.
- Toda la información catalogada por las áreas como critica debe contar con copias de respaldo para garantizar su seguridad. (Esta política aplica a los perfiles de usuario administrativo 1 y administrativo 2)
- No se permitirá bajo ningún concepto la instalación de software que no vaya acompañado de su correspondiente licencia y en caso de que algún usuario precise la instalación de componentes adicionales, su instalación se hará tras la solicitud mediante el formato de instalación de software al Departamento de Informática. *ver formato de instalación de software Anexo 7*
- La Utilización de dispositivos móviles, tales como PDAs, Smartphone, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización o externos a ella, deben ser usados de forma tal que no afecte el desempeño laboral propio como del personal que se encuentre a su alrededor.
- El uso del Internet con fines ajenos a actividades diferentes a la del ámbito laboral ó investigación quedan prohibidas.

DEFINICIÓN DE PERFILES Y SU ACCESO A LA INFORMACIÓN

A continuación, se definirá las necesidades de cada usuario para el acceso a los sistemas de información y necesidades de utilización de la red de datos de la Empresa:

PERFIL ADMINISTRATIVO 1: El perfil Administrativo 1 cuenta con acceso total tanto para los sistemas de información como el uso de la red de datos.

PERFIL ADMINISTRATIVO 2: El perfil Administrativo 2 cuenta con acceso a algunos sistemas de información del área al cual pertenece; Es decir quién es jefe de presupuesto, no puede tener acceso al módulo de nómina.

PERFIL OPERATIVO 1: El perfil Operativo 1 cuenta con acceso a los sistemas de información relacionado con la ejecución de sus funciones, es decir quién es médico tendrá acceso ingresar a los aplicativos y diligenciará la información de su competencia.

PERFIL OPERATIVO 2: El perfil Operativo 2 cuenta con acceso a los sistemas de información y a las páginas de consulta de los estados de los usuarios; y tendrá acceso ingresar a los aplicativos y como digitador alimentará los aplicativos autorizados.

PERFIL OPERATIVO 3: El perfil operativo 3 cuenta con acceso al software de facturación únicamente y a las páginas de comprobación de derechos de los usuarios (página externa de Sisben, Fosyga); y tendrá acceso ingresar a los aplicativos de facturación de los servicios de salud autorizados.

PERFIL OPERATIVO 4: El perfil operativo 4 solo hace uso de los equipos de cómputo para la ejecución de las actividades propias de sus funciones.

12. POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO

Objetivo

Protección de la información institucional, administrando el acceso a través de los sistemas informáticos, considerando: perfiles, permisos, cuentas, contraseñas y protectores de pantalla.

Sanciones

En caso de existir incumplimiento de la presente Política de Seguridad de la Información, por parte de un usuario del sistema de información, se comunicará a la Junta Directiva de la E.S.E. IMSALUD, para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas.

Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad de la información. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlarla asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Políticas

- El Jefe del Departamento De Informática se encargará de que las contraseñas de los equipos informáticos que deben ser cambiadas mensualmente de acuerdo con las políticas de seguridad de la compañía.
- Todos los perfiles de usuarios son responsables por las actividades realizadas bajo su nombre y contraseña asignada, estás no deben almacenarse en sitios públicos y se debe reportar cualquier violación a las normas de control de acceso.
- El Administrador deberá hacer una depuración mensual de los usuarios registrados en los sistemas de información, para negar el acceso a personal que ya no labore en la E.S.E IMSALUD

- El acceso no autorizado a los sistemas de información y uso indebido de los recursos informáticos según se ha definido en su perfil de usuario en la E.S.E. IMSALUD, acarreará sanciones administrativas y penales según sea el caso.
- Se considera que hay uso indebido de la información y de los recursos, cuando la persona incurre en cualquiera de las siguientes conductas:

a) Suministrar la información a quien no tiene derecho a conocerla.

b) Usar la información con el fin de obtener beneficio propio o de terceros.

c) Ocultar la información maliciosamente causando cualquier perjuicio.

d) Hacer pública la información sin la debida autorización.

e) Hurtar software de la E.S.E. IMSALUD (copia o reproducción entre usuarios).

f) Realizar copias no autorizadas de software de la E.S.E. IMSALUD, dentro y fuera de sus instalaciones.

g) Falsificar y duplicar un producto informático de la E.S.E. IMSALUD.

h) Descargar software, a través de Internet sin la debida autorización.

i) Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.

j) Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.

k) Utilizar la infraestructura de la E.S.E. IMSALUD (computadores, software, información o redes) para acceder a recursos externos con propósitos ilegales o no autorizados.

l) Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil o destructiva.

m) Uso personal de cualquier recurso informático de la E.S.E. IMSALUD para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material pornográfico.

n) Violar cualquier ley o regulación nacional respecto al uso de sistemas de información.

13. POLÍTICA DE SEGURIDAD FÍSICA

Objetivo

Mantener una adecuada protección física de los equipos, soportes de procesamiento, transmisión y conservación de la información de la E.S.E. IMSALUD.

Sanciones

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un usuario del sistema de información, se comunicará a la junta directiva, para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

Políticas

- Los centros de cómputo y procesamiento de información son áreas de acceso restringido por tal motivo el ingreso y permanencia debe ser controlado y supervisado. (Esta política aplica a los perfiles de usuario operativo 1, operativo 2, operativo 3 y operativo 4).
- Todos los servidores de la E.S.E. IMSALUD deberán ubicarse en las salas de servidores y el acceso físico debe ser restringido al personal no autorizado. (Esta política aplica a los perfiles de usuario administrativo 1 y administrativo 2).

- Todos los cambios que se realices a las áreas de servidores o centro de cableado sea por funcionarios de la E.S.E IMSALUD o por contratistas se deberán registrar en la bitácora de cambios que se encuentran en cada una de las áreas, si estas están situadas en las Unidades Básicas el coordinador será el responsable de que estos cambios sean anexados a las bitácoras.

- Los Empleados de la E.S.E. IMSALUD, deberá informar cualquier conducta sospechosa que ponga en riesgo potencial, el normal funcionamiento de la E.S.E.
- El personal de la E.S.E. IMSALUD, tiene la obligación de proteger los implementos, inmuebles e infraestructura de la organización.
- Los movimientos de equipos de cómputo y telecomunicaciones solo serán realizados con autorización del jefe del área correspondiente y aprobados por el jefe del departamento de informática y su cambio será registrado en la bitácora de traslados.
- Las áreas de trabajo no pueden ser usadas, como sitio de consumo de cualquier tipo de alimentos o bebida.
- El mantenimiento de equipos de tecnología de la información, únicamente será autorizado por el jefe del departamento de informática y sus cambios serán anexados a la bitácora de mantenimiento.
- El equipo de cómputo o cualquier recurso de tecnología de la información que sufra algún daño por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo o accesorio afectado, será sancionado por parte de las Junta Directiva de la E.S.E IMSALUD según lo crean conveniente.
- Queda prohibido que el usuario y/o personal no autorizado abra, desarme o realice actividades de mantenimiento a los equipos de cómputo de la E.S.E IMSALUD.

14. POLÍTICA DE SEGURIDAD PARA LA ADMINISTRACIÓN DE OPERACIONES DE INFRAESTRUCTURA IT

Objetivo

Gestionar y/o controlar el manejo de las actividades relacionadas con la infraestructura de la tecnología de la información, de esta manera lograr un buen uso de la misma.

Sanciones

En caso de existir incumplimiento de la presente Política de Seguridad de la Información por parte de un usuario del sistema de información, se comunicará a la junta directiva de la E.S.E. IMSALUD, para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a más de las responsabilidades civiles y penales a que hubiere lugar.

Políticas

- EL administrador debe realizar el respaldo semanal de la información, que garantiza la continuidad del negocio y operaciones de la E.S.E. IMSALUD.
- Los usuarios y contratistas del sistema de información de la E.S.E. IMSALUD, no deben crear conexiones remotas a redes internas, para el intercambio de información con otros equipos de cómputo y de ser necesario se debe contar con el permiso del jefe del Departamento de informática y las actividades realizadas en dichos equipos serán informadas por escrito.
- El Jefe del Departamento de Informática deberá ejecutar los antivirus en la red organizacional por lo menos una vez a la semana, en las horas de menos demanda de información
- La totalidad de los perfiles de usuarios del sistema, no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas.
- El acceso a internet será limitado por el tipo de usuario que se ha definido y a páginas corporativas, entes reguladores y correos personales y/o institucionales, con previa autorización del Jefe del Departamento de Información.
- Los usuarios del servicio de internet, al aceptar el servicio están aceptando que:

a. Estarán en continuo monitoreo por el administrador de la red, de las actividades que realizan en internet.
b. Acceso denegado a páginas no autorizadas.
c. Está prohibido, la transmisión de datos reservados y/o confidenciales.

d. No se permite la descarga de software, sin autorización del jefe del Departamento de Informática.
e. El uso de Internet es exclusivamente para desempeño de su función y puesto en la E.S.E. IMSALUD, no para propósitos personales.

15. POLÍTICA CUMPLIMIENTO DE SEGURIDAD DE LA INFORMACIÓN

Objetivo

Establecer los lineamientos necesarios que permitan resguardar la información institucional y los recursos tecnológicos relacionados a su gestión y consumo.

Sanciones

- En caso de existir incumplimiento de las presentes Políticas de Seguridad de la Información por parte de un perfil de usuario sea cual fuera del sistema de información, se comunicará a la Junta Directiva de la E.S.E. IMSALUD, para que tomen las medidas de sanción respectivas por incumplimiento de acuerdo a las normativas internas oficiales a de más de las responsabilidades civiles y penales a que hubiere lugar.
- El Departamento de Informática y la Junta Directiva de la E.S.E IMSALUD debe diseñar, desarrollar, proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas, para la salvaguarda de equipos e

instalaciones de computo, así como la custodia y resguardo de la basa de datos de la E.S.E. IMSALUD.

- Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
- Debido a la regulación existente en Colombia en función de resguardo de información y derechos de autor ningún software o información debe ser respaldada o utilizada sin previa autorización del autor o la compra de la licencia para la utilización de la herramienta tecnológica.
- El Departamento de Informática de la E.S.E. IMSALUD, podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno y 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 se detecte será reportado de acuerdo a las políticas de seguridad de los usuarios.
- Las pruebas de fallas detectadas en la implementación de las políticas de seguridad de la información serán realizadas solo por el departamento de Informática, las personas distintas a estas áreas que realicen este tipo de actividad serán sancionadas de acuerdo a lo establecido en el presente documento.

  Es un deber de la E.SE IMSALUD diseñar y ejecutar de manera permanente un programa de concientización en seguridad de la información involucrando a todos los funcionarios y funcionarios suministrados por terceros, para garantizar la protección adecuada de su información y los recursos de TI.

16. RECOMENDACIONES DE SEGURIDAD

16.1. GENERALES

- Utilizar los recursos informáticos con criterios de racionalidad y únicamente para las labores propias de su función y en beneficio de la Compañía.

- Conocer y cumplir las normas, los procedimientos y estándares establecidos y velar por su adopción en su área de influencia.
- Desarrollar comportamientos seguros frente al uso de la tecnología.
- Manejar la información con criterios de confidencialidad. Se deberá restringir el acceso general y cifrar los datos sensibles cuando sea requerido.
- La información de la Empresa no debe ser compartida, copiada, ni divulgada por ningún medio incluyendo el verbal sin las debidas autorizaciones de la alta gerencia.
- Se deberá mantener la disponibilidad de la información de acuerdo con las normas legales y las necesidades del negocio.

16.2.CONTROL DE ACCESO

- Cada usuario debe responder por el uso y mantenimiento de la(s) palabra(s) clave(s), el identificador de usuario y las tarjetas de control de acceso, las cuales son personales e intransferibles.
- Los usuarios son responsables por las actividades realizadas bajo su nombre y contraseña asignada.
- Reportar cualquier violación a las normas de control de acceso.
- Las contraseñas deben ser cambiadas regularmente de acuerdo con las políticas de seguridad de la compañía, no deben almacenarse en sitios públicos y no pueden repetirse.
- No se deben intentar examinar, escanear o violar la seguridad de las medidas de autenticación de los sistemas o red.

16.3.SERVICIOS

- Solicitar formalmente los servicios informáticos que requiera, no se deberá acceder a sitios o servicios que no han sido autorizados expresamente.
- Seguir con criterios de eficiencia, el procedimiento establecido para el reporte de fallas e incidentes de seguridad.
- Devolver a la Gerencia de Tecnología los recursos que ya no requiera.

- Notificar al área de servicios de tecnología cuando: Sea transferido o cambie su función.
- No va a hacer uso de los servicios por más de 20 días.
- No requiera alguno de los servicios autorizados.
- El total de los archivos personales de los empleados no podrá sobrepasar en ninguno de los casos un 10% de la capacidad total del disco duro del computador que le sea asignado.
- Los usuarios deberán crear una carpeta en su disco duro que identifique claramente que contiene archivos personales (c:\personal).
- No es permitido conectar a la red de la compañía computadores personales o de tercero sin previa autorización y verificación de las condiciones de seguridad, software y licenciamiento del software que tiene instalado.

16.4.CORREO ELECTRÓNICO

- No permitir a otro usuario enviar mensajes utilizando su cuenta, sin aclarar el remitente.
- No propagar información confidencial la cual debe enviarse cifrada o entregarse en forma personal.
- No solicitar donativos, promover cadenas de mensajes de cualquier índole, promover obras de caridad, enviar mensajes políticos, religiosos, mensajes que puedan ser interpretados como difamatorios, intimidatorios u ofensivos.
- El uso del correo para fines personales deberá ser racional.
- No discutir temas para los cuales sea más efectivo utilizar otro medio, como el teléfono, personalmente o convocar a una reunión.
- Verificar que los archivos que se adjunten a los mensajes no contengan virus.
- Evitar enviar anexos pesados, tales como fotos, que pueden bajar la velocidad del sistema y perjudicar su uso.
- Responder por el contenido de los mensajes enviados y no alterar los recibidos sin la autorización del emisor.
- Mantener el buzón de correo dentro de los límites de espacio asignados a cada usuario.

- Los mensajes enviados a nivel corporativo deberán ser canalizados a través de la Jefatura de Comunicaciones o en su defecto de la Gerencia autorizada para este tipo de comunicados.
- No se debe acceder al buzón de entrada de otra persona u otras carpetas de correo electrónico.

16.5. INTERNET Y NAVEGACIÓN

- Utilizar mensajería instantánea para actividades relacionadas con la gestión de negocio, y que estén expresamente autorizadas por la Presidencia de la Compañía o la Gerencia de Tecnología. La transmisión de archivos por este medio deberá ser restringida.
- Responder por el uso de Internet (correo, grupos de discusión, etc.) ante terceros, eximiendo a la Empresa de cualquier responsabilidad derivada del uso indebido de estos recursos.
- El uso de este servicio para fines personales deberá ser racional.
- El uso de Internet para la adquisición y contratación de bienes y servicios para la E.S.E IMSALUD deberá seguir y/o ajustarse la normatividad definida, en este tema.
- Cualquier adquisición de bienes y servicios que un usuario haga, vía Internet y a título personal, desde la infraestructura informática y de telecomunicaciones de la empresa, correrá por cuenta y riesgo de este y eximirá a la empresa de cualquier responsabilidad.
- No se deberá utilizar para funciones de la Empresa, software adquirido a través de Internet. Sólo la gerencia de tecnología está autorizada para esto.
- No use los sistemas de la Empresa para bajar o distribuir software, canciones, vídeos u otros datos con derechos de autor o propiedad intelectual.

16.6. ACCESO REMOTO

- La disponibilidad del servicio de Acceso Remoto es de 24 horas, 7 días a la semana. Ocasionalmente, y previo aviso, el servicio será suspendido cuando se realicen labores de mantenimiento a los equipos involucrados en la prestación del servicio.

- El soporte técnico relacionado, solo se prestará a equipos de la empresa, dentro de las instalaciones de la **E.S.E IMSALUD** y con los estándares establecidos.
- Si el usuario requiere acceso a un servidor o servicio más especializado deberá justificar y especificar las direcciones IP y las aplicaciones o servicios a los cuales debe ingresar.
- El usuario del servicio de acceso remoto deberá utilizar esta herramienta tecnológica, única y exclusivamente para apoyar sus funciones o roles dentro de la **E.S.E IMSALUD**
- El usuario del servicio de acceso remoto responderá por el uso directo o indirecto de este servicio, por la información y los programas a los que llegue a tener acceso a través de este medio, por su manejo, así como por las consecuencias derivadas de la utilización del servicio.

16.7.SOFTWARE

- Utilizar solamente software legalmente adquirido. En caso de presentarse algún tipo de reclamación, ésta recaerá sobre el usuario responsable del activo en el que se encontrase dicho software.
- No copiar, vender, regalar, distribuir o enajenar el software o su documentación sin permiso del autor.
- No ejecutar un programa en dos o más computadores simultáneamente, a no ser, que esté específicamente permitido en la licencia.
- No infringir las leyes sobre copias no autorizadas, por orden de funcionarios con jerarquía de dirección en la empresa, o grupos de apoyo que lo soliciten.
- No prestar los programas para que sean copiados, o copiar los programas que han sido pedidos en préstamo.
- No estimular, permitir, obligar o presionar a los empleados a crear o utilizar copias no autorizadas.
- No alterar, modificar o adaptar el software y la documentación, incluyendo, entre otras acciones, la traducción, ingeniería reversa del código, desensamblado o creación de trabajos derivados.
- No utilizar hardware o software de monitoreo de actividades (analizadores de protocolos, software catalogado como “hacking”, etc.) sin la debida autorización.

- Mantener activa en el equipo la última versión del antivirus autorizada para la empresa y efectuar periódicamente revisiones al disco duro.
- Utilizar el software de detección de virus antes de leer un disquete, CD, DVD o memoria USB y antes de utilizar un nuevo software.
- Desconectarse de la red antes de probar software sospechoso (información bajada de Internet, software en demostración, software de libre distribución, entre otros).
- Verificar la confiabilidad de la fuente de origen de la información que se baja de Internet, antes de efectuar la operación. Por ejemplo: Sitios reconocidos como IBM o Microsoft tienen menos probabilidad de que contengan virus.

16.8.RADIOS Y TELECOMUNICACIONES

- Los radios y dispositivos móviles deben ser usados solo para propósitos laborales.
- Está prohibido el acceso indebido a la codificación y programación de los equipos.
- No se debe transmitir mensajes con palabras obscenas, apodos, comentarios políticos o religiosos que afecten la integridad de los usuarios de este sistema de comunicación.
- El uso indebido de los radios podrá ser causal de amonestaciones o medidas disciplinarias por parte de la **E.S.E IMSALUD**
- En los equipos celulares no está permitido retirar la sim card y colocarla en un computador portátil o un en un módem USB para efectos de ingresar a internet desde la computadora.
- Con respecto a la reposición de los equipos celulares la misma será tramitada cuando por desgaste, daño de fábrica u otra razón no atribuible a responsabilidad directa del empleado requiera el reemplazo del equipo. En dichos casos la empresa de manera discrecional tramitará el reemplazo por un modelo que se considere conveniente.
- Si los costos mensuales del uso de celular exceden los minutos y valores del plan asignado, la **E.S.E IMSALUD** podrá exigir la justificación y/o pedir el pago por parte del empleado de los valores de exceso en los que incurra en la facturación mensual.

16.9.CUSTODIA DE RECURSOS INFORMÁTICOS

- Los usuarios de cualquier activo informático de la infraestructura de Hardware, Software y Telecomunicaciones de la **E.S.E IMSALUD** no deben fumar, comer ni beber cerca o sobre ellos y tampoco realizar acciones riesgosas o inadecuadas para su seguridad física.
- Está restringido el uso y copia de información de la compañía en memorias USB, Flash o memory key. En caso de ser necesario el copiado de información en estos dispositivos: Deberá garantizar que la información de estas memorias es borrada luego de ser copiada; En caso de entrega de información a terceros a través de este medio, notifique por correo electrónico el tipo de información entregada, la fecha y entidad o persona a la que se entrega.
- Responder por los recursos informáticos que le sean asignados de acuerdo con las normas de la Empresa sobre el manejo de activos fijos. En el caso de que se compruebe que el daño o pérdida es causado por omisión o descuido del funcionario, este deberá asumir el costo de reposición del recurso informático a su cargo.
- Cumplir con los procedimientos establecidos para el manejo de pérdidas y daños en los activos o recursos informáticos.
- Garantizar que la información a su cargo esté disponible siempre que se requiera.
- Mantener actualizado el inventario de hardware y software que esté bajo su responsabilidad.
- Verificar las condiciones de los equipos y del software antes y después de cada mantenimiento o de cada visita o intervención de Servicios de Tecnología.
- Realizar periódicamente procedimientos de copias de respaldo y seguridad (backup) y recuperación de sus datos y software.
- Identificar adecuadamente los medios magnéticos de almacenamiento, disquetes, memorias USB y cintas, entre otros.
- Avisar oportunamente a Servicios de Tecnología cuando ocurran cambios de computador (hardware) y software asignado para soporte de las funciones o cuando el hardware vaya a ser transferido a otro usuario, dependencia o lugar.
- Asumir y responder por las consecuencias de pérdidas y daños de activos informáticos, por descuido u omisión de las recomendaciones de uso de los equipos.

16.10. RESPONSABILIDADES

La junta directiva de la E.S.E. IMSALUD es responsable de desplegar los medios técnicos y humanos necesarios para garantizar la confidencialidad, integridad y disponibilidad de sus datos de negocio. Para ello instaurará las políticas, normativas, procesos y procedimientos que sean requeridos, y se compromete a distribuirlos entre todo el personal involucrado.

Es responsabilidad de la junta directiva de la E.S.E. IMSALUD establecer y revisar periódicamente los diferentes controles de acceso a los sistemas de información que sostienen el negocio. Para ello, determinará perfiles de usuario y limitará los accesos al sistema en función de las necesidades requeridas por cada empleado para el desarrollo de sus actividades laborales. Adicionalmente, siempre que sea de obligado cumplimiento, se tratará cualquier elemento introducido en los sistemas de información gestionados, según los requisitos establecidos por la legislación vigente sobre Propiedad Intelectual y Protección de Datos de Carácter Personal.

Por otra parte, el Equipo de Seguridad Informática está compuesto por los representantes de los distintos departamentos del sistema integral de la información, así como por el Coordinador de Seguridad de la Información, el coordinador de Telecomunicaciones (cuando exista), y el abogado o representante legal de la E.S.E. IMSALUD. Este equipo de trabajo está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a la seguridad en informática y telecomunicaciones.

También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones trimestrales, el Equipo de trabajo efectuará la evaluación y revisión de la situación de la Compañía en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad.

El equipo de la seguridad de la información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la junta directiva de la E.S.E. IMSALUD y la Gerencia de Telecomunicaciones (cuando exista). También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades

necesarias para garantizar un ambiente informático seguro. Además, debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

El Coordinador de Seguridad de la Información es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

El Administrador del Sistema Integral de la información, es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra.

El Administrador del Sistema Integral de la información, también es responsable de informar al Coordinador de Seguridad de la Información y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Coordinador de Seguridad de la Información, el equipo de Seguridad de la información es el encargado de asignar Coordinador de Seguridad de la Información temporalmente, este será luego asignado en la próxima reunión de la junta directiva de la E.S.E. IMSALUD.

Los usuarios son responsables de cumplir con todas las políticas de la E.S.E. IMSALUD relativas a la seguridad informática y en particular:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial de la E.S.E. IMSALUD a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la la junta directiva de la E.S.E. IMSALUD a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con las funciones del área de trabajo.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Reportar inmediatamente a su jefe inmediato a un integrante del equipo de Seguridad Informática, cualquier evento que pueda comprometer la seguridad de la junta directiva de la E.S.E. IMSALUD y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

Cada usuario es responsable del equipamiento que la E.S.E. IMSALUD, le ha confiado para el desarrollo de sus funciones laborales. Por ello, sólo podrá extraer de las instalaciones de la E.S.E. IMSALUD, aquellos equipos y dispositivos autorizados por la dirección. Cualquier desperfecto ocasionado por el uso o traslado inadecuado de los recursos, será atribuible al usuario. Igualmente, el usuario es responsable de proteger y mantener la confidencialidad de la información perteneciente o confiada a E.S.E. IMSALUD, y deberá contribuir de manera activa al secreto de la misma.

Imsalud
EMPRESA SOCIAL DEL ESTADO

17. GUÍA COPIAS DE SEGURIDAD

Objetivo

Respaldar y duplicar activos de información mediante la utilización de elementos tecnológicos de almacenamiento externo o diferente a los utilizados en la operación normal para garantizar la confidencialidad, integridad, disponibilidad y una alternativa de respaldo eficiente ante la posibilidad de pérdida de los datos.

Alcance

Inicia con la operación de respaldo de la información en el datacenter o centro de almacenamiento de la información y termina con la identificación, rotulación y almacenamiento de la copia de seguridad en los lugares establecidos de acuerdo a los requisitos de retención establecidos en las Tablas de Retención Documental de la entidad.

Responsabilidades

- **Oficial de Seguridad de la Información:** Encargado de velar por el cumplimiento de las normas establecidas en la presente guía.
- **Administradores de sistemas de información de E.S.E. IMSALUD:** Cumplir las normas definidas en la presente guía.
- **Usuarios de la E.S.E. IMSALUD:** Dar cumplimiento a lo establecido en la Ley 1712 de 2014 en particular los Artículos 11, 18 y 19 y demás las normas establecidas en la presente guía.
- **Responsable de la Información**: Verificar la integridad de la información en caso de restauración.

Definiciones

Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Entidad y, en consecuencia, debe ser protegido.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Integridad: es la protección de la exactitud y estado completo de los activos.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de E.S.E. IMSALUD.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los

activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

SSI: Subsistema de Seguridad de la Información.

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por E.S.E. IMSALUD o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Generalidades

Ésta guía está alineada a la norma ISO 27001:2013 en el Anexo A 12.

El Grupo de Infraestructura y Soporte de TI y el Grupo de Administración y Seguridad de la Información de la Oficina de Tecnología de la Información deben proveer el respaldo de los activos de información mediante la utilización de elementos tecnológicos de almacenamiento externo o diferente a los utilizados en la operación normal de manera segura.

Los mecanismos para brindar controles de seguridad a la red de E.S.E. IMSALUD, al igual que los funcionarios y terceros deben acogerse a los controles de seguridad establecidos.

A. Se debe garantizar la salvaguarda de la información que esté alojada en los equipos que requieran servicio de mantenimiento donde se deba reinstalar el sistema operativo, formatear el o los disco(s) duro(s) de que disponga, mediante una copia de respaldo que deberá dejar en Sistemas de Almacenamiento durante el tiempo que dure el mantenimiento y puesta a punto del equipo.
B. Antes de adelantar un mantenimiento correctivo para el caso de daño de un disco duro, el responsable del mantenimiento deberá contar con las herramientas y mecanismos técnicos y tecnológicos para buscar salvar la información almacenada en el dispositivo averiado.
C. Para las Oficinas se ha dispuesto un recurso de ***almacenamiento en la red***, donde debe reposar la información propia de su gestión.
D. El tipo de información que debe ser resguardada en el servidor de archivos de acuerdo a la Ley 1712 de 2014 es Publica Clasificada Artículo 18 y Pública Reservada. Artículo 19.

E. La información que es considera Pública de acuerdo a la Ley 1712 de 2014 en su artículo 11, debe ser guardada en el ***almacenamiento en la nube***, donde se cuenta con las medidas de aseguramiento y respaldo de la información que cada funcionario allí deposita, por tanto, la Entidad garantiza la disponibilidad de la información allí almacenada.
F. En el Servidor de Archivos donde se almacena la información de cada una de las dependencias se tiene control de Modificación/cambios /eliminación: La información que se almacena a través de las carpetas compartidas en la red cuentan con logs (registros de auditoria)
G. Es deber de los responsables de la información de cada sistema de información verificar la integridad de la información, una vez sea restaurada.
H. Se debe hacer backup de la información contenida en las estaciones de trabajo cuando hay retiro de un funcionario de la Entidad.

Actividades para respaldo de la información en los activos de T.I.

No.	Actividad	Descripción	Responsable
1.	Identificar los datos a los que se va a realizar backup.	Se identifica el servidor o la base de datos a la que se le va a hacer copia de seguridad, si el backup requiere que no exista ingreso de usuarios o si el backup se puede realizar en caliente.	Propietario de la información Oficina de Tecnologías de la Información
2.	Alistar, configurar y verificar hardware para copias de respaldo.	Dependiendo de los datos a los cuales se le efectuará la copia de seguridad, se establecen parámetros para conocer si es necesario el bloqueo de entrada de usuarios al sistema; si se efectuará una copia completa o parcial a partir del último backup realizado; el tipo de sistema de almacenamiento, o si la copia se realizará de manera automática o manual.	Oficina de Tecnologías de la Información
	Verificar el estado de los medios de almacenamiento	Antes de comenzar a operar la copia de seguridad es necesario verificar el estado de los medios de almacenamiento activos, a	Oficina de Tecnologías de la Información

No.	Actividad	Descripción	Responsable
3.	en disco duro, cinta u otro dispositivo.	través de herramientas ofimáticas establecidas para este fin, los sistemas de backups informan a los administradores las fallas o eventos que puedan presentar los medios de almacenamiento usados.	
4.	Ejecutar copia de seguridad y respaldo.	Para realizar la copia de seguridad y respaldo de información, se realizan las siguientes instrucciones: • Acceder al sistema de copias de respaldo • Crear la tarea programada de copia de respaldo o Indicando el recurso al que se va a hacer el backup - ruta o El tipo de backup y la frecuencia o El horario de la ejecución de la tarea. • Ejecutar las tareas programadas – tarea ejecutada automáticamente por el software de backup. El esquema de rotación de las copias de seguridad se basa en las condiciones de la operación.	Oficina de Tecnologías de la Información
5.	Verificar que el backup realizado haya quedado bien ejecutado en el medio de almacenamiento.	Los datos grabados, se deben verificar al finalizar la copia, debido a que estos pueden presentar errores, para esto se debe ingresar al software de backup y verificar la operación realizada, en dado caso de que algún backup haya presentado errores se debe informar al responsable para su corrección.	Oficina de Tecnologías de la Información
6.	Monitorear frecuencia de backup	La frecuencia establecida debe ser probada para establecer su practicidad y si es necesario replantear o mejorarla sobre la marcha, verificando que el backup se puede hacer correctamente en los tiempos previstos.	Oficina de Tecnologías de la Información
		Todo medio o sistema de almacenamiento, deberá ser rotulado con la siguiente información: Servidor o Base de datos - año - mes – día - hora - consecutivo generado por el sistema.	Oficina de Tecnologías de la Información

No.	Actividad	Descripción	Responsable
7.	Identificar, rotular y almacenar y Cerrar Operación.	En caso de que algún funcionario necesite copias de sus archivos almacenados en el servidor de backup, debe solicitar mediante oficio.	
8.	Restauración backup	Como tarea programada trimestralmente se restaura una copia de seguridad aleatoriamente, para verificar su integridad y la disponibilidad de la información, esta tarea deja un registro en la herramienta de gestión de TI.	Oficina de Tecnologías de la Información

Documentación de Referencia

- Norma NTC ISO IEC 27001:2013 Anexo A12

Registros

- Herramienta de Gestión de TI

CONTROL DE CAMBIOS				
ASPECTOS QUE CAMBIARON EN EL DOCUMENTO	**DETALLES DE LOS CAMBIOS EFECTUADOS**	**RESPONSABLE DE LA SOLICITUD DEL CAMBIO**	**FECHA DEL CAMBIO DD/MM/AAAA**	**VERSIÓN**
Adopción del documento	Solicitud de creación mediante memorando Se realiza aprobación Mediante memorando	Jefe Oficina de Tecnologías de la Información		1
Actualización del documento				2

Imsalud
EMPRESA SOCIAL DEL ESTADO

18. GRUPOS DE WHATSAPP EN EL TRABAJO

Hemos encontrado que ningún grupo tiene reglas establecidas de comportamiento, algo que sería MUY útil para evitar que saturen con basura digital, memes, debates sin sentido, herir susceptibilidades y provocar reacciones negativas.

Por esta razón incluimos este anexo y establecemos una serie de puntos para que se tengan en cuenta al crear grupos de trabajo dentro de la empresa y promover como código de comportamiento:

- Respete el propósito/objetivo de cada grupo. Un grupo de trabajo NO debe ser utilizado para mandar mensajes/contenido de índole personal, NO deben ser utilizados para la promoción de productos y servicios de trabajo. (Para eso están los mensajes directos).

- No use los grupos solo para mandar memes, videos, fotografías y noticias, y jamás leer e interactuar. El propósito de los grupos es establecer comunicación, pero cuando solamente colocas contenido, pero jamás lees o interactúas, pierde propósito la existencia del mismo. A nadie le gustan los monólogos.

- Jamás mandes contenido que NO haya sido verificado. Colocar contenido cuya autenticidad no haya sido comprobada puede ser MUY peligroso y perjudicar a muchas personas. En Whatsapp circulan muchas mentiras a las que es mejor ponerles un ALTO que difundirlas.

- Si te sientes incómodo en el grupo por cualquier razón, siéntete en libertad de salirte o “silenciar” las notificaciones. Es mejor que te critiquen por haberte salido que por tus comentarios negativos y quejas.

- Antes de mandar una queja al grupo, identifica al “administrador” del mismo y transmítesela a él/ella.

- No te enfades si alguien no responde a los mensajes en un grupo. Nadie está obligado a hacerlo. Mejor mándale un mensaje directo.

- Antes de mandar un video, fotografía, meme o cualquier contenido, analiza si será de interés de la mayoría de los integrantes y aporta para el fin que fue creado el grupo.

- Cuando vayas a dar “reenviar” a un mensaje/foto/video y estés escogiendo a varios destinatarios, evita mandarlo a todos tus grupos, ya que difícilmente el mismo contenido será apto o de interés para todos.

- Evita colocar contenido que difícilmente todos tendrán las mismas creencias religiosas y preferencias políticas. Evita los debates innecesarios.

- Evita mandar cualquier contenido que sea violento o pornográfico, es importante SIEMPRE tener presente que muchas personas pueden sentirse incómodas, sobre todo cuando el contenido afecta la reputación y honorabilidad de alguien.

- Cuando quieras responder a un comentario en específico de una persona, utiliza la función de “responder” para darle sentido a tu comentario y evitar confusiones.

- Al darte cuenta que estás teniendo un diálogo con un solo integrante del grupo, considera mejor cambiar la conversación a mensaje directo, debido a que al resto del grupo quizás no les interesa estar leyendo tus mensajes con otra persona.

- No pierdas de vista que tus palabras pueden ser interpretadas de múltiples formas, así que utiliza frases cortas que no puedan ser malinterpretadas.

- No abuses de los emojis. Hay unos como este 😂 o 😢 que no requieren explicación, pero otros como este 😆 o pueden ser interpretados de distintas formas generando confusión.

- Evita mandar videos/archivos que sean muy pesados/grandes, ya que a nadie le gusta que se sature la memoria de su teléfono o se agote su plan de data/internet.

- Estipula el horario de utilización del grupo