E.S.E HOSPITAL SAN FELIX
LA DORADA – CALDAS-

PRESENTACION PLANES

- 1. PLAN ESTRATEGICO DE TECNOLOGIAS DE INFORMACION Y LAS COMUNICACIONES – PETI y/o PETIC 2023.
- 2. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2023.
- 3. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2023.

PRESENTACION POLITICAS

- ANEXO 1. POLITICA O PLAN DE TRATAMIENTO DESEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2023.
- ANEXO 2. POLITICA O PLAN DE TRATAMIENTO DE LOS DATOS PERSONALES 2023.

INTRODUCCIÓN

Es deber de las instituciones públicas velar por la información que cada una de estas obtiene, de acuerdo a esta compilación se captura, se procesa y finalmente arroja resultados que son objeto de análisis y estudios para el mejoramiento continuo y de calidad. El modelo integral de gestión estratégica con tecnología cuya base fundamental es la alineación entre la gestión de tecnología y la estrategia sectorial o institucional facilita el desarrollo de una gestión de TI que genera valor estratégico para el sector, la entidad, sus clientes y usuarios.

Plan Estratégico de Tecnologías de la Información es el conjunto de herramientas claves que le permitirán a cualquier entidad establecer y cumplir unos parámetros ideales para mejoramiento en el procesamiento, almacenamiento y gestión tanto de los Sistemas de información, así como de los medios y métodos en las tecnologías de información que se requieren para establecer como políticas dentro de las entidades.

PLAN ESTRATETICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICAICONES

¿Qué es?

Es un modelo que busca que la tecnología contribuya al mejoramiento de la gestión apoyando los procesos para alcanzar una mayor eficiencia y transparencia en su ejecución, facilite la administración y el control de los recursos y brinda información objetiva y oportuna para la toma de decisiones en todos los niveles.

¿Cómo funciona?

- Planea, ejecuta, mejora y muestra resultados en la organización.

- Conociendo el resultado del diagnóstico inicial se podrá establecer el plande trabajo **(Número de horas, días de trabajo, talento humano, experticia, clima laboral, aptitudes y otros detalles que puedan ser necesarios para la construcción del (PETI).**

¿Qué se hace en la definición de PETI y/o PETIC?

- Definir el adecuado uso y apropiación de las Tecnologías de la Información.
- Relación con sistemas de información actuales y futuros.
- Relación y dependencia entre servicios de Tecnología de la Información.
- Análisis financiero del PETI

¿Qué empresas lo necesitan?

- Todo tipo de organización que desee establecer un Plan Estratégico de las tecnologías de información y las comunicaciones, para contribuir a los planes estratégicos de la organización.

¿Quiénes lo realizan?

- Deben utilizarse y aplicarse por un equipo humano líder, encabezado por el director o coordinador de tecnología y sistemas de información y con unos equipos de trabajo orientados a gestión de información, sistemas de información y servicios tecnológicos, entre otras cosas. Independientemente del nivel jerárquico, deben reunir las siguientes características: que tengan un pensamiento estratégico, que cuenten y cultiven sus habilidades gerenciales y de comunicación, con orientación al logro para siempre conseguir excelentes resultados.

- El área de sistemas puede hacer un diagnóstico presuntivo y estimativo para ser presentado y evaluado de acuerdo a los lineamientos de la Infraestructura tecnológica y los Sistemas de información y las comunicaciones que se tiene en la ESE.

Definiciones:

TI: Tecnología de la Información puede tratarse como lo medios, dispositivos que requieren las empresas u organizaciones para que los sistemas de información operen de una forma adecuada. Trátese del Hardware (equipos de cómputo, impresoras, escáner, switches), redes o medios necesarios para la captura y transmisión de datos, voz o video.

SI: Sistema de información. Es el Software necesario para la captura, almacenamiento, procesamiento, vigilancia y control de la operación de las instituciones.

PLAN DE TRATAMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Introducción

La administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Objetivos

➢ Objetivo general

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

Objetivos específicos

- Concientizar a todos los colaboradores, áreas, procesos, proveedores internos y externos y en general sobre la importancia de administrar de manera adecuada el plan de tratamiento de seguridad y privacidad de la información.
- Involucrar a todos los funcionarios en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos para los sistemas de información y las comunicaciones.
- Establecer, mediante una adecuada administración del riesgo, una base de datos confiable para salvaguardar y conservar toda la información de la institución.

Alcance

Esta guía, puede proporcionar la metodología establecida por la E.S.E Hospital San Félix de La Dorada - Caldas, para la administración y gestión de los riesgos a nivel de procesos.
Orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y mejoramiento continuo de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

Ámbito de aplicación

Los lineamientos definidos en este plan, aplica para la gestión de los riesgos dentro del Hospital San Félix sede central, así como los centros y puestos de salud.

Definiciones

Aunque se puede determinar muchas causales que pueden favorecer o provocar riesgos en la seguridad de la información, vamos a trabajar en la matriz para minimizar factores que obstruyan el orden correcto de la conservación de la información, contemplando solo el enfoque tecnológico, de sistemas de información y tecnológico para la administración del riesgo, se tendrán en cuenta las siguientes definiciones y términos.

- **Acciones asociadas:** Son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.

- **Administración de riesgos:** Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

- **Amenaza:** Situación externa que no controla la entidad y que puede afectar su operación.

- **Análisis del riesgo:** Etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

- **Asumir el riesgo:** Opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

- **Causa:** Medios, circunstancias y/o agentes que generan riesgos bien sean por intrusiones, descargas, usuarios internos o externos.

- **Calificación del riesgo:** Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

- **Compartir o transferir el riesgo:** Opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

- **Consecuencia:** Efectos que se pueden presentar cuando un riesgo se materializa.

- **Contexto estratégico:** Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

- **Control preventivo:** Acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

- **Control correctivo:** Acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

- **Debilidad:** Situación interna que la entidad puede controlar y que puede afectar su operación.

- **Evaluación del riesgo:** Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evitar el riesgo:** Opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.

- **Frecuencia:** Ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

- **Identificación del riesgo:** Etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos deriesgo definidos.

- **Impacto:** Medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

- **Mapa de riesgos:** Documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

- **Materialización del riesgo:** Ocurrencia del riesgo identificado.

- **Opciones de manejo:** Posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

- **Plan de contingencia:** Conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio.

- **Procedimiento:** Conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

- **Proceso:** Conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos,misionales, de apoyo y de evaluación.

- **Probabilidad:** Medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

- **Riesgo:** Eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

- **Riesgo inherente:** Es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Riesgo institucional:** Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional.

Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

- **Riesgo residual:** Nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

- **Valoración del riesgo:** Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y sí la necesita

ROLES Y RESPONSABILIDADES POR AREAS FRENTE A LA ADMINISTRACIÓN DEL RIESGO EN

LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

El éxito de la administración del riesgo depende de la participación de los directivos, servidores públicos y contratistas, es decir todos en conjunto, por esto, es preciso identificar los actores que intervienen:

- **Alta Dirección:** Aprueba y es la responsable de la ejecución de todas las directrices para la administración, fortalecimiento del riesgo en la seguridad y privacidad de la información.

- **Proceso Administración del Sistema Integrado de Gestión:** Genera la metodología para la administración del riesgo de la entidad, coordina, lidera, capacita y asesora en su aplicación (área de sistemas, proveedor externos o expertos)

- **Responsables de los procesos:** Identifican, analizan, evalúan y valoranlos riesgos de la entidad (por procesos institucionales) al menos una vez al año. Sí bien los Líderes del área de ITSI apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada área se encargará de garantizar y definir los riesgos que identifiquen, también deberán establecer los planes y las estrategias para tratarlos. Las personas que trabajan en cada uno de los procesos son los que conocen mucho mejor los riesgos existentes en el desarrollo de sus actividades.

- **Servidores públicos y contratistas:** Ejecutar los controles y acciones definidas, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad para la administración de los riesgos.

- **Control Interno:** Deberán realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

¿Qué es?

La Política de Seguridad y Privacidad de la Información representa para la ESE Hospital San Félix del municipio de la Dorada Caldas la oportunidad para utilizar la tecnología, atender las necesidades y apoyar el logro de los objetivos institucionales; se evalúan las alternativas en términos de impacto, de esfuerzo, de costos, de tiempo. No solamente se analizan los recursos, sino las implicaciones y se establecen las acciones a seguir para llevarla a cabo.
Con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la entidad apoyan la implementación de la política o plan de tratamiento de seguridad y privacidadde la información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión.

La Ese Hospital San Félix sostiene adecuadamente el direccionamiento estratégico de la entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información, correspondientes a:

- Mantener la confianza de los funcionarios, contratistas y terceros, así como la de los pacientes.
- Apoyar la innovación tecnológica
- Mitigar los riesgos en la entidad.
- Cumplir con los principios de seguridad de la información.
- Proteger los activos de información.
- Implementar el sistema de gestión de seguridad de la información
- Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos.
- Garantizar la continuidad del servicio.

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

¿Cómo se hace?

La E.S.E Hospital San Félix de La Dorada – Caldas con el propósito de salvaguardar la información de la entidad en todos sus aspectos garantizando la seguridad de los datos y en el cumplimiento de las normas legales, establece la implementación de el PLAN DE SEGURIDAD YPRIVACIDAD DE LA INFORMACION, esto con el fin de no que no se presenten pérdidas, robos, accesos no autorizados y duplicación, dela misma manera promueve una política de seguridad de la información de manera física y digital de acuerdo a la caracterización de la población de usuarios internos y externos. La cual está compuesta por:

- **Confidencialidad:** Garantizar que la información sea accesible sólo a aquellas personas autorizadas.

- **Integridad:** proteger la exactitud y totalidad de la información y los métodos de procesamiento.

- **Disponibilidad:** Responder de manera oportuna que los usuarios tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los siguientes conceptos:

- **Auditoria:** Define que todos los eventos de un sistema deben ser registrados para su seguimiento y control posterior.

- **Protección a la duplicidad:** Consiste en asegurar que una transacción sólo se realiza una vez, a menos de que se requiera nuevamente. Restringir el acceso a una transacción para duplicarla posteriormente, representando de manera fraudulenta al remitente original.

- **Rechazo institucional:** Se refiere a la negación de una entidad que haya enviado o recibido información y se refute ante terceros no haberlo hecho.

- **Legalidad:** Concerniente al cumplimiento de las leyes, normas, decretos, reglamentos o disposiciones a las que está sujeto el Organismo.

Para efectos de una correcta interpretación del presente plan, se realizan las siguientes definiciones:

- **Información:** Refiérase a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Sistema de Información:** Indíquese un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- **Tecnología de la Información:** Se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Ese, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

ANEXO 1.

POLITICA O PLAN DE TRATAMIENTO DE SEGURIDAD YPRIVACIDAD DE LA INFORMACIÓN.

1. Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.

2. Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos de su desconocimiento.

3. Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para elefecto.

4. Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.

5. Reportar los eventos de riesgo, utilizando los procedimientos e instrumentos establecidos para mitigar el efecto.

6. Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de losusuarios y partes interesadas.

7. Aumentar nuestra eficacia y efectividad en los procedimientos e instrumentos establecidos.

Para lograr lo anteriormente mencionado en **el PLAN DE TRATAMIENTO DE SEGURIDADY PRIVACIDAD DE LA INFORMACION** y en la respetiva **POLÍTICA DE ADMINISTRACIÓN DEL RIESGO EN LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION,** la alta dirección se compromete con la donación del recurso humano, tecnológico, presupuestal necesarios para la ejecución de esta política.

Hospital San Félix
E.S.E. LA DORADA - CALDAS
"ATENCION CON SENTIDO HUMANO"

DECLARACIÓN DEL COMPROMISO

La institución con el ánimo de proteger los activos de información busca establecer medidas organizacionales, técnicas, físicas y legales que permitan proteger la información crítica y de gestión para sus clientes internos y externos.

ALCANCE:

Promover el uso de tecnologías seguras mediante normas simples aplicables al usuario del sistema de información, apoyado mediante herramientas que permitan prestar servicios de salud eficientes y confiable, mejorando y ayudando así con la calidad de información capturada y procesada para generar indicadores, reportes y demás para los diferentes entes de control asimismo para el análisis y desarrollo interno.

EJECUCION DE LA POLÍTICA:

La política o plan de tratamiento de seguridad y privacidad de la información se refiere a la capacidad que se tiene para que con sistemas de información especializados o herramientas alternas de información y que trabajen simbióticamente con el sistema de información integrado actual, permita evitar amenazas latentes en el entorno y coadyuven a generar unas pautas claras para el manejo y utilización de las herramientas informáticas y la información con el fin de garantizar una adecuado soporte para el desarrollo de los procesos misionales e institucionales.

En términos generales esta política, determina los pasos y procedimientos más adecuados para la ejecución de la gestión de la información en los diferentes niveles de la organización, en los cuales tenemos los siguientes cuatro pilares fundamentales.

1. SEGURIDAD ORGANIZACIONAL

Dentro de ésta, se establece el marco formal de seguridad que tiene la institución, incluyendo servicios o contrataciones externas a la infraestructura tecnológica y de seguridad, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones de inseguridad.

2. SEGURIDAD LEGAL

2.1. Equipos e infraestructura tecnológica:

- ✓ Los servicios y equipos de la red institucional son de uso exclusivo de la institución y solo para el desarrollo de actividades laborales y misionales.

- ✓ Se garantiza el acceso a internet para soportar el desarrollo de los procesos institucionales, por esto los servicios como las páginas P2P, chats y las páginas web son restringidos por seguridad de la información empresarial y se permite su uso de acuerdo a las necesidades de los responsables de servicios o de los requerimientos misionales para reportes a entes de control.

- ✓ El usuario interno o colaborador será el principal responsable de la información que genere y se requiera guardar o custodiar para efectos de copias de seguridad y el área de sistemas o centro de datos será el responsable en segunda instancia de estas copias de seguridad que producen los usuarios; para la segunda instancia se hará cronograma de copias de seguridad anuales para transferir en los equipos especializados y para extraerlas en medios alternos (unidades de cinta, DVD o almacenamiento, pagos en la nube o discos duros móviles)

- ✓ Para todos los casos, ni en los equipos de las áreas asistenciales ni administrativas se podrá almacenar información personal (archivos de Word, Excel power point, pdf, bases de datos, imágenes, música, etc.) ni tampoco requerir que se custodie o se garantice copia de seguridad de la misma, ya que no se articula con los lineamientos misionales de la ESE Hospital San Félix.

2.2. Software

Con el fin de fructificar las mejoras realizadas a los programas, se harán las actualizaciones del software utilizado por la E.S.E. siempre y cuando se cuente con condiciones básicas de seguridad para la estabilidad del sistema de información, así como para:

El Software CNT deberá estar actualizado con la póliza al día lo que garantizará el soporte o mantenimiento que se debe hacer cada año con el fabricante de este software; en caso de cambio de este sistema de información se tendrán que establecer los tiempos y forma de mantenimiento del software con el fabricante del mismo y teniendo en consideración la normatividad de ley así lo exige.

- ✓ Se realizan revisiones o pruebas minuciosas sobre las aplicaciones, de forma aleatoria, sobre distintas fases, antes de ponerlas en un entorno operativo real, con el objetivo de evitar redundancias en las salidas de información.

- ✓ Únicamente se utiliza software certificado o en caso de contingencia software licenciado revisado y aprobado, por personal calificado en el área

2.3. Usuarios del sistema

El área brinda capacitación a los usuarios del sistema de la E.S.E Hospital San Félix sobre los lineamientos de la política de seguridad Informática.

Es responsabilidad de los colaboradores que tengan usuario, realizar el reporte de fallas administrativas relacionadas con los sistemas de información y recursos informáticos, así como de los componentes de hardware, por los siguientes medios dispuestos:

- ✓ Correos corporativos que utiliza y administrativa el área de sistemas
- ➡ sistemas@hospitalsanfelix.gov.co
- ➡ comunicaciones@hospitalsanfelix.gov.co
- ➡ Teléfonos móviles: 3178935591 – (6)8392000 Ext 111
- ➡ Chat o mensajería interna a las cuentas de: sistemas o soportesistemas

2.4. Restricciones de acceso a la información

- ✓ No debe existir sobre el escritorio o ventana inicial de los equipos decómputo información confidencial o de importancia que solo sea para uso interno y no debe estar al alcance de un tercero.

- ✓ Los usuarios y claves para los aplicativos son únicos, personales e intransferibles.

- ✓ Las claves para logueo a los pc se facilitan a todos los usuarios internos (médicos, especialistas, terapeutas, auxiliares de enfermería, enfermeros, personal administrativo entre otros) para el acceso a los equipos de cómputo y aplicativos, de igual forma no pueden ser transmitidos, copiados, cedidos, duplicados o entregados a personal externo bajo ninguna circunstancia; se tomará como una violación a este documento en el temade política y se generará reporte a la administración para los correctivos necesarios.

- ✓ Se restringe el acceso a las dependencias de sistemas, archivo central, archivo clínico, tesorería y nómina, al personal no autorizado, con el fin de salvaguardar la información que allí se almacena. Sólo funcionarios encargados de dichos procesos, se encuentran autorizadas para accedera esta información, por lo tanto cuando se detecte personal no autorizado o haya indicios de que se ha producido un acceso no autorizado, se hará constar este hecho como falla administrativa en el medio correspondiente.

- ✓ Cuando se solicite o requiera información por parte de clientes internos o externos, se deben aplicar los lineamientos contemplados en los procedimientos respectivos para tal fin.

- ✓ Los integrantes del área, realizan rondas de seguridad dos veces al año, en las cuales verifican el cumplimiento de los ítems de la política, si se encuentra alguna debilidad brindaran la capacitación necesaria a los funcionarios entrevistados.

3. SEGURIDAD LÓGICA

Establece e integra los mecanismos y procedimientos, que permiten monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software sospechoso.

3.1 Administración del Acceso

El acceso a la información es un derecho, se busca garantizar que esté disponible para todos los actores cuando la requieran, en otras palabras, la información no es de nadie pero es de todos y por lo tanto está disponible para que los públicos definidos la utilicen.

3.1.1 Responsabilidades de la entidad

Asignar a todos los usuarios del sistema una cuenta de acceso, identificando previamente los procesos en los cuales participa y los permisos explícitos a los sistemas a los cuales accederá. Dichas cuentas se activan en el momento en el cual se valida la contratación o vinculación de los funcionarios a los procesos institucionales.
La activación e inactivación de las claves de acceso a los aplicativos de la organización, está a cargo del coordinador de sistemas, al igual que su depuración.

Como autocontrol, el personal técnico de soporte informático actualizará:

- ✓ Listado de correos electrónicos.
- ✓ Listado de funcionarios que egresaron de la entidad para proceder con la inactivación de su USER + PASSWORD.
- ✓ El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al coordinador de sistemas.

Los funcionarios de la E.S.E, son usuarios limitados, estos tendrán acceso únicamente a los servicios de la red y recursos compartidos, cualquier cambio sobre los servicios a los que estos tengan acceso, será motivo de revisión y modificación de la presente política.

El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante autorización de la gerencia o convenios establecidos.
El área de sistemas e informática restringe el acceso a las bases de datos en las que se almacena la información institucional, para asegurar su correcta utilización.
La longitud mínima de caracteres permisibles en una contraseña se establece en 6 caracteres, los cuales tendrán una combinación alfanumérica, incluido caracteres especiales mientras que la longitud máxima de caracteres permisibles en una contraseña se establece en 12 caracteres, siendo esta una combinación de Mayúsculas y minúsculas.

3.1.2 Responsabilidades del Usuario

Las contraseñas son de uso personal e intransferible, cada usuario es responsable exclusivo de mantener a salvo su contraseña, para ello debe evitar guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas.
Se debe reportar al área de sistemas, los archivos en los cuales se almacene información concerniente al desarrollo de los procesos institucionales y que estas se encuentren protegidas de tal forma que se guarde allí un respaldo dela contraseña y disminuir así el riesgo de pérdida de información por olvido dela misma.

Realizar el cambio de su contraseña como mínimo cada tres meses o cuando sospeche de algún ingreso por parte de un tercero.

Al ausentarse del puesto de trabajo, aunque sea por un momento, se deben cerrar las aplicaciones que se estén utilizando y bloquear el acceso al equipo de cómputo.

3.1.3 Control para las Aplicaciones

Se tiene definido y estructurado el nivel de permisos sobre las aplicaciones, de acuerdo al nivel de ejecución o archivos, haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o perdida de información.

La creación de perfiles es necesaria para los aplicativos ya que soportan el sistema de información siendo estos operados por funcionarios de la entidad
Los perfiles para la E.S.E están definidos en dos grandes grupos ASISTENCIAL y ADMINISTRATIVOS.

El perfil asistencial es para los integrantes del equipo de salud, quienes tienen acceso a la información clínica de los usuarios en el software, información que es indispensable para el desarrollo de sus labores.

El perfil administrativo es definidos de acuerdo a las funciones administrativas y financieras, los cuales no tendrán acceso a la historia clínica del paciente por seguridad de la información.

El alcance de cada perfil es definido por los líderes de cada proceso, los cuales son parametrizados y revisados por el administrador o coordinador de sistemas, igualmente el mantenimiento de los permisos funcionales, generando en cada ajuste un acta que evidencie los cambios realizados.

El administrador o coordinador del sistema en forma conjunta con los responsables de los servicios, documenta y envía los requerimientos del software a los respectivos proveedores.

El correo electrónico es de uso exclusivo, para los empleados de la E.S.E Hospital San Félix y para manejo de información interna, por ello la entidad está facultada para revisar las cuentas de los empleados con autorización de la gerencia cuando la situación lo amerite.

Los funcionarios deberán tener su cuenta de correo electrónico depurada, es decir, sin correos electrónicos con antigüedad que supere el mes o con un tamaño mayor de 100 MB. De lo contrario el administrador del sistema podrá depurar (llevar a una cuenta alterna o repositorio, a manera de consulta) sin autorización previa, de verificarse ese hallazgo el empleado se hará acreedora un llamado de atención por el área correspondiente.

Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal o según sea necesario la eliminación parcial o total de la cuenta dentro del sistema.

Se restringe del uso del correo para:

- ✓ Conductas extorsivas o de plagio.
- ✓ Prácticas de explotación o pornografía infantil o de alguna otra índole.
- ✓ Suplantaciones

El usuario será responsable de la información que sea enviada desde sucuenta y de la información que se descargue desde los equipos de la institución.

No se permite el envío de cadenas de correo en las cuentas institucionales.

No se deben abrir correos desconocidos, en otros idiomas o con mensajes extraños por el riesgo de ingreso de un virus.

El correo electrónico debe ser revisado por los funcionarios por lo menos dos veces al día, el no realizarlo no lo exime de la responsabilidad de conocer la información suministrada por este medio.

El área de sistemas emplea dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico evitando el acceso o flujo de información no autorizada hacia la red interna o hacia el exterior.

3.3 Virus

- ✓ La institución garantiza la permanencia y actualización de plataformas de antivirus que permitan fortalecer la seguridad informática.
- ✓ Los Usuarios del Sistemas de información son los responsables de solicitar soporte informático en caso de encontrar situaciones sospechosas.
- ✓ Todos los medios extraíbles que ingresen a la institución se debe realizar previamente el proceso de vacunación.
- ✓ No instalar "vacunas" sin la autorización de área de sistemas, estas, aunque parezca no representen un riesgo, pueden estar infectadas.
- ✓ El área de sistemas es la responsable de velar por la actualización del antivirus en toda la plataforma tecnológica de computadores y portátiles.

4. SEGURIDAD FÍSICA

Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de recursos utilizados.

- ✓ El cableado de red, se instala físicamente separado de cualquier otro tipo de cables, como de corriente o energía eléctrica, para evitar interferencias, por ello todos los puntos de red datos o de voz de se deben tener certificados y estandarizados a Categoría 6 o 6ª o un nivel superior si es posible.
- ✓ Los equipos críticos de información y proceso, se ubican en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el personal de sistemas y las personas responsables por esos activos, quienes deberán poseer su debida identificación.
- ✓ Sólo el personal de sistemas puede realizar aseo y/o limpieza a los equipos de cómputo.
- ✓ En ningún momento se deben dejar desprotegidos equipos que almacenen información confidencial, estos no podrán ser manipulación por ningún motivo.

Se realiza a los servidores control exhaustivo del mantenimiento preventivo y correctivo.

- ✓ La institución vela por el buen estado del software y hardware que soportan los sistemas de información.

- ✓ Se lleva un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación en las hojas de vida de cadaequipo y con el tiempo esto será objeto de sistematización y manejo por medios que contribuyan al medio ambiente y manejo digital de la información de estos.

- ✓ La institución garantiza la dotación de seguridad necesaria para proteger la integridad de los recursos tecnológicos y la información (extintores, medidores de humedad, lámparas, reguladores, ups, circuitos regulados de energía, entre otros.)

- ✓ Se llevará con el paso del tiempo a circuitos regulados de energía que alimenta los equipos informáticos para disminuir el riesgo de pérdida o daño de información por alteraciones en el suministro de energía eléctrica, mediante una estación de alimentación ininterrumpida o UPS para proteger la información.

- ✓ Todos los colaboradores con usuario deben velar por la seguridad de los activos informáticos.

- ✓ Los servidores, al igual que las estaciones de trabajo, tienen instalado y configurado correctamente software antivirus actualizable y activa la protección en tiempo real.

- ✓ El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del área de sistemas y personal de soporte.

- ✓ Por seguridad de la información no se permite el consumo de alimentos ni bebidas en los puestos de trabajo, para evitar el daño o deterioro por dicha causa.

- ✓ Se deben vacunar los medios magnéticos personales que se conectan a los equipos de la red institucional.

- ✓ Se deben apagar los equipos, cortapicos de energía y reguladores al terminar la jornada laboral o en las pausas prolongadas como en el tiempo de almuerzo.

- ✓ Se debe apagar la pantalla cuando se deje de utilizar el equipo por espacios mayores de 15 minutos.

5. SEGURIDAD LEGAL

Integra los requerimientos de seguridad que deben cumplir todos losfuncionarios y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como acciones relacionadas con la legislación y contrataciones externas.

5.1. Licenciamiento de Software

Todo el software comercial que utiliza la Institución, se encuentra legalmente registrado, con sus respectivas licencias.
La adquisición de software por parte de personal que labore en la institución, no expresa el consentimiento de la institución, por ende, la institución no se hace responsable de las actividades de sus empleados.

El software comercial licenciado a la E.S.E es propiedad exclusiva de la institución, la misma se reserva el derecho de reproducción, sin el permiso de sus autores, respetando el y/o distribución a terceros.

Cualquier cambio en la política de utilización de software comercial o software libre, se hará con modificación de un documentado y con base en las disposiciones de la respectiva licencia.

El software desarrollado internamente, por el personal que labora en la ESE es propiedad exclusiva de la institución.

Los contratos con terceros, en la gestión o prestación de un servicio, deben especificar, las medidas necesarias de seguridad, nivel de prestación del servicio, y/o el personal involucrado en tal proceso cuando se utiliza el sistema de información institucional.

La instalación de software y hardware se realiza exclusivamente por parte del personal de sistemas.

DIEGO LUIS ARANGO NIETO
Gerente

Proyecto HENRY ALBERTO VILLAMIL
Ingeniero de Sistemas