POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

Teniendo en cuenta lo establecido en el Plan Vive Digital, el nuevo Modelo Integrado de Planeación y Gestión reglamento por el decreto 1499 de 2017, liderado por el Ministerio de las Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública, en cuanto a la infraestructura, los servicios, las aplicaciones y los usuarios en el marco de un ecosistema digital; las recomendaciones brindadas en el Plan Nacional de Desarrollo en cuanto a la necesidad de reconocer la seguridad informática como un factor primordial para la apropiación de las TIC; la constante evolución de los mercados; y la dinámica de las instituciones, se plantea un marco de seguridad de la información en el Hospital Departamental San Rafael de Zarzal E.S.E. para la prestación de servicios a los ciudadanos a través de las tecnologías de la información, el cual deberá ser respaldado por una gestión, unas políticas y unos procedimientos adecuados, que resaltan el papel de las personas como el primer eslabón de una compleja cadena de responsabilidades y que esté orientado a preservar los pilares fundamentales de la seguridad de la información.

Para el Hospital Departamental San Rafael de Zarzal E.S.E., la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

OBJETIVO GENERAL Y ESPECÍFICOS.

OBJETIVO GENERAL

Gestionar el Sistema de Gestión Seguridad y Privacidad de la Información (SGSPI) en el Hospital Departamental San Rafael de Zarzal E.S.E. para la toma de decisiones frente a la seguridad y privacidad de información por medio del Modelo Integrado de Planeación y Gestión (MIPG) del Hospital Departamental San Rafael de Zarzal E.S.E. y mantener niveles óptimos de seguridad y privacidad de la información, implementando políticas, controles y procedimientos que permitan de manera oportuna la atención de riesgos en los activos de la institución formulando para la Política de Seguridad y Privacidad de la Información PSPI.

OBJETIVOS ESPECÍFICOS

- Establecer las directrices a las que se deben ceñir los responsables de la Política de Privacidad y Seguridad de la Información alineado al Sistema de Gestión de Calidad.
- Establecer el Sistema de Gestión de Seguridad y Privacidad de la Información en el Hospital Departamental San Rafael de Zarzal E.S.E. SGSPI, su responsable y frecuencia de actualización.
- Establecer el responsable del SGSPI, la instancia articuladora y sus funciones.
- Mantener una adecuada gestión de los riesgos y activos de la institución en materia de seguridad y privacidad

ALCANCE, ACTUALIZACIÓN Y ROLES.

El marco institucional de seguridad y privacidad de la información será la carta de navegación para garantizar el cumplimiento del componente de seguridad y privacidad de la información enmarcada en la estrategia de Gobierno Digital, cuyo alcance comprende:

- Oficinas y dependencias de Hospital Departamental San Rafael de Zarzal E.S.E. y líderes de proceso.
- Servidores públicos
- Contratistas

Propiciando de esta manera el fortalecimiento de los sistemas de gestión institucional mediante el manejo adecuado de la información. La **actualización** de la Política de Seguridad y Privacidad de la Información estará bajo la responsabilidad de la Oficina de Sistemas y el Gerente a través del Comité Institucional de Gestión de Gestión, es decir de la Línea estratégica, primera y segunda línea de Defensa, actividad que se realizar por lo menos **1 vez al año**.

ROLES DESDE EL MIPGU

Alta Dirección (Línea estratégica – MIPG – Dimensión de Control Interno)- Comité Coordinador de Control Interno

- (representante legal o el designado por la institución, Gerente del Hospital Departamental San Rafael de Zarzal E.S.E.), Se encarga de la revisión y puesta en marcha de la PSPI, así como de su aprobación o en su defecto sanción de probarse por los medios del debido proceso para lo cual se remitirá al procedimiento de control interno disciplinario en su última versión, así mismo se encarga de la aprobación del presupuesto o recursos necesario para la ejecución del Sistema de Seguridad y Privacidad de La Información dentro del Modelo de Seguridad y Privacidad de La Información.

Líderes de Procesos (Primera línea de defensa – MIPG – Dimensión de Control Interno)

- (Líderes de proceso identificados en el manual de procesos y procedimientos vigente). Para este caso se fija a cada uno de los líderes de proceso los cuales son los responsables de:
  - Identificación de los activos
  - Custodia, resguardo y aplicación de controles para los riesgos identificados para los activos de información a cargo.

- Remitir al área de Sistemas.

Cada líder de proceso será responsable de la administración de las siguientes matrices:

- **Matriz de sistemas de información** (Identificación de activos): Instrumento que actualiza los líderes de proceso y subproceso anualmente donde registra los sistemas de información a su cargo y la información que rinde en estos. El responsable debe también velar porque el sistema de información a su cargo cuente con los recursos necesarios para su operación, así como de la información necesaria de actualización según los módulos o links que lo conformen (internet, hardware entre otros) así como de su inventario de activos.
- **Matriz de comunicación** (Identificación de activos): Instrumento que actualiza los líderes de proceso y subproceso anualmente donde registra la información que rinde y publica tanto en la página web como plataformas gubernamentales. El responsable debe velar por el registro de identificación de esta información (activos) a través del formato que disponga la Institución.

- Identificar los activos de información y administrar los controles identificados a los riesgos existentes.
- Identificar los riesgos y controles de procesos y proyectos a cargo en cada vigencia.
- Realizar seguimiento y análisis a los controles de los riesgos según periodicidad establecida.
- Actualizar el mapa de riesgos cuando la administración de los mismos lo requiera.

Dirección Administrativa (Segunda Línea de defensa – MIPG – Dimensión de control Interno).

Se integrarán al análisis y valoración de los riesgos con la metodología dispuesta para tal fin frente a la seguridad y privacidad de la información, es decir que en los periodos de reunión se abrirán los espacios necesarios para el seguimiento correspondiente a los controles donde se involucrará al responsable del área de sistemas y CIO (quién designe el gerente por acto administrativo). Seguidamente en el Comité Institucional de Gestión y Desempeño se presentará informe del avance en la implementación de la PSPI que conste por medio de acta, mecanismo a través del cual se oficializará las decisiones necesarias para ser reglamentadas por la Línea estratégica a través de actos administrativos.

- Acompañar y orientar sobre la metodología para la identificación, análisis, calificación y valoración del riesgo.
- Consolidar el Mapa de riesgos institucional.
- Monitorear cambio de entorno y nuevas amenazas.
- A la Subgerencia Administrativa le corresponde liderar su elaboración y consolidación. Debe ser elaborado por cada responsable de las áreas y/o de los procesos, junto con su equipo de trabajo.

Jefe de Control Interno (Tercera línea de defensa – MIPG – Dimensión de Control Interno)

- (Control Interno) le corresponde el rol de evaluación independiente quién de manera subjetiva realizará los procesos de auditoría interna y seguimiento al mapa de riesgos teniendo presente la presente Política de Seguridad y Privacidad de la Información. (PSPI).
- Se considera al responsable de sistemas como trasversal en todo el proceso de Seguridad de la Información por lo que se debe involucrar en las decisiones que correspondan al SGSPI en cualquiera de las líneas de defensa. Esta área será la responsable del control tecnológico y funcionamiento óptimo ayudado por la gestión de la Mesa de Ayuda, actualización de los procedimientos de Gestión TICs, revisión del mapa de riesgos de TICs con la ejecución controles, administración de hardware y software, procedimiento de backup, mantenimientos preventivos y correctivos y demás procedimientos establecidos en el manual de procesos y procedimientos de Gestión de la Información.
- Asesorar en la identificación de los riesgos institucionales.
- Revisar como mínimo una vez al año o cuando circunstancias lo ameriten (cambios en la normatividad, que la institución asuma nuevas funciones, cambios de gobierno, etc.), la política de riesgo.
- Brindar una evaluación objetiva sobre la administración de los riesgos, valorar si los controles son efectivos, realizar seguimiento a las acciones establecidas en los planes de manejo y emitir informes periódicos Al Gerente o Comité Coordinador de Control Interno.
- Reportar seguimiento a los riesgos de corrupción.

GLOSARIO

Para un mejor entendimiento se proporcionan las siguientes definiciones.

Autenticidad: Los activos de información los crean, editan y custodian usuarios reconocidos quien es validan su contenido.

Confiabilidad de la Información: Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos instituciones o procesos no autorizados.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una institución autorizada.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

Legalidad: Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución territorial.

Mesa de ayuda o Help Desk: Mecanismo o Sistema de información diseñado para la atención de las solicitudes de reparación, revisión, cambio o notificación en cuanto a hardware y software de la administración municipal a la cual responde el encargado del área de sistemas como parte de sus funciones de velar por el correcto funcionamiento de los activos de información institucionales.

No repudio: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.

Política: Declaración de alto nivel que describe la posición de la institución sobre un tema específico.

Posibilidad de Auditoría: Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y

se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la institución, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Protección a la duplicación: Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.

Seguridad de la información: La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad de la información se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información.

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Hospital Departamental San Rafael de Zarzal E.S.E., entendiendo la importancia de una adecuada gestión de la información, se compromete con la implementación de un sistema de gestión de seguridad y privacidad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los usuarios, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la institución.

Para el Hospital Departamental San Rafael de Zarzal E.S.E., la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Institución según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y usuarios en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSPI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la institución.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuarios del Hospital Departamental San Rafael de Zarzal E.S.E.
- Garantizar la continuidad del negocio frente a incidentes.

A continuación, se establecen 12 principios de seguridad que soportan el SGSPI del Hospital Departamental San Rafael de Zarzal E.S.E.:

1. El Hospital Departamental San Rafael de Zarzal E.S.E. ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de

Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la institución, y a los requerimientos regulatorios.

2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, o terceros.

3. El Hospital Departamental San Rafael de Zarzal E.S.E. protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

4. El Hospital Departamental San Rafael de Zarzal E.S.E. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

5. El Hospital Departamental San Rafael de Zarzal E.S.E. protegerá su información de las amenazas originadas por parte del personal.

6. El Hospital Departamental San Rafael de Zarzal E.S.E. protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7. El Hospital Departamental San Rafael de Zarzal E.S.E. controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. El Hospital Departamental San Rafael de Zarzal E.S.E. implementará control de acceso a la información, sistemas y recursos de red.

9. El Hospital Departamental San Rafael de Zarzal E.S.E. garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. El Hospital Departamental San Rafael de Zarzal E.S.E. garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. El Hospital Departamental San Rafael de Zarzal E.S.E. garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

12. El Hospital Departamental San Rafael de Zarzal E.S.E. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

GESTIÓN DE ACTIVOS

Se entenderá como activo de información a cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad son activos, elementos como aplicaciones de la organización, servicios web, redes, información física o digital, la gestión de activos se dará desde los responsables de los procesos y presentará informes al Comité Institucional de Gestión y Desempeño lo cual comprenderá:

1. Inventario de activos de información según su categoría y uso
2. Determinar el proceso responsable
3. Determinar posibles riesgos asociados al manejo de activos de información
4. Proteger los activos según lo determinado por el Modelo de Seguridad y Privacidad de la información o sus políticas

CONTROL DE ACCESO.

Corresponderá al delegado por la alta dirección, determinar la forma de gestionar y actualizar medidas de control de acceso garantizando el uso exclusivo de los activos de información para la realización de funciones u obligaciones de los servidores públicos y contratistas gestionando la trazabilidad y el no repudio del uso de los accesos

ADMINISTRACIÓN DE REDES Y EQUIPOS

Los equipos tecnológicos del Hospital Departamental San Rafael de Zarzal E.S.E., son herramientas que deben operar para las funciones propias para las que fueron destinadas por la gerencia. Por lo tanto, el delegado por la alta dirección, a través

de los responsables de almacén y sistemas (Gestión de la Información) dispondrá de los lineamientos necesarios para garantizar la disponibilidad, soporte y mantenimiento de redes y equipos.

USO DE SOFTWARE Y SISTEMAS DE INFORMACIÓN, CORREO ELECTRÓNICO Y USO DE INTERNET

Todos los servidores públicos y contratista del Hospital Departamental San Rafael de Zarzal E.S.E. son responsables del buen uso del software, sistemas de información, correo electrónico y uso de internet, respetando la legalidad del software, evitando instalar software no licenciado de equipos.

El uso de sistemas de información, herramientas de correo electrónico o el acceso a internet que provee o delega el Hospital Departamental San Rafael de Zarzal E.S.E. para las funciones u obligaciones del servidor público o contratistas deberá solo ser usado con fines institucionales evitando cualquier uso con interés personal.

RESPONSABLES Y CONTRASEÑAS

Todos los servidores públicos y contratistas del Hospital Departamental San Rafael de Zarzal E.S.E. a los que se asignen contraseñas tendrán un uso adecuado a los fines institucionales. Por lo tanto, cada servidor o contratista debe asumir la responsabilidad del cuidado del usuario y de la información que se maneje con dicha firma electrónica (usuario y contraseña). Se solicita evitar el préstamo de contraseñas y otra actividad que suponga el uso indebido de los activos de información.

SEGURIDAD FÍSICA DEL ENTORNO

El Hospital Departamental San Rafael de Zarzal E.S.E. a través de la alta dirección determinará las áreas seguras donde reposan activos de información crítico, proponiendo planes para impedir el acceso no autorizado, evitar pérdida, daño entre otros que pueden afectar los activos de información, medios de procesamiento y comunicaciones.

GESTIÓN DE RIESGOS

Para la gestión de riesgos asociados al manejo de la información, la institución trabajará conjuntamente con la oficina de control interno y el Modelo Integrado de

Planeación y Gestión a través con la segunda línea de defensa de la dimensión de Control Interno (Equipo operativo MECI/Comité de riesgos) con el fin de apoyar la identificación de riesgos a las dependencias, establecer controles a los riegos y realizar monitoreo periódico.

GESTIÓN DEL CONOCIMIENTO

La institución establecerá políticas de operación que garanticen la conservación y trasmisión del conocimiento relacionado con seguridad de la información y otros temas de carácter estratégico, para lograr proceso de mejora continua y permitir acciones de cumplimiento de la política de Gobierno Digital.

GESTIÓN DE INCIDENTES

La Institución establecerá los procedimientos o mecanismo de preparación, detección y análisis, contención/respuesta, erradicación y recuperación ante incidencias asociadas a la seguridad de la información de acuerdo a la capacidad institucional disponible.

CONTINUIDAD DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN.

Se deberá desarrollar planes de continuidad para aquellos servicios que son críticos para el Hospital Departamental San Rafael de Zarzal E.S.E. Los planes deben considerar medidas tanto técnicas como administrativas para garantizar la disponibilidad de los servicios de TI, por lo que se deberán adelantar o establecer las contingencias.

MANUAL DE POLÍTICAS ESPECÍFICAS

Establecer el Manual de Políticas Específicas y Aclaraciones, el cual es complemento a la Política General De Privacidad Y Seguridad De La Información y de estricto cumplimiento para los funcionarios y contratista del Hospital Departamental San Rafael de Zarzal E.S.E..

ANEXO 1

MANUAL DE POLÍTICAS ESPECÍFICAS Y ACLARACIONES

POLÍTICAS, CONTROLES Y PROCEDIMIENTOS.

COMPUTADORES, PORTÁTILES, SERVIDORES

Políticas

- Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas del Hospital Departamental San Rafael de Zarzal E.S.E. sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones.

- Los computadores de la institución sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

Controles

- El usuario deberá reportar de forma inmediata al responsable de Sistemas cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, incendios u otros.

- El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.
- Es responsabilidad del usuario evitar en todo momento la fuga de la información de la institución que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

- Los usuarios deberán asegurar que toda la información que desean sea respaldada se deberá guardar en los servidores, ya que la oficina de sistemas no se hace responsable por perdidas de información que no se encuentren dentro del servidor.

- En caso de que haya pérdida de información dentro del servidor podrán recuperar su información solicitándolo con un incidente indicando el nombre del archivo y la ruta del mismo para poder encontrarlo dentro del sistema de respaldos.

- Los centros de cómputo de la Institución son áreas restringidas, por lo que sólo el personal autorizado por el responsable de Sistemas puede acceder a ellos.

- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del responsable de Sistemas, en caso de requerir este servicio deberá solicitarlo.

- El responsable del manejo de Inventarios será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el responsable de Sistemas.

- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la institución.

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

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

- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.

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

- Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al responsable de Sistemas a través de un plan detallado.

- Queda prohibido que el usuario abra o desarme los equipos de cómputo.

- Únicamente el personal autorizado por el responsable de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.

- Los usuarios deberán asegurarse de respaldar en el servidor la información que consideren relevante cuando el equipo sea enviado a reparación y borrar

aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

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

- El usuario deberá dar aviso inmediato al responsable de Sistemas y del Almacén institucional de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

- El uso de los grabadores de discos compactos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

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

- Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el departamento de informática.

- El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantara un reporte de incumplimiento de políticas de seguridad

- Los equipos de la institución sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

- Debe respetarse y no modificar la configuración de hardware y software establecida por el área de sistemas.

- Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

- Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder interrumpibles (UPS).

- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

- Si un computador tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en computadores que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Institución.

- A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- Los usuarios no deben copiar a un medio removible (como una USB), el software o los datos residentes en las computadoras de la Compañía, sin la aprobación previa de la gerencia.

- No pueden extraerse datos fuera de la institución sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner el computador en cuarentena hasta que el problema sea resuelto.

- Sólo pueden descargarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otras dependencias de la institución.

- No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el responsable del área de sistemas.

- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el responsable del área de sistemas.

- Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

- No deben usarse USB u otros medios de almacenamiento en cualquier computador de la institución a menos que se haya sido previamente verificado que están libres de virus u otros agentes dañinos.

- Periódicamente debe hacerse el respaldo de los datos guardados en computadores y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones.

- Los programas y datos vitales para la operación de la institución deben guardarse en otra sede, lejos del edificio.

- Los usuarios de computadores son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los líderes de procesos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

- La información de la institución clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando

herramientas de encriptado robustas y que hayan sido aprobadas por el departamento de Informática.

- No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.

- El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

- Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad.

- Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la institución.

- No debe dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la institución.

- El personal que utiliza un computador portátil que contenga información confidencial de la institución, no debe dejarlo desatendido, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

SWITCHES Y ROUTERS

Política

- El responsable del área de sistemas es absolutamente responsable del manejo de los dispositivos de red entiéndase por Routers y Switches de los que dispone la institución, velando porque estén dispuestos en lugares seguros y protegidos a nivel físico, así como también a nivel lógico.

Controles

- Las contraseñas predefinidas que traen los dispositivos nuevos, deben cambiarse inmediatamente al ponerse en servicio el dispositivo.

- Se deberá designar al personal que efectuará las actividades de instalación, desinstalación, mantenimiento y conexión física de estos dispositivos.

- Definir procedimientos de recuperación ante eventualidades físicas.

- Se debe llevar un registro con la información necesaria de las personas u organizaciones que deberán ser notificadas en caso de que la red se vea comprometida por un malfuncionamiento o intrusión.

- Se debe mantener identificada la información relevante a ser capturada y retenida.

- Definir procedimientos de respuesta, autoridades y los objetivos de la respuesta después de un ataque exitoso, incluir esquemas de preservación de la evidencia.

- Se deberán enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interfaz, así como los procedimientos para su autorización.

- Se deberán identificar los servicios de configuración dinámica de los Routers, y las redes permitidas para acceder a dichos servicios.

- Se deben tener plenamente identificados los protocolos de ruteo a utilizar, y los esquemas de seguridad que proveen Seguridad en el Router.

- Se deberán designar mecanismos y políticas de actualización del reloj (manual o por NTP).

- Se deben identificar los algoritmos criptográficos autorizados para levantar VPN’s.

CORREO ELECTRÓNICO INSTITUCIONAL

Política

- El correo electrónico es de carácter personal e intransferible, es deber de cada uno de los usuarios mantener el uso de este y de su contraseña siguiendo estas dos premisas y por ningún motivo se debe permitir a otra persona acceder a este recurso o la eliminación de información de este que obstruya con la reconstrucción de información importante o de investigación.

Controles

- Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la institución, a menos que cuente con la autorización del departamento de informática.

- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del Hospital Departamental San Rafael de Zarzal E.S.E. los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones

- Queda prohibido falsear, esconder, suprimir o sustituir la institución de un usuario de correo electrónico.

- Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

BASES DE DATOS

Política

- Es obligación de la institución y en especial del administrador de la base de datos controlar todo tipo de manejo que se efectúe sobre la base de datos y velar por mantenerla protegida contra todo tipo de ataque daño o intrusión sean de naturaleza externa o interna, y en caso de presentarse este tipo de situaciones deben aplicarse los procedimientos correctivos necesarios para restaurar el funcionamiento de la misma sin que ocurra pérdida de información.

- Es política de la institución prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información

propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

Controles

- Es función del administrador especificar los privilegios que un usuario tiene sobre la base de datos
- La base de datos debe estar protegida contra el fuego, el robo y otras formas de destrucción.
- Se debe garantizar que los datos sean reconstruidos en caso de daño, efectuando periódicamente un respaldo de la información
- Los datos deben poder ser sometidos a procesos de auditoría. La falta de auditoría en los sistemas de computación ha permitido la comisión de grandes delitos.
- El sistema debe diseñarse a prueba de intromisiones. Los programadores, por ingeniosos que sean, no deben poder pasar por alto los controles.
- El sistema debe tener capacidad para verificar que sus acciones han sido autorizadas. Las acciones de los usuarios deben ser supervisadas, de modo tal que pueda descubrirse cualquier acción indebida o errónea.
- Se deberá demorar la respuesta de la base de datos ante claves erróneas aumentando la demora cada vez y se alertará si hay demasiados intentos.
- Registrar todas las entradas cada vez que un usuario entra, se debe chequear cuándo y desde dónde entró la vez anterior.
- Hacer chequeos periódicos de claves fáciles de adivinar, procesos que llevan demasiado tiempo corriendo, permisos erróneos, actividades extrañas (por ejemplo, cuando usuario está de vacaciones).
- Identificar y autorizar a los usuarios: uso de códigos de acceso y palabras claves, exámenes, impresiones digitales, reconocimiento de voz, barrido de la retina, etc.

- Se deberá contar con un sistema de manejo de autorizaciones con el fin de usar derechos de acceso dados por el terminal, por la operación que puede realizar o por la hora del día.

- Uso de técnicas de cifrado para proteger datos en la base de datos

- Diferentes tipos de cuentas que contarán con permisos para: creación de cuentas, concesión y revocación de privilegios y asignación de los niveles de seguridad.

- Manejo de la tabla de usuarios con código y contraseña, control de las operaciones efectuadas en cada sesión de trabajo por cada usuario y anotadas en la bitácora, lo cual facilita la auditoría de la BD.

CIRCUITOS LAN Y RED TRONCAL

Política

- Será considerado como un ataque a la seguridad y una falta grave, cualquier actividad no autorizada por la oficina de sistemas, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la institución, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad

Controles

- El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reacomodo de cables con el personal de Sistemas.

- La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y responsable del área de sistemas.

- Todos los cambios en la central telefónica y en los servidores y equipos de red de la institución, incluyendo la instalación del nuevo software, el cambio de direcciones IP, la configuración de Routers y Switches, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios

apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

- El acceso a Internet provisto a los usuarios de la institución es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

- Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la institución, en caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por el responsable del Área de Sistemas.

- Los usuarios de Internet de la institución tienen que reportar todos los incidentes de seguridad informática al responsable del Área de Sistemas inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

- Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

    - Serán sujetos de monitoreo de las actividades que realiza en Internet.
    - Saben que existe la prohibición al acceso de páginas no autorizadas.
    - Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
    - Saben que existe la prohibición de descarga de software sin la autorización del responsable del Área de Sistemas la cual verificará los derechos de autor para su instalación
    - La utilización de Internet es para el desempeño de su función y puesto en el Hospital Departamental San Rafael de Zarzal E.S.E. y no para propósitos personales.

- Los servidores de red y los equipos de comunicación (Routers, switches, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

CONTRASEÑAS Y EL CONTROL DE ACCESO

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o sustancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem la sesión debe ser inmediatamente desconectada.

- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la institución, pudiendo ser causal de despido.

- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

- Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dichos archivos son importantes para la detección de intrusos, brechas en la

seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

CUMPLIMIENTO SEGURIDAD INFORMÁTICA

Política

La oficina de sistemas o su encargado del Hospital Departamental San Rafael de Zarzal E.S.E. tiene como una de sus funciones la de proponer y revisar el cumplimiento de la política de seguridad, que garanticen acciones preventivas y correctivas para el respaldo de equipos e instalaciones de cómputo, así como la de los bancos de datos de información automatizada en general.

Controles

- El responsable del área de sistemas podrá implantar mecanismos de control que permitan identificar tendencias en el uso de los recursos informáticos por parte del personal interno o externo. El mal uso de los recursos informáticos que sea detectado debe ser reportado

- Está absolutamente prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el departamento de informática

- Ningún funcionario del Hospital Departamental San Rafael de Zarzal E.S.E. puede intentar probar fallas en la Seguridad, a menos que estas pruebas sean controladas y aprobadas por el departamento de Informática.

- Se prohíbe absolutamente la escritura, generación, compilación, copia, colección, propagación, ejecución o intento de introducir cualquier tipo de código malicioso o potencialmente dañino conocidos como virus, gusanos o caballos de Troya, diseñados con el único fin de auto replicarse para dañar o afectar el desempeño o acceso a los centros de cómputo, redes o información del Hospital Departamental San Rafael de Zarzal E.S.E.

PROCEDIMIENTO MANEJO DE INCIDENTES ESTÁNDAR PARA TRATAMIENTO DE FALLOS. Entiéndase por Incidente todo aquel evento extraordinario que ocurra con los activos evaluados del Hospital Departamental San Rafael de Zarzal E.S.E., por ejemplo, Mantenimiento preventivo de uno o todos los computadores (Anual o Preventivo), Fallo de Activos, etc. El procedimiento en cualquiera de estos casos se debe registrar teniendo en cuenta los siguientes pasos:

1. Tipo de Solicitud.
- ✓ Incidente

2. Estado de la solicitud.
- ✓ Cerrado
- ✓ Abierto
- ✓ En espera
- ✓ Resuelto

3. Modo de solicitud.
- ✓ E-mail
- ✓ Vía Web
- ✓ Sistema de información de implementarse

4. Nombre del usuario solicitante.
- ✓ En este punto se agrega el nombre con la falla o el problema.

5. Técnico.
- ✓ Es el responsable de resolver el problema en cuestión.

6. Prioridad.
- ✓ Alta (1 Hora)
- ✓ Baja (8 Horas)
- ✓ Media (2 Horas)
- ✓ Normal (4 Horas)
- ✓ Sin tiempo de respuesta (51 Días)

QUE DEBO TENER EN CUENTA PARA IMPLEMENTAR SEGURIDAD AL INTERIOR DE LA INSTITUCIÓN

¿QUÉ ES SEGURIDAD?

Si nos remitimos al diccionario, nos encontramos con algunas definiciones:

• Sustantivo femenino. Certeza, firmeza, confianza. Sin riesgo
• Dícese de las cosas ciertas, firmes y/o libres de peligro o riesgo. Estado de las cosas bajo protección
• Confianza, tranquilidad de una persona procedente de la idea de que no hay ningún peligro que temer

SEGURIDAD DE LA INFORMACIÓN. La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad de la información se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una institución autorizada.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos instituciones o procesos no autorizados.

SEGURIDAD DE LA INFORMACIÓN AL INTERIOR DE LA INSTITUCIÓN

La alta dirección de la institución debe apoyar activamente la seguridad al interior de ella, mediante un compromiso demostrado definiendo roles y responsabilidades dentro de la empresa tendientes a garantizar la seguridad de la información.

ES IMPORTANTE, iniciar la implementación de seguridad de la información en los procesos misionales de la entidad o a los procesos que son considerados el núcleo de la institución.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

¿QUE ES UNA POLÍTICA?

Conjunto de orientaciones o directrices que rigen la actuación de una persona o institución en un asunto o campo determinado.

¿QUE ES UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN?

Conjunto de Directrices que permiten resguardar los activos de información

COMO DEBE SER UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Debe definir la postura de la dirección o la gerencia con respecto a la necesidad de proteger la información corporativa
- Orientar a los funcionarios con respecto al uso de los recursos de información
- Definir la base para la estructura de seguridad de la organización
- Ser un documento de apoyo a la gestión de TI y Seguridad Informática
- Ser general sin comprometerse con tecnologías específicas (Principio de Neutralidad Tecnológica)
- Debe abarcar toda la organización
- Debe ser de larga vigencia, manteniéndose sin grandes cambios en el tiempo.
- Debe ser clara y evitar confusiones o interpretaciones
- No debe generar nuevos problemas
- Debe permitir clasificar la información en confidencial, uso interno, publica
- Debe identificar claramente funciones específicas de los empleados como: Responsables, Custodio, o Usuario.

QUE DEBE CONTENER UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Políticas específicas.
- Procedimientos.

- Estándares o prácticas.
- Controles .
- Estructura organizacional.

QUE SON LAS POLÍTICAS ESPECÍFICAS

Definen en detalle los aspectos específicos que regulan el uso de los recursos tecnológicos y recursos de información y suelen ser más susceptibles al cambio, a diferencia de la política general de la organización.

QUE SON LOS PROCEDIMIENTOS

- Define los pasos para realizar una actividad específica.
- Evita que se aplique el criterio personal.

QUE SON LOS ESTÁNDARES

Es un documento establecido por consenso que sirve de patrón, modelo o guía que se usa de manera repetitiva. Los estándares de seguridad suelen ser actualizados periódicamente ya que dependen directamente de la tecnología.

QUE SE DEBE TENER EN CUENTA EN LA CREACIÓN DE UNA POLÍTICA

- **Objetivo:** Que se desea lograr.
- **Alcance:** Que es lo que se protege y quienes deben cumplirla.
- **Definiciones:** Aclaración de términos utilizados.
- **Responsabilidades:** Que debe y no debe hacer cada persona
- **Revisión:** Como será monitoreado el cumplimiento (Seguimiento, Indicadores, Resultados)
- **Aplicabilidad:** En qué casos será aplicable.
- **Referencias:** Documentos complementarios (Anexos).

SENSIBILICE A LOS EMPLEADOS

Realizar periódicamente capacitaciones sobre las políticas de seguridad de la información de la institución y las actualizaciones de las mismas. Además de esto sensibilizar a los empleados sobre las amenazas a las que están expuestos.

Para ello es recomendable crear un plan de comunicaciones que como mínimo contenga lo siguiente:

- Introducción
- Objetivo
- Alcance
- Divulgación y sensibilización
- Mostrar la problemática que genera el cambio
- Beneficios de la seguridad de la información
- Un plan de gestión de la cultura de seguridad de la información
- Validación de la situación actual de la institución
- Situaciones evidenciadas de casos registrados
- Una encuesta
- Presentación de resultados
- Plan de comunicaciones

COMO REALIZAR UN INVENTARIO DE ACTIVOS DE INFORMACIÓN

El inventario de activos que se va a utilizar para la gestión de la seguridad no debería duplicar otros inventarios, pero sí que debe recoger los activos más importantes e identificarlos de manera clara y sin ambigüedades.
El inventario de activos es la base para la gestión de los mismos, ya que tiene que incluir toda la información necesaria para mantenerlos operativos e incluso poder recuperarse ante un desastre.

La información que describe a un activo debe contener como mínimo:

- **Identificación del activo – SERIE DOCUMENTAL:** Un código para ordenar y localizar los activos.
- **Tipo de activo – SUBSERIE DOCUMENTAL:** A qué categoría de las anteriormente mencionadas pertenece el activo.
- **Descripción – IDIOMA, MEDIO DE CONSERVACIÓN Y/O SOPORTE, FORMATO:** Una breve descripción del activo para identificarlo sin ambigüedades.
- **Propietario - RESPONSABLE:** Quien es la persona a responsable del activo.
- **Custodio – INFORMACIÓN PUBLICADA O DISPONIBLE:** Quien resguarda el activo

- **Ubicación – LUGAR DE CONSULTA:** Dónde está físicamente el activo. En el caso de información en formato electrónico, en qué equipo se encuentra.
- **Adicionales o específicos para activos en el campo de Seguridad de la información:** Clasificación del activo, clasificación de la información, determinar la criticidad del activo, identificar si existe ICC (Índice de Criticidad Cibernética) no aplica para el Hospital Departamental San Rafael de Zarzal E.S.E.

DETERMINAR LAS POSIBLES VULNERABILIDADES Y AMENAZAS DE LA ARQUITECTURA TECNOLÓGICA QUE PROCESA LA INFORMACIÓN.

VULNERABILIDADES

A continuación, se describen algunas vulnerabilidades dependiendo de su origen de generación; esto no quiere decir que sean las únicas.

Físicas
Posibilidad de que el sistema tiene de ser atacado físicamente, por alteración, robo o destrozo del sistema informático.
Contramedidas
Cámaras de vigilancia

Natural
Grado en el que el sistema puede verse alterado por sucesos naturales, como un incendio, una inundación, terremotos.

Contramedidas
Por ejemplo, para los incendios, medidas anti incendio, como extintores, detectores de humo.

Hardware y Software

Fallos y debilidades de los aparatos informáticos, como un fallo en el disco duro el cabezal del dispositivo, a los tres meses, se estropea, por un defecto de fabricación. También son vulnerabilidades de este nivel el software que da errores, “bugs”, pudiendo afectar al acceso a los datos o a la integridad de las aplicaciones.

Contramedidas
Servicio técnico de la empresa que proporciona el software, a nuestra disposición para detectar esos fallos y subsanarlos.

El clustering, que consiste en una colección de discos interconectados que se comportan como un único disco virtual, con la diferencia del aumento de prestaciones y de las características de redundancia. La implementación más sencilla de un clúster es con dos servidores y el único propósito es garantizar la funcionalidad del conjunto; es decir, que si uno se cae el otro tome la responsabilidad, justo en el punto del proceso donde se produjo el fallo. Los usuarios sólo notaran una demora de unos segundos mientras se regeneran los datos y, superado ese momento, el funcionamiento será el normal. El objetivo del clustering es minimizar las consecuencias de las caídas de los servidores por medio de una arquitectura que, al menos mantendrá un servidor activo ante cualquier fallo del resto de los componentes del sistema.

Comunicaciones
Ahora, debido a la proliferación de redes locales, intranets, la Internet, etc., existe la posibilidad de que se vean vulneradas, por ejemplo, por culpa de un hacker que entra en nuestra base de datos a través de Internet.

Contramedidas
Firewalls, administradores que supervisan las comunicaciones, IDS, IPS entre otras.

Humana:
Es la más sutil de todas. Los usuarios pueden alterar la seguridad de nuestro sistema informático, las personas que están en contacto directo con nuestros sistemas informáticos, como los administradores, personas autorizadas, empleado, etc., Teóricamente son las más controlables.

Contramedidas
Por ejemplo, que dos personas a la vez tengan que introducir una clave cada uno.

Otra posibilidad es que un usuario que disponga de una cuenta en nuestra base de datos provoque una vulnerabilidad. Una solución ante esto podría ser separar cada servicio en un equipo distinto, como tener el servidor de correo electrónico en un equipo y el servidor de cuentas en otra, no todo en un solo equipo (como es el caso de anubis.uji.es). Es importante para evitar estas vulnerabilidades no tener usuarios directos.

AMENAZAS

Clasificadas desde el punto de vista del efecto que causan al aprovechar una vulnerabilidad.

Intercepción:
Cuando se consigue acceso a una parte del sistema sin autorización. Son difíciles de detectar porque se accede sin modificar los datos.

Modificación:
Cuando alguien accede de manera no autorizada a una parte del sistema y además se modifican datos.

Interrupción:
Puede ser indefinida o momentánea. Una interrupción del funcionamiento del sistema puede ser accidental, y entonces es difícilmente controlable. Este tipo de amenazas son las más frecuentes y las menos dañinas.

Generación:
Cuando existe la posibilidad de añadir programas no autorizados. Es el caso, por ejemplo, de los virus.

EVALÚE LOS RIESGOS A LOS QUE ESTÁN EXPUESTOS SUS ACTIVOS

El enfoque de riesgos se basa en la identificación de las amenazas y vulnerabilidades presentes en los activos de información de los procesos de una organización, y cómo pueden afectar las actividades impidiendo lograr sus objetivos.

Una buena práctica sería tener en cuenta los siguientes puntos a la hora de analizar riesgos de seguridad de la información.

- Definir el enfoque organizacional para la valoración del riesgo
- Desarrollar criterios para la aceptación de riesgos, e identificar los niveles
- de riesgo aceptables teniendo en cuenta la metodología aplicada en la institución.
- Identificar los Riesgos
- Identificar las amenazas a los activos relacionados previamente.
- Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.
- Identificar los riesgos teniendo en cuenta la Confidencialidad, Disponibilidad y la Integridad de los activos.
- Analizar y evaluar los riesgos:
- Estimar los niveles de los riesgos.

RECOMENDACIONES

- Actualice y licencie sus cortafuegos y su antivirus.
- Realice revisión periódica de su listado de contactos y practique la utilización de firma digital o autenticación del mensaje a través de hash.
- No realice transacciones desde páginas web no confiables
- No instale herramientas de escritorio remoto, siempre y cuando no se almacene un llavero de claves seguro y confiable.
- Evite conectarse desde redes inalámbricas abiertas que no tienen ninguna seguridad.
- Cerciórese de la información de contacto con el fin de verificar el auténtico originador del mensaje.
- No descomprima archivos de extensión desconocida sin antes verificar el "vista previa" el contenido del mismo.
- Elimine correos electrónicos "Spam", de esta forma evitará ir a sitios web no seguros.
- Actualice los parches de seguridad del navegador web.
- Gestión adecuada de información confidencial y de terceros (títulos financieros, chequeras, tarjetas, productos crediticios, etc.)
- Implemente servidor de correos electrónicos SPF (Sender Polcy Framework).

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición del Hospital Departamental San Rafael de Zarzal E.S.E. con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Institución y apoyan la implementación del Sistema de Gestión de Seguridad de 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 de la seguridad de la información.

El Hospital Departamental San Rafael de Zarzal E.S.E., para asegurar la dirección estratégica de la Institución, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la institución.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuarios del Hospital Departamental San Rafael de Zarzal E.S.E.
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la institución, sus funcionarios, contratistas y terceros del Hospital Departamental San Rafael de Zarzal E.S.E. y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

METODOLOGÍA DE PRUEBAS DE EFECTIVIDAD

Tiene como finalidad, indicar los procedimientos de seguridad que pueden generarse durante el proceso de evaluación en los avances en la implementación del modelo de seguridad y privacidad de la información.

Se procura que el Hospital Departamental San Rafael de Zarzal E.S.E. tenga un enfoque de seguridad en el cual se incluya el desarrollo y mantenimiento de la misma, realizando mejoras en las áreas que se requiera.

La metodología de pruebas de efectividad es una serie de actividades, que tienen por finalidad comprobar o medir la eficiencia de la implementación del modelo de seguridad en las instituciones.

Esta metodología ha sido diseñada para ayudar a la institución a entender y comprender, la realización de unas pruebas, los objetivos de las mismas y el beneficio que se obtiene al identificar sus etapas y gestionarlas.

Esta metodología es desarrollada en diferentes etapas que permiten concluir que tanto ha avanzado la institución con la implementación del modelo; de esta manera, través de la valoración de diferentes aspectos se permitirá identificar vulnerabilidades y amenazas a las cuales está expuesta la institución, así como también posibles debilidades en los controles implementados.

Un factor externo de mucho impacto, que se alinea con la ejecución de las pruebas de seguridad y privacidad y sus resultados, son los intereses de lo que se denomina Alta Dirección, que para nuestro caso son los directivos de la institución del estado, estos se ven reflejados en las capacidades de la institución de llevar a buen término la implementación del modelo de seguridad para dar cumplimiento a la normatividad vigente; así como llevar a la institución al siguiente nivel de seguridad que permite que sus procesos y atención al ciudadano deje una buena imagen en la sociedad colombiana.

ALCANCE

La metodología busca desde el primer momento de la ejecución, crear una línea base del estado de seguridad de la institución, es decir, facilitar la identificación de la brecha en la implementación del modelo de seguridad, entiéndase como línea base la primera medición; las siguientes mediciones darán a la institución la percepción de seguridad que manifiestan en la implementación del modelo de seguridad.

El alcance en la institución es de total cobertura, dada la orientación del Gobierno Digital, de la normatividad y demás, la seguridad y privacidad en la institución debe desarrollarse de manera estratégica, debe tener un ciclo de vida, que permita llegar a las partes más expuestas al riesgo.

LEVANTAMIENTO DE INFORMACIÓN

En esta fase la institución debe recopilar la información necesaria para iniciar la actividad, dicha información puede ser organizada por parte del equipo de seguridad de la información de la institución.

La información recogida no solo debe permitir identificar los activos más importantes de la institución, relacionados con los procesos de la misma, ya sea misionales o de apoyo. También me debe permitir el conocer el contexto de la institución, es decir, el entorno donde se proyectan los objetivos de la institución.

El grupo de personas que hace la recolección de información, debe reconocer el organigrama de la institución, mapa de procesos, política de seguridad, manual de políticas, metodología de riesgos, identificación de riesgos, planes de gestión de riesgos, entre otros, esta información es la base para la identificación de la brecha de seguridad que tiene la institución.

En esta fase también se debe identificar los grupos de interés, al interior de la institución.

•Reunión de inicio - Equipo de Seguridad
•Recolección de Información
•Identificación de grupos de Interés - Dueños de Procesos.
•Mapa de procesos
•Levantamiento de Información

IDENTIFICACIÓN DE AMENAZAS

La identificación de amenazas no es otra cosa que la evaluación del riesgo que se realiza en la institución, es decir, es la evaluación de las actividades donde se ven involucradas las personas, la infraestructura y los procesos; con el objetivo de identificar las amenazas que se ciernen sobre la institución.

El resultado de estas actividades permite desarrollar planes de mitigación para las vulnerabilidades encontradas, orientar mejor los recursos y la ayuda a las áreas de la institución que más lo requieren; la búsqueda de estas amenazas debe ser desde que se crean los procesos y durante su ciclo de vida.

Estas actividades deben tener un enfoque simple, es decir, descomponer los procesos a través de la evaluación manual, de manera que se sepa cómo funciona y su interrelación con las otras actividades.

- Definir y clasificar los activos de la institución, evaluando su criticidad, sus posibles vulnerabilidades técnicas, operacionales y de gestión.
- Desarrollar una matriz con las amenazas potenciales, con sus vectores de ataque.
- Elaborar planes de mitigación para cada amenaza real.

El resultado de todo esto puede ser una serie de documentos, listas o diagramas, en los cuales se plasma los análisis de riesgo de la institución y sus planes de mitigación a través de los controles sugeridos

PRUEBAS Y ANÁLISIS

En esta fase la institución deben identificar los riesgos que se manifiestan a través de las debilidades en la implementación del modelo de seguridad y privacidad de la información y las vulnerabilidades que se presentan por la falta de controles de seguridad, que mitiguen los riesgos.

Estas pruebas están orientadas a evaluar la estructura de seguridad en la institución.
Para esto la institución deben revisar varios frentes de trabajo, como son el anexo de la ISO 27001:2013, el ciclo de vida de la seguridad (PHVA), el nivel de madurez de la institución de acuerdo a los niveles expuestos en el modelo de seguridad y privacidad y recomendaciones para que la institución llegue a plasmar el concepto de Ciberseguridad.

Las pruebas de vulnerabilidad en resumen son unas técnicas empleadas para comprobar la seguridad de una institución. Las pruebas son esencialmente las pruebas sobre aplicaciones, procesos y usuarios para encontrar vulnerabilidades.

TIPOS DE PRUEBAS DE EFECTIVIDAD

Pueden realizarse 3 tipos de pruebas de efectividad, basados en el nivel de conocimiento del entorno o infraestructura de la institución:

- **Pruebas Con Conocimiento Nulo Del Entorno:** Es un tipo de prueba que simularía a un atacante real, ya que se basa en que tiene muy poco o nulo conocimiento del objetivo o su infraestructura.

- **Pruebas Con Conocimiento Medio Del Entorno:** Es cuando para la prueba de pentesting, se tiene más información sobre el ambiente que será atacado, es decir, direcciones IP, sistemas operativos, arquitectura de red etc… pero es información de igual manera limitada o media. Esto emula a alguna persona dentro de la red con conocimiento básico de la misma.

- **Pruebas Con Conocimiento Completo Del Entorno**: Es cuando el hacker tiene toda la información relacionada al sistema objetivo del ataque. Es generalmente para temas de auditoría.

ALCANCE DE LAS PRUEBAS

Deben existir reglas específicas para la ejecución de las pruebas de efectividad técnicas, para asegurar que dichas actividades no incurran en fallas mayores y se pueda afectar la infraestructura o las operaciones de la institución. Dentro del alcance se pueden definir los siguientes aspectos:

1. Plan De Trabajo: Debe definirse durante cuánto tiempo se realizarán las pruebas, los sistemas que harán parte de las pruebas, las actividades específicas, los procedimientos de contingencia en caso de alguna afectación etc.

2. Insumos: Que recursos son necesarios para realizar las actividades: Personal adicional, ventanas de tiempo, equipos etc…

3. Responsables: Quienes serán los encargados de efectuar las pruebas (sean proveedores o funcionarios de la institución).

4. Afectaciones Posibles: El tipo de afectación que puede llegar a darse sobre cada sistema, también debe definirse si el objetivo es realizarlo en horario de producción o en horario de baja actividad laboral.

5. Multas o Sanciones: En caso de incumplir los parámetros anteriormente mencionados, deberán fijarse las sanciones disciplinarias o multas.

El ajuste del Manual Específico De Políticas y Aclaraciones se realizará conforme se decida en el Comité Institucional de Gestión y Desempeño CIGD.