PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION.

Carrera 5 N° a 45-103 Fondo Obrero – Puerto Nare
Teléfono: 57 834 70 50 – Celular: 310 653 26 01
pnarehoo@gmail.com

Tabla de contenido

1 INTRODUCCIÓN

Mediante el Plan de Seguridad y Privacidad de la Información la ESE. Hospital Octavio Olivares, poder así aplicar los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC basados en los componentes de Gobierno en línea en el Eje Temática de la Estrategia en seguridad y privacidad de la información, el cual busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

Ante el esquema de globalización que las tecnologías de la información han originado, principalmente por el uso masivo y universal de la Internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear y robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crackers, etc., es decir en transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

El objetivo principal de la oficina de sistemas es brindar a los usuarios los recursos informáticos con la calidad y la cantidad que demanden, es decir, prestando servicios con continuidad los 365 días del año de manera confiable. Ya que la cantidad de recursos de cómputo y de telecomunicaciones con que cuenta el hospital son de consideración y se requiere que se protejan para garantizar su buen funcionamiento.

Así pues, ante este panorama surgen las políticas rectoras que hacen que la oficina de sistemas pueda disponer de los ejes de proyección que en materia de seguridad la Institución requiere.

En la actualidad, la seguridad en la información es una de las preocupaciones más grandes que puede llegar a tener una compañía, ya que se refiere a garantizar la calidad, disponibilidad, veracidad y confidencialidad de su activo más preciado: la información.

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge, y más aún con el carácter globalizado como son la de Internet y en particular la relacionada con la Web, la visión de nuevos horizontes explorando más allá de las fronteras naturales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

Lo anterior ha llevado a que muchas organizaciones gubernamentales y no gubernamentales internacionales desarrollen políticas que normen el uso adecuado de estas destrezas tecnológicas y brinden recomendaciones para aprovechar estas ventajas, y evitar su uso indebido, ocasionando problemas en los bienes y servicios de las entidades.

De esta manera, las políticas de seguridad en informática de la institución emergen como el instrumento para hacer consciencia entre los miembros de la organización a cerca de la importancia

y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten al área de sistemas cumplir con su misión.

La política de seguridad en informática requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

2 MARCO LEGAL

- Acceso a la Información Pública Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (**Ley 1712 de 2014, art 4**).

- Activo En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- Archivo Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (**Ley 594 de 2000, art 3**).

- Ley 1266/08 Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países".

- Autorización Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (**Ley 1581 de 2012, art 3**).

- Datos Personales Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (**Ley 1581 de 2012, art 3**).

- Datos Personales Públicos Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (**Decreto 1377 de 2013, art 3**).

- Decreto 1499 del 11 de septiembre de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- Decreto 612 del 04 de abril de 2018 Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- Decreto 1008 del 14 de junio de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

3 MARCO TEÓRICO

3.1 DEFINICIONES

ACTIVOS DE INFORMACIÓN: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

AVISO DE PRIVACIDAD: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

BAKDOOR: Vulnerabilidad de un sistema operativo, página Web o aplicación que puede ser motivo de entrada para hackers, crackers, o gusanos. Uno de los más usados es la aplicación Back Orifice creado específicamente para entrar en sistemas operativos Windows usando troyanos. Puerta trasera.

BACKUP: Copia de ficheros o datos de forma que estén disponibles en caso de que un fallo produzca la perdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables, problemas si se realiza de forma habitual y periódica.

CRACKER: Persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los hackers, y pueden disponer de muchos medios para introducirse en un sistema.

CLASIFICACIÓN DE INFORMACIÓN: Es la clasificación que se debe dar en función de los requisitos legales, valor, criticidad, y susceptibilidad a divulgación o modificaciones no autorizadas.

CONFIDENCIALIDAD: La información debe ser accesible sólo a aquellas personas autorizadas.

CORREO ELECTRÓNICO: Sistema para enviar mensajes en Internet. El emisor de un correo electrónico manda los mensajes a un servidor y éste, a su vez, se encarga de enviárselos al servidor

del receptor. Para acceder al correo electrónico es necesario que el receptor se conecte con su servidor

CONTROL: Los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

DATO PERSONAL: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley.

DATO PÚBLICO: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

DATO SEMIPRIVADO: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

DISPONIBILIDAD: La información y los servicios deben estar disponibles en el momento que sea requerido.

DATO PRIVADO: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

DATO SENSIBLE: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

DOCUMENTO EN CONSTRUCCIÓN: Es aquella información preliminar o no definitiva. (artículo 6, literal k Ley 1712 de 2014).

FIREWALL: Programa que sirve para filtrar lo que entra y sale de un sistema conectado a una red. Suele utilizarse en las grandes empresas para limitar el acceso de Internet a sus empleados, así como para impedir el acceso de archivos con virus.

GUSANO: Programa informático que se auto duplica y auto propaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en la revista ACM Communications (marzo 1982).

HACKER: Persona que, gracias a sus grandes conocimientos informáticos, puede introducirse sin permiso en la información que tengan otros ordenadores o redes informáticas de particulares, empresas o instituciones si están conectados a Internet.

HARDWARE: Componentes físicos de un ordenador o de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar.

INTEGRIDAD: La información y sus métodos de procesamiento deben ser completos y exactos.

INTRANET: Internet es una Red informática de transmisión de datos para la comunicación global que permite el intercambio de todo tipo de información (en formato digital) entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional). Se llaman así a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo TCP/IP y servicios similares como WWW.

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN: Es un código para ordenar y localizar los activos de información dentro de la institución.

INFORMACIÓN CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados estipulados en el artículo 18 de la Ley 1712 de 2014 y su acceso pudiere causar un daño a los siguientes derechos:

a. El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado;
b. El derecho de toda persona a la vida, la salud o la seguridad;
c. Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la Ley 1474 de 2011.

Estas excepciones tienen una duración ilimitada y no deberán aplicarse cuando la persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable. (Artículo 6, literal c y 18 Ley 1712 de 2014).

INFORMACIÓN PÚBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía de manera motivada y por escrito, por daño a intereses públicos y bajo el cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. Se podrá negar el acceso a esta

información cuando concurra una de las siguientes circunstancias y siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional:

- La defensa y seguridad nacional;
- La seguridad pública;
- Las relaciones internacionales;
- La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;
- El debido proceso y la igualdad de las partes en los procesos judiciales;
- La administración efectiva de la justicia;
- Los derechos de la infancia y la adolescencia;
- La estabilidad macroeconómica y financiera del país;
- La salud pública.

Se exceptúan también los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos.
(Artículo 6, literal d y artículo 19 Ley 1712 de 2014).

MALWARE: Cualquier programa cuyo objetivo sea causar daños a ordenadores, sistemas o redes y, por extensión, a sus usuarios.

PHISHING: Duplicación de una página Web con el objeto o con el efecto de hacer creer al visitante que se encuentra en la en la página original.

SOFTWARE: Programas o elementos lógicos que hacen funcionar un ordenador o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos del ordenador o la red.

SPAM: Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico. Literalmente quiere decir loncha de mortadela

SPYWARE: Programa que acompaña a otro y se instala automáticamente en un ordenador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal (datos de acceso a Internet, acciones realizadas mientras navega, páginas visitadas, programas instalados en el ordenador, etc.).

TRANSFERENCIA: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país

TROYANO: Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema en el que se introduce de manera subrepticia (de ahí su nombre).

4 OBJETIVOS

4.1 Objetivo General

Implementar y desarrollar el plan de seguridad y privacidad de la información, partiendo de la identificación activos y riesgos de información asociados a los diferentes procesos que la ESE. Hospital Octavio Olivares, posee dentro del modelo organización, de tal manera que se puedan medir los riegos inherentes y residuales de la entidad, como también desarrollar un plan de contingencia informático que nos permita actuar de forma segura frente a ciertas situaciones.

4.2 Objetivos Específicos

- Enseñar a los funcionarios a utilizar las herramientas tecnológicas para minimizar el riesgo de pérdida de información.
- Realizar el despliegue de la política de seguridad de información.
- Revisar cada una de las políticas actuales con la que cuenta el hospital.
- Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en el Hospital para tener un Plan de Seguridad y Privacidad de la Información.
- Comunicar e implementar la estrategia de seguridad de la información.
- Incrementar el nivel de madurez en la gestión de la seguridad de la información.
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
- Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

5 ALCANCE

Los lineamientos del Modelo de seguridad y privacidad de la información (MSPI) y sus correspondientes guías de apoyo, serán aplicadas a los procesos estratégicos, misionales, de apoyo, de evaluación y control por tal motivo, deberán ser conocidas y cumplidas por todas las partes interesadas, que accedan a los sistemas de información, repositorios e instalaciones físicas.

6 POLITICA

6.1 POLÍTICA DE USO Y MANEJO DE INFORMACIÓN CONFIDENCIALIDAD

La ESE Hospital Octavio Olivares, se compromete a dar cumplimiento la normatividad vigente para definir los estándares para salvaguardar la información contra el uso no autorizado, divulgación o revelación, modificación, daño o pérdida de la información para impedir que terceros no autorizados tengan acceso a la misma; generando un círculo de confianza que facilite el acceso a nuestros usuarios internos y externos a los servicios de salud.

6.2 POLÍTICA DE SEGURIDAD INFORMÁTICA

La ESE. Hospital Octavio Olivares, comprometida con la prestación de servicios de salud y exhibiendo unos altos estándares de calidad, enmarcados dentro de la normatividad que regula el sector, velará porque todos los funcionarios, contratistas, y entidades de vigilancia y control, cumplan con los procesos y procedimientos estipulados por la empresa para la generación, transmisión, uso, almacenamiento, conservación y divulgación de la información generada, ya sea en forma magnética o física y de esta manera generar información oportuna y veraz, manteniendo la confidencialidad y seguridad de la misma, a través de la evaluación e innovación tecnológica que soporte la gestión clínica, académica y administrativa.

6.3 POLITICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

La ESE. Hospital Octavio Olivares, somos respetuosos de los datos personales de los titulares, y buscamos informar de manera suficiente a las personas sobre los derechos que tienen en su calidad de titulares de la información, como es el de conocer, actualizar y rectificar o suprimir sus datos personales frente a la entidad en su condición de responsable del tratamiento y en los términos de ley. Así mismo el hospital velará por el uso adecuado del tratamiento al cual serán sometidos los datos personales y finalidad de los mismos de todos sus usuarios, niños, niñas y/o adolescentes, enmarcados siempre dentro del cumplimiento de la misión institucional como prestador de servicios de salud, y demás funciones administrativas, constitucionales y legales de la Entidad."

6.4 POLITICA DE TRANSPARENCIA Y ACCESO DE LA INFORMACIÓN PÚBLICA

La ESE. Hospital Octavio Olivares, se compromete a garantizar el acceso de la información pública, generada, adquirida, transformada o que posea la entidad, información que estará disponible y publicada en su página web para que los usuarios y entes de control puedan acceder a la información.

6.5 POLÍTICA DE USO RACIONAL DE PAPEL

La ESE. Hospital Octavio Olivares, se compromete a promover acciones encaminadas reducir gastos administrativos a través del uso racional del papel a través de lineamientos que permitan el control y reducción de la utilización inadecuada del papel, por medio de buenas prácticas de operaciones preventivas y correctivas aplicables a todos los servicios mediante de la sustitución de documentos en físicos por soportes y medios electrónicos.

7 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.

7.1 DEL HARDWARE

7.1.1 De la adquisición de equipos

La compra de equipos se realiza por compra directa o a través de invitación pública según los estatutos de contratación. Los equipos de cómputo, que se adquieren tienen una garantía como mínimo de tres años en el puesto de trabajo, y el proveedor realiza dos mantenimientos preventivos el primer año, los cuales son acordados con el coordinador de sistemas del hospital.

Los monitores son tipo LCD, con tres años de garantía. Estos equipos permiten un mejor desempeño a los funcionarios pues disminuye los síntomas de fatiga, ojos rojos, y sequedad ocular.

Las impresoras tienen como mínimo una garantía de seis meses.

Inmediatamente después de tener completamente instalada la plataforma de hardware en la institución, se inicia un periodo de inducción y capacitación del personal del área de sistemas.

7.1.2 De la instalación de equipo de cómputo.

Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores y equipos periféricos), que esté o Sean conectado en la institución o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe cumplir con los siguientes requisitos:

- Visto bueno por el área de sistemas.
- Estar cubierto por el seguro contra corriente débil.
- Estar plaqueteado y relacionado en el inventario del área a la cual se ha asignado.
- Contar con una adecuada instalación eléctrica.
- Verificar que el área de trabajo sea segura y cuente con el inmobiliario mínimo para su uso.
- Los equipos informáticos no deben instalarse cerca de ventanales en los cuales entra directamente la luz del sol, ya que el calor puede dañar los circuitos electrónicos.

- La oficina de sistemas tiene un registro de todos los equipos propiedad del hospital.

- El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, será ubicado en un área que cumpla con los requerimientos de: Seguridad física, las condiciones ambientales, la alimentación eléctrica.

- La protección física de los equipos corresponde a quienes en un principio se le asigna, y corresponde notificar los movimientos en caso de que existan, a la oficina de sistemas.

- Todo equipo que se conecte a la red de datos de la empresa debe tener instalado programa de antivirus debidamente licenciado y actualizado. El programa debe residir en memoria, en los casos en que el usuario inhabilite esta funcionalidad será responsable por los daños causados.

- La instalación de equipos de cómputo del hospital debe ser autorizado y realizado por personal de la oficina de sistemas.

- La capacitación al usuario debe ser realizado por el líder de la aplicación o por el funcionario que éste delegue.

- La inducción sobre el manejo específico de los recursos informáticos que el hospital entregue al usuario final está a cargo de la oficina de sistemas.

- Todas las personas que requieran del sistema de información para el desempeño de sus funciones deben previamente acreditar conocimientos básicos del sistema operativo WINDOWS, y del software de oficina OFFICE, y en lo posible certificados por instituciones reconocidas en el medio.

7.1.3 Del mantenimiento de equipo de cómputo.

- A la oficina de sistemas le corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin se desarrolla un plan de mantenimiento preventivo y correctivo con dos visitas al año por equipo, y de una visita para el cableado estructurado.

- Los equipos con menos de un año de adquisición por parte de la empresa, se les realiza la programación de dos visitas de mantenimiento preventivo, actividad que está definida dentro del contrato de compra de los equipos.

- La oficina de sistemas tiene el listado de los equipos con los respectivos usuarios de estos, así mismo como la lista de los aplicativos que puede utilizar con las respectivas licencias y la fecha de actualización si es el caso.

7.1.4 De la reubicación del equipo de cómputo.

La reubicación del equipo de cómputo se realiza diligenciando la plantilla de traslado de inventario físico de la empresa.

7.1.5 Del control de accesos

7.1.5.1 Del acceso a áreas críticas

El acceso al área de Informática está restringido:

- Sólo ingresa al área el personal que trabaja en la misma.
- El ingreso de personas extrañas solo podrá ser bajo una autorización del responsable del área que para todos los efectos es uno de los ingenieros de Sistemas.
- Siempre ésta área debe permanecer cerrada, limpia y organizada.
- Las visitas al área de Informática o centro de cómputo por personas ajenas a la entidad, podrán hacerlo con previa identificación personal y sólo para realizar labores propias del área.
- Esta área debe recibir aseo y mantenimiento por lo menos una vez al día y sus adecuaciones físicas se realizan de acuerdo con las normas de seguridad industrial establecidas para tal fin.

7.1.6 Del control de acceso al equipo de cómputo.

Cualquier Terminal que pueda ser utilizada como acceso a los datos de un Sistema controlado, es encerrada en un área segura o guardada, de tal manera que no sean usadas, excepto por aquellos que tengan autorización para ello.

Restricciones que se aplican:

- Determinación de los períodos de tiempo para los usuarios a las terminales.
- Designación del usuario por la Terminal o de la Terminal por usuario.
- Limitación del uso de programas para usuario o terminales.
- Límite de tentativas para la verificación del usuario.
- Tiempo de validez de las contraseñas. la contraseña, cuando una Terminal no sea usada pasado un tiempo Predeterminado (10 - 20 minutos).

- Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la oficina de sistemas tiene la facultad de acceder a cualquier equipo de cómputo del hospital.

- Los equipos cuentan con mecanismos de seguridad según su uso o tipo, los monitores LCD que sean expuestos al público o que sean de fácil acceso al público cuentan con mecanismos físicos que les brindan seguridad.

- En los lugares donde se tienen instalados los equipos informáticos está prohibido consumir alimentos.

7.1.7 Del control de acceso local a la red.

Los programas de control de acceso identifican los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas:

a. **Nivel de consulta de la información:** El privilegio de lectura está disponible para cualquier usuario y sólo se requiere un conocimiento de la estructura de limitaciones para información confidencial o por su importancia estratégica para la empresa, así como de control).

b. **Nivel de mantenimiento de la información:** El concepto de mantenimiento de la información consiste en:

- **Ingreso:** Permite insertar datos nuevos, pero no se modifica los ya existentes.
- **Actualización:** Permite modificar la información, pero no la eliminación de datos.
- **Borrado:** Permite la eliminación de datos.

- La oficina de sistemas es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

- Dado el carácter unipersonal del acceso a la red, la oficina de sistemas verifica el uso responsable de las tecnologías de la información.

- El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, etc.) conectado a la red es administrado por la oficina de sistemas.

- Todo el equipo de cómputo que esté o sea conectado a la Red o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe sujetarse a los procedimientos de acceso que emite la oficina de sistemas.

7.1.8 De acceso a los sistemas administrativos.

La instalación y uso de los sistemas de información se rigen por las políticas de la oficina de sistemas:

- A los servidores de bases de datos administrativos, se prohíbe el acceso de cualquier usuario, excepto para el personal del departamento de Informática.

- El control de acceso a cada sistema de información de la entidad es determinado por la oficina de sistemas quien es responsable de asignar los perfiles de los usuarios y definir los grupos de trabajo.

7.1.9 De acceso a la información.

- Todas las personas que laboran en el hospital o terceros autorizados para acceder a la red corporativa deben identificarse mediante la utilización de códigos de usuario, claves de acceso. Los códigos de usuarios son asignados por la oficina de sistemas, previa autorización escrita del coordinador de área, informando en que módulos va a trabajar y cuáles son las funciones asignadas.

- Las solicitudes de códigos de usuarios son realizadas a la oficina de sistemas, certificando su capacitación, indicando el perfil, previa autorización del coordinador del área.

- La clave de acceso a la red tiene fecha de expiración y el usuario está obligado a modificarla. Si después de tres (3) solicitudes de cambio no lo realiza, el sistema rechazará todo intento de ingreso, y solo podrá reactivarse el usuario comunicándose con los administradores del sistema.

- Cuando un usuario se retira del hospital o es trasladado a otro servicio es deber del coordinador del servicio solicitar oportunamente el retiro o cambio de permisos a la oficina de sistemas.

7.2 De la Web

- La oficina de sistemas emite las normas para el uso de los servidores Web, el manejo de las bases de datos, el uso de la Intranet, así como las especificaciones para que el acceso a estos sea seguro.

- Los accesos a las páginas Web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan por la oficina de sistemas.

- La oficina de sistemas es la responsable de la verificación de respaldo y protección adecuada.

- El material que aparezca en la página de Internet del Hospital debe ser aprobado por la Gerencia y la oficina de sistemas, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

- La oficina de sistemas tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información, y conservar información del tráfico.

7.2.1 De utilización de los recursos de la red

- Los recursos disponibles a través de la red del hospital serán de uso exclusivo para asuntos relacionados con las actividades del hospital.
- Le corresponde a sistemas administrar, mantener y actualizar la infraestructura de la red del hospital.
- Dado el carácter confidencial que involucra el correo electrónico la oficina de sistemas deberá emitir la reglamentación, acorde a políticas.
- Los equipos de la tecnología de la información no se utilizan para realizar trabajos personales.

7.2.2 Del manejo de las contraseñas

- Evite utilizar contraseñas que tengan palabras que se pueden encontrar en el diccionario, ya que son más fáciles de violar mediante el uso de software especializado.
- Evite el uso de información que lo defina y que sea fácil de encontrar, como los números de su teléfono o los nombres de personas allegadas etc.
- Evite utilizar la misma contraseña.
- Cambie sus contraseñas con frecuencia.
- Utilice claves que son mezclas aleatorias de números y letras. Si es posible, también mezcle caracteres en mayúsculas y minúsculas.
- No revele su contraseña. De nada sirve crear una palabra clave que no se pueda violar, si la deja apuntada en un papel pegado a su computador.
- La contraseña debe contener como mínimo 8 caracteres.
- La contraseña se inactivará después de tres intentos fallidos.

7.3 Del Software

7.3.1 De la adquisición de software.

- Los productos de software que se adquieren cumplen con los requisitos y requerimientos específicos de la institución, en cuanto a la plataforma de software y de hardware. Tienen una alta

calidad en cuanto al grado que satisface los requerimientos de la institución: precisión requerida, cantidad de recursos utilizados, control del acceso, facilidad de uso, facilidad de mantenimiento y prueba, portabilidad del software y facilidad de ínter operación. Todos los aplicativos trabajan en ambiente WEB.

- Todo el software de la empresa está licenciado respetando los derechos de autor y se mantiene actualizado permanentemente con los parches y mejoras que le realizan al software.

- Las licencias que se adquieren son las últimas que existen en el mercado y están probadas, por ningún motivo se debe adquirir software en fase de desarrollo o beta.

- Se vela por las actualizaciones periódicas de los programas antivirus, sistemas operativos, software de oficina, manejador de bases de datos, utilitario etc.

- En cuanto a la paquetería sin costo se respeta la propiedad intelectual intrínseca del autor.

- La oficina de sistemas promueve y propicia que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

7.3.2 De la instalación de software.

La oficina de sistemas brinda la asesoría, y supervisa la instalación del software básico para cualquier tipo de equipo.

- En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permite la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.

- La instalación de software que desde el punto de vista de la oficina de sistemas pudiera poner en riesgo los recursos de la institución no está permitida.

- Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).

- La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento a la oficina de sistemas.

- Si se instala software en el servidor principal se saca una copia de seguridad completa de éste, y se guarda en el servidor de reserva, el cual está preparado para la instalación definitiva de un sistema operativo virtual.

- El software será probado antes de instalarse en el servidor principal para evaluar posibles alteraciones o conflictos de memoria.

7.3.3 De la actualización del software.

- La oficina de sistemas autoriza cualquier adquisición y actualización del software.

- Las actualizaciones del software de uso común o más generalizado se llevan a cabo en línea y para ello se destinan unos puntos de actualización a los cuales los usuarios pueden tener acceso.

7.3.4 De la auditoria de software instalado.

- La oficina de sistemas y de control interno son las responsables de realizar revisiones periódicas para asegurar que sólo programas con licencia estén instalados en las computadoras de la institución.

- Se cuenta con un inventario detallado del software instalado en cada máquina.

7.3.5 Del software propiedad de la institución.

- Toda la programática adquirida por la institución sea por compra, donación o cesión es propiedad de la institución y mantiene los derechos que la ley de propiedad intelectual le confiere.

- La oficina de sistemas tiene un registro de todos los paquetes de programación propiedad del Hospital.

- Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfases) desarrollados con o a través de los recursos del Hospital se mantienen como propiedad de la institución respetando la propiedad intelectual del mismo.

- Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.

- Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución están resguardados.

7.3.6 De la propiedad intelectual.

- La oficina de sistemas procura que todo el software instalado en el hospital esté de acuerdo a la ley de propiedad intelectual a que dé lugar.

7.3.7 De supervisión y evaluación

- Las auditorias de cada actividad donde se involucren aspectos de seguridad lógica y física se realizan periódicamente y deben sujetarse al calendario que establezca la oficina de sistemas en conjunto con la oficina de control interno.

- Los sistemas considerados críticos, están bajo monitoreo permanente.

7.3.8 De las copias de seguridad

- La oficina de sistemas realiza dos (2) copias de seguridad diariamente, de todo el sistema de CNT, Laboratorio, Vacunación (Paisoft).

- La información que genera cada dependencia se graba semanalmente en discos ópticos para lo cual el hospital destina un acceso al servidor de reserva en el cual se puede grabar la información de cada área, y esta es almacenada en discos ópticos, los cuales se archivan en orden cronológico, así mismo se graban en discos externos.

- Las copias de seguridad se almacenan en Disco Duro Externo, los cuales son llevados fuera de la institución y se evalúa la posibilidad de almacenarse en un hospital cercano o alcaldía.

- Los backups del sistema operativo, software de base, software del aplicativo se realizan cuando hay actualizaciones del software o instalación de nuevos aplicativos. Esta copia se saca en el servidor de reserva y tiene el servidor de reserva otra con el sistema operativo virtual en el caso de ocurra una contingencia.

- Se lleva formato de copia de seguridad.

- Los backups se reemplazan en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).

- Se realizan pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

7.3.9 Del manejo de la seguridad

- El hospital instalo servidores y sistemas de detección de intrusos que le permiten bloquear los intentos de acceso no autorizados a nuestro sistema de información.

- Las canalizaciones y ductería de la red de datos son de uso exclusivo de la oficina de sistemas y cualquier uso diferente que se le quiera dar debe ser autorizado y documentado por esta área.

7.4 De las condiciones físicas

- El hospital cuenta con un sistema de energía regulada que le permite minimizar las variaciones de voltaje, así mismo en los puntos críticos de la organización cuenta con sistemas de alimentación interrumpida UPS, y una planta de energía que le permite mantener corriente eléctrica en forma permanente en la institución.

7.4.1 Tomas a tierra

- La entidad en la actualidad cuenta con tomas de tierra y se verifica la polaridad con un equipo el cual es usado por el área de mantenimiento, las tomas son marcados como uso exclusivo para la red de computo de la empresa

7.4.2 FUSIBLES

- Si una parte de un computador funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo.

- A continuación, debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible.

- Entre las causas menos problemáticas para que se fundan los fusibles o salten los diferenciales se encuentra la sobrecarga de un circuito eléctrico. Para corregir esto se necesita reorganizar la distribución de enchufes sobre las placas, distribuyendo la carga de forma más uniforme.

7.4.3 Extensiones Eléctricas y capacidades

- Las extensiones eléctricas están fuera de las zonas de paso, siempre que sea posible.

- Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.

- Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esta cifra el amperaje total de todos los aparatos conectados a ellas.

- Tanto las tomas corrientes de pared como las extensiones eléctricas tienen toma a tierra.

7.4.4 Caídas y Subidas de Tensión

- Las caídas y subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen los computadores personales, los monitores, las impresoras y los demás periféricos. Si las oscilaciones se encuentran fuera de este margen, se recomienda pedir que un electricista revise el cableado e invertir en algún equipo de acondicionamiento de corriente (Estabilizadores de Voltaje).

7.4.5 De los discos magnéticos y discos duros

- En general los discos magnéticos son medios de almacenamiento "delicados", pues si sufren un pequeño golpe puede ocasionar que la información se dañe o producir un CRASH al sistema.

- No está permitido mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

- Está prohibido colocar el equipo en una zona donde se acumule calor, ya que el calor puede dilatar algunas piezas más que otras, o secar los lubricantes. Con ello se modifican la alineación entre el disco y los cabezales de lectura-escritura, pudiéndose destruir la información.

- Evitar en lo posible, la introducción de partículas de polvo que pueden originar serios problemas.

7.5 De las buenas prácticas en el uso de equipos Informáticos

- Reducción del consumo energético en los equipos informáticos.

- La Misión de una salva pantalla o protectores de pantalla es proteger la pantalla a una sobre exposición del fósforo, generada por el cañón de rayos catódicos. Esta actividad no reduce el consumo energético por lo anterior se debe colocar salva pantallas en modo "Blank Screen" Pantalla en negro, para tiempos mayores a 10 minutos.

- El tiempo en que el ordenador no está siendo utilizado interactivamente por el usuario es del orden de 3 horas por usuario día1. Por lo tanto, se debe apagar equipo en los horarios prolongados de inactividad más de media hora y en el horario de almuerzo.

- Igualmente, la impresora debe estar encendida solo si se necesita imprimir documentos.

7.6 Disposición final de los equipos informáticos

La decadencia, el deterioro y el agotamiento son componentes necesarios de la vida y del crecimiento; tenemos que aprender a valorarlos y gestionarlos. De todos los seres vivos, los humanos somos los supremos creadores de desechos, aunque sólo recientemente hemos empezado a pensar seriamente sobre las formas en que desechamos. Va quedando claro que nuestros desechos nos afectan profundamente; nuestras sensaciones, nuestra salud, nuestro confort cotidiano, y hasta nuestra supervivencia, están amenazados por ellos.

El hospital apoya las iniciativas de la presidencia de la república y participa en el programa computadores para educar entregando todos los equipos informáticos que se retiren por obsolescencia tecnológica o se den de baja por problemas técnicos.

Para realizar la baja de los equipos la oficina de sistema genera un listado de los equipos a dar de baja con el respectivo informe técnico emitido por un tercero, el cual es enviado a la gerencia para su aprobación y presentación a la Junta Directiva de la empresa, teniendo en cuenta el procedimiento de baja de inventarios.

Los equipos que son dados de baja, están sin ningún tipo de información de la empresa, ya que han sido previamente formateados.

8 PROTECCIÓN DE DATOS

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en sí mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.

Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

En muchos Estados existen normas jurídicas que regulan el tratamiento de los datos personales, como por ejemplo en España, donde existe la "Ley Orgánica de Protección de Datos de Carácter Personal" que tiene por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar

Sin embargo, el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuada o arbitrariamente.

Pero una buena Gestión de riesgos no es una tarea única sino un proceso dinámico y permanente que tiene que estar integrado en los procesos (cotidianos) de la estructura institucional, que debe incluir a todas y todos los funcionarios -¡¡la falla el eslabón más débil de la cadena!!- y que requiere el reconocimiento y apoyo de las directivas. Sin estas características esenciales no están garantizados, las medidas de protección implementadas no funcionarán y son una pérdida de recursos.

8.2 AMENAZAS Y VULNERABILIDADES

AMENAZAS

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Desde el punto de vista de la entidad que maneja los datos, existen amenazas de origen externo como por ejemplo las agresiones técnicas, naturales o humanos, sino también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos.

Generalmente se distingue y divide tres grupos:

- **Criminalidad:** son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.

- **Sucesos de origen físico:** son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.

- **Negligencia y decisiones institucionales:** son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

Existen amenazas que difícilmente se dejan eliminar (virus de computadora) y por eso es la tarea de la gestión de riesgo de preverlas, implementar medidas de protección para evitar o minimizar los daños en caso de que se realice una amenaza

VULNERABILIDADES

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos: Ambiental, Física, Económica, Social, Educativo, Institucional y Política.

9 CONVENIOS CON TERCEROS

- Los terceros que se conecten a la red de datos del hospital están obligados a seguir las políticas de seguridad existentes.

- Los terceros que tengan o traigan equipos de cómputo al Hospital, deben reportarlos a la oficina de sistemas, indicando los componentes de hardware que posea y presentar las copias de las licencias de software instalados en cada equipo.

- El hospital no asume ninguna responsabilidad por pérdida de equipos de cómputo propiedad de terceros, ni por la información almacenada en dichos equipos.

10 RECURSOS

- **Humano:** Gerente General, Líderes del Proceso, Ingeniero de sistema Personal Externo.

- **Físico:** Infraestructura Tecnológica.

- **Financieros:** No se cuenta.

11 RESPONSABLES

- Gerente.
- Subdirección administrativa.
- Líderes del Proceso
- Ingeniero de sistema

11.1 PAPEL O ROL QUE DESEMPEÑA CADA ÁREA DE LA INSTITUCIÓN EN LA ACTIVIDAD INFORMÁTICA.

11.1.1 Área de sistemas

Es un área de servicios encargada de proporcionar en forma óptima la tecnología de sistemas que requiere la institución. Es responsable de que los equipos, herramientas informáticas, telecomunicación y sistemas de información, funcionen oportuna y adecuadamente. Adicionalmente es responsable de la administración y control de las bases de datos de la institución, servidores. Esta área es responsable del desarrollo de las actividades descritas en el plan (actividades entregables) y cronograma. Su verificación se realizará; la primera con corte al 31 de diciembre del 2021 donde informará sobre todo lo concerniente a las actividades realizadas y el diagnostico situacional de la institución partiendo de aquí se ejecuta todo, al igual que el seguimiento se realizará semestral por parte de la oficina de control interno.

12 ACTIVIDADES ENTREGABLES

1. Diagnostico institucional.
2. Gestión de Activos.
3. Política de tratamientos de Datos.
4. Cifrado de la información
5. Seguridad física y ambiental
6. Relaciones con los proveedores.
7. Aspectos de seguridad de la información en la gestión de continuidad del negocio.
8. Informe de avance o resumen ejecutivo
9. Acta de Reunión.
10. Productos de cada fase o etapa.

13 CRONOGRAMA

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFROMACION AÑO 2021

No.	Actividades	Enero				Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Adopción del plan de seguridad y privacidad de la información.																																															
2	Determinar el Estado Actual de la gestión de seguridad y privacidad de la información. (Diagnostico)																																															
3	Politica de Gobierno Digital.																																															
4	Politica de Seguridad Digital.																																															
5	Política de tratamiento de datos																																															
6	Gestión de activos																																															
7	Cifrado de la información																																															
8	Seguridad física y ambiental																																															
9	Relaciones con los proveedores																																															
10	Aspectos de seguridad de la información en la gestión de continuidad del negocio.																																															

CONTROL DE CAMBIOS DEL DOCUMENTO

FECHA DE APROBACIÓN	VERSIÓN	DESCRIPCION DEL CAMBIO	ELABORACIÓN O ACTUALIZACIÓN
16/11/2021	01	Creación del documento.	Jeison Palacio Díaz Leonor Avendaño Rolón

REVISO	CARGO	DESCRIPCION DEL CAMBIO	CARGO
Leonor Avendaño Rolón	Asesora MIPG	Ciro Gomez Barrios	Gerente