GUÍA PARA GESTIÓN DE MEDIOS REMOVIBLES PARA UN HOSPITAL

TRABAJO DE GRADO

PARTICIPANTES
CRISTIAN RENE JAIMES VERA
JOSE GREGORIO RODRIGUEZ DUARTE

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

GUÍA PARA GESTIÓN DE MEDIOS REMOVIBLES PARA UN HOSPITAL

TRABAJO DE GRADO

PARTICIPANTES
CRISTIAN RENE JAIMES VERA
JOSE GREGORIO RODRIGUEZ DUARTE

ASESOR
ALEJANDRO CASTIBLANCO CARO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Ciudad, Fecha

INTRODUCCIÓN

Las nuevas tecnologías de la información y de las comunicaciones, al ser incorporadas en los distintos procesos institucionales y al quehacer personal de los funcionarios en el desarrollo de sus labores, presentan una serie de beneficios, ventajas y oportunidades, pero también conlleva una serie de riesgos que pueden afectar los activos de información de la entidad. Por esta razón se deben implementar actividades o procesos para establecer los niveles de seguridad para la institución, con el fin de definir un ciclo de mejoramiento continuo y sostenible en el tiempo, permitiendo lograr niveles de confidencialidad, disponibilidad e integridad de la información aceptables según la norma.

El uso de medios de almacenamiento de medios removibles, para los diferentes equipos de cómputo, unidades de red y servidores de la entidad, son una herramienta que facilita la trasferencia de información entre los colaboradores y las distintas áreas de la organización y a su vez pueden exponer la información a diversos riesgos y peligros que se encuentran latentes.

En el hospital, se hace necesario definir una guía de uso de medios removibles, con el fin de asegurar que la información de la entidad que se encuentra bajo la custodia del personal de la entidad no este supeditada a fuga, uso no autorizado, posibles modificaciones o divulgación de información de uso exclusivamente reservado, la cual debe ser protegida adecuadamente según parámetros establecidos. De esta manera la Dirección de Sistemas y Tecnologías con el fin de implementar un Sistema de seguridad de la información define una política que parametriza el uso de estos dispositivos.

ÍNDICE

AGRADECIMIENTOS

Primero que todo queremos agradecer a nuestro padre superior Dios, que fue quien nos guio en todo momento con su sabiduría y divinidad en el andar de esta experiencia.

Agradecemos inmensamente a nuestros padres que sin ellos no habría sido posible empezar y culminar esta etapa tan importante de la vida, como lo es formarnos como especialistas y con sentido social apoyados por los valores inculcados en nuestro hogar puestos a prueba en la universidad.

Igualmente le agradecemos al docente, el ingeniero Alejandro Castiblanco Caro por compartir tantos conocimientos y su constante colaboración en la realización de este proyecto, y también nuestro primer docente el ingeniero Diego Alejandro Corrales Caro por iniciar este proceso y orientarnos con sus aportes.

Por último, a todas aquellas personas, amigos y familiares que de alguna u otro manera estuvieron involucradas en el transcurso de nuestra formación y de este proyecto agradecemos toda su colaboración y paciencia.

RESUMEN EJECUTIVO

El presente proyecto brinda los lineamientos para la adecuada gestión de los medios removibles en el Hospital, a fin de propender por la disponibilidad, integridad y confidencialidad de la información que maneja la entidad.

Considerando que las tecnologías de la información y las telecomunicaciones al estar siendo incorporadas masivamente a los procesos institucionales y al que hacer diario de los funcionarios que las utilizan para ejecutar sus labores en el Hospital se presentan una serie de beneficios de diversa índole, pero que también conllevan asociación de ciertos riegos que pueden afectar los activos de información de la institución.

Por consiguiente, gestionar la seguridad de la información es una obligación que se debe cumplir en el marco de la normativa gubernamental vigente, y que consiste en la realizar todas aquellas prácticas que sean necesarias para establecer los niveles de seguridad que la institución determine. Con el propósito de lograr niveles de integridad, confidencialidad y disponibilidad, con todos sus activos de información relevantes para la institución.

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información del Hospital, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.

La Dirección de Sistemas y Tecnología es responsable de implementar los controles necesarios para asegurar que en los sistemas de información del Hospital sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles.

La gestión de medios removibles se aplicará a todos los usuarios ya sean de planta, contrato, honorarios asesores, consultores, practicantes y otros trabajadores. Aplicara a todos los medios removibles autorizados para su uso en la entidad. Así mismo el funcionario se debe asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de la entidad. Cada funcionario deberá conocer, adoptar y acatar los procedimientos establecidos y a sus ves será responsable por el uso de la información a su cargo y de los dispositivos de almacenamiento que emplee para el trasporte de dicha información.

El almacenamiento, asignación, etiquetado y eliminación de cualquiera de estos medios removibles debe estar acorde con el esquema de clasificación e inventario consolidado de TI y de la clasificación de activos de la entidad.

ABSTRACT

This project provides the guidelines for the adequate management of removable media in the Hospital, in order to promote the availability, integrity and confidentiality of the information handled by this entity.
Considering that the information technology and telecommunications that are being massively incorporated into the processes of the institution and into daily activities of the officials who use them to carry out their work at the Hospital, present a number of benefits of a different nature, they also may involve certain risks that could affect the information assets of the institution.
Therefore, managing the security of information is something that must be fulfilled within the framework of current government regulations, which consists of performing all those practices that are necessary to determine the levels of security that the institution needs, in order to achieve the levels of confidentiality, integrity and availability, for all the relevant information assets of the institution.

The use of removable media devices (eg CDs, DVDs, USBs, flash memory, external hard disks, Ipods, cell phones, tapes) on the Hospital information processing, will be authorized only for those employees whose position profile and functions requires.

The Systems and Technology Division is responsible for implementing the necessary control measures to guarantee that only authorized officials use the removable storage media in Hospital information systems.

The management in the use of removable media will apply to all users whether they are plant, contract, advisory fees, consultants, practitioners and other workers. It will also apply to all removable media authorized for their use in the entity. Likewise, the official must physically and logically secure the device in order not to put the information of the entity at risk. Each official must know, adopt and abide by the established procedures and in that manner be responsible for the use of the information at his expense and the storage devices that he uses for the transportation of such information.

The storage, allocation, labeling and disposal of any of these removable media must be in accordance with the IT consolidated classification and inventory scheme and the asset classification of the entity.

JUSTIFICACIÓN

La seguridad de la información permite asegurar la confidencialidad, integridad y disponibilidad de la información. Los medios removibles permiten transportar datos, esto expone a la misma a riesgo de pérdida o alteración, incluso, divulgación no autorizada además de que se expone la red a amenazas de virus y accesos no autorizados.

El Departamento de Seguridad Informática del Hospital es el encargado de la gestión de los dispositivos por lo que debe llevar un estricto control tanto de los dispositivos autorizados como de los usuarios, así como de aplicarlas políticas necesarias para limitar y responsabilizar su uso.

El Hospital identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que La Entidad establezca una guía la cual determine los procedimientos adecuados para asegurar que la información contenida en medios de almacenamiento removible sea protegida, transportada, gestionada y dado el caso eliminada según los protocolos establecidos para dicho fin.

La implementación de un procedimiento para la gestión de medios removibles demuestra el compromiso del Departamento de seguridad informática con la organización puesto que le proporciona a la entidad unas herramientas y los medios necesarios para la protección de su información y de esta manera contribuir a la consecución de los objetivos institucionales de la entidad.

Este documento describe el procedimiento de seguridad de la información definido para la puesta en marcha de un procedimiento que permita gestionar de manera efectiva el uso de los medios removibles.

PLANTEAMIENTO DE PROBLEMA

En la actualidad el avance de la tecnología genera nuevos riesgos y amenazas a las empresas, pues estas deben prepararse para enfrentar los nuevos retos que trae consigo estos desarrollos tecnológicos. Como la perdida de la confiabilidad, integridad o disponibilidad de la información por el uso no adecuado de medios de almacenamiento removibles.

Por esta razón en el Hospital es necesario definir un procedimiento que permita la correcta gestión de medios de almacenamiento removibles (CDS, DVD, USB, DISCOS DUROS, CELULARES, TABLET, IPAD), para evitar que estos sean utilizados sin ningún control por porte de los usuarios y funcionarios, poniendo en riegos la información contenida en las estaciones de trabajo de la entidad, razón por la cual se han venido presentado divulgaciones no autorizadas de información de carácter privado de los pacientes, además varios casos de infección de virus por la falta de concientización y sensibilización de los colaboradores que no escanean los dispositivos en busca de posibles infecciones y amenazas generando esto posibles pérdidas y corrupción de información, también se evidencia una clara perdida de la trazabilidad de la información puesto no existe una cadena de custodia que me permita identificar el origen y el destino que tiene la información contenida y transportada en el medio removible, encontrándose además la falta de un control que permita conocer que funcionarios están autorizados y cuales no tienen permitido el uso de estos dispositivos de almacenamiento. Se identificó además que los usuarios de la entidad no tienen una cultura de seguridad de la información puesto que no se les ha instruido y capacitado en los procedimientos que deben seguir al momento de manipular el dispositivo o almacenar, guardar, trasportar y eliminar información contenida en el medio removible.

OBJETIVO

Definir una política para el de uso de medios removibles que permita disminuir y mitigar las consecuencias generadas por la pérdida de la confidencialidad, integridad y disponibilidad de la información, en las historias de atención e información del Hospital.

Objetivos Específicos

- Diseñar la política, alcance y objetivos para el uso de dispositivos de almacenamiento removibles.
- Definir el procedimiento de gestión de medios removibles, con el fin de garantizar que la información se salvaguarde adecuadamente según está estipulado en el procedimiento.
- Diseñar un plan de trabajo de campañas de concientización para disminuir los riesgos asociados a la perdida de la confidencialidad, disponibilidad e integridad de la información, que se presenta por la manipulación inadecuada de medios removibles.
- Diseñar una matriz de riesgos para identificar los riesgos y amenazas asociados al uso de medios removibles.

ALCANCE

Este proyecto abarca el diseño del procedimiento para la gestión de los medios removibles del Hospital, el cual está orientado a definir una guía que permita establecer el uso adecuado de los dispositivos removibles y generar conciencia en el usuario sobre prácticas responsables de estos dispositivos tecnológicos, esta fase corresponde a la etapa de planeación.

Abarcara la sede principal de la entidad, por lo tanto el proceso de clasificación de activos y definición de riegos solo se realizara para esta sede, en el desarrollo del proyecto se tendrá como guía principal la norma NTC-ISOIEC 27001 versión 2013, que corresponde a un estándar referente a nivel mundial que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, además de la ISO 31000 encargada de la gestión de riesgos. Cubrirá todos los procedimientos asociados la autorización, asignación, reasignación, eliminación, trasporte y uso de los equipos tecnológicos removibles que sean utilizados en la entidad.

MARCO TEÓRICO

ANÁLISIS DEL ENTORNO DEL HOSPITAL

El hospital localizado en un departamento de Colombia, en la región Orinoquía, es uno de los departamentos menos densamente poblado.

Además, en la región el municipio capital quedó como zona de alto riesgo.[1]
En el departamento la amenaza es de nivel intermedio. Esto quiere decir que sus terrenos están constantemente influenciados por el choque de placas tectónicas y la liberación de energía a través de las fallas geológicas, de ahí que se produzcan los temblores.[2]

Ser funcionario público, es una profesión de alto riesgo según la Defensoría del Pueblo. Informes de la Defensoría del Pueblo revelan que no solo la rama judicial está amenaza, todos los funcionarios públicos están en riesgo por la inseguridad.

Desde el año 2008 el Sistema de Alertas Tempranas de la Defensoría del Pueblo, advierte sobre el peligro que afrontan los funcionarios públicos y sus familias, por culpa de las amenazas del ELN.

El año pasado, en junio, fueron asesinados funcionarios del hospital, mientras en otras zonas el rio continúa aumentando su caudal, el río contantemente amenaza con inundar algunas viviendas de la capital.

El comandante de la Defensa Civil, dijo que la mayoría de la zona rural, corre el riesgo de inundación, puesto que el río alcanzó la cota de desbordamiento (6,40).[3]

Ubicación del Hospital.

Este está ubicado en la Carrera 16 - Calle 15 Nro. 16-17, la carrera 16 es una de las vias con mas densidad de transito veicular de la ciudad, la cual converge en el ronboi de la calle 15 que a su ves es una calle con gran flujo veicular puesto que es la via de entrada a la ciudad,la carrera 15 a su ves en los horarios pico de las 6 am, 12 pm y 6 pm presenta congestion veicular dado que sobre esta carrera se ubican dos entidades educativas que, la calle 17 presenta un flujo veicular liviano.

---

[1] Modelo tomado: https://llanera.com/arauca-ciudad-de-alto-riesgo-segun-la-policia-nacional/9624
[2] http://caracol.com.co/radio/2016/05/07/nacional/1178533080_423838.html
[3] http://www.eltiempo.com/archivo/documento/MAM-300134

Entrada principal del Hospital, esta entrada esta localizada sobre la calle 15 y es por donde ingresa el personal que labora en el postital, los pacientes y las ambulancias, dado que esta entrada se necuentra sobre la calle 15 cuando ingresan y salen las ambulacias se produce congetionamiento en la via, lo cual dificulta el transito de pacientes y peatones.

Misión

Somos una empresa social del estado, que presta servicios integrales de salud de mediana complejidad, con recursos tecnológicos y un talento humano comprometido con la calidad, seguridad, innovación, y responsabilidad social, garantizando la satisfacción del usuario y su familia.

Visión

En el año 2020 el Hospital será reconocido por la fidelización de los usuarios, la auto sostenibilidad y el mejoramiento continuo.[4]

Objetivos Institucionales

- Aumentar la eficiencia y calidad en el desarrollo de los procesos, mediante la prestación de servicios de salud oportunos, seguros y continuos.
- Brindar servicios de salud, centrados en el usuario y su familia, cumpliendo cada uno de los atributos de la calidad y orientados a la satisfacción de las necesidades de salud de las personas pensando en atención humanizada a todos los usuarios del hospital.
- Lograr la plena satisfacción de los usuarios del hospital como instrumento de fidelización a los servicios en salud que el hospital brinda.
- Fortalecer la gestión de los procesos asistenciales y administrativos en pro de la mejora continua de la institución.

[4] Modelo tomado: http://www.hospitalsanvicente.gov.co/index.php/explore/quienes-somos/mision-vision

- Implementar Estrategias de Intervención a los Servidores Públicos y Colaboradores de la ESE en el Marco de Fortalecer sus Competencias con el Fin de Crear Valor en los Resultados Individuales.
- Fortalecer la sostenibilidad económica y el crecimiento financiero de la entidad, mediante un modelo de gestión empresarial que maximice las ganancias operacionales y generen una rentabilidad económica y social.
- Mejorar la eficiencia de los recursos tecnológicos existentes en la institución, para que sean el apoyo vital en la toma de decisiones y brinden una ventaja competitiva mediante la generación de valor agregado.[5]

Servicios que ofrece el Hospital

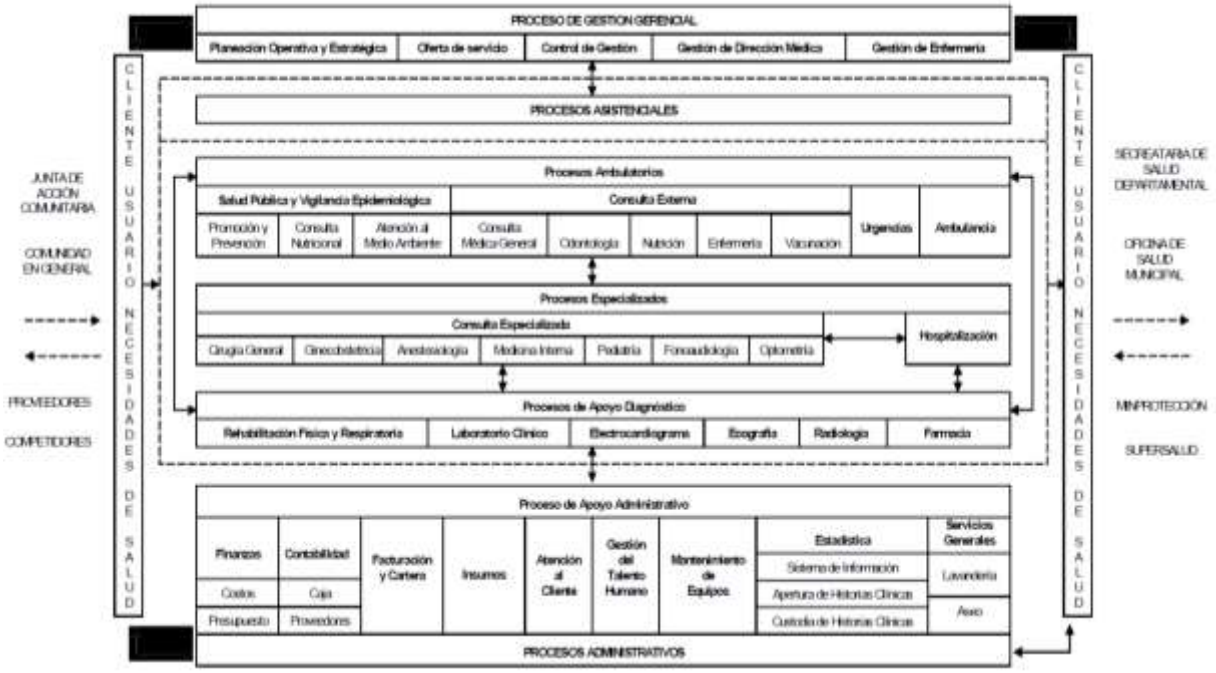
El Hospital cuenta con diferentes especialidades para atención de sus usuarios dentro de las cuales se encuentra:[6]

- Medicina general
- Pediatría
- Anestesiología
- Cardiología
- Cirugía general
- Cirugía maxilofacial
- Cirugía plástica y reparadora
- Dermatología
- Tomografía
- Medicina interna
- Nefrología
- Neumología
- Neurocirugía
- Neurología
- Ginecología
- Oftalmología
- Oncología médica
- Oncología radioterapia
- Otorrinolaringología
- Psiquiatría
- Rehabilitación
- Ortopedia
- Urología
- Psicología
- Ginecología
- Medicina general
- Pediatría
- Anestesiología
- Cardiología
- Cirugía general
- Cirugía maxilofacial
- Nutrición
- Optometría
- Terapia respiratoria
- Periodoncia
- Obstetricia
- Endoscopia
- Mamografía

[5]Modelo tomado: http://www.hospitalsanvicente.gov.co/index.php/explore/quienes-somos/objetivos-institucionales

[6] Modelo tomado:http://www.hospitalsanvicente.gov.co/index.php/content-category-4/206-que-especialidades-ofrece-el-hospital

Mapa de Procesos



FUENTE: Dirección Nacional de Hospitales, Ministerio de Salud

ORGANIGRAMA HOSPITAL

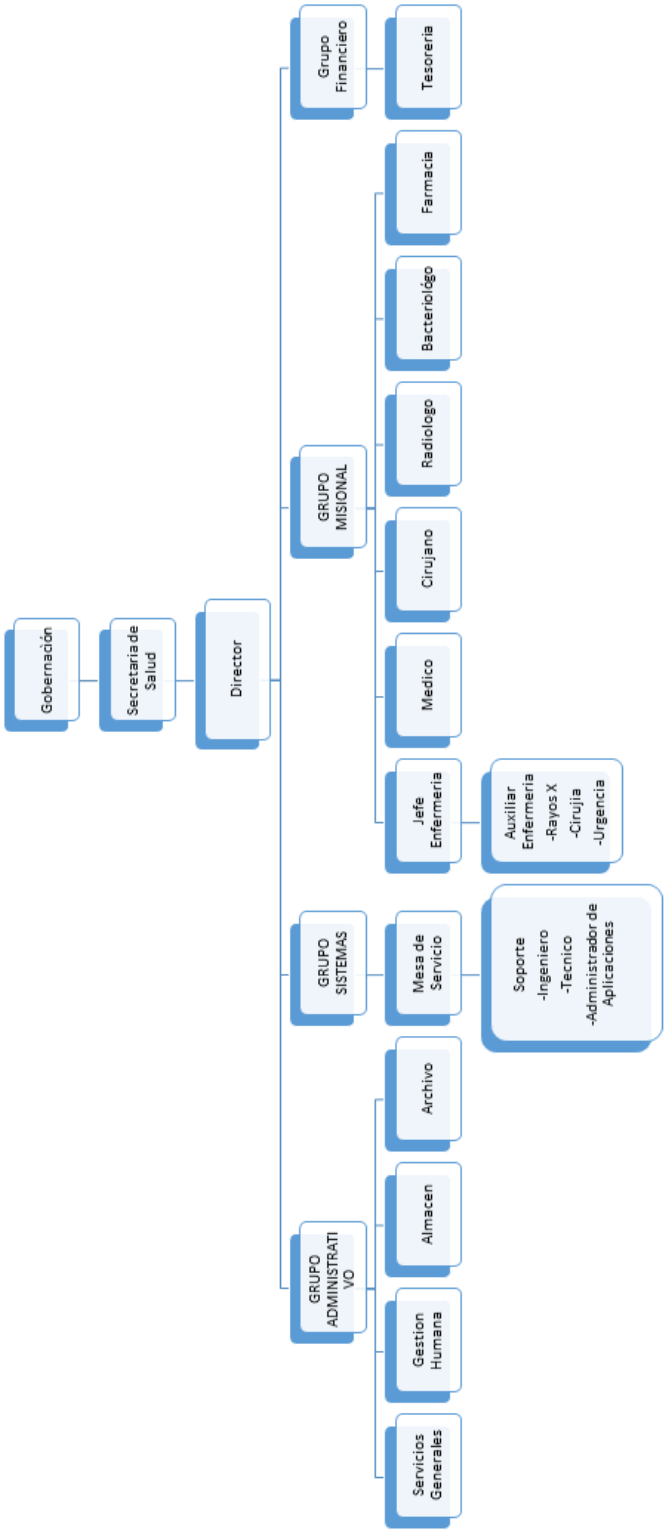


Imagen de Diseño Propio

Conceptos Claves

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

Acuerdo de Confidencialidad: es u documento en los que los funcionarios, contratistas o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información del instituto, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Capacity Planning: es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

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

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

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy

útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

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

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

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

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

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

Guías de clasificación de la información: directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

Hacking ético: es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas

o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencia, el número de veces ocurrido o el origen (interno o externo).

Integridad: es la protección de la exactitud y estado completo de los activos.
Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes al instituto.

ISO/IEC27000: esta norma proporciona una visión general de las normas que componen la serie 27000, indicando parad cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información.

ISO/IEC27001: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.[7]

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de

---

7 https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

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

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

Registros de Auditoría: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos del instituto. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar proteger dichos activos a su cargo.

SGSI: Sistema de Gestión de Seguridad de la Información.

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

Sistemas de control ambiental: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el instituto (amenazas), las cuales se constituyen en fuentes de riesgo.[8]

Identificación de los Actores Relevantes

Directivos: son los encargados de dirigir la prestación del servicio público al gerenciar y administrar la entidad.

Asesor: Asesorar a la Dirección General y a las áreas misionales, en la formulación, diseño, articulación, seguimiento y control de las políticas, lineamientos, planes, programas y proyectos, así como en la definición de políticas de articulación interinstitucional al interior del sector de la Inclusión Social y Reconciliación y con otros sectores, velando porque se cumplan los objetivos y metas establecidos en el plan estratégico de la entidad.

Profesional Especializado: Brindar asistencia profesional o asesoría en el desarrollo y seguimiento de las políticas, programas, proyectos, procesos y procedimientos, velando porque se cumplan los objetivos y misión de la Institución.

Profesional Universitario: Brindar asistencia técnica y profesional en el desarrollo y seguimiento de las políticas, programas, proyectos, procesos y procedimientos, velando porque se cumplan los objetivos y misión de la Institución.

Técnico Administrativo: Dar apoyo técnico en el diseño, aplicación, instalación, actualización y operación de los procesos y procedimientos propios del área, teniendo en

[8] http://mpp.pedagogica.edu.co/download.php?file=seguridad_de_la_informacion.pdf

cuenta necesidades del servicio, normas y lineamientos institucionales, con el fin de contribuir al logro de los objetivos y propósitos institucionales.

Auxiliar Administrativo: Realizar actividades de orden administrativo y operativo que apoyen el desarrollo de funciones y responsabilidades de los niveles superiores en la gestión administrativa de la dependencia, con el fin de contribuir al logro de los objetivos del área y a los propósitos institucionales.

Usuario: Es para quién se crea y diseñan los servicios que se brindan en la entidad.

Tercero: Contratistas y Aliados Estratégicos que no tienen vinculación directa con la compañía, pero que tienen acceso a algunos aplicativos, de acuerdo a su rol o relación con la compañía.

Guardas de Seguridad: Es un profesional de carácter privado que vela por la seguridad, primordialmente en relación a las personas, edificios y bienes materiales de cuya protección, vigilancia y custodia estuviera principalmente encargado por la empresa u organismo contratante como complemento y contribución a la seguridad pública proporcionada por las fuerzas de seguridad del estado.

Personal de Servicios Generales: Las funciones de este puesto se centran en la limpieza diaria y programada de los centros o zonas asignadas a cada trabajador.

Mesa Informática de Soluciones: Es la encargada de recibir los casos que se presentan en la entidad para luego asignarlos a los profesionales encargados de brindar solución.

NORMATIVIDAD

- **Ley Estatutaria 1266 de 2008,** Por la cual se dictan las disposiciones generales de hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [9]
- Ley de Protección de Datos Personales en Colombia
- **Ley 1581 de 2012,** la cual se dictan disposiciones generales para la Protección de Datos Personales.
- **ISO 27001**
- **ISO 31000**

---

[9] http://derechoinformatico.co/centro-de-documentacion/presentaciones/ley-de-proteccion-de-datos-personales-en-colombia/

METODOLOGIA

Para el desarrollo de esta metodología iniciamos realizando una contextualización del entorno de la empresa para poder identificar los activos de información que se gestionan en cada proceso. Posteriormente se identifican los riesgos asociados a la falta de un procedimiento para la gestión y uso de medios removibles como alternativa para almacenar y trasportar dicha información.

Una vez identificado los activos procedemos a realizar el levantamiento de riesgos de la información para esto utilizamos las guías del MINTIC y la ISO 31000 de Gestión de Riesgos, como modelos para establecer un procedimiento de levantamiento de activos y poder identificar su nivel de criticidad según el riesgo que este contenga.

Adicionalmente procedemos a estructurar una política para el uso de medios removibles, según que contendrá los objetivos y procedimientos para el uso correcto de los mismos.

A continuación, se muestra la Guía para identificación de Activos y la Matriz de Riesgos.

Matriz De Impacto

Permite establecer prioridades en cuanto a los posibles riesgos de un proyecto en función tanto de la probabilidad de que ocurran como de las repercusiones que podrían tener sobre el proyecto.

	CATEGORÍA					
Nivel	**Operacional**	**Legal**	**Financiero**	**Tecnológico**	**Imagen**	**Ambiental**
Insignificante	Llamados de atención a nivel grupal.	Sanciones a nivel de grupo.	Pérdidas Económicas menores al 5% del Valor de un día de la Nomina	Daños pequeños de la infraestructura de la entidad, por un valor inferior al 0,3% de los gastos en infraestructura al año	Afectación Imagen grupo a nivel área o proceso.	Producción de RAESS y Basuras 632 kg mensual
Menor	Llamados de atención a nivel Macro-proceso.	Sanciones a nivel Macro-procesos.	Pérdidas Económicas inferiores del 8% del Valor de un día de la Nomina	Daños pequeños de la infraestructura de la entidad, por un valor inferior al 0,5% de los gastos en infraestructura al año	Afectación Imagen grupo o área a nivel del Macro proceso	Producción de RAESS y Basuras entre 632 kg a 790 kg mensual
Moderado	Llamados de atención a nivel Organizacional.	Sanciones a nivel de Oficina Jurídica o Control Interno.	Pérdidas Económicas menores al 10% del Valor de un día de la Nomina	Daños pequeños de la infraestructura de la entidad, por un valor inferior al 0,7% de los gastos en infraestructura al año	Afectación Imagen del proceso o área a Nivel de la Entidad.	Producción de RAESS y Basuras entre 790 kg a 948 kg mensual
Mayor	Llamados de atención a nivel nacional.	Sanciones a nivel de Oficina Jurídica o Control Interno.	Pérdidas Económicas menores al 12% del Valor de un día de la Nomina	Daños pequeños de la infraestructura de la entidad, por un valor inferior al 0,8% de los gastos en infraestructura al año	Afectación Imagen a nivel Nacional	Producción de RAESS y Basuras entre 948 kg a 1106 kg mensual
Catastrófico	Llamados de atención a nivel internacional	Sanciones de la Auditoría General de la República	Pérdidas Económicas menores al 15% del Valor de un día de la Nomina	Daños pequeños de la infraestructura de la entidad, por un valor inferior al 1% de los gastos en infraestructura al año	Afectación Imagen a nivel Internacional.	Producción de RAESS y Basuras superior a 1264 kg mensual

Matriz Identificación De Activos

Esta herramienta permite identificar los activos de información que se pueden ver afectados por el mal uso de los medios removibles.

I. IDENTIFICADOR					
ID	**PROCESO**	**Activo de Información**	**Tipo de Activo**	**Descripción del Activo**	**Contiene Datos Personales**
1	Gestión Hospitalaria	ACTAS COMITÉ DE HISTORIAS CLÍNICAS	Físico/Electrónico	Documento administrativo que muestran decisiones relevantes que guían el destino del Hospital.	NO
2	Gestión Hospitalaria	HISTORIAS CLINICAS	Electrónico	Documento donde se plasma los registros médicos en una forma cronológica, secuencial y coherente.	SI
3	Gestión Hospitalaria	INFORMES Y REPORTES DE EXÁMENES DE APOYO DIAGNÓSTICO: Cardiología-Gastroenterología-Patología-Imagenología-Laboratorio Clínico	Electrónico	Documentos de apoyo del diagnóstico que hacen parte de la HC.	SI
4	Gestión Hospitalaria	SOLICITUD HISTORIAS CLINICAS ENTES JUDICIALES Y OTROS	Físico/Electrónico	Documentos de solicitud de información a la Institución.	SI

II. PROPIEDAD		Valoración de Activo			III. UBICACIÓN	
Custodio del Activo	**Contenedor**	**Legal**	**Financiero**	**Imagen**	**Física**	**Electrónica Información Publicada (WEB)**
Alexander Méndez	Computador del Coordinador de Área	Sanciones a nivel de Oficina Jurídica o Control Interno.	Pérdidas Económicas inferiores del 8% del Valor de un día de la Nomina	Afectación Imagen del proceso o área a Nivel de la Entidad.	Archivo Hospital	Equipo Asistente Dirección
Medico de Turno	Computador de Consultorio	Sanciones a nivel de Oficina Jurídica o Control Interno.	Pérdidas Económicas inferiores del 8% del Valor de un día de la Nomina	Afectación Imagen del proceso o área a Nivel de la Entidad.	N/A	Equipo consultas
Medico de Turno	Computador de Consultorio	Sanciones a nivel de Oficina Jurídica o Control Interno.	Pérdidas Económicas menores al 10% del Valor de un día de la Nomina	Afectación Imagen del proceso o área a Nivel de la Entidad.	N/A	Equipo consultas
Encargado de Gestión Documental	Archivo Hospital / Equipo de funcionario encargado de Gestión Documental	Sanciones a nivel de Oficina Jurídica o Control Interno.	Pérdidas Económicas inferiores del 8% del Valor de un día de la Nomina	Afectación Imagen del proceso o área a Nivel de la Entidad.	Archivo Hospital	Equipos Archivo hospital

Probabilidad de Ocurrencia

Es el nivel de certeza que tenemos de que ocurra un suceso, es la razón entre el número de veces en que ocurrió dicho evento y el número de repeticiones de este en un año.

Probabilidad de Ocurrencia en un año	
Concepto	**Frecuencia**
Casi Certeza	Al menos 2 veces al año
Probable	Al menos de 1 vez en el último año.
Moderado	Al menos de 1 vez en los últimos 2 años.
Improbable	Al menos de 1 vez en los últimos 3 años.
Raro	No se ha presentado en los últimos 5 años.

Matriz impacto - Probabilidad

Permite establecer prioridades en cuanto a los posibles riesgos de un proyecto en función tanto de la probabilidad de que ocurran como de las repercusiones que podrían tener sobre el proyecto.

		IMPACTO				
		INSIGNIFICANTE	**MENOR**	**MODERADO**	**MAYOR**	**CATASTRÓFICO**
PROBABILIDAD	**Raro**	**1 - BAJO**	**2- BAJO**	**3- MODERADO**	**4- ALTO**	**5- ALTO**
	Improbable	**2- BAJO**	**4- BAJO**	**6- MODERADO**	**8- ALTO**	**10- CRITICO**
	Moderado	**3- BAJO**	**6- MODERADO**	**9 - ALTO**	**12- CRITICO**	**15- CRITICO**
	Probable	**4- MODERADO**	**8- ALTO**	**12- ALTO**	**16- CRITICO**	**20- CRITICO**
	Casi Certeza	**5- ALTO**	**10- ALTO**	**15- CRITICO**	**20- CRITICO**	**25- CRITICO**

Tratamiento de Riesgo

Categoría	Descripción
Evitar el Riesgo	Tomar las acciones encaminadas a prevenir su materialización, a través de la formulación de Planes de Mejoramiento de tipo preventivo o la inclusión de acciones en los Planes de acción.
Reducir Riesgo	Tomar acciones para disminuir la probabilidad y el impacto a través de la formulación de Planes de Mejoramiento de tipo preventivo o correctivo y el fortalecimiento o implementación de controles o la inclusión de acciones en los Planes Operativos.
Compartir o Transferir Riesgo	Acciones que reducen el efecto a través del traspaso de las pérdidas a otras organizaciones.
Asumir Riesgo	luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

ZONA DE RIESGO		
Zona	**Leyenda**	**Descripción**
BAJO	**B**	Riesgo BAJO, se puede asumir el riesgo
MODERADO	**M**	Riesgo MODERADO, se debe reducir el riesgo.
ALTO	**A**	Riesgo ALTO, debe ser reducido, compartido o transferido
CRITICO	**C**	Riesgo CRITICO, debe ser reducido, evitado, compartido o transferido

Gráfico de Dispersión

Permite validar los cambios que tienen los riesgos al momento de aplicar los controles que puedan disminuir la probabilidad de ocurrencia del riesgo.

Grafico Dispersión SIN CONTROLES					
Casi Certeza					
Probable					
Moderado		R4		R1 R3	
Improbable			R2		
Raro					
	INSIGNIFICANTE	**MENOR**	**MODERADO**	**MAYOR**	**CATASTRÓFICO**

De los 4 riesgos identificados como se muestra en el grafico de Dispersión dos riesgos están categorizados en critico y los otros dos en riesgo moderado, de esta manera podemos identificar la importancia de los riesgos y su posible impacto.

Grafico Dispersión CON CONTROLES					
Casi Certeza					
Probable					
Moderado					
Improbable		R4	R3		
Raro			R1 R2		
	INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO

De los 4 riesgos identificados, al aplicar los controles podemos apreciar que 3 de los 4 riesgos quedaron en riesgo moderado y uno en riesgo bajo.

Matriz de Riesgos

La **Matriz de Riesgos** es una herramienta de gestión que permite determinar objetivamente cuáles son los **riesgos** relevantes para la seguridad y salud de los trabajadores que enfrenta una organización. Su llenado es simple y requiere del análisis de las tareas que desarrollan los trabajadores.[10]

[10] http://prevencionlaboralrimac.com/Herramientas/Matriz-riesgo

IDENTIFICACION DEL RIESGO								
PROCESO	**ACTIVO DE INFORMACION**	**Descripción del Activo**	**RIESGO**	**Categoría Impacto**	**Descripción Impacto**	**IMPACTO**	**PROBABILIDAD**	**NIVEL**
Gestión Hospitalaria	ACTAS COMITÉ DE HISTORIAS CLÍNICAS	Documento administrativo que muestran decisiones relevantes que guían el destino del Hospital.	R1 Borrado no autorizado de informacion	Operacional	Llamados de atención a nivel nacional.	Moderado	Moderado	9 - ALTO
				Legal	Sanciones a nivel de Oficina Jurídica o Control Interno.			
				Financiero	Pérdidas Económicas menores al 12% del Valor de un día de la Nomina			
				Imagen	Afectación Imagen a nivel Nacional			
				Tecnológico	Daños pequeños de la infraestructura de la entidad, por un valor inferior al 0,3% de los gastos en infraestructura al año			
				Ambiental	Producción de RAESS y Basuras entre 632 kg a 790 kg mensual			

PLAN DE MANEJO - APLICACIÓN DE CONTROLES						EVALUACIÓN RESIDUAL			
CONTROLES	**Categoría Impacto**	**Descripción Impacto**	**IMPACTO**	**PROBABILIDAD**	**NIVEL**	**CATEGORÍA DE TRATAMIENTO**	**RESPONSABLE**	**FECHA DE INICIO**	**FECHA FINALIZACIÓN**
Establecer un política de uso de medios removibles para concientizar a los usuarios, en los lineamientos que se debe tener al momento de almacenar información	Operacional	Llamados de atención a nivel nacional.	Moderado	Raro	3- MODERADO	Reducir Riesgo	Alexander Méndez	11/04/2017	31/12/2017
	Legal	Sanciones a nivel de Oficina Jurídica o Control Interno.							
	Financiero	Pérdidas Económicas menores al 12% del Valor de un día de la Nomina							
	Imagen	Afectación Imagen a nivel Nacional							
	Tecnológico	Daños pequeños de la infraestructura de la entidad, por un valor inferior al 0,3% de los gastos en infraestructura al año							
	Ambiental	Producción de RAESS y Basuras entre 632 kg a 790 kg mensual							

PLAN DE TRABAJO

Acción	Actividades	Responsable	Recursos	Duración en Semanas
Diseñar la política, alcance y objetivos para el uso de dispositivos de almacenamiento removibles.	• Contextualización de la Entidad. • Identificación de documentos. • Revisar los requerimientos de Hospital. • Identificar los objetivos estratégicos. • Identificar los procesos del Hospital.	**Oficina Grupo de Sistemas - Dirección de Tecnología**	**José Gregorio Rodríguez Cristian Rene Jaimes**	**3 semanas**
Diseñar una matriz de riesgos para identificar los riesgos y amenazas asociados al uso de medios removibles.	• Elaboración de matriz de activos de información. • Identificación de activos de información. • Diseño de matriz de riesgos de información asociados al uso de medios removibles. • Establecer metodología para el diligenciamiento de la matriz.			**2 semanas**
Definir el procedimiento de gestión de medios	• Diseñar la guía para el uso de medios de			**2 semanas**

removibles, con el fin de garantizar que la información se salvaguarde adecuadamente según está estipulado en el procedimiento.	almacenamiento removibles.			
Diseñar un plan de trabajo de campañas de concientización para disminuir los riesgos asociados a la perdida de la confidencialidad, disponibilidad e integridad de la información, que se presenta por la manipulación inadecuada de medios removibles.	• Se identificaron los procesos críticos del hospital. • Se diseñaron presentaciones sobre el uso de medios removibles. • Se elaboró un plan de acción para sensibilizar a los funcionar del hospital.			**1 semana**

RESULTADOS Y DISCUSIÓN
ENTREGABLES DESCRIPCIÓN

Los entregables para el desarrollo de este proyecto serán cuatro documentos que se describen a continuación:

- **Política de uso de medios removibles. ANEXO 1. Y ANEXO 1.1**

Esta política es un medio por el cual le comunicamos de manera formal a los usuarios y a los directivos, las normas y procedimientos que rigen el uso de los medios removibles en la entidad.

En ella se busca orientar las decisiones que se toman en relación al uso de los medios removibles, por lo tanto se requiere un compromiso por parte de los miembros del Hospital para lograr una visión conjunta y de esta manera cumplir con los objetivos estratégicos de la entidad hospitalaria.

En la política de gestión de medios removibles se consideraron los siguientes aspectos:

- Alcance incluyendo factores tecnológicos y del personal que labora en esta entidad.
- Objetivos acordes a la visión estratégica de la entidad.
- Responsabilidades por cada uno de los servicios, recursos informáticos y responsabilidades del personal.
- Dediciones de riegos, impacto y consecuencias asociados al no cumplimiento de la política de gestión de medios removibles.

La política de gestión de medios removibles como un documento dinámico de la entidad, debe seguir un proceso de actualización periódica dada la naturaleza cambiante de los riegos de la información.

- **Matriz de riesgos. ANEXO 2. Y ANEXO 2.1**.

Es una herramienta para identificar los riesgos inherentes a la gestione de dispositivos removibles y recursos informáticas de una entidad, teniendo en cuanta el uso, trasporte y tratamiento de la información contenida en el dispositivo., es un instrumento que permite mejorar el control de riesgos y la seguridad de la información de la entidad Hospital.
En la matriz de gestión de riegos de medios removibles se consideraron los siguientes aspectos:

- Definición de los criterios a partir de los cuales se admitirán riesgos.
- Establecer los riegos inherentes al uso de los medios removibles y el tratamiento de la información contenida en el dispositivo.

- Monitoreo y medición de todas las categorías de impacto que pueden que se puedan generar por la manifestación de un riego de la información asociado a la gestión de medios removibles.
- Diseñar mecanismos de control que permitan mitigar, evitar, trasferir o asumir un riego de la información.

Con la matriz de riesgos se busca la identificación de los activos de información con relevancia para la gestión de los procesos de la entidad con el fin de identificar los riegos inherentes a estos activos y de esta manera prever los posibles incidentes o factores que intervienen en su manifestación y grado de afectación a la entidad.

- **Procedimiento de uso de medios removibles. ANEXO 3.**

Es un procedimiento que suministra los pasos que deben seguir los funcionarios y colaboradores del hospital para el uso de medios removibles, para esto inicialmente se debe socializar que son medios removibles para que posteriormente los funcionarios gestionen las solicitudes de permisos e usos ante el departamento de sistemas para que estos definan si es procedente o no dar los permisos de uso.

Este documento establece la normatividad para el uso adecuado de los medios removibles en la red de área local de la entidad, es de suma importancia que tanto los directivos como el personal que uso de estos dispositivos sigan a cabalidad lo que este documento estipula con el fin de salvaguardar la integridad, disponibilidad y confidencialidad de la información contenida en el medio removible.

Por medio del manual de uso de medios removibles se establecen los siguientes pasos a seguir en la gestión de estos dispositivos:

- Informar sobre la política de gestión de medios removibles del Hospital
- Aceptar la puesta en marcha de la política de uso de medios removibles.
- Establece la normatividad para realizar solicitud de la autorización asignación del medio removible.
- Reglamenta los procedimientos para la asignación y alta de los medios removibles.
- Permite documentar los procedimientos realizados con el fin identificar los hallazgos y llevar un control de las operaciones realizadas.

Con el manual de uso de los medios removibles se busca tener un documento de referencia que le permita tanto a usuarios como la personal de sistemas y tecnología esclarecer los procedimientos para la gestión y uso de los medios removibles.

- **Plan de sensibilización a los funcionarios del hospital. ANEXO 4.**

Para la construcción de este plan de sensibilización el grupo de trabajo se basó en las necesidades por concientizar a los funcionarios en el uso adecuado de medios removibles, con el fin de mitigar los incidentes de seguridad que se puedan presentar por el uso inadecuado de medios removibles.

Los directivos deben tener en cuenta que un plan de sensibilización de seguridad en la entidad conlleva a que los funcionarios se capaciten y se comprometan a seguir los lineamientos establecidos, para el correcto desarrollo de sus actividades.

En este proceso se realizaron las siguientes etapas para una buena construcción de un plan de trabajo de sensibilización:

- Objetivos del plan de sensibilización.
- Población objeto.
- Actividades a desarrollar.
    - **Realizar concurso Inducción**: Los concursos son una buena actividad para que los funcionarios se interesen más.
    - **Realizar charlas de sensibilización a los funcionarios**: Las charlas refrescan los temas de seguridad de la información a los funcionarios.
    - **Envió de correos o tics Seguros a los funcionarios**: se enviarán correos de forma periódica con el fin de mantener actualizado al personal en temas seguridad de la información a los funcionarios.
- Cronograma de actividades
- Seguimiento del Plan de Trabajo

El desarrollo de este plan de sensibilización permitirá a los funcionarios tener unas nociones de cómo manejar los medios de almacenamiento removibles, para dar cumplimiento a las políticas de la entidad.

CONCLUSIONES

Las pérdidas, robo, y divulgación no autorizada de información gestionada por medio de dispositivo removibles se han convertido en una de las principales causas de pérdida de di imagen y operatividad en el Hospital, razón por la cual debía implementar un procedimiento para la gestión de medios removibles.

Se realizó un análisis del ciclo de vida de la gestión de los medio removibles con el fin de identificar, enumerar y describir las vulnerabilidades que puedan que puedan ser aprovechadas por los atacantes y por los mismos usuarios con el fin de atentar contra la información gestionada en medios removibles del Hospital.

Contar con una buena implementación de políticas de seguridad de la información debe ser un punto clave en toda entidad, puesto que si no es así se puede estar ocasionando grandes perdidas que se pudieron haber prevenido, para ellos se debe tener en cuenta un plan de capacitación ya que es necesario generar conciencia en los usuarios sobre la importancia de la seguridad de la información para la entidad.

Hoy en día casi todas las personas que hacemos uso de estaciones de trabajo poseemos además un dispositivo removible con el cual trasportamos y gestionamos información y con el ritmo de vida que llevamos muchas veces no acatamos los controles mínimos para salvaguardar y proteger la información. Por tal razón en las organizaciones se deben implementar procedimientos que garanticen la adecuada gestión de los medios removibles.

Los dispositivos de almacenamiento removibles que se conectan a través del puerto USB constituyen uno de los mayores focos de propagación/infección de códigos maliciosos. Por lo tanto, es necesario tener establecidos ciertos controles y procedimientos que limiten el uso de estos puertos solo a los medios autorizados por la entidad y para los usuarios que igualmente posean autorización para el uso de los mismos.

BIBLIOGRAFIA

[1] Derecho Informático [En Linea]
http://derechoinformatico.co/centro-de-documentacion/presentaciones/ley-de-proteccion-de-datos-personales-en-colombia/
[2] Seguridad de la Información [En Linea]
http://mpp.pedagogica.edu.co/download.php?file=seguridad_de_la_informacion.pdf
[3] Matriz Riesgos de Prevención [En Linea]
http://prevencionlaboralrimac.com/Herramientas/Matriz-riesgo
[4] Manual de Seguridad [En Linea]
https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf
[5] Hospital [En Linea]
www.hospitalsanvicente.gov.co/index.php/component/phocadownload/category/57-proceso-de-empalme-2012-2015%3Fdownload%3D132:informe-de-empalme-01+&cd=2&hl=es-419&ct=clnk&gl=co
[6] Hospital Misión [En Linea]
http://www.hospitalsanvicente.gov.co/index.php/explore/quienes-somos/mision-vision/94-institucional
[7] Hospital Procesos [En Linea]
http://www.hospitalsanvicente.gov.co/index.php/component/phocadownload/category/57-proceso-de-empalme-2012-2015?download=132:informe-de-empalme-01