PLAN INSTITUCIONAL:

SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2024

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital en el Hospital Mental de Antioquia – María Upegui, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo en la entidad, de manera que, al comprender el concepto de riesgo, así como el contexto, a través de este instrumento se planean las acciones que reduzcan la afectación a la entidad en caso de materialización de estos, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el mundo en el Entorno Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos del estándar ISO 27001:2013, alineado con ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el Departamento Administrativo de la Función Pública y aquellas que él Hospital defina.

2. JUSTIFICACIÓN

Para el HOMO la información es un activo muy importante y de alto valor que determina el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad, disponibilidad en el ciclo de vida de la información.

El plan de Seguridad y Privacidad de la Información comprende todas aquellas actividades que contribuyen a la protección de la información, entre estas: Definición del Alcance, Identificación de procesos y servicios. Identificación de Activo.

Mediante la definición del Plan el HOSPITAL MENTAL DE ANTIOQUIA – MARIA UPEGUI se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad, Perdida de Integridad y Perdida de Disponibilidad), en la información digital, evitando aquellas situaciones que impidan el logro Estratégicos del Hospital El Plan de Seguridad y privacidad de la información se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes en los activos de información del Hospital, estas acciones son organizadas en forma de medias de seguridad denominados controles, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

Las anteriores medidas se definen teniendo en cuenta la información del análisis de riesgos, sobre la plataforma informática y las necesidades del Proceso de Gestión de la Infraestructura de TIC del Hospital, en cuanto a la seguridad de la información y proporciona las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

3. OBJETIVO

Definir e implementar un Plan de Seguridad y Privacidad de la Información para la ESE HOMO, donde se adopten marcos de trabajo para la gestión y gobierno de T I, donde estén claramente definidas las actividades a desarrollar para llevar a cabo los lineamientos de seguridad y privacidad de la información, y políticas de seguridad que se tienen establecidos en la Entidad. Deben definirse los planes de continuidad y de recuperación, estos deben contener el cronograma de actividades, con sus responsables, las metas, fechas propuestas de realización.

Específicos

- ✓ Contar con lineamientos frente a la seguridad y privacidad de la información que se genera en los diferentes procesos de la Entidad, como son: La gestión de activos, el uso aceptable de los activos, acceso a intenet, correo electrónico, recursos tecnológicos como software y hardware, acuerdos sobre la confidencialidad, la clasificación de la información, la seguridad de los recursos humanos, roles y responsabilidades, educación y concientización sobre la Seguridad de la Información, controles de acceso, protección contra la perdida de datos, desarrollo de software seguro, entre otros.
- ✓ Tener un Gobierno de Seguridad adecuado representado por una estructura organizacional definida y aprobada por la Entidad, que permitirá la correcta toma de decisiones y ofrecerá una alineación y rumbo adecuado en las actividades para proteger los activos de información.
- ✓ Contar con un Oficial de Seguridad - CISO (Chief Information Security Officer), quien será el encargado de proteger la información de la Entidad.
- ✓ Contar con un plan de contingencia que le permita al equipo de T I y a los funcionarios de le Entidad, tener mayor probabilidad de poder reaccionar de manera organizada y en un tiempo menor a situaciones no planificadas,

debido a que se cuenta con una serie de pautas a realizar ante diferentes situaciones que puedan ocurrir.

- ✓ Contar con un plan de continuidad y de recuperación del negocio.
- ✓ Determinar los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, como pueden ser durante una crisis o desastre.
- ✓ Disminuir la probabilidad de ocurrencia e impacto de los incidentes de Seguridad y Privacidad de la Información de forma efectiva.
- ✓ Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, y privacidad de la información de la ESE Hospital Mental de Antioquia HOMO.
- ✓ Asegurar y hacer uso eficiente y seguro de los recursos de Tecnologías de Información y Comunicaciones, así como aquellos equipos biomédicos que almacena información referente a los servicios prestados, con el fin de garantizar la continuidad de la prestación de los servicios.
- ✓ Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la Información, Seguridad Digital y protección de la información personal.
- ✓ Minimizar el riesgo de vulnerabilidad de la información en el desarrollo de los procesos.
- ✓ Mantener la confianza de sus clientes internos y externos.
- ✓ Asegurar la continuidad de funcionamiento de la plataforma informática
- ✓ Cumplir con la legislación nacional e institucional sobre seguridad de la información
- ✓ Garantizar la disponibilidad de la información para la eficiente toma de decisiones.
- ✓ Fortalecer la cultura de la seguridad de la información a nivel de clientes internos y externos.
- ✓ Proteger los activos tecnológicos y apoyar su desarrollo.

4. MARCO NORMATIVO

Norma	Detalle
Constitución Política de Colombia 1994 art 15	Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
PETI institucional	Plan estratégico de tecnología de la información PETI HOMO 2021-2024
Plan de desarrollo	En el Plan de desarrollo 2021 2024 aprobado por la Junta Directiva, se definió en una de las líneas estratégicas 2 crecimiento y sostenibilidad financiera, 2.2 infraestructura y equipamiento, 2.2.4 “Renovación y actualización de la Tecnología de la información y comunicación”.
Decreto 612 del 4 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 de 14 de junio de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Resolución 0093 de 11	Por la cual se delegan unas funciones, se conforman unos comités y se dictan otras disposiciones. Título XI – Capítulos Segundo y Tercero
Resolución 500 de marzo 10 de 2021	por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Constitución Política de Colombia 1991	Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
Norma Técnica Colombiana NTC/ISO 27001:2013	Sistemas de Gestión de la Seguridad de la Información.
Modelo de Seguridad y Privacidad de la Información	Ministerio de Tecnologías y Sistemas de Información.

Dentro del contexto organizacional requerido para el desarrollo del PETI en la E.S.E HOMO, como una entidad que administra recursos de interés público es fundamental tener en cuenta la normatividad vigente que define el objetivo misional de las entidades, sus responsabilidades y el desarrollo de algunas de las funciones requeridas para apoyar el cumplimiento de dicho objetivo misional.

Ley 1266 de 2008	"Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países
Ley 1581 de 2012.	"Por la cual se dictan disposiciones generales para la Protección de Datos Personales"
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las Comunicaciones, entre otras disposiciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

5. DEFINICIONES

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de una no conformidad, de tal forma que no se vuelva a repetir.

Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

Aceptación del riesgo: Después de revisar las consecuencias que puede acarrear un riesgo, se toma la decisión de asumirlo.

Activo: Se entiende información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de la Entidad. Se pueden clasificar de la siguiente manera:

- ✓ **Datos**: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Entidad.
- ✓ **Aplicaciones**: Es todo el software que se utiliza para la gestión de la Información del HOMO, ejemplo SXG5 ADVANCED, SAIA.

- ✓ **Personal**: Es todo el personal de la Entidad, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que interactúen de una manera u otra con los activos de información de la Entidad.
- ✓ **Servicios**: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.
- ✓ **Tecnología**: Son todos los equipos utilizados para gestionar la Información y las comunicaciones
- ✓ **Instalaciones**: Son todos los lugares espaciales donde se alojan los Sistemas De Información.

Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad

Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

- Detectar cualquier alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

APT: (Advance Persistent Threat) Amenaza Avanzada Persistente Especie ciberataque que es responsable del lanzamiento de ataques de precisión y tienen como objetivo comprometer una máquina en donde haya algún tipo de información valiosa.

Alcance: Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información – SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si solo incluye una parte de la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Almacenamiento en la nube: Del inglés Cloud Storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar

de Internet. Esos lugares son ubicaciones remotas cuya finalidad es ofrecer seguridad a la información o procesos allí alojados.

Amenaza: Según ISO 13335-1:2004; causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o a la organización.

Análisis de riesgos: A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

Base de datos de gestión de configuraciones (CMDB, Configuration Management Database): Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de T.I y las relaciones entre componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un (CI) puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.

BS7799: Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información – no es certificable- y la parte

segunda especifica el sistema de gestión de seguridad de la información – es certificable- Asimismo la parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001. – como tal el estándar, ha sido derogado ya, por la aparición de estos últimos.

Características de la información: Las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

Cheklist: Lista de apoyo para el auditor con los puntos a auditor, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

CobiT – Control Objectives for information and related technology: (Objetivos de Control para la información y tecnologías relacionadas): Publicados y mantenidos por ISACA, sus siglas en inglés (Information System Audit and Control association) Asociación de auditoría y control de tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Compromiso de la dirección: Alineamiento firme de la dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Cómputo forense: El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, de otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes esté autorizados, según ISO 1335-1:2004, característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: Control que reduce la posibilidad de materialización de una amenaza, ejemplo por medio de avisos disuasorios.

Control preventivo: control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Directiva: según ISO 13335-1:2004: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: según ISO 13335-1:2004: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según ISO guía 73:2002: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: según ISO 18044:2004: suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos, relacionados con la confidencialidad, integridad o disponibilidad de una proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

FTP: (File transfer protocol) Es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos en él.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gusano: (Worm): es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo excesivo de ancho de banda del canal de internet y su gran facilidad de mutar.

Impacto: resultado de un incidente de seguridad de la información.

Incidente: Según ISO 18044:2004: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónica, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Ingeniería social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten Información con clasificaciones confidencial o superior.

En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos

electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

IPS: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

ITIL IT INFRAESTRUCTURE LIBRARY: Un marco de gestión de los servicios de tecnologías de la información.

KEYLOGGERS: Software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este término con malware del tipo Daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

Legalidad: El principio de legalidad o primacía de la ley es un principio fundamental del derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al imperio de la ley) . Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, seguridad de información, seguridad informática y garantía de la información.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PDCA - PLAN DO CHECK ACT: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (Implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

PHISHING: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

Plan de continuidad del negocio (BUSSINES CONTINUITY PLAN): Plan orientado a permitir la continuación de las principales funcionales de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (RISK TREATMENT PLAN): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad y privacidad de la información: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Punto único de contacto (PUC): Entiéndase como mesa de ayuda de acuerdo a las mejores prácticas basadas en ITIL.

Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de acceso y escucharla.

RANSOMWARE: Código malicioso para secuestrar datos, una forma de explotación en el cual el atacante encripta o codifica los datos de la víctima y exige un pago por la clave de descifrado.

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o negligencia.

Seguridad de la información: Según ISO 27002:20005: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Servicio de tratamiento de información: Según ISO 270002:2013: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

SPAMMING: Se llama spam, correo basura o SMS basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviado en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

SNIFFERS: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también se usa con fines maliciosos.

SPOOFING: falsificación de la identidad origen en una sesión la identidad es por una dirección IP o MAC Address.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad de los equipos de cómputo.

Usuario: En el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de la E.S.E Hospital Mental de Antioquia, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red del HOMO y a quienes se les otorga un nombre de usuario y una clave de acceso.

Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

VPN: (Virtual Prívate Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

6. METODOLOGÍA Y RECURSOS FISICOS, HUMANOS Y ECONOMICOS

METODOLOGIA

Para la vigencia 2024 continúan las siguientes actividades para Seguridad y Privacidad de Información, las cuales se encuentran enmarcadas en la Estrategia 2 del Plan de Acción de la oficina de sistemas de información.

La planificación e implementación de la Seguridad y Privacidad de la Información, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad. El Modelo de Seguridad y Privacidad de la Información, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información, los cuales, a lo largo de los últimos años, han sido utilizados por las diferentes entidades tanto del orden nacional como territorial, para mejorar sus estándares de seguridad de la información. El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; así mismo recoge además de los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública.

ITEMS QUE AFECTAN LA INTEGRIDAD DE LOS DATOS

- **Problemas de comunicación del cliente con el servidor, problemas en el cableado eléctrico de las estaciones de trabajo, problemas con los recursos compartidos de la red y la caída de las bases de datos**: Ocasionarían pérdidas totales o parciales, por lo tanto, se produce una interrupción en las actividades, hasta solucionar el problema.

- **Caída temporal del o los servidores/es por falla técnica**: Ocasionarían pérdidas totales o parciales, por lo tanto, se produce una interrupción en las actividades, hasta solucionar el problema. Evaluar costo de reparación del desperfecto técnico.

- **Pérdida total del servidor**: Ocasionaría pérdidas totales o parciales, por lo tanto, hay una interrupción en las actividades, hasta solucionar el problema, además evaluar costo de reparación o de reposición.

- **Falla total o parcial del cableado**: Ocasionaría pérdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema.

- **Pérdida total o parcial de las estaciones de trabajo**: Ocasionaría pérdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema, en caso de pérdida total, evaluar costos.

- **Pérdida total o parcial de conexión a internet**: Ocasionaría pérdidas parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema con el acceso al internet en forma inalámbrica o por módems de otro prestador de servicios de internet.

Lo que incluye el comité de seguridad y privacidad de la información y sus funciones:

- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información SGSI de la ESE HOMO.
- Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SCSI de la ESE HOMO.
- Supervisar la integración del Sistema de Gestión de Seguridad de la Información - SGSI con el Sistema Integrado de Gestión- SIGC de la ESE HOMO.
- Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información para la ESE HOMO.
- Adoptar las medidas y acciones a que haya lugar, de conformidad con los resultados de los diagnósticos del estado de la seguridad de la información para LA ESE HOMO, con el fin de tomar y establecer las medidas necesarias.
- Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual que puedan generar pérdidas patrimoniales o afectar los recursos de información de la entidad.
- Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información.
- Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.
- Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello.
- Evaluar los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información.

- Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información.
- Las demás funciones inherentes a la naturaleza del Comité.

Tener en cuenta las estrategias y actividades de las siguientes fases:

Fase de diagnóstico:

- Controles de seguridad establecidos para protección de la información y su nivel de madurez.
- Cumplimiento de la legislación de Habeas Data.
- Identificar posibles buenas prácticas tecnológicas y de sistemas para a protección y seguridad de la información.

Fase de planificación:

- Establecer necesidades y expectativas de las partes interesadas con respecto a los controles para la seguridad y privacidad de la información.
- Liderazgo.
- Identificar riesgos relacionados con la seguridad y privacidad de la información.
- Asignación de Recursos.
- Documentar todos los procedimientos y controles para garantizar la seguridad y privacidad de la información.
- Inventario de activos de la información.

Fase de implementación:

- Control operacional frente a los riesgos.
- Indicadores de gestión.

Fase de evaluación de desempeño:

- Revisión y seguimiento a la implementación.
- Plan de ejecución de auditorías.

RECURSOS HUMANOS FINANCIEROS

La administración y operación de los sistemas para la seguridad de la información de nuestro sistema actual debe ser siempre una de las prioridades en cada uno de los centros hospitalarios, clínicas y todo tipo de instituciones públicas o privadas que esta es una operación que debe ser ejecutada por personal capacitado y con las competencias

necesarias para la manipulación de estos equipos, por lo general, técnicos, tecnólogos o ingenieros del área para que estos planes de seguridad y privacidad de la información sean operativos y seguros con las herramientas que tenemos actualmente. Sin embargo, cabe aclarar que en este campo la experiencia también es un factor determinante que juega a favor de aquellos que llevan más tiempo desempeñando esta labor, y en algunos casos, esta misma experiencia les ha permitido desarrollar ajustes o avances para el mejoramiento del funcionamiento de estas herramientas de seguridad y privacidad de la información.

Por lo tanto, como recurso humano para el desarrollo de este Plan se Requiere:

1. Un ingeniero de telecomunicaciones directamente contratado por el hospital, que pueda gestionar toda la parte administrativa que conlleva el subproceso y al mismo tiempo que pueda sustentar las auditorias que se presenten, además del soporte y apoyo al área de telemedicina y otros servicios que estén relacionados con estos servicios en representación directa de la E.S.E. HOSPITAL MENTAL DE ANTIOQUIA MARIA UPEGUI HOMO.

2. Un ingeniero de sistemas o afines directamente contratado por el hospital o contratista por prestación de servicios, que pueda gestionar toda la parte administrativa que conlleva el subproceso y al mismo tiempo que pueda sustentar las auditorias que se presenten, además del soporte o apoyo al área de tecnología en centro de datos, servidores, equipos de cómputo, otros dispositivos y servicios que necesita este área para su operación en representación directa de la E.S.E. HOSPITAL MENTAL DE ANTIOQUIA MARIA UPEGUI HOMO.

3. Un técnico, tecnólogo o ingeniero de sistemas o afines directamente contratado por el hospital o contratista por prestación de servicios, que pueda gestionar el sistema de información actual que tiene la empresa con la versión SXG5 Advacend de la empresa XENCO sobre motor de bases de datos ORACLE aplicación cliente servidor y otras funciones de apoyo al área de sistemas que necesita esta área para su operación en representación directa de la E.S.E. HOSPITAL MENTAL DE ANTIOQUIA MARIA UPEGUI HOMO.

4. Dos técnicos o tecnólogos directamente contratados por el hospital, contratistas de prestación de servicios o por cooperativa, para el servicio de mantenimiento y soporte a la infraestructura de sistemas y comunicaciones, para todas las actividades técnico operativas y apoyo a la gestión correspondiente a la ejecución de los mantenimientos predictivos, preventivos y correctivos programados y no programados que se puedan presentar con los sistemas de información actual más el soporte a los usuarios finales en

representación directa de la E.S.E. HOSPITAL MENTAL DE ANTIOQUIA MARIA UPEGUI HOMO.

5. Un contratista técnico, tecnólogo en mantenimiento, para todas las actividades técnico operativas y apoyo a la gestión correspondientes la ejecución de los mantenimientos predictivos, preventivos y correctivos programados y no programados que se puedan presentar con la infraestructura de datos, comunicaciones, potencia, regulada, sistema de seguridad de cámaras y otros dispositivos para los sistemas de información en representación directa de la E.S.E. HOSPITAL MENTAL DE ANTIOQUIA MARIA UPEGUI HOMO.

PRESUPUESTO:

<table>
<tr><th colspan="2">PLAZO CONTRACTUAL</th></tr>
<tr><td colspan="2">El plazo contractual se estima en doce (12) meses, contados a partir del primero (01) de enero de 2024 hasta el Treinta y uno (31) de diciembre de 2024, previo el cumplimiento de las obligaciones de expedición de pólizas o garantías a que haya lugar.</td></tr>
<tr><th colspan="2">LUGAR DE EJECUCIÓN</th></tr>
<tr><th colspan="2">VALOR ESTIMADO Y JUSTIFICACIÓN</th></tr>
<tr><td>Rubro y disponibilidad presupuestal; con un valor de OCHO CIENTOS NOVENTA Y CUATRO MILLONES TRECIENTOS SESENTA Y TRES MIL SETECIENTOS TREINTA Y TRES PESOS M/L ($894.363.733).</td><td>Rubro: Servicios de tecnología de la información (TI) de consultoría y de apoyo Según certificado de Disponibilidad Presupuestal expedido por la técnica administrativa</td></tr>
<tr><td colspan="2">El presente presupuesto ha sido estimado de acuerdo con:</td></tr>
</table>

DETALLE	VALOR
Nómina de 5 personas (Personal de departamento TI proyectado y actual. (esta mano de obra es total del servicio para todos los planes).	$300.000.000 (Aprox.)
AZURE – Nube y correos	$85.000.000 (Aprox.)

Antivirus Secure actual está vigente.	$16.000.000 (Aprox.)
Endian Firewall	$0
Microtick y UTM Fisicos (Administraciónde dispositivos)	$45.000.000 (Aprox.)
TOTAL:	**$446.000.000 (Aprox.)**

MODALIDAD DE SELECCIÓN		
El proceso de selección que debe ser utilizado para suplir las necesidades que le asisten a esta entidad hospitalaria y contenidas en el presente estudio previo es:		
Contratación Directa o Privada	Contratación con una sola oferta	**X**
	Contratación con tres ofertas	
Convocatoria Pública		
El objeto de lo contratado se prestará en las instalaciones de la ESE Hospital Mental de Antioquia del municipio de Bello, calle 38 No. 55-310. Y donde por necesidades del servicio el Hospital necesite prestar algún servicio extramural, siempre y cuando sea afín a su Misión.		

7. ACTIVIDADES (CRONOGRAMA)

ACTIVIDAD N°	ACTIVIDADES/ ACCIONES A DESARROLLAR	PRODUCTO O EVIDENCIA	AREA RESPONSABLE	FECHA DE ENTREGA											
				Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
1.	Definir el marco de seguridad y privacidad de la información	Archivo en formato Excel - Definir las actividades a desarrollar de seguridad y privacidad y de mitigación del riesgo de Seguridad de la Información, en el marco de SGSI de la Entidad.	Ingeniero de Sistemas o Telecomunicaciones			X			X			X			X
2.	Ejecutar las actividades del plan de aplicación y mejoramiento del Sistema de Gestión de seguridad de la Información - SGSI.	Archivo en formato Excel - Ejecutar las actividades que hacen parte del plan de aplicación y mejoramiento del Sistema de Gestión de Seguridad de la Información – SGSI	Ingeniero de Sistemas o Telecomunicaciones			X			X			X			X
3.	Aplicar y mejorar la seguridad y privacidad de la información en el marco de SGSI de la Entidad.	Archivo en formato Excel - Se realizarán las actividades para el seguimiento que permitan la medición, análisis y evaluación del desempeño de la seguridad y privacidad de la información, con	Ingeniero de Sistemas o Telecomunicaciones			X			X			X			X

		el fin de generar los ajustes o cambios que se requieran pertinentes y oportunos.													
4.	Realizar un análisis de riesgos, que dé respuesta a los riesgos a los que están expuestos los sistemas de información en la ESE HOMO, tomado como base la guía de gestión de riesgos de MINTIC, la norma NTC ISO 27001, seleccionando los controles que esta norma propone y la norma NT C-ISO/IEC 27005	Documentos de evidencia de realización del análisis.	Ingeniero de Sistemas o Telecomunicaciones				X				X			X	
5.	Establecer el Modelo de Privacidad y Seguridad de la Información – MSPI, donde se cuenta con un documento con la política de la protección y privacidad de la información, conforme a lo establece MINT IC.	Documento de modelo de privacidad de la información o actualizar de acuerdo al documento vigente de la ESE	Ingeniero de Sistemas o Telecomunicaciones					X							
6.	Documentar el Plan de Contingencia de Sistemas de Información, donde se establezcan las acciones a seguir en la ESE HOMO	Documento o actualización del plan de contingencia actual da entidad – revisión del documento o actualización.	Ingeniero de Sistemas o Telecomunicaciones				X				X				

	ante la posible pérdida de información, destrucción, robo y otras amenazas, que presenten los equipos de cómputo, la red o el sistema de información.														
7.	Definir planes de gestión de continuidad del negocio, de acuerdo con lo que establece la norma técnica NT C/ISO 27001 y los controles establecidos en el anexo técnico de la norma NT C/ISO 27002.	Documento de planes de gestión de la continuidad del negocio. – revisión si el documento se aprueba.	Ingeniero de Sistemas o Telecomunicaciones							X					X
8.	Gestionar la adquisición de herramientas para soportar la infraestructura del Datacenter en esquemas de alta disponibilidad para dispositivos de seguridad	Herramienta o evidencias de gestión de adquisición de programas o hardware. – Un seguimiento si se implementa.	Ingeniero de Sistemas o Telecomunicaciones						X					X	
9.	Adquisición de Software o servicio de análisis de vulnerabilidades y hacking Ético.	Licencia, herramienta o gestión de adquision de software para análisis de vulnerabilidades.	Ingeniero de Sistemas o Telecomunicaciones			X									
10.	Desarrollar el programa de capacitación y sensibilización en seguridad de la información para empleados, contratistas proveedores y	Documento y cronograma para sensibilización de la seguridad. Y desarrollar el cronograma.	Ingeniero de Sistemas o Telecomunicaciones			X			X			X			X

	terceros.														
11.	Gestionar una solución de DLP (Data Loss Prevention) para el correo Electrónico y equipos críticos	Herramienta o licencia, o gestión de adquision de DLP. – Y un seguimiento si se implementa.	Ingeniero de Sistemas o Telecomunicaciones			X							X		

8. DIFUSIÓN

Mecanismo de elaboración	La metodología utilizada para la realización fue basada con la normatividad vigente, adaptándola a la E.S.E. Hospital Mental de Antioquia María Upegui – HOMO.
Mecanismo de difusión	El Plan será dado a conocer a los líderes involucrados, estos a su a vez lo darán a conocer a sus colaboradores; posteriormente se montará en la página web institucional para la consulta del público en general.
Mecanismos de capacitación	Se socializara de forma verbal por parte del líder o responsable de ejecución del plan con su equipo de trabajo y las partes interesadas.
Mecanismos de evaluación	Será evaluado y monitoreado por medio de un seguimiento según el cronograma de ejecución de cada actividad, y será la oficina de Planeación quien lo realice.
Mecanismos de retroalimentación	Se hará un acompañamiento constante a las áreas que intervengan en cada plan, para que las mismas entreguen oportunamente y con claridad el desarrollo de las actividades programadas.

9. SEGUIMIENTO

Desde el área de planeación se realiza seguimiento de forma mensual y se lleva indicador de resultado de forma trimestral en el comité de gestión y desempeño.

Indicador de seguimiento:

Número de actividades ejecutadas en el período / Número de actividades programadas en el plan durante el periodo.

RANGO		
0 – 60%	Rojo	Baja
61 – 89%	Amarillo	Media
90 – 100%	Verde	Alta

10. NOMBRES DE RESPONSABLE DE DILIGENCIAMIENTO Y EJECUCIÓN DEL PLAN

Nombre	Cargo
Carlos Andres Muñoz Velez	Ingeniero de Sistemas (TI)
Mauricio Pulgarín	Ingeniero de Telecomunicaciones (TI)
Henry Restrepo Molina	Técnico
Edwin Agudelo	Técnico
NorvyYadira Agudelo Zuluaga	Subgerente administrativa y financiera

11. CONTROL DE CAMBIOS

ELABORÓ	Carlos Andrés Muñoz Vélez
ACTUALIZÓ	N/A
APROBÓ	Alberto Aristizabal Ocampo Gerente
VERSIÓN	01
MOTIVO DE ACTUALIZACIÓN	N/A
FECHA DE ACTUALIZACIÓN	02/01/2024