E.S.E. HOSPITAL REGIONAL SUR ORIENTAL

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Carrera 3 Calle 10 Esquina Barrio El Dique. Chinácota – Norte de Santander
Teléfono: +7 5864120 Fax: +7864499 Correo: suroriental@gmail.com www.esesuroriental.gov.co

TABLA DE CONTENDO

1 INTRODUCCIÓN

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

Lo anterior conlleva la necesidad y obligación de mejorar las herramientas de seguridad en la E.S.E. Hospital Regional Sur Oriental a través del El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El presente documento pretende exponer una serie de lineamientos para implementar las mejores prácticas de Seguridad Informática en la E.S.E. Hospital Regional Sur Oriental, con el fin de optimizar la disponibilidad, la integridad, la confidencialidad/privacidad, entre otros principios relevantes, teniendo en cuenta la infraestructura y limitaciones actuales

2 OBJETIVOS

Planificar, orientar y desarrollar los mecanismos necesarios para dotar de disponibilidad, confidencialidad e integridad al conjunto de datos y activos de información de la Entidad.

1.1 OBJETIVOS ESPECÍFICOS

1. Incrementar los niveles de madurez y fortalecer las capacidades en la apropiación de aspectos de seguridad y privacidad de la información.
2. Contar con un modelo de gestión de TI para el Estado, articulado, que incorpore aspectos de seguridad y privacidad de la información.
3. Generar confianza en las entidades y en los ciudadanos respecto al uso y apropiación de TI en el Estado.

3 TÉRMINOS Y DEFINICIONES

Es necesario tener claras ciertas definiciones para el tema a tratar, así:

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

Amenazas Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Adware Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.

Advertencia Mensaje que comunica al usuario que una acción puede ocasionar u ocasionara la pérdida de datos del sistema del usuario.

Alarma Sonido o señal visual que se activa cuando se produce una condición de error.

Alerta Notificación automática de un suceso o un error.

Amenaza Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Antispam Es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Arquitectura de Seguridad Conjunto de principios que describe los servicios de seguridad que debe proporcionar un sistema para ajustarse a las necesidades de sus usuarios, los elementos de sistema necesarios para implementar tales servicios y los niveles de rendimiento que se necesitan en los elementos para hacer frente a las posibles amenazas.

Blacklisting o Lista Negra La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

Bot Un bot es una computadora individual infectada con malware, la cual forma parte de una red de bots (botnet).

Botnet Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección.

Caballo de Troya Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

Exploits o Programas intrusos Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

Firewall Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Grooming Es una nueva forma de acoso y abuso hacia niños y jóvenes que se ha venido popularizando con el auge de las TIC, principalmente los chats y redes sociales. Inicia con una simple conversación virtual, en la que el adulto se hace pasar por otra persona, normalmente, por una de la misma edad de víctima

Gusanos Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, a diferencia de un Virus.

Ingeniería Social Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

Keystroke Logger o Programa de captura de teclado (Keylogger) Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón,

generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Malware El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas.

Pharming Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del re-direccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento.

Phishing Método más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Riesgo El riesgo es el efecto de la incertidumbre sobre los objetivos.

Rootkits Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final.

Spam También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios.

Spyware o Software Espía El software espía consta de un paquete de software que realiza un seguimiento y envía información confidencial o personal a terceros. La información personal es información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no desearía compartir con otras, como detalles bancarios, números de tarjetas de créditos y contraseñas. Terceros puede hacer referencia a sistemas remotos o partes con acceso local.

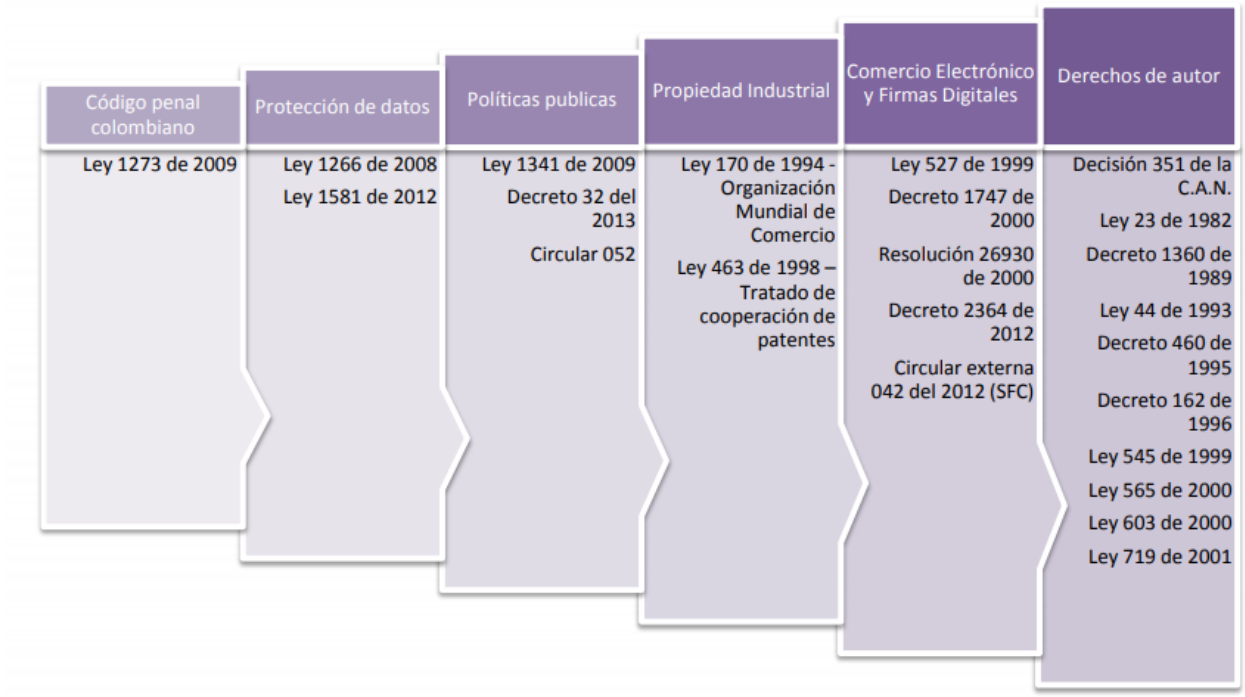
Virus Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

- Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.

- Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Vulnerabilidad Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas

4 NORMATIVIDAD VIGENTE



5 SEGURIDAD DE LA INFORMACIÓN

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

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

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

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411- 1:2006].

6 POLÍTICA DE SEGURIDAD

La E.S.E. Hospital Regional Sur Oriental, entidad del Estado que promueve la salud y previene la enfermedad mediante la prestación de servicios de salud de primer nivel de complejidad, cumpliendo los requisitos legales y organizacionales suscritos frente al Sistema Integrado de Gestión y dando cumplimiento a los lineamientos establecidos por el Gobierno Nacional en materia de Seguridad de la información según el alcance establecido para el Subsistema de Seguridad de la Información y en concordancia a los lineamientos vigentes de la Norma NTC – ISO - IEC 27001, se compromete a:

1. Gestionar los riesgos en seguridad de la información que facilite la identificación, valoración, implementación de controles, monitoreo y seguimiento de los niveles de riesgos.
2. Asegurar la confidencialidad, integridad y disponibilidad de la información, así como la información de terceros en su poder; acorde con el nivel de riesgo aceptado por la Entidad
3. Mantener y evaluar el Subsistema de Seguridad de la Información.

Para lograr lo anteriormente enunciado la Gerencia asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

Las responsabilidades frente a la Seguridad de la Información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas y/o terceros de La E.S.E. Hospital Regional Sur Oriental.

6.1 LINEAMIENTOS GENERALES DE MANEJO DE INFORMACIÓN

6.1.1 Sobre Acceso a la Información

Los propietarios de los activos de información deben establecer medidas de nivel de acceso a nivel de Red, sistema operativo, sistemas de información con el fin de mitigar riesgos asociados al acceso de información de personal no autorizado, salvaguardando la integridad, disponibilidad y confidencialidad de la información de la E.S.E. HRSO.

En el caso de que personas ajenas a la E.S.E Hospital Regional Sur Oriental requieran información específica y confidencial, es exclusivamente el Gerente quien puede y debe autorizar el acceso o entrega de dicha información, previa solicitud formal en donde se describa la información requerida y el uso que le dará a la misma.

6.1.2 Uso de Usuario y contraseñas

Los sistemas de información deberán protegerse por medio de un modelo de claves de acceso que sean seguras y que garanticen un nivel de confiabilidad aceptable para la protección de información de accesos no deseados ni permitidos.

Cada funcionario o contratista deberá tener una clave personal e intransferible de acceso que le permitirá ingresar de forma exclusiva tanto a los sistemas operativos, a las bases de datos y a los aplicativos a los que está autorizado.

Cada funcionario o contratista es responsable del uso de su clave de acceso y es su responsabilidad mantenerla en secreto, ya que cualquier modificación no autorizada de la información, daño o acceso irregular que ocurra y se detecte, es responsabilidad del usuario que maneje la clave y por tanto puede hacerse acreedor a las sanciones de tipo legal y disciplinario que esto conlleve.

Las claves de acceso deben ser cambiada, mínimo cada 3 meses, y en ningún caso debe ser igual a la anterior.

La clave de acceso debe tener una longitud mínima de ocho caracteres, al menos una Letras mayúscula, un número, y un carácter especial. debe ser diferente al nombre del usuario, la fecha de nacimiento o el número de identificación

En caso de que el usuario requiera algún permiso especial o algún cambio en la configuración del perfil de usuario, estos cambios deberán ser solicitados a la Oficina de Sistemas por el gerente, funcionario del nivel directivo o asesor responsable del área o dependencia en donde se solicita el cambio.

6.1.3 Uso de Internet / Intranet de la E.S.E.

El acceso al servicio de Internet/Intranet utilizado por funcionarios, contratistas o practicantes conlleva responsabilidades y compromisos para su uso.

Se espera que los usuarios de este servicio conserven normas de buen uso, confidencialidad y criterio ético. Todos los funcionarios, contratistas y practicantes con autorización al uso y acceso a estos servicios deben:

- Utilizar este servicio exclusivamente para fines laborales.

- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas o practicantes con acceso a este servicio.

- Descargar documentos o archivo tomando las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

- Está Prohibido el envió, descarga y/o visualización de paginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten con la integridad moral de las personas o instituciones.

Si se determina que alguna de las páginas previamente restringidas por el Ingeniero de sistemas es requerida para el desempeño de funciones de algún funcionario, contratista o practicante esta será habilitada únicamente con el consentimiento y solicitud del Gerente.

6.1.4 Uso de dispositivos de almacenamiento externo

La E.S.E es consciente que este tipo de herramientas son muy útiles para el resguardo y transporte de información pero igualmente son elementos que permiten extraer información sin dejar huella física ni registro de dicha acción; Por esta razón define los compromisos frente al uso de Dispositivos de Almacenamiento Externo para asegurarse de que la información propietaria, adquirida o puesta en custodia en la entidad no está supeditada a fuga, uso no autorizado, modificación, divulgación o pérdida y que esta debe ser protegida adecuadamente según su valor, confidencialidad e importancia.

El uso de dispositivos de almacenamiento externo está permitido para los funcionarios, contratistas y practicantes, con el fin de facilitar el compartir y transportar información que no sea de carácter clasificado ni reservado de la Institución dentro de las normas y responsabilidades del manejo de información institucional.

Los dispositivos de almacenamiento de uso externo comprenden las unidades que se pueden conectar como una memoria USB, por medio de un cable de datos, mediante una conexión inalámbrica directa a cualquier equipo de cómputo.

En concordancia con lo anterior, queda RESTRINGIDO el uso de Dispositivos de Almacenamiento Externo, en las siguientes dependencias:

Secretaria General

Servidores

Archivo

Almacén

Tesorería

Contabilidad

Presupuesto.

6.1.5 Gestión de activos de información

La E.S.E. establecerá y divulgará los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información, con el objetivo de garantizar su protección.

- *Inventario de activos de información*: La E.S.E mantendrá un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información, discriminado por IPS y procesos, teniendo en cuenta la Guia para desarrollo de Inventario y clasificación de Activos.

- *Propietarios de los activos de información:* La E.S.E. HRSO es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato. La E.S.E es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).

6.1.6 Seguridad de los recursos humanos

Se debe asegurar que los funcionarios, contratistas y demás colaboradores adopten sus responsabilidades en relación con las políticas de seguridad de la información de La E.S.E y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información

- A la firma del contrato laboral o posesión del cargo el funcionario debe firmar un acuerdo de confidencialidad para con La E.S.E HRSO
- Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información.
- Los funcionarios deben cumplir con el Codigo Ética y Buen Gobierno.
- En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de la ley 734 de 2013, ley 200 de 1995 y demás normas que reglamenten los procesos disciplinarios para los empleados del estado.

6.1.7 Administración del cambio

Los cambios generados en la plataforma de software de la empresa deben realizarse de conformidad al procedimiento establecido por la E.S.E Hospital Regional Sur Oriental y contar con un registro de operaciones a fin de hacer un seguimiento y control de su ejecución.

- Todo cambio (creación, eliminación o modificación de programas, aplicativos, formatos y reportes) que afecte los recursos informáticos, debe ser solicitado formalmente por los usuarios de la información y aprobado formalmente por el responsable de la administración de la misma, el nivel de jefe inmediato o por quienes estos formalmente deleguen. El responsable de la administración de los accesos a la información tendrá la facultad de aceptar o rechazar la solicitud.
- Bajo ninguna circunstancia un cambio de la información o de los sistemas de información puede ser aprobado, realizado e implantado por la misma persona o por una misma área.
- Todos los requerimientos de mantenimiento de los sistemas de información (software o hardware) y/o necesidades de suministros o elementos, deben ser solicitados de forma escrita al Jefe de la Oficina Sistemas de manera formal mediante oficio, correo electrónico o en el formato oficialmente establecido y adoptado por la empresa.

6.1.8 Seguridad de la Información

Los trabajadores de planta y contratistas son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales establecidos por la entidad, por las normas que reglamenten el archivo documental, con el fin de garantizar su custodia, integridad, confidencialidad, disponibilidad y confiabilidad y así evitar pérdidas, accesos no autorizados, exposición, modificación y/o utilización indebida de la

misma, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

- Los trabajadores de planta, contratistas y pasantes no deben suministrar información de la E.S.E Hospital Regional Sur Oriental a ningún ente externo sin las autorizaciones respectivas.
- Los funcionarios, contratistas y terceros vinculados a la E.S.E Hospital Regional Sur Oriental deberán firmar y renovar cada tres meses o un año en el caso que lo permita, un acuerdo de cumplimiento de las políticas de seguridad de la información, de confidencialidad y de buen manejo de la información que manejen o a la que tengan acceso durante la vinculación a la E.S.E Hospital Regional Sur Oriental. Después de que el trabajador deja de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez desvinculados los funcionarios o contratistas, ellos deben comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los trabajadores que detecten el mal uso de la información están en la obligación de reportar el hecho al jefe de la Oficina de Control Interno o a los entes de vigilancia y control pertinentes (sistemas).
- El software adquirido y desarrollado por funcionarios de la E.S.E Hospital Regional Sur Oriental, es exclusivo para el funcionamiento de las operaciones de la institucion y en ningún momento debe ser copiado o prestado o vendido para otros fines distintos a los que se adquirieron o se desarrollaron. En caso de que terceros requieran de éstos, debe ser autorizado por la Gerencia General.
- Las políticas, normas y procedimientos relacionados con la seguridad de la información que tiene establecida la E.S.E Hospital Regional Sur Oriental, se deben socializar a funcionarios, contratistas y clientes externos, para efectos de aplicabilidad y uso**.**

6.1.9 Uso de Impresoras

Ningún recurso informático de la E.S.E podrá usarse para fines diferentes a los asuntos de trabajo. Las impresiones que se elaboren con estos recursos en ningún momento podrán ser de carácter personal.

En caso de presentar problemas en el momento de imprimir debe evitar manipular los elementos de la impresora, se debe comunicar área de sistemas.

6.1.10 Seguridad física y en el entorno

Todas las áreas de la empresa relacionadas directa o indirectamente con el procesamiento o almacenamiento de información de la entidad, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considerarán como áreas de acceso restringido y por lo tanto se deben implementar medidas de control de acceso del personal a dichas áreas.

- Se restringe el acceso de funcionarios, contratistas, proveedores de materiales y demás personas ajenas a la Oficina de Sistemas, al Centro de Cómputo, sitio donde están ubicados los Servidores, Planta Telefónica y Equipos de Comunicaciones. Este lugar deberá permanecer en todo momento cerrado con llave. La llave de este sitio debe ser manejada por el Profesional Universitario de la Oficina de Sistemas.
- Todo visitante o personal ajeno a la empresa debe ser identificado mediante un sistema de registro y control de forma previa al ingreso a cualquier área o dependencia de la entidad.
- Cualquier persona que ingrese a centros de cómputo o áreas de almacenamiento de información que la entidad considere críticas o de acceso restringido, deberá registrar el motivo del ingreso y estar acompañado permanentemente por el personal que labora cotidianamente en estos lugares.
- En los centros de cómputo o áreas de almacenamiento de información que la entidad considere críticas, deberán existir elementos de control de incendio, control de inundación y alarmas y deberán contar con demarcación de las zonas de circulación y zonas de acceso restringido.
- Las centrales de conexión de los sistemas de información o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

6.1.11 Seguridad en comunicaciones

Todo funcionario o contratista de la empresa deberá conocer y ejecutar cuando se requiera, el procedimiento oficial para la administración, configuración e implementación de la infraestructura de la red corporativa, así como su uso, cambios u operaciones de gestión definidas por prácticas seguras para la información que por ellas fluye.

- Todo intercambio electrónico de información o interacción entre sistemas de información de la empresa con entidades externas, deberá estar soportado con un acuerdo, convenio o documento de formalización de dicho procedimiento.
- Los equipos de cómputo que se conecten de forma directa con un proveedor externo para suministrar un servicio se realizarán a través de VPN (redes privadas virtuales o IP pública) mediante conexiones seguras, previa autorización de la Oficina de Sistemas y con los debidos mecanismos y sistemas de seguridad informática de la empresa y del proveedor de servicios.
- Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Entidad e Internet deberá contemplar cifrado o encriptación el cual debe ser garantizado por el proveedor de servicio de comunicaciones bajo el monitoreo y supervisión de la Oficina Asesora de Comunicación y Sistemas.

6.1.12 Control de Virus Informáticos

La E.S.E Hospital Regional Sur Oriental para la protección de su información, deberá contar con herramientas informáticas para el control de los software malicioso incluidos los virus informáticos, así como un grupo de prácticas que eviten su masificación y su influencia negativa.

- La empresa mantendrá instalado en todos sus equipos de cómputo un software anti malware o antivirus que garantice la seguridad en la información, el cual se actualizará a través de la red una vez a la semana al iniciar sesión el equipo.
- En caso de que el usuario detecte la presencia de un virus en algún archivo o algún comportamiento anormal de las funciones dentro de los equipos de cómputo, Tiene el deber de notificar el hecho a la Oficina de Sistemas, para que se tomen las acciones pertinentes y evaluar su impacto en los demás equipos o en la red.
- No se deben abrir o reenviar archivos de dudosa procedencia para evitar el contagio de software mal intencionado o virus.
- Se debe evitar al máximo el usar medios extraíbles de almacenamiento como CD, DVD, memorias USB etc. que pueden infectar a los equipos con software mal intencionado o virus.
- Se deben eliminar correos electrónicos de remitentes desconocidos, o con mensajes o archivos adjuntos sospechosos, ya que estos pueden traer keyloogers, virus, sniffer, spam, etc. Esto puede ocasionar un ataque a nuestra red corporativa de datos a través de hackers y/o crackers informáticos.

6.1.13 Almacenamiento y respaldo de la información

La Oficina de Sistemas implementará mecanismos para el almacenamiento seguro y protección de la información en medios magnéticos o electrónicos, perpetuarla y garantizar su recuperación en caso de fallas de los equipos de cómputo u ocurrencia de eventos de contingencia o situaciones fortuitas.

- La realización de copias de respaldo debe ser acorde al procedimiento para copias de seguridad de los sistemas de información establecido en la empresa, lo cual permitirá garantizar la oportuna recuperación de la información en la eventualidad que ocurra algún percance.
- Se debe mantener las copias de seguridad de la información según la periodicidad establecida en el procedimiento de backups y proveer de un lugar externo a las instalaciones de la E.S.E Hospital Regional Sur Oriental. la cual permita recuperar la información en caso de una contingencia.
- Es responsabilidad de la Oficina de Sistemas, verificar mensualmente que se hayan realizado todas las copias de seguridad de la información almacenada en

cada equipo y que estas se encuentren en buen estado para su almacenamiento y posterior restauración.

- Al final de cada año, la Oficina de Sistemas, guardará una copia de seguridad de toda la información almacenada en la vigencia, en medios magnéticos, para su conservación y custodia.
- La Oficina de Sistemas deberá garantizar la privacidad y confidencialidad de la información en aquellas áreas que la soliciten mediante el manejo de claves de seguridad y la encriptación de la información.
- Se debe informar a la oficina de sistemas del retiro de funcionarios o contratistas que manejen contraseñas, permisos de usuarios o claves de seguridad cuando estos finalicen su contrato o terminen labores con la empresa, desactivar las cuentas de usuario, claves, contraseñas, permisos y similares, dentro de los sistemas de información de la empresa.
- Los dispositivos o medios que contengan copias de seguridad (backups) deberán mantenerse almacenados en un lugar seguro previamente definido por la Oficina de Sistemas y su manejo será exclusivo de dicha área.

7 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica **El Modelo de Seguridad y Privacidad de la Información (MSPI),** el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Para garantizar una adecuada implementación del Modelo de Seguridad de la Información en las entidades del Estado, se describe una estrategia de trabajo que está estructurada a partir de etapas alineadas con los niveles de madurez de manual de Gobierno en línea 3.1, las cuales se detallan y son coherentes con los lineamientos del estándar NTC:ISO/IEC 27001:2005.

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

7.1 CICLO DE OPERACIÓN

El ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. Estas fases, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.

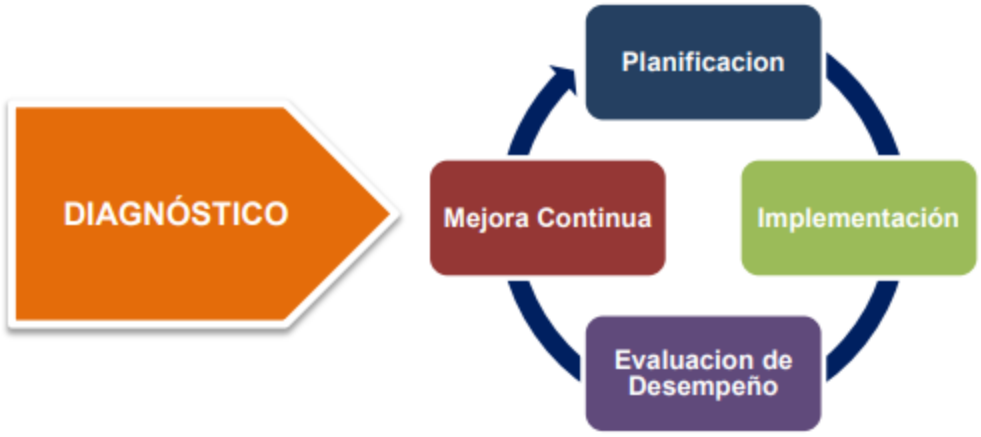


Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información
fuente: Modelo de Seguridad y Privacidad de la Información MIN TIC

7.2 PLAN DE ACCIÓN

COMPONENTE	ACTIVIDADES	RESPONSABLE	META / ENTREGABLE	Fecha
DIAGNOSTICO	Determinar el Estado Actual de la gestión de seguridad y privacidad de la información	Ingeniero de Sistemas	Herramienta de Diagnostico	2020
PLANIFICACION	Revisión de la política de seguridad y privacidad de la información	Ingeniero de Sistemas	Documento de la política revisado	2020
	desarrollar y formalizar procedimientos para gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.	Ingeniero de Sistemas	procedimientos de seguridad de la informacion	2020
	Definir los roles y las responsabilidades de seguridad de la información	Ingeniero de Sistemas	Roles y responsabilidades de seguridad y privacidad de la información.	2020
	Generar un Inventario de activos de información	Ingeniero de Sistemas	Inventario de activos de información	2020
	Alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental	Ingeniero de Sistemas	Integración del MSPI con el Sistema de Gestión documental	2020
	Identificación, Valoración y tratamiento de riesgo	Ingeniero de Sistemas	Plan de tratamiento de riesgos de seguridad	2020
	Diseñar el Plan de Comunicación de la estrategia de seguridad	Ingeniero de Sistemas	Plan de Comunicación de seguridad	2020
	Diagnóstico de la transición de IPv4 a IPv6	Ingeniero de Sistemas	documento diagnóstico de la transición de IPv4 a IPv9	2020
IMPLEMENTACION	Verificar el cumplimiento de la política de seguridad de la información y socialización dentro de la entidad.	Ingeniero de Sistemas	Informes seguimiento plan de acción anual	2020

	Implementación del plan de tratamiento de riesgos.	Ingeniero de Sistemas	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	2020
	Indicadores De Gestión.	Ingeniero de Sistemas	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	2020
	Plan de Transición de IPv4 a IPv6	Ingeniero de Sistemas	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.	2020
EVALUACION DEL DESEMPEÑO	Realizar el plan de revisión y seguimiento, a la implementación del MSP	Ingeniero de Sistemas	Plan de revisión y seguimiento, a la implementación del MSP	2020
	Diseño del Plan de Ejecución de Auditorias	Ingeniero de Sistemas	Plan de Ejecución de Auditorias	2020
MEJORA CONTINUA	Plan de mejora continua	Ingeniero de Sistemas	Plan de mejora continua	2020