Política De Seguridad Digital
E.S.E Hospital Nuestra Señora Del Carmen

Vigilada Supersalud

Jorge Alberto Lemus Bello
Gerente

Guamal Magdalena, 19 marzo de 2024

INTRODUCCIÓN

El incremento en el uso masivo de las Tecnologías de la Información y las Comunicaciones – TIC- en Colombia, ha reflejado la intensificación de las redes de telecomunicación como parte del implemento del uso de la participación digital de la ciudadanía, convirtiendo de esta manera los procesos institucionales en formas significativas de transformación de la información digital.

En este sentido, de acuerdo al Departamento Administrativo de la Función Pública, la política de Seguridad Digital permite a esta entidad de salud fortalecer las habilidades y capacidades de los grupos del valor de la entidad, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades en el entorno digital.

La E.S.E Hospital Nuestra Señora del Carmen, diseña esta política adoptando los lineamientos del Modelo de Gestión de Riesgos de la Seguridad Digital -MGRSD- y el Modelo de Seguridad y Privacidad de la Información-MSPI, diseñados por el Ministerio de las Tecnologías de la Información y Comunicación de Colombia Mintic, los cuales son desarrollados para las entidades públicas para implementar la Política Nacional de Seguridad Digital Conpes 3854 de 2016.

Objetivo General

Identificar las capacidades la E.S.E Hospital Nuestra Señora del Carmen, para fortalecer, tratar y mitigar los riesgos de seguridad digital que puedan afectar la seguridad digital y el uso de las tecnologías de la información y comunicación TIC

Objetivos específicos

- Trazar los elementos para la planeación estratégica ante posibles riesgos y amenazas cibernéticas
- Crear las herramientas propicias para la identificación, valoración y controles de riesgo cibernético
- Implementar acciones para dar seguimiento a los riesgos asociados a la seguridad digital e información y las comunicaciones.

Alcance

El presente documento presenta los aspectos relevantes para la implementación de la Política de Seguridad Digital en la E.S.E. Hospital Nuestra Señora del Carmen, del mismo modo, se define un alcance para la política, la organización para un modelo de gestión y los aspectos para el establecimiento, implementación, operación y seguimiento de los riesgos de seguridad de digital dados en la entidad.

Este documento va dirigido e involucra a todo el personal la E.S.E. Hospital, funcionarios asistenciales, administrativos, operativos y grupos de valor, debido a que la implementación, operación y cumplimiento de lo dispuesto en la Política de Seguridad Digital.

Términos y definiciones

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854:2016, pág.56).

Activo cibernético: En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

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

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO 2700:2016).

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).

Actitud hacia el riesgo: Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo. (NTC ISO 31000:2011).

Ataque cibernético: Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).

Cibercrímen (Delito cibernético): Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).

Ciberdefensa: Empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (CONPES 3854, pág. 88).

Ciberseguridad: Conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).

Ciberdelincuencia: Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia).

Ciberdelito/Delito cibernético: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Cibernética: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Diccionario de la lengua española).

Marco Legal

- **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”.

- **Norma Técnica Colombiana NTC ISO 27000:2013:** Requisitos para la Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la información.

- **Decreto 103 de 2015:** “por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”. Derogado Parcialmente por el Decreto 1081 de 2015.

- **Ley estatutaria 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.

- **Ley 1712 de 2014 .** “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan 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”

- **Conpes 3854 de 2016**. Política Nacional de Seguridad Digital.

- **Acuerdo 02 de 2018.** “Por el cual se establece la estructura de la Jurisdicción Especial para La Paz – JEP”

- **Ley 1928 de 2018** “Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en budapest.

Direccionamiento Estratégico De La E.S.E. Hospital Nuestra Señora Del Carmen De Guamal, Magdalena

Misión

Somos un hospital público de baja complejidad que ofrece servicios de salud con criterios de calidad, seguridad y oportunidad; contamos con un recurso humano idóneo comprometido con la mejora continua de los procesos asistenciales orientados hacia la satisfacción del usuario y su familia.

Visión

En el 2023 seremos reconocidos como un hospital que ofrece servicios de salud oportunos y de calidad, apoyado en su equipo humano e infraestructura física y tecnológica, fijando como propósito el fortalecimiento de los servicios habilitados y dando apertura a nuevas estrategias de atención que permitan convertirnos en una institución eficiente y humanizada.

Valores Institucionales:

La ESE Hospital Nuestra Señora del Carmen tiene establecido en su Código de Ética y Buen Gobierno el marco de la filosofía del servicio que presta, las normas morales y éticas, además de los valores cotidianos que se constituyen en las creencias que nos unen en torno a nuestros usuarios y partes interesadas, y a través de ello, se rige la conducta y actuar de cada integrante de la E.S.E los cuales se recogen en los siguientes valores:

- **ORIENTACION AL USUARIO:** El hospital actuará en todo momento en función de satisfacer las necesidades y expectativas del usuario en materia de servicios de salud, impulsando una atención y trato personalizado.

- **DILIGENCIA:** Los Funcionarios cumplirán con los deberes, funciones y responsabilidades asignadas a su cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos.

- **EFICACIA:** La actuación de los funcionarios del Hospital se orientará hacia la adopción de decisiones que garanticen el mejor resultado, concreción de logros que afecten los servicios de salud que se prestan al usuario.

- **EFICIENCIA:** Los funcionarios del Hospital actuarán responsablemente con el uso de los recursos para lograr los

  mejores resultados, reconociendo que éstos son limitados, y eligiendo entre alternativas que pueden suministrar el mayor beneficio.

- **INNOVACIÓN:** El Hospital y los funcionarios de este, deberán tener orientación a fomentar y crear nuevas ideas imprimiendo creatividad e imaginación lo que nos permitirá mejorar y fortalecer nuestra competitividad y liderazgo.

- **HONESTIDAD:** Nos comprometemos en actuar y desarrollar nuestra misión en un ambiente de transparencia de cara a la verdad y en cumplimento a la ley.

- **RESPETO:** Propiciamos el respeto a la persona, reconocimiento y compromiso al valor de la diversidad de ideas y puntos de vista de los colaboradores, de los usuarios y sus familias. Tenemos especial preocupación por aquellos que se encuentran en estado de vulnerabilidad.

- **TRABAJO EN EQUIPO**: Fomentamos la colaboración al interior del hospital, con la red asistencial y la comunidad, respetando y valorando nuestras diferencias, fortaleciendo las relaciones interpersonales y priorizando el éxito del equipo por encima del éxito individual.

- **COMPROMISO:** Trabajamos comprometidos más allá de nuestro simple deber, generando siempre nuestro mayor esfuerzo consecuentes a la capacidad de la entidad.

- **ÉTICA:** Los funcionarios del Hospital sostendrán una conducta transparente, honesta y preocupada por la dignidad de todas las personas con las que se interactúa.

- **VOCACION DE SERVICIO**: Los funcionarios del Hospital actuaran de manera solidaria y con un accionar desinteresado inclinándose a brindar en todo instante colaboración y/o ayuda.

- **JUSTICIA:** Todos los funcionarios actuaran con imparcialidad garantizando los derechos de las personas, con equidad, igual dad y sin discriminación.

- **CALIDAD:** La orientación hacia la calidad nos exige procedimientos para evaluar la eficiencia, la efectividad y la seguridad de las intervenciones preventivas, de apoyo y curativas.

  Actuaremos aplicando nuestro recurso maximizando los beneficios de salud con el mínimo riesgo, y la máxima satisfacción del paciente con el proceso.

- **CONFIANZA:** Entregaremos esperanza y seguridad en nuestro actuar.

Principios Institucionales:

- **COMPROMISO EN EL SERVICIO:** desarrollamos y mantenemos una destacada actitud de servicio frente a los usuarios y sus familiares, buscando soluciones eficaces que contribuyan a la mejora continúa reflejada en la satisfacción de la asistencia generada por nuestro personal.

- **TRANSPARENCIA INSTITUCIONAL:** Buscamos dar cumplimiento a nuestra misión y visión corporativa, con apego y cumplimiento a los valores éticos que permitan generar un ambiente transparente y una relación de mutuo beneficio entre usuarios, familiares y partes interesadas.

- **MOVILIZADORES DE CAMBIO:** Como institución sabemos que nuestras acciones no solamente pueden quedar trazadas en nuestro compromiso de trabajo cotidiano, es por ello que procuramos llevar soluciones innovadoras haciendo uso de la capacidad institucional.

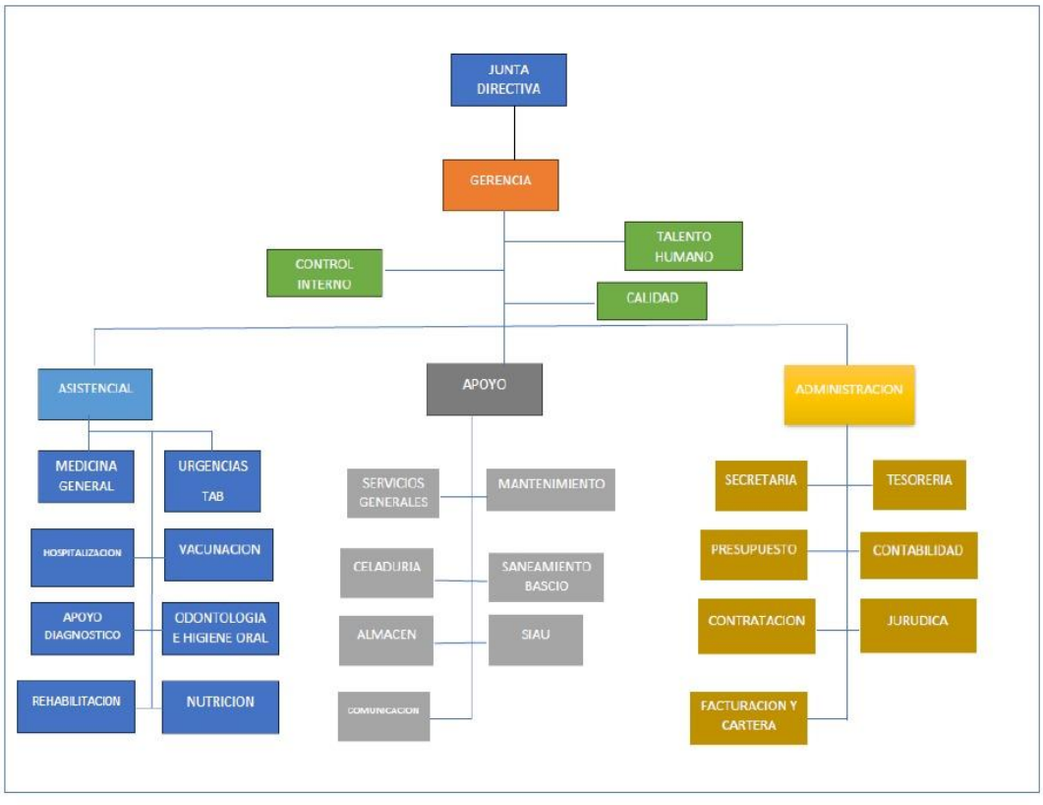
- **COMPROMISO CON LA CALIDAD:** Nos comprometemos con el logro de los mejores resultados a través de la prestación de nuestros servicios, desplegando una gestión efectiva, eficiente y oportuna de nuestros procesos y recursos.

- **RESPONSABILIDAD SOCIAL:** A través de nuestro servicio, nos comprometemos con el desarrollo, el bienestar y el mejoramiento de la calidad de vida de nuestros funcionarios y las partes interesadas, apoyados en acciones responsables.

- **ARMONÍA CON EL MEDIO AMBIENTE:** Nos comprometemos en que nuestras acciones estén ligadas en respetar, preservar y conservar un medio ambiente saludable.

Mapa de Procesos:

Organigrama



Elaboración y consolidación de la Política

El Gobierno Nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC, da cumplimiento a la Política Nacional con la implementación del Modelo Nacional de Gestión de Riesgos de Seguridad Digital, de ahora en adelante (MGRSD), que contribuye a unas mejores prácticas en la ejecución y desarrollo de la gestión de riesgos digitales en las organizaciones carácter público o privado.

La Empresa Social del Estado Hospital Nuestra Señora del Carmen de Guamal Magdalena, mediante la política de Seguridad digital, preserva la confidencialidad, integridad, disponibilidad, autenticidad, mediante una gestión de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua.

La Política Nacional de Seguridad Digital busca “fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el País”. (CONPES 3854 del 11 de abril de 2016 - numeral 5.1 objetivo general).

Principios De La Política De Seguridad Digital

El Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) plantea principios fundamentales y generales para que las partes interesadas puedan gestionar la seguridad digital, fomentando confianza con el entorno digital. A continuación de relacionan:

- **Principios Fundamentales:**

- Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos
- Adoptar un enfoque basado en la gestión de riesgos
- Adoptar un enfoque incluyente y colaborativo
- Asegurar una responsabilidad compartida entre las múltiples partes interesada

- **Principios Generales:**

- La Gestión de Riesgos de Seguridad Digital facilita la mejora continua de la organización.
- La Gestión de Riesgos de Seguridad Digital es transparente e inclusiva
- La Gestión de Riesgos de Seguridad Digital toma en consideración los factores humanos y culturales
- La Gestión de Riesgos de Seguridad Digital se basa en la mejor información disponible
- La Gestión de Riesgos de Seguridad Digital es parte de la toma de decisiones, una vez evaluada las posibles consecuencias de las amenazas y vulnerabilidades digitales
- La Gestión de Riesgos de Seguridad Digital aborda explicitamente la
- Incertidumbre
- La Gestión de Riesgos de Seguridad Digital es una parte integral de todos los procesos del Instituto
- La Gestión de Riesgos de Seguridad Digital crea y protege el valor

Metodología

Desde la E.S.E Hospital Nuestra Señora del Carmen, en coherencia con, las dimensiones, componentes y elementos que hacen parte del Modelo Integrado de Planeación y Gestión MIPG, se compromete a ejercer el control efectivo de los eventos de Riesgos de Seguridad Digital, que puedan afectar negativamente el desarrollo de sus procesos a través del diagnóstico, identificación, análisis, valoración y administración del Riesgo de Seguridad digital.

Fases de la política de seguridad digital

La E.S.E Hospital Nuestra Señora del Carmen de Guamal Magdalena, en relación con la política de Seguridad Digital, adopta para la implementación de ésta el Modelo de Gestión de Riesgos de Seguridad Digital desarrollado por Min Tic, el cual contempla cuatro fases para su ejecución:

Fase # 1. Planificación De La Gestión De Riesgo De Seguridad Digital (GRSD)

Esta primera fase del modelo de gestión de riesgos de seguridad digital, es fundamental en las entidades públicas, debido a que, se establecen los elementos necesarios como punto de inicio para los procesos y procedimientos de los riesgos informáticos.

- **Compromiso de la Alta Dirección:**

La alta gerencia de la E.S.E Hospital Nuestra Señora del Carmen de Guamal Magdalena, entiende lo importancia de la ejecución y gestión de la seguridad de la seguridad digital, por ello, se compromete con la implementación del Modelo de Gestión del Riesgo de la Seguridad Digital –MGRSD fundando garantías que propicien la confianza ante los derechos entre el estado y los ciudadanos, en el marco del cumplimiento de las leyes y la ruta estratégica de la entidad de salud.

- **Contexto Estratégico:**

Desde la E.S.E Hospital Nuestra Señora del Carmen, en materia de riesgos de la seguridad digital para el debido análisis en el contexto estratégico se fundamenta bajo los lineamientos planteados en la política de Planeación Institucional de esta entidad de salud.

En este sentido, el análisis estratégico se realiza partiendo de los conocimientos de las diferentes situaciones presentes desde los entornos internos y externos de la

entidad, los cuales se pueden identificar tanto de carácter social, económico, cultural, ambiental, de orden público, político, legal y/o cambios tecnológicos, infraestructura, personal entre otros; basándose al mismo tiempo en los resultados de los componentes de ambiente de control, estructura organizacional, modelo de operación, cumplimiento de los Planes y Programas, sistemas de información, procesos y procedimientos y los recursos económicos, entre otros.

- **Identificación de las partes interesadas:**

Para la Administración del Riesgo en la entidad, se determinan los roles de los diferentes actores, de acuerdo con la directriz del Departamento Administrativo de la Función Pública así:

- ✓ Identificar y construir los mapas de riesgos de los procesos a su cargo, teniendo en cuenta los aspectos ambientales, de seguridad de la información, seguridad y salud ocupacional, gestión ambiental, entre otros, que afecten el cumplimiento de los objetivos organizacionales.

- ✓ Adelantar la revisión, actualización periódica y seguimiento de los mapas de riesgos, en todos aquellos aspectos que les fueren asignados.

- ✓ Adoptar las medidas necesarias para el cabal desempeño de la Gerencia o Administración de Riesgos en cumplimiento de las funciones, la entrega de los productos y prestación de los servicios y/o la ejecución de los procesos asignados a sus cargos, con miras a la realización de los fines del Estado.

- ✓ Corresponde a todos los responsables de los procesos, identificar e implementar acciones preventivas cuando el cálculo del riesgo residual los ubique en zona de riesgo extrema, alta o moderada.

- ✓ Los responsables de los procesos deben realizar la medición de sus controles en términos de eficacia, eficiencia y efectividad, para determinar la pertinencia y la necesidad de ajuste o modificación en caso de presentarse.

- **Asociación de la política de gestión de riesgos de seguridad digital con políticas existentes**

La E.S.E Hospital Nuestra Señora del Carmen de Guamal Madalena, para implementar el Modelo de Gestión de Riesgos determina en la política de Planeación Institucional los lineamientos para la administración del riesgo y el diseño de controles para los Riesgos de gestión, corrupción y seguridad digital de acuerdo a la guía de la Función Pública.

- **Definición de roles y responsabilidades para la gestión de riesgos de seguridad digital (GRSD)**

Para la gestión del riesgo de la Seguridad Digital de la E.S.E Hospital Nuestra Señora del Carmen, desde la alta gerencia se establecen las responsabilidades, empezando desde este órgano, pero así mismo los líderes de procesos, jefes de áreas, servidores, contratistas asistenciales y administrativos tienen responsabilidades ante el control de los riesgos tecnológicos y los sistemas informáticos que se puedan presentar en esta entidad

- **Recursos para el desarrollo de la gestión de riesgos de seguridad digital**

Para la planeación y ejecución del desarrollo del Modelo de Gestión de Riesgos de Seguridad Digital, la E.S.E Hospital Nuestra Señora del Carmen establece se los recursos económicos y de talento humano requeridos para tal fin para la definición, seguimiento, control y mejoramiento continuo de las actividades a ejecutar establecidas en el Plan Anual de Adquisiciones y el PETI.

- **Los criterios para la gestión del riesgo de seguridad digital**

Para la gestión del riesgo de seguridad digital, la E.S.E Hospital Nuestra Señora del Carmen de Guamal, tiene a consideración los criterios de probabilidad e impacto, su valoración, el tratamiento de los riesgos, los criterios de riesgo y el apetito o zona de aceptación del riesgo presentes desde los diferentes contextos que involucran la entidad de salud.

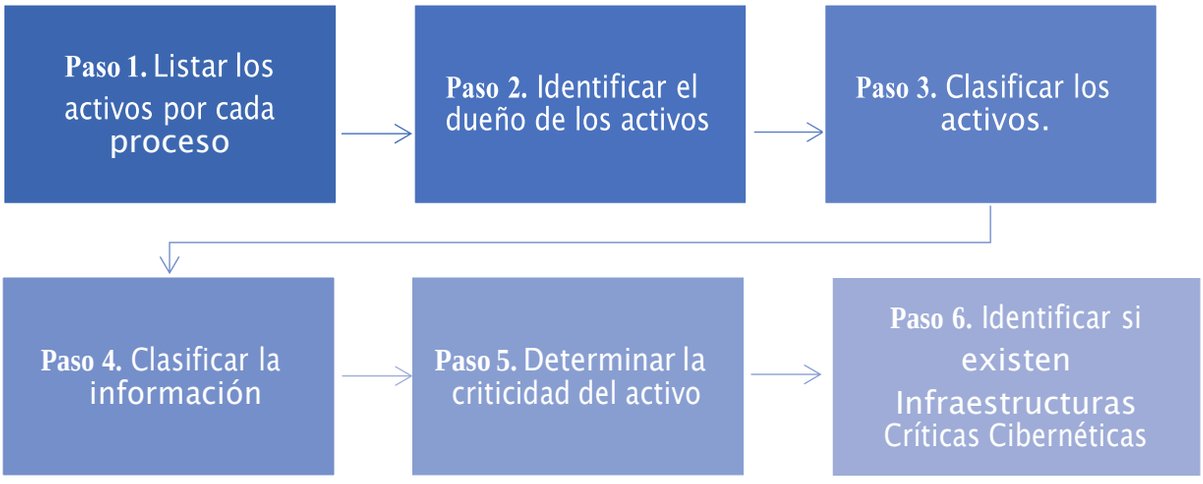
Fase #2. Ejecución Del Modelo De Gestión De Riesgos De Seguridad Digital (MGRSD)

Esta fase sigue los lineamientos planteados en la fase anterior, en implementar la planificación de la gestión de riesgo de Seguridad Digital y los riesgos definidos anteriormente, en esta fase la línea estratégica debe dar cumplimiento con el propósito de ofrecer recursos necesarios iniciar con el control y tratamiento de los riegos digitales y tecnológicos de los cuales la entidad pueda ser vulnerable.

El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes apliquen los controles necesarios para la mitigación del riesgo.

- **Identificación de activos de información**

Si a seguridad digital nos referimos, un activo hace referencia a cualquier elemento que tenga valor para la organización, como: aplicaciones, servicios web, redes, información física o digital, que utiliza la entidad para su funcionamiento. para la generación de este inventario, la entidad debe tener en cuenta los siguientes pasos:



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Paso 1- Listar los activos para cada proceso: En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

Paso 2 – Identificar el dueño de los activos: Cada uno de los activos identificados deberá tener un dueño designado, si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

Paso 3 – Clasificar los Activos: Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: información, software, hardware, componentes de red entre otros.

Paso 4 - Clasificar la información: La información se clasifica de acuerdo a:

✓ **Confidencialidad:** se refiere a que la información no esté disponible ni sea revelada individuos, entidades o procesos no autorizados.

✓ **Integridad:** se refiere a la exactitud y completitud de la información.

✓ **Disponibilidad:** es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en elfuturo.

Clasificación de acuerdo a la confidencialidad:

Información Pública Reservada	**Información disponible solo para el proceso de la Entidad y que en caso de ser conocida por terceros si autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen y/o económica.**
Información Pública Clasificada	**Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede llevar un impacto negativo para los procesos de la misma.** **Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.**
Información Pública	**Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.**
No Clasificada	**Activos de información que deben ser incluidos en el inventario y que aún no ha sido clasificados, deben ser tratados como activos de INFORMACIÓN PÚBLICARESERVADA.**

Esquema de clasificación por confidencialidad - fuente guía para la gestión y clasificación de activos de información MINTIC

Clasificación de acuerdo a la integridad:

A (ALTA)	**Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.**
M (MEDIA)	**Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.**
B (BAJA)	**Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.**
No Clasificada	**Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.**

Esquema de clasificación por integridad- fuente guía para la gestión y clasificación de activos de información MINTIC

1 (ALTA)	**La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.**
2 (MEDIA)	**La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.**
3 (BAJA)	**La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.**
No Clasificada	**Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.**

Clasificación de acuerdo a la disponibilidad:

Esquema de clasificación por disponibilidad- fuente guía para la gestión y clasificación de activos de información MINTIC

Paso 5 – Determinar la criticidad del activo (Valoración del activo): El cálculo de la criticidad lo determina el valor general del activo de acuerdo con la clasificación de la información

Calculo de la criticidad del activo:

CONFIDENCIALIDAD	INTEGRIDAD	*DISPONIBILIDAD*
Información Pública Reservada	**ALTA (A)**	***ALTA (1)***
Información Pública Clasificada	**MEDIA (M)**	***MEDIA (2)***
Información Pública	**BAJA (B)**	***BAJA (1)***
No Clasificada	**No Clasificada**	***No Clasificada***

Criterios de clasificación - fuente guía para la gestión y clasificación de activos de información MINTIC

ALTA	**Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.**
MEDIA	**Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.**
BAJA	**Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.**

Niveles de clasificación - fuente guía para la gestión y clasificación de activos de información MINTIC

Paso 6 – Identificar si existen Infraestructura Críticas Cibernéticas –ICC-: Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios:

IMPACTO SOCIAL	IMPACTO ECONÓMICO	IMPACTO AMBIENTAL
(0,5%) de Población Nacional	**PIB de un Día o 0,123% del PIB Anual**	

Criterio infraestructura cibernética - fuente guía para la gestión y clasificación de activos de información MINTIC

FASE#3. MONITOREO, REVISIÓN Y REPORTE DEL MGRSD

En esta fase en coordinación con la alta gerencia, la oficina de control interno y sistemas de información, periódicamente se están realizando el monitoreo con el fin determinar qué tan efectivos están siendo los planes tratamiento y de controles ejercidos para ante la política.

Así mismo, a través de las auditorías internas realizadas por la oficina de control interno permiten determinar y controlar si los procesos, procedimientos, planes se alineas a las estrategias establecidas para la prevención de los riesgos citados expuestos por esta entidad, con el objetivo de estudiar y evaluar acciones de mejora.

Además, para la medición del desempeño, se formulan indicadores logros enfocados a los lineamientos establecidos en la política de Planeación Institucional, acogiéndose al procedimiento establecido por la E.S.E Hospital Nuestra Señora del Carmen, que describe los lineamientos para la identificación, seguimiento, control y análisis de los indicadores. También se diligencia el reporte oficial de la implementación de la política a través del FURAG, propuesto por el Departamento Administrativo de la Función Pública.

FASE #4. MEJORA PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

Desde esta entidad garantiza la mejora en los procesos, procedimientos y acciones tomadas desde la alta gerencia, además de eso, ante los hallazgos presentes, falencias o incidentes presentados de seguridad digital, cuenta con una respuesta inmediata ante las crisis presentes con el fin de mitigar el impacto y tomar acciones que permitan mejorar y fortalecer los sistemas tecnológicos dispuestos por la E.S.E

Para la prevención de los riesgos digitales la entidad establece acciones de mejora continua para la gestión de riesgos de seguridad digital de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.