ESE Hospital Regional de Duitama

Programa: Modelo De Seguridad Y Privacidad De La Información

	ESE Hospital Regional de Duitama **Proceso**: Gestión de la Información **Subproceso**: Tecnologías de la información **Programa**: Modelo De Seguridad Y Privacidad De La Información	**Código** HRD-PA-GI-TI-PG-01 **Fecha** 2023-07-12 **Versión** 1.0

Estratégico	Misional	Apoyo	Evaluación

Introducción

La E.S.E. Hospital Regional de Duitama es consciente de que cada vez, con la evolución tecnológica, es más propensa a sufrir incidentes de seguridad digital, lo cual puede afectar el funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía. Razón por la cual, decide realizar el Programa del Modelo de Seguridad Y Privacidad de la Información y a partir de este mejorar la infraestructura documental y tecnológica en pro de los objetivos de la entidad.

Apoyados en la política de gobierno digital, la cual tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para dar confianza en el uso del entorno digital,
propendiendo por el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.

Se establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Entidad.

Por tal motivo se documenta el Modelo de Seguridad y Privacidad de la Información – MSPI con el objetivo de formalizar un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en unciclo PHVA (Planear, Hacer, Verificar y Actuar.

El modelo consta de cinco (5) fases las cuales permiten gestionar y mantener adecuadamente la seguridad y privacidad de los activos de información.

1. Diagnóstico: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI.

2. Planificación: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo.

3. Operación: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

4. Evaluación de desempeño: Determinar el sistema y forma de evaluación de la adopción del modelo.

5. Mejoramiento Continuo: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Objetivo General

Definir un sistema de gestión de seguridad de la información y seguridad digital para la E.S.E Hospital Regional de Duitama, que contemple su operación en un ciclo PHVA (Planear, Hacer, Verificar y Actuar) mediante las fases de diagnóstico, planificación, operación, evaluación de desempeño y mejoramiento continuo.

Alcance

Aplica para la gestión de seguridad de aplicaciones o sistemas de información, seguridad de la red, seguridad de internet y protección de la infraestructura de información critica de la E.S.E. Hospital Regional de Duitama bajo las cinco (5) fases del Modelo de Seguridad y Privacidad de la Información.

Responsables

ÁREA O ROL INSTITUCIONAL	RESPONSABILIDADES
Directivos de la Entidad	Encargados de la aprobación de los proyectos de inversión en temas de seguridad y privacidad de la información.
Contro Interno, Planeación Institucional y Gestión de Calidad.	Responsables de auditorias, control y seguimiento a la implementación del MSPI.
Gestión Juridica y Contractual.	Brinda asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
Lider de Tecnologías de la Información	Responsables de la implementación y seguimiento de la seguridad y privacidad de la información.
Responsable de la seguridad Institucional	
Personal de seguridad de la Información	
Líderes y Coordinadores institucionales	Apoyan y adoptan la gestión de buenas prácticas de seguridad y privacidad de la información.
Equipo de Tecnologías de la Información	Encargados de la implementación del MSPI.
Colaboradores y/o funcionarios de la entidad	Adoptan las buenas prácticas de seguridad y privacidad de la información.
Proveedores	Adoptan las políticas institucionales de seguridad y privacidad de la información.
Comité de Gestión y Desempeño	Espacio en el cual se reporta y hace seguimiento sobre temas de seguridad y privacidad de la Información.

Marco Legal y/o Teórico

COMPES 4070 2021. "Lineamientos de Política para la Implementación de un Modelo de Estado Abierto.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 2106 de 2019. establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 612 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 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Directiva 02 2000. Gobierno en línea.

Ley 1341 2009. Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley 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.

Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

N003 NTC27002 2007. Técnicas de seguridad. Código de práctica para la gestión de la seguridad.

NQA ISO 22301 2019. Guía de Implantación de la Continuidad de Negocio

NTC 27001 2006. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI) Requisitos.

Resolución 500 2021. 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.

Pólitica
Resolución N° 116 de fecha del 05 de julio de 2023. Politica de Gobierno Digital y Seguridad Digital.

Recursos, Materiales, Insumos y Equipos

Recursos

- Proyectos de inversión: para fortalecer la seguridad y privacidad de la información, en los cuales se identifica el costo beneficio, riesgo y demás variables para la intervención financiera. El proceso de TI en los estudios, debe relacionar recursos financieros, humanos (dedicación horas/hombre) de sus colaboradores y en general de cualquier recurso que permita la adopción, implementación, mantenimiento y mejora continua del MSPI.
- Talento humano: implementación, seguimiento y control del MSPI.
- Recursos Financieros.

Equipos

- Hardware y/o software de seguridad de la Información.

Definiciones
Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
Activos de Información y recursos: 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.
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 dicho riesgo. (ISO/IEC 27000).
Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
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).
Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
Datos Personales Mixtos: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley

1581 de 2012, art 3 literal h)
Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales
Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
disposiciones.
Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).
Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).
Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Desarrollo

El modelo de seguridad y privacidad tiene en cuenta las siguientes fases para su gestión, las cuales se identifican en la fase de diagnóstico, planificación, operación, evaluación de desempeño y mejoramiento continuo.

Fuente: Anexo 1 Modelo de Seguridad y Privacidad de la información. Ministerio de Tecnologías de la Información.

En la cual se deben tener en cuenta distintos ámbitos o campos de acciones de la información, como es la ciberseguridad y la infraestructura tecnológica.

Fuente: Relación entre la ciberseguridad y otros ámbitos de la seguridad. Ministerio de Tecnologías de la Información.

FASE 1: Diagnóstico

Esta fase permite a la E.S.E Hospital Regional de Duitama, establecer el estado actual de la implementación de la seguridad y privacidad de la información, en el cual se utiliza el "instrumento de evaluación MSPI" con el que se identifica los controles implementados y faltantes y asi tener los insumos fundamentales para la fase de planificación.

El objetivo principal es identificar el nivel de madurez de seguridad y privacidad de la información en que se encuentra la entidad, teniendo en cuenta los aspectos internos como el talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional entre otros.

El futuro digital es de todos | Gobierno de Colombia MinTIC

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

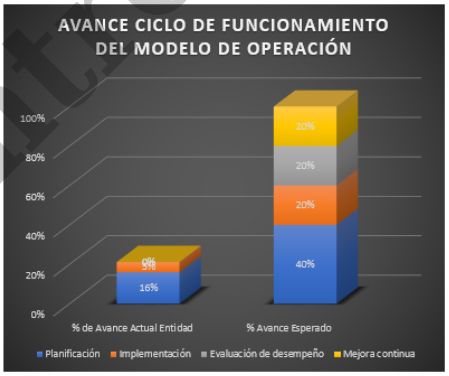
ENTIDAD EVALUADA	E.S.E. Hospital Regional de Duitama
FECHAS DE EVALUACIÓN	13/06/2023
CONTACTO	Cristian Eduardo Rincón Bosigas
ELABORADO POR	Cristian Eduardo Rincón Bosigas

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	26	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	23	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	17	100	INICIAL
A.9	CONTROL DE ACCESO	46	100	EFECTIVO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	60	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	60	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	51	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	46	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	43	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	60	100	EFECTIVO
A.18	CUMPLIMIENTO	43,5	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**43**	**100**	EFECTIVO

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	16%	40%
	Implementación	5%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
TOTAL		21%	100%



NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	INTERMEDIO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

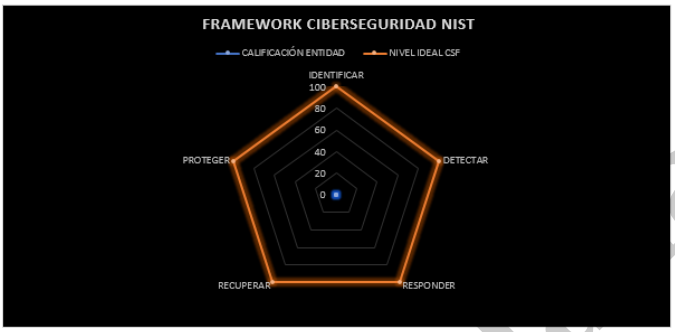
Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorias al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de f	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	0	100
DETECTAR	0	100
RESPONDER	0	100
RECUPERAR	0	100
PROTEGER	0	100

d



Planificación

Teniendo en cuenta el resultado de la fase anterior, el proceso de tecnologías de la información procede a la elaboración del Plan de Seguridad y Privacidad de la Información, en la cual se realiza la planeación del tiempo, recursos y presupuestos sobres las actividades a desarrollar relacionadas al MSPI.

En el cual se debe tener:

Documento	Estado	Soporte
Alcance MSPI	Realizado	MSPI
Acto administrativo con las funciones de seguridad y privacidad de la información.	Realizado	Resolución No. 194 de 2022.
Política de seguridad y privacidad de la información.	Realizado	Resolución No. 242 de 2020.
Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información	Realizado	MSPI
Procedimiento de inventario y Clasificación de la Información e infraestructura crítica	Realizado	MSPI
Metodología de inventario y clasificación de la información e infraestructura crítica	Realizado	MSPI
Procedimiento de gestión de riesgos de seguridad de la información	Realizado	MSPI
Plan de tratamiento de riesgos de seguridad de la información	Programado	
Declaración de aplicabilidad	Programado	Resolución No. 116 de 2023.
Manual de políticas de Seguridad de la Información	Sin Iniciar	
Plan de capacitación, sensibilización y comunicación de seguridad de la información	Programado	

1. **Contexto**

- ***Comprensión de la organización y de su contexto***

Se determinan los elementos externos e internos que son relevantes con las actividades que realiza la Entidad en el desarrollo de la misión, alineado con los objetivos estratégicos de la Entidad, teniendo en cuenta los aspectos relacionados en el Manual Operativo MIPG y el Plan de desarrollo institucional.

Como producto o salida, la entidad gestiono la Resolución No. 054 (de 17 de abril de 2023), por medio de la cual se adopta la política de planeación institucional en el marco de implementación del modelo integrado de planeación y gestión MIPG promovido por el gobierno nacional.

- ***Necesidades y expectativas de los interesados***

La necesidad de la entidad radica en tener procesos de seguridad, seguros y confiables, que garanticen la seguridad y privacidad de la información de los actores principales como los lideres institucionales, operadores internos, proveedores, entidades que se relacionan con la misión de la entidad, entre otros, ya que pueden verse afectados en caso de que la entidad se vea comprometida.

2. Liderazgo

- ***Liderazgo y compromiso***

La entidad incluyo dentro de las funciones del comité institucional de gestión y desempeño, aprobado por la Resolución No. 194 de 2022, por medio de la cual se ajusta la conformación del comité de gestión y desempeño y calidad de la E.S.E. Hospital Regional de Duitama, 6 funciones relacionadas con seguridad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI. Adicionalmente se contemplan las siguientes acciones:

- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la Entidad.
- Comunicar en la Entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI.

- ***Política de seguridad y privacidad de la información.***

La E.S.E Hospital Regional de Duitama, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes, en concordancia con la misión y visión de la entidad y los procesos establecidos para su operación. Para la E.S.E Hospital Regional de Duitama, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

La entidad gestiono la Resolución No. 242 de 2020 Política de Seguridad, Privacidad de la Información y Seguridad Digital, teniendo en cuenta:

- Misión de la Entidad
- Normatividad vigente.
- Compromisos del cumplimiento de los requisitos relacionados con la seguridad y privacidad de la información, así como también el de la mejora continua una vez el MSPI sea adoptado.
- Estar alineada con el contexto de la Entidad, así como la identificación de las áreas que hacen parte de la implementación de seguridad de la información.
- Roles y responsabilidades que se identifiquen.
- Comunicación al interior de la Entidad y a los interesados que aplica.

3. Planificación

- ***Identificación, gestión y clasificación de los activos de la información e infraestructura critica***

El proceso de Tecnologías de la Información en apoyo de los procesos institucionales debe identificar, gestionar y clasificar los activos de la información y la infraestructura critica de la entidad. Que para ello utiliza como insumo el índice de información clasificada y reservada de la entidad, en el cual tiene identificada la información importante de la entidad y es clasificada mediante confidencialidad, integridad y disponibilidad.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

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.

Clasificación de acuerdo a la confidencialidad: La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBCLCA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar 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.
INFORMACION 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 han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Clasificación de acuerdo a la integridad: La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

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.

Clasificación de acuerdo a la 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 el futuro, al igual que los recursos necesarios para su uso.

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.

Cuyo resultado se muestra en la siguiente imagen y en el archivo adjunto "Plantilla Registro de Activos de la Informacion e Información Clasificada y Reservada.xlsx" para los 145 activos de la información.

Nombre o titulo de la categoría de la Informaci	Nombre o titulo de la información	Idioma	Medio de conservación y/o soporte	Fecha de Generación de la Informaci	Nombre del Responsable de la Producción de la Informaci	Nombre del Responsable de la Informaci	Objetivo Legitimo de la Excepción	Fundamento Constitucional o Legal	Fundamento Jurídico de la Excepción	Excepción Parcial o Total	Fecha de la Calificación	Plazo de la Clasificación o Reserva
ACCIONES CONSTITUCIONALES	Acción de grupo	ES	Físico y Electrónico	Anual	Defensa Jurídica	Defensa Jurídica	publica reservada	LEY 1712 DE 2014 artículo 19 literal a) información exceptuada por daño de los intereses públicos, en concordancia con lo estipulado por el artículo 24 de la Ley 1437 de 2011 - Decreto 103 de 2015 artículo 28 " Pueda afectar la estabilidad de la economía o los mercados, la eficacia de la política macroeconómica y financiera o el cumplimiento de las funciones de las entidades que tienen a su cargo el diseño y la implementación de estas políticas"	Ley 1712 Artículo 18 literal a) Ley 1712 Artículo 19	Total	N/A	10 años
ACCIONES CONSTITUCIONALES	Acción de tutela	ES	Físico y Electrónico	Mensual	Defensa Jurídica	Defensa Jurídica	publica reservada	LEY 1712 DE 2014 artículo 19 literal a) información exceptuada por daño de los intereses públicos, en concordancia con lo estipulado por el artículo 24 de la Ley 1437 de 2011 - Decreto 103 de 2015 artículo 28 " Pueda afectar la estabilidad de la economía o los mercados, la eficacia de la política macroeconómica y financiera o el cumplimiento de las funciones de las entidades que tienen a su cargo el diseño y la implementación de estas políticas"	Ley 1712 Artículo 18 literal a) Ley 1712 Artículo 19	Total	N/A	10 años
ACCIONES CONSTITUCIONALES	Acción Popular	ES	Físico y Electrónico	trimestral	Defensa Jurídica	Defensa Jurídica	publica reservada	LEY 1712 DE 2014 artículo 19 literal a) información exceptuada por daño de los intereses públicos, en concordancia con lo estipulado por el artículo 24 de la Ley 1437 de 2011 - Decreto 103 de 2015 artículo 28 " Pueda afectar la estabilidad de la economía o los mercados, la eficacia de la política macroeconómica y financiera o el cumplimiento de las funciones de las entidades que tienen a su cargo el diseño y la implementación de estas políticas"	Ley 1712 Artículo 18 literal a) Ley 1712 Artículo 19	Total	N/A	10 años
								LEY 1712 DE 2014 artículo 19 literal a)				

Por otra parte, hace la identificación y valoración de la infraestructura critica de la entidad, la cual es registrada en el documento anexo “Identificación, gestión y clasificación de la infraestructura critica.xlsx”.

Id	Proceso	Nombre Activo	Descripción / Observaciones	Ubicación	Propietario	Tipo	Infraestructura Critica
1	Tecnologías de la Información	Bases de datos	Acceso a la información de las bases de datos mediante los motores de bases de datos.	Centro de Datos	Tecnologías de la Información / Proveedores Tecnológicos.	Información	Impacto Social
2	Tecnologías de la Información	Programas, políticas, planes, procedimientos y formatos.	Acceso a los Documentos que soportan la gestión del procesos de Tecnologías de la Información y guían al área para el cumplimiento de los objetivos.	Sistema de Información Almera	Tecnologías de la Información	Información	NO
3	Tecnologías de la Información	Servidores	Acceso a los equipos que tienen sistemas de información de la entidad.	Centros de Datos	Tecnologías de la Información	Hardware	Impacto Social
4	Tecnologías de la Información	Switch	Acceso a los equipos que controlan la red de datos institucional.	Centros de datos y en la entidad en general.	Tecnologías de la Información	Hardware	NO
5	Tecnologías de la Información	Computadores	Acceso a los equipos asignados para los usuarios de la entidad para la ejecución de actividades relacionadas con su contratación.	Procesos administrativos y asistenciales.	Tecnologías de la Información	Hardware	NO
6	Tecnologías de la Información	Impresoras	Acceso a los equipos para la impresión de historias clínicas y documentos que apoyan la gestión de los usuarios.	Procesos administrativos y asistenciales.	Tecnologías de la Información	Hardware	NO
7	Tecnologías de la Información	Teléfonos IP	Acceso a los equipos utilizados para la comunicación interna y externa de la entidad.	Procesos administrativos y asistenciales.	Tecnologías de la Información	Hardware	NO
8	Tecnologías de la Información	Scanner	Acceso a los equipos utilizados para copia o escanear documentos de la entidad.	Procesos administrativos.	Tecnologías de la Información	Hardware	NO
9	Tecnologías de la Información	Dinámica Gerencial Hospitalaria	Acceso a la información del sistema de Información Principal de la entidad, que contiene la información clínica de los pacientes y datos financieros de la entidad, que tiene un acceso controlado mediante usuarios, contraseñas y permisos.	Procesos administrativos y asistenciales.	Tecnologías de la Información	Software	Impacto Social
10	Tecnologías de la Información	MediSystem	Acceso a la información del sistema de Información que tiene las imágenes clínicas de los pacientes, cuyo acceso debe ser mejorado por un, **acceso controlado mediante usuarios, contraseñas**	Procesos Asistenciales.	Tecnologías de la Información / Proveedores Tecnológicos.	Software	Impacto Social
11	Tecnologías de la Información	Almera	Acceso a la información del sistema de Información de la gestión de calidad de la entidad, que tiene un acceso controlado mediante usuarios, contraseñas y	Procesos administrativos y asistenciales.	Tecnologías de la Información / Proveedores Tecnológicos.	Software	NO
12	Tecnologías de la Información	PACH	Acceso a la información del sistema de Información desarrollado por la entidad, que tiene un acceso controlado mediante usuarios, contraseñas y	Procesos administrativos y asistenciales.	Tecnologías de la Información	Software	NO
13	Tecnologías de la Información	Mipres.com	Acceso a la información del sistema de Información para realizar procesos asistenciales, que tiene un acceso controlado mediante usuarios, contraseñas y	Procesos Asistenciales.	Tecnologías de la Información / Proveedores Tecnológicos.	Software	NO
14	Tecnologías de la Información	Pagina WEB Institucional	Acceso a la información del sitio web de la entidad que contiene la información publica de la entidad, los tramites y servicios entre otros beneficios para el usuario interno y externo.	Centro de Datos	Tecnologías de la Información	Software	NO
15	Tecnologías de la Información	Almacenamiento en NAS	Acceso a la información de los equipos de almacenamiento interno que se habilita para usuarios específicos, que tiene un acceso controlado mediante usuarios, contraseñas y permisos.	Procesos Estratégicos	Tecnologías de la Información	Software	NO

16	Tecnologías de la Información	Red de datos	Acceso a la Red de datos institucional que comunica a los usuarios internos, con los servicios institucionales, sistemas de información y demás infraestructura física de la entidad.	Procesos administrativos y asistenciales.	Tecnologías de la Información	Servicios	NO
17	Tecnologías de la Información	Internet	Acceso a la Servicio de conectividad internet, habilitada para consulta de información y acceso a servicios institucionales.	Procesos administrativos y asistenciales.	Tecnologías de la Información / Proveedores Tecnológicos.	Servicios	NO
18	Tecnologías de la Información	Telefonía	Acceso a la Servicio de comunicaciones habilitado para la comunicación interna y externa de la entidad.	Procesos administrativos y asistenciales.	Tecnologías de la Información / Proveedores Tecnológicos.	Servicios	NO
19	Tecnologías de la Información	Correos electrónicos	Acceso a la Servicio tecnológico habilitado para usuarios específicos de la entidad, que permite la comunicación formal entre procesos y entes externos.	Procesos administrativos y asistenciales.	Tecnologías de la Información	Servicios	NO
20	Tecnologías de la Información	Sistema de audio	Servicio habilitado para la comunicación de códigos institucionales e información importante.	Procesos administrativos y asistenciales.	Tecnologías de la Información	Servicios	NO
21	Tecnologías de la Información	Lider del proceso de Tecnologías	Responsable del proceso de tecnologías de la Información.	Proceso de TI	Tecnologías de la Información	Recurso Humano	NO
22	Tecnologías de la Información	Administrador de la conectividad institucional	Encargado de los servicios de conectividad institucional que se relacionan a la red de datos, internet, telefonía, correos electrónicos y el sistema de	Proceso de TI	Tecnologías de la Información	Recurso Humano	NO
23	Tecnologías de la Información	Administrador de la seguridad institucional	Encargado de la seguridad institucional encargado de la configuración y administración de la seguridad institucional en relación a la seguridad perimetral UTM y seguridad interna ERD.	Proceso de TI	Tecnologías de la Información	Recurso Humano	NO
24	Tecnologías de la Información	Administrador de Sistemas de Información	Encargado de administrar los servidores, sistemas de información y parametrización de los mismos, en relación a DGH, MediSystem, PACH, Almera entre	Proceso de TI	Tecnologías de la Información	Recurso Humano	NO
25	Tecnologías de la Información	Apoyo técnico a la infraestructura	Encargado de intervenir la infraestructura física de tecnologías para garantizar un correcto funcionamiento de los sistemas de información y servicios institucionales.	Proceso de TI	Tecnologías de la Información	Recurso Humano	NO
26	Tecnologías de la Información	Proveedores	Encargados de proveer servicios tecnológicos de calidad, robustos y seguros acorde a las necesidades de la entidad.	Externo	Tecnologías de la Información	Recurso Humano	NO
27	Tecnologías de la Información	Centro de Cableado Principal	Acceso al Espacio principal de la entidad utilizado para instalar servidores, Switch y servicios complejos de tecnologías de la información.	Centro de Datos	Tecnologías de la Información	Instalaciones	NO
28	Tecnologías de la Información	Centros de cableado secundarios	Acceso al Espacio secundario para instalar servidores Backups, Switch y servicios complejos de tecnologías de la información.	Centros de datos secundarios	Tecnologías de la Información	Instalaciones	NO
29	Tecnologías de la Información	Seguridad Externa UTM	Acceso a la Seguridad principal de la entidad encargada de proteger la información y los servicios institucionales de ataques externos de la entidad.	Centro de Datos	Tecnologías de la Información	Infraestructura Crítica Cibernética	Impacto Social
30	Tecnologías de la Información	Seguridad Interna EDR	Acceso a la Seguridad principal de la entidad encargada de proteger la información y los servicios institucionales de ataques internos en la entidad.	Nube	Tecnologías de la Información	Infraestructura Crítica Cibernética	Impacto Social

Un activo es considerado infraestructura critica si su impacto o afectación podría superar alguno de los siguientes criterios:

- Impacto social (0.5%) de la Población Nacional: 250.000 Personas
- Impacto Económico PIB de un Día o 0.123% del PIB Anual: $ 464.619.736
- Impacto Ambiental: 3 años de recuperación.

- ***Riesgos inherentes de seguridad de la Información***

Para efectos del presente modelo se podrán identificar los siguientes (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Por lo cual es importante identificar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

TIPO	AMENAZA
Daño Físico	Fuego
	Agua
	Contaminación
	Destrucción del equipo o medios
	Polvo, Corrosión o congelamiento
Eventos naturales	Fenómenos climáticos, sísmicos o inundaciones.
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado.
	Perdida de suministro de energía.
Compromiso de la Información	Escucha encubierta
	Hurtos de medios o documentos
	Hurto de equipo.
	Recuperación de medios reciclados o desechados.
	Manipulación con hardware o software

Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento
Acciones no autorizadas	Uso no autorizado del equipo
	Corrupción de los datos
	Procesamiento ilegal de datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal

Amenazas dirigidas por el hombre:

FUENTE DE AMENAZA	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal.	Piratería Ingeniería Social Intrusión, accesos forzados al sistema Acceso no autorizado
Criminal de la computación	Crimen por computador Acto fraudulento Soborno de la información Suplantación de identidad. Intrusión en el sistema. Penetración en el sistema Manipulación en el sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Código malicioso Venta de información personal Errores en el sistema Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema.

Vulnerabilidades:

TIPO	VULNERABILIDAD
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla

Recurso Humano	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
Instalaciones	Uso inadecuado de los controles de acceso
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general

- **Identificación de los riesgos**

Segun la guia de la administración del riesgo de la función publica, se muestra un ejemplo para la identificación de los riesgos de seguridad de la información para la E.S.E Hospital Regional de Duitama.

Seleccionar las vulnerabilidades asociadas a la amenaza identificada

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

Que para efectos de la identificación de los riesgos, se utiliza el el sistema de información Almera para la identificación de los riesgos de Seguridad y Privacidad de la Información y su valoración.

Código	R-TI01
Riesgo	Posibilidad de afectación en la atención de los servicios de salud e interrupción en la ejecución de actividades administrativas.
Unidad de riesgo	Tecnologías de la información **(Riesgos Administrativos DAFP 2022)**
CONTEXTO DEL RIESGO	
Clase de riesgo	Riesgo de Gestión
Tipo de objetivo al que impacta	Estratégico
Objetivo(s)	Disponer de una infraestructura de hardware actualizada para servidores, switch y computadores con mantenimientos preventivos ejecutados y una buena gestión o intervención de mano de obra.
Áreas de impacto	Afectación Económica o Presupuestal
IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO	
Factor	Tecnología
Descripción	Perdida de Integridad
Clasificación del riesgo	Hardware
IDENTIFICACIÓN DEL RIESGO DE GESTIÓN	
¿Que? (Impacto)	CONSECUENCIA Lentitud en las estaciones de trabajo final. Pérdida de conexión de los sistemas de información a las estaciones de trabajo. Daño total o parcial de los equipos tecnológicos. Reprocesos en el registro de la información.
¿Como? (Causa Inmediata)	AMENAZA Polvo, Corrosión o congelamiento. Fallas en el sistema de suministro de agua o aire acondicionado. Pérdida de suministro de energía. Fallas del equipo. Mal funcionamiento del equipo. Mal funcionamiento del software. Saturación del sistema de información. Incumplimiento en el mantenimiento. Error en el uso.
¿Por qué? (Causa Raíz)	VULNERABILIDAD Ausencia de acuerdos de nivel de servicio (ANS o SLA). Ausencia del personal. Conexión deficiente de cableado y direccionamiento IP. Mantenimiento insuficiente. Ausencia de esquemas de reemplazo periódico. Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad). Falta de cuidado en la disposición final.

Código	R-TI02
Riesgo	Posibilidad de encriptación o secuestro de la información digital de las bases de datos de los sistemas de información y archivos de los equipos de cómputo.
Unidad de riesgo	Tecnologías de la información **(Riesgos Administrativos DAFP 2022)**
CONTEXTO DEL RIESGO	
Clase de riesgo	Riesgo de Gestión
Tipo de objetivo al que impacta	Estratégico
Objetivo(s)	Implementar una solución tecnológica de seguridad cibernética, para proteger los activos de la información e Infraestructura Tecnológica mediante un aliado estratégico con experiencia en ciberseguridad y una plataforma segura y confiable.
Áreas de impacto	Reputacional,Afectación Económica o Presupuestal
IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO	
Factor	Tecnología
Descripción	Perdida de Confidencialidad
Clasificación del riesgo	Infraestructura Critica Cibernética
IDENTIFICACIÓN DEL RIESGO DE GESTIÓN	
¿Que? (Impacto)	CONSECUENCIA: Pérdida total o parcial de la información de las bases de datos de los sistemas de información. Reprocesos en la ejecución de las actividades para la prestación de servicios de salud. Inoportunidad en la atención de los usuarios.
¿Como? (Causa Inmediata)	AMENAZA: Intrusión. Accesos no autorizado o forzado. Sabotaje. Código malicioso.
¿Por qué? (Causa Raíz)	VULNERABILIDAD: Ausencia de mecanismos de monitoreo para brechas en la seguridad. Ausencia de protección. Ausencia de políticas de uso aceptable. Falta de conciencia en seguridad. Entrenamiento insuficiente. Ausencia del personal. Contraseñas sin protección.

Código	R-TI03
Riesgo	Posibilidad de uso inadecuado del software e información digital institucional.
Unidad de riesgo	Tecnologías de la información **(Riesgos Administrativos DAFP 2022)**
CONTEXTO DEL RIESGO	
Clase de riesgo	Riesgo de Gestión
Tipo de objetivo al que impacta	Estratégico
Objetivo(s)	Hacer buen uso del software institucional para los fines designados en cada uno de los roles de la entidad mediante la actualización del software, gestión del conocimiento compartido y una correcta administración.
Áreas de impacto	Reputacional,Afectación Económica o Presupuestal
IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO	
Factor	Tecnología
Descripción	Perdida de Confidencialidad
Clasificación del riesgo	Sotfware
IDENTIFICACIÓN DEL RIESGO DE GESTIÓN	
¿Que? (Impacto)	CONSECUENCIA Vulneración de la seguridad y privacidad de la información del paciente. Afectación total parcial del software. Lentitud o mal funcionamiento del sistema. Agotamiento de los recursos de hardware de los sistemas de información.
¿Como? (Causa Inmediata)	AMENAZA Acceso no autorizado o intrusión en el sistema. Suplantación de identidad. Manipulación o sabotaje del sistema. Observar información reservada. Uso inadecuado del computador. Ingreso de datos falsos o corruptos Venta o publicación de información personal. Errores en el sistema
¿Por qué? (Causa Raíz)	VULNERABILIDAD Ausencia o insuficiencia de pruebas de software. Ausencia de terminación de sesión. Ausencia de registros de auditoría. Asignación errada de los derechos de acceso. Interfaz de usuario compleja. Fechas incorrectas. Contraseñas sin protección. Software nuevo o inmaduro. Entrenamiento insuficiente. Ausencia de procedimiento de registro/retiro de usuarios .

Código	R-TI04
Riesgo	Posibilidad de falla en los servicios tecnológicos de la red de datos, internet, telefonía y correos electrónicos.
Unidad de riesgo	Tecnologías de la información **(Riesgos Administrativos DAFP 2022)**
CONTEXTO DEL RIESGO	
Clase de riesgo	Riesgo de Gestión
Tipo de objetivo al que impacta	Proceso
Objetivo(s)	Garantizar el correcto funcionamiento de los servicios tecnológicos mediante configuraciones empresariales y asociaciones con proveedores tecnológicos con experiencia en su campo de acción.
Áreas de impacto	Reputacional,Afectación Económica o Presupuestal
IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO	
Factor	Tecnología
Descripción	Perdida de Disponibilidad
Clasificación del riesgo	Servicios
IDENTIFICACIÓN DEL RIESGO DE GESTIÓN	
¿Que? (Impacto)	CONSECUENCIA Desconexión de los equipos de uso final a los servicios tecnológicos institucionales. Incomunicación entre dependencias internas y entidades externas para las gestiones asistenciales y administrativas. Falla en los servicios y consulta de información externa que dependa de internet.
¿Como? (Causa Inmediata)	AMENAZA Manipulación en el sistema. Crimen por computador. Fraude. Errores en el sistema.
¿Por qué? (Causa Raíz)	VULNERABILIDAD Conexión deficiente de cableado. Proveedores tecnológicos sin experiencia en su campo y equipos obsoletos. Software nuevo o inmaduro. Mantenimiento insuficiente.

Código	R-TI05
Riesgo	Probabilidad de incidentes en los centros de datos de la entidad.
Unidad de riesgo	Tecnologías de la información **(Riesgos Administrativos DAFP 2022)**
CONTEXTO DEL RIESGO	
Clase de riesgo	Riesgo de Gestión
Tipo de objetivo al que impacta	Estratégico
Objetivo(s)	Controlar el acceso a los centros de cableado y acondicionar los mismos para evitar fallas en la infraestructura crítica tecnológica de la entidad.
Áreas de impacto	Reputacional,Afectación Económica o Presupuestal
IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO	
Factor	Tecnología
Descripción	Perdida de Disponibilidad
Clasificación del riesgo	Instalaciónes
IDENTIFICACIÓN DEL RIESGO DE GESTIÓN	
¿Que? (Impacto)	CONSECUENCIA Falla crítica en el hardware de los servicios tecnológicos y software institucional. Hurto, sabotaje o destrucción total del hardware contenido dentro de esta área. Interrupciones en el normal funcionamiento de los servicios tecnológicos y los sistemas de información en las estaciones finales.
¿Como? (Causa Inmediata)	AMENAZA Acceso no autorizado. Fraude y hurto. Fuego, agua, contaminación, polvo, corrosión o congelamiento. Fenómenos climáticos, sísmicos o inundaciones. Fallas en el sistema de suministro de agua o aire acondicionado. Pérdida de suministro de energía. Abuso de derechos.
¿Por qué? (Causa Raíz)	VULNERABILIDAD Uso inadecuado de los controles de acceso. Áreas susceptibles a inundación. Red eléctrica inestable. Ausencia de protección en puertas o ventanas. Ausencia de procedimiento de registro/retiro de usuarios . Ausencia de proceso para supervisión de derechos de acceso . Ausencia de procedimientos y/o de políticas en general. Falta de conciencia en seguridad.

Código	R-TI06
Riesgo	Posibilidad de alteración de información sensible debido a la manipulación de los sistemas de información por intereses de terceros o particulares
Unidad de riesgo	Tecnologías de la información **(Riesgos Administrativos DAFP 2022)**
	CONTEXTO DEL RIESGO
Clase de riesgo	Riesgo de Corrupción
Tipo de objetivo al que impacta	Estratégico
Objetivo(s)	Garantizar condiciones de seguridad y privacidad de la información en los aplicativos institucionales
Áreas de impacto	Reputacional,Afectación Económica o Presupuestal
	IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO
Factor	Tecnología
Descripción	Perdida de Integridad
Clasificación del riesgo	Recurso Humano
	IDENTIFICACIÓN DEL RIESGO DE GESTIÓN
¿Que? (Impacto)	CONSECUENCIA Pérdida de información institucional. Violación de la privacidad del usuario y la información. Alteración de datos.
¿Como? (Causa Inmediata)	AMENAZA Manipulación en el sistema. Acceso no autorizado o Intrusión en el sistema. Acto fraudulento. Observar información reservada. Ingreso de datos falsos o corruptos. Soborno de información.
¿Por qué? (Causa Raíz)	VULNERABILIDAD Favorecer intereses particulares. Falta de conciencia en seguridad. Ausencia de proceso para supervisión de derechos de acceso.

	Calificación del impacto
1. ¿Afectar al grupo de funcionarios del proceso?	Si
2. ¿Afectar el cumplimiento de metas y objetivos de la dependencia?	Si
3. ¿Afectar el cumplimiento de misión de la entidad?	Si
4. ¿Afecta el cumplimiento de la misión del sector al que pertenece la entidad?	Si
5. ¿Generar pérdida de confianza de la entidad, afectando su reputación?	Si
6. ¿Genera perdida de recursos económicos?	Si
7. ¿Afecta la generación de los productos o la prestación de los servicios?	No
8. ¿Dar lugar al detrimento de la calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?	No
9. ¿Generar pérdida de información de la entidad?	Si
10. ¿Generar intervención de os órganos de control, de la Fiscalía u otro entre?	Si
11. ¿Dar ligar a procesos sancionatorios?	Si
12. ¿Dar lugar a procesos disciplinarios?	Si
13. ¿Dar lugar a procesos fiscales?	Si
14. ¿Dar lugar a procesos penales?	Si
15. ¿Generar pérdida de credibilidad del sector?	Si
16. ¿Ocasionar lesiones físicas o pérdida de vidas humanas	No
17. ¿Afectar la imagen regional?	Si
18. ¿Afecta la imagen nacional?	Si
19. ¿Genera daño ambiental?	No
Cantidad de respuestas afirmativas	15

- **Valoración de riesgos**

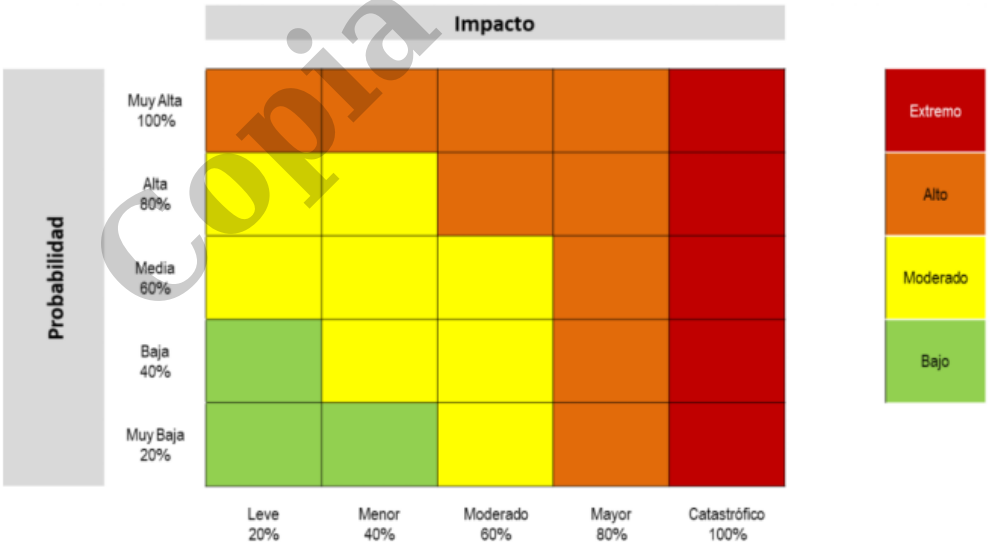
Se asocian las tablas de probabilidad e impacto definidas en la guia.

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Teniendo en cuenta que se puede tener una consecuencia, economica o reputacional que se genera por la materialización del riesgo.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

En la cual se aplica la matriz de calor



Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

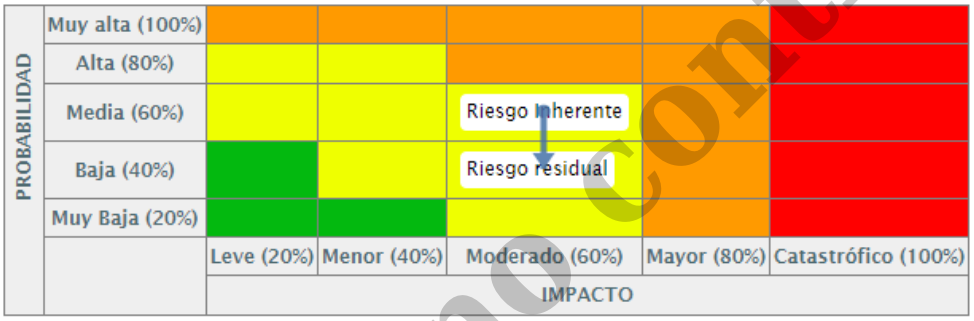
La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

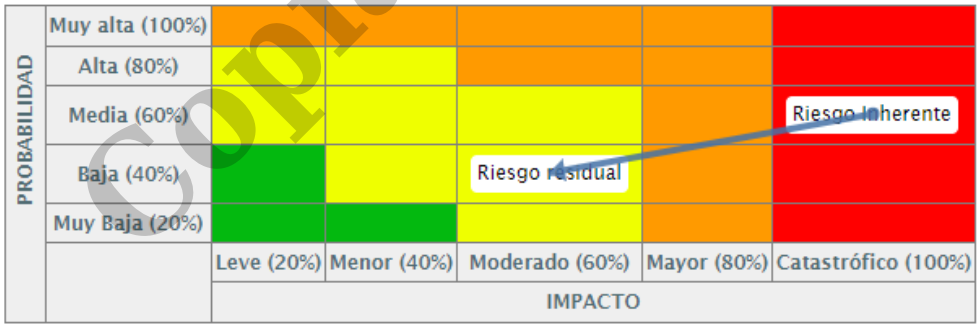
R-TI01

Evaluación

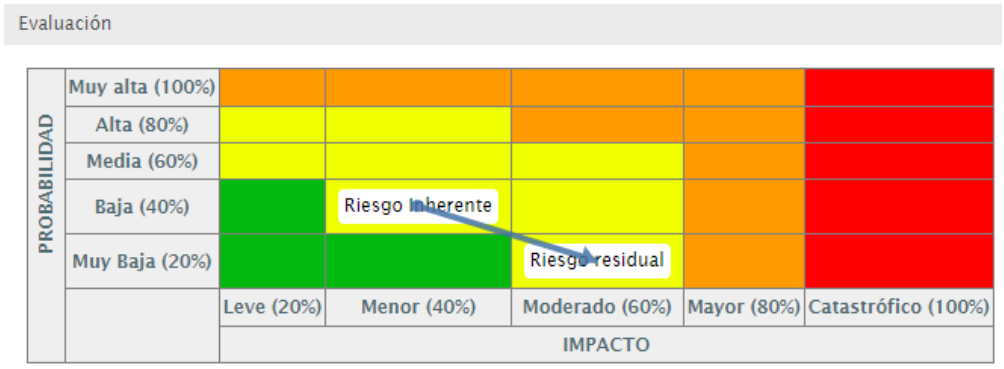


R-TI02

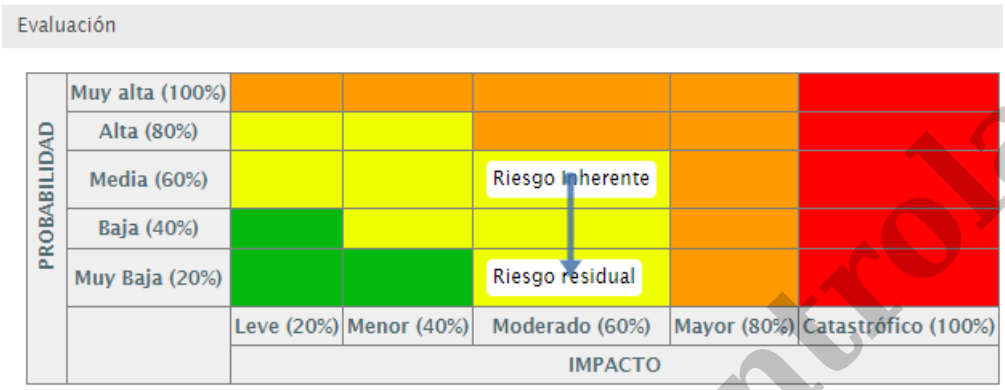
Evaluación



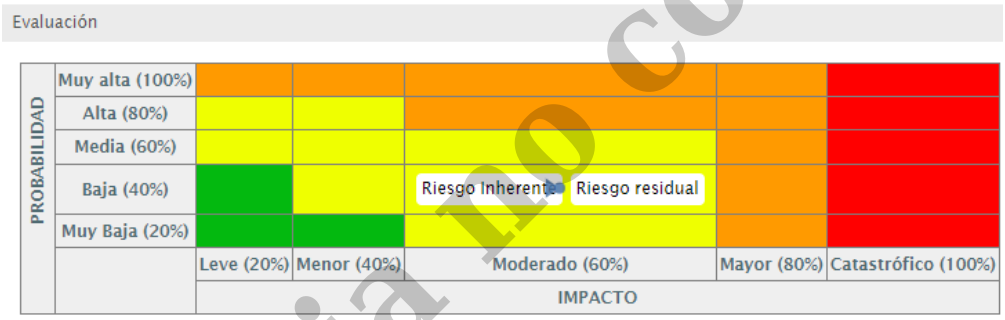
R-TI03



R-TI04



R-TI06



- ***Plan de Tratamiento de Riesgos de Seguridad de la Información***

Una vez definidos y valorados los riesgos, procede crear el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el cual es un documento aparte del presente Modelo de Seguridad y Privacidad. El cual se realiza bajo la estructura de la guía "Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5".

FASE 2: Operación

En esta fase el objetivo es la implementación de los controles, con el objetivo de dar cumplimiento a los requisititos del MSPI. En el cual se debe realizar el plan de implementación de controles de seguridad y privacidad de la información y tener en cuenta los siguientes lineamientos:

8.1 Planificación e implementación

Lineamiento: **La Entidad debe realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, esta información debe estar documentada por proceso según lo planificado. Estos documentos deben ser aprobados por el comité institucional** de gestión y desempeño.

Propósito: Implementar los planes y controles para lograr los objetivos del MSPI

Entradas recomendadas	Salidas
• 7.3.2 Valoración de los riesgos de seguridad de la **información** • Plan de 7.3.3 Plan de tratamiento de los riesgos de seguridad **de la información**	• Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto. • Evidencia de la implementación de los controles de seguridad y privacidad de la información.

FASE 3: Evaluación de Desempeño

Una vez culminada las actividades del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación:

9.1.1 Seguimiento, medición, análisis y evaluación

Lineamiento: Es importante que las Entidades conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo establece el MIPG. Es importante incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG.

Propósito: Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.

Entradas recomendadas	Salidas
• Documento con los resultados de la valoración de los riesgos • Documento con los resultados del tratamiento de riesgos de seguridad de la información • Resultado de la implementación de controles	• Hoja de vida de indicadores[3], los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el decreto 612 de 2018. • Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.

9.1.2 Auditoría Interna

Lineamiento: Realizar las auditorías internas con el fin de obtener información sobre el cumplimiento del MSPI.

Entradas recomendadas	Salidas
• Todos los documentos producto de las salidas de las fases anteriores del MSPI. • El informe de los resultados de las evaluaciones independientes, seguimientos y auditorías. • Informes y compromisos adquiridos en los comités institucional de gestión y desempeño.	• Resultados de las auditorías internas. • No conformidades de las auditorías internas. • Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, este plan debe estar aprobado por el Comité de Coordinación de Control Interno.

FASE 4: Mejoramiento Continuo

Una vez culminada las actividades del MSPI de la fase evaluación y desempeño, se debe consolidar los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

10.1 Mejora

Lineamiento: Es importante que las Entidades elaboren un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI.

Propósito: Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.

Entradas recomendadas	Salidas
• Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI. • Resultados de auditorías y revisiones independientes al MSPI.	• Plan anual de mejora del MSPI

Funciones de los Integrantes del Programa

Roles y responsabilidades asociadas a la seguridad y privacidad de la información

Responsable	Responsabilidad	Funciones
Lider de Implementación del MSPI.	Seguridad de la Información	• Fomentar la implementación de la Política de Gobierno Digital. • Asesorar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información para la entidad de conformidad con la regulación vigente. • Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad. • Realizar la estimación, planificación y cronograma de la implementación del MSPI. • Liderar la implementación y hacer seguimiento a las tareas y cronograma definido. • Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI. • Realizar el acompañamiento a los procesos y /o proyectos en materia de seguridad y privacidad de la información. • Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia. • Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información. • Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas. • Apoyar a los procesos de la Entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información. • Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad. • Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información. • Poner en conocimiento de las dependencias con competencia funcional, cuando se detecten irregularidades, incidentes o prácticas que atentes contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.
Comite de Gestión y Desempeño de la Entidad	Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información	• Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información. • Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad. • Aprobar acciones y mejores prácticas que en la implementación del MSPI. • Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información. • Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información
Oficina de Contratación y gestión juridica.		• Brindar asesoría a los procesos de la Entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los sujetos obligados, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso. • Representar a la Entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente
Gestión de Talento Humano		• Controlar y salvaguardar la información de datos personales del personal de planta de la Entidad, en concordancia con la normatividad vigente. • Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.
Directivos, Control Interno, Planeación Institucional y Gestión de Calidad.	Servicios Tecnologicos	• Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. • Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. • Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. • Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
	Estrategia TI	• Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. • Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
	Gobierno TI	• Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información
	Sistemas de Información	• Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
	De Información	• Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. • Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.
	Uso y Apropiación	• Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. • Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. • Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

Proceso de Tecnologias de la Información	Responsable del tratamiento de los datos personales.	• Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales. • Tramitar las consultas, solicitudes y reclamos. • Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran. • Respetar las condiciones de seguridad y privacidad de información del titular. • Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.
Equipo del Proyecto	Equipo del Proyecto	• Apoyar al líder de proyecto al interior de la entidad. • Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto. • Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura. • Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto. • Las que considere el líder del proyecto o el comité de seguridad de la entidad.

Socialización y Estrategias de Comunicación

Competencias, toma de conciencia y comunicación: El Plan de comunicación, capacitación, sensibilización y concientización está programado para su gestión en la vigencia 2023, el cual tiene el objetivo de incluir:

- Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información.
- Involucrar al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI.
- Concientizar a los funcionarios y partes interesadas en la importancia de la protección de la información.
- Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Se deberá definir qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo.

Bibliografía

- Ministerio de Tecnologias de la Información y comunicaciones. (Febrero 2021). Anexo 1. Modelo de Seguridad y Pirvacidad de la Información.
- Ministerior de Tecnologias de la Información y las Comunicaciones. (Junio 2021). Guia para la gestión y Clasificacion de Incidentes de Seguridad de la Información.
- Ministerior de Tecnologias de la Información y las Comunicaciones. (Octubre 2021). Documento maestro del Modelo de Seguridad y Privacidad de la Información. Modelo de Seguridad y Pirvacidad de la Información.
- Ministerior de Tecnologias de la Información y las Comunicaciones. (Octubre 2021). Indicadores de gestión de Seguridad de la Información. Modelo de Seguridad y Pirvacidad de la Información.
- Ministerior de Tecnologias de la Información y las Comunicaciones. (Octubre 2021). Inventario y Clasificación de Activos deInformación e Infraestructura Critica Cibernética Nacional. Modelo de Seguridad y Privacidad de la Información.
- Ministerior de Tecnologias de la Información y las Comunicaciones. (Octubre 2021). Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Publicas. Anexo Técnico.
- Ministerior de Tecnologias de la Información y las Comunicaciones. (Octubre 2021). Roles y Responsabilidades. Modelo de Seguridad y Pirvacidad de la Información.

Anexos

- Instrumento de Evaluación MSPI. Nivel de Madurez Modelo de Seguridad y Privacidad de la Información.xlsx
- Plantilla Registro de Activos de la Informacion e Información Clasificada y Reservada.xlsx
- Identificación, gestión y clasificación de la infraestructura critica.xlsx

Archivos adjuntos

- articles-150507_Instrumento_Evaluacion_MSPI.xlsx

- Identificación gestión y clasificación de la infraestructura critica.xlsx

- Plantilla Registro de Activos de la Informacion e Información Clasificada y Reservada.xlsx

- RESOLUCION N242-2020 Politica de Seguridad Privacidad de la Informacion y Seguridad Digital.pdf

- RESOLUCION N87-2020 Politica de Tratamiento y Proteccion de Datos Personales.pdf

Documentos asociados

Clase	Código	Nombre	Versión
Formato	HRD-PA-GI-TI-PG-01-FO-01	HRD-PA-GI-TI-PG-01-FO-01 ACUERDO DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN DE LA E.S.E HOSPITAL REGIONAL DE DUITAMA	1.0