MANUAL PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	ELABORADO POR	REVISADO POR	APROBADO POR
CARGO	LIDER DE GSTION DE LA INFORMACION	SUBGERENTE ADMINISTRATIVA	GERENTE
NOMBRE	EMERSON GONZALEZ	YANNETH LUCIA VILLAE	LIFAN MAURICIO CAMACHO.
FIRMA			
FECHA	23 DE DICIEMBRE DE 2020	23 DE DICIEMBRE 2020	29 DE DICIEMBRE 2020

CONTROL DE CAMBIOS		
VERSIÓN No	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO
00	29 DE DICIEMBRE DE 2020	NORMALIZACION DE MANUAL PLAN ESTRATEGICO DE SERGURIDAD Y PRIVACIDAD DE LA INFORMACION

INTRODUCCIÓN

La E.S.E Hospital Regional de Duitama en la resolución 242 de 03 de noviembre de 2020 estableció la política de seguridad, privacidad de la información y seguridad digital en la cual se ha 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 con lo cual reconoce la información como un activo importante para la atención de los pacientes y el desarrollo de sus procesos internos, lo que requiere definir lineamientos que permitan mitigar los posibles riesgos para la Información.

El plan de seguridad y privacidad de la información contiene los lineamientos que operativizan la gestión y administración de los planes y procedimientos de seguridad de la información estableciendo las prácticas de seguridad aplicadas en la institución.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Definir una estrategia de Seguridad de la información, en adelante PESI, liderada por la Oficina de Gestión de la Información a partir de la vigencia 2021 y hasta la vigencia 2024, que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información.

1.2 OBJETIVOS ESPECIFICOS

- Comunicar e implementar la Estrategia de seguridad de la información.
- Contribuir al incremento de la transparencia en la gestión pública.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MPSI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
- Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

2. ALCANCE

El PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN contempla la estructura de gobierno y los lineamientos principales para la seguridad de la información en la E.S.E Hospital regional de Duitama por lo cual los lineamientos definidos en este documento deben ser conocidos y cumplidos por empleados, contratistas, todos los terceros y partes interesadas que tengan acceso, almacenen, procesen o trasmitan información de la institución o sus pacientes.

3. DEFINICIONES

- **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).

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de información:** Los activos de información son el resultado de la construcción de un inventario y clasificación de los activos que posee la entidad de acuerdo con la Política General de Seguridad y Privacidad de la información, la cual determina que activos posee la entidad, cómo deben ser utilizados, así como los roles y responsabilidades que tienen los funcionarios sobre los mismos. 1 En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **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)
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **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).
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

[1] https://www.mintic.gov.co/portal/inicio/101640:10-6-Activos-de-informacion

- **Control:** Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal 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:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **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 debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **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 Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **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)
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **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).

- **Disponibilidad:** Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.
- **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)
- **Evento de seguridad de la información:** Es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.
- **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).
- **Guía:** Documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **Incidente de seguridad de la información:** Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.
- **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)
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **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.
- **Norma:** Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

- **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).
- **Parte interesada:** (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Propietario/responsable de activo de información:** Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
- **Política:** Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.
- **Procedimiento:** Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.
- **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. (ISO/IEC 27000).
- **Servicio:** Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de

actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **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).
- **Usuario:** Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
-

4. NORMATIVIDAD RELACIONADA

Para la construcción de este plan se tiene como base, la norma ISO – IEC 27001:2013 Sistema de Gestión de la Seguridad de la Información y la resolución 242 de 3 de noviembre de 2020 y Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL.

5. COMPROMISO DE LA DIRECCIÓN

La Junta Directiva y Alta Dirección de la E.S.E Hospital Regional de Duitama muestra su compromiso y apoyo en el diseño, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información a través de la asignación de recursos, los lineamientos de seguridad y el establecimiento del Gobierno de seguridad, cuya conformación y responsabilidades se describen a continuación.

6. ESTRUCTURA ORGANIZACIONAL

Conforme a lo establecido en el decreto ordenanzal No. 1525 de 27 de diciembre de 2005, la ESE Hospital Regional de Duitama cuenta con una estructura organizacional que incluye tres áreas a saber:

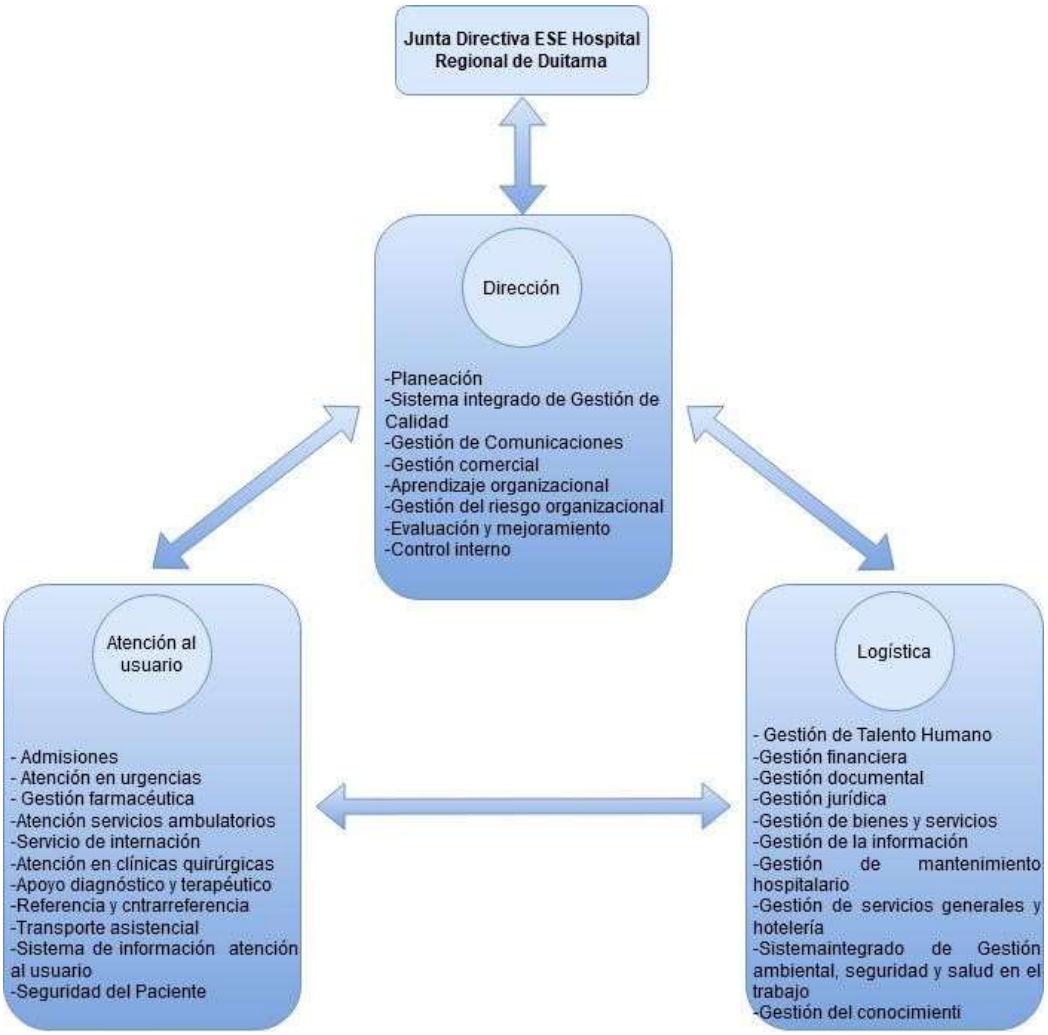
•Dirección: Su propósito principal es mantener la unidad de objetivos e interés de la organización en torno a la misión y objetivos institucionales. Esta área tiene a su cargo las

funciones de planeación, Sistema Integrado de Gestión de la Calidad – SIGC, gestión de comunicaciones, gestión comercial, aprendizaje organizacional, gestión del riesgo organizacional, evaluación y mejoramiento y control interno.

•Atención al usuario: Área conformada por todas las unidades orgánico-funcionales encargadas de todo el proceso de producción y prestación de servicios de salud. Tiene a su cargo las funciones de: Admisiones, atención en urgencias, gestión farmacéutica, atención en servicios ambulatorios, atención en servicio de internación, atención en clínicas quirúrgicas, apoyo diagnóstico y terapéutico, referencia y contrarreferencia, transporte asistencial, sistema de información y atención al usuario y la seguridad del paciente.

•Logística: Tiene como funciones la gestión del talento humano, gestión financiera, gestión, documental, gestión jurídica, gestión de bienes y servicios, gestión de la información, gestión de mantenimiento hospitalario, gestión de servicios generales y hotelería, gestión del sistema integral de gestión ambiental, salud y seguridad en el trabajo y gestión del conocimiento

Con base en la estructura organizacional y las funciones de cada área, se adopta como estructura organizacional básica la siguiente:



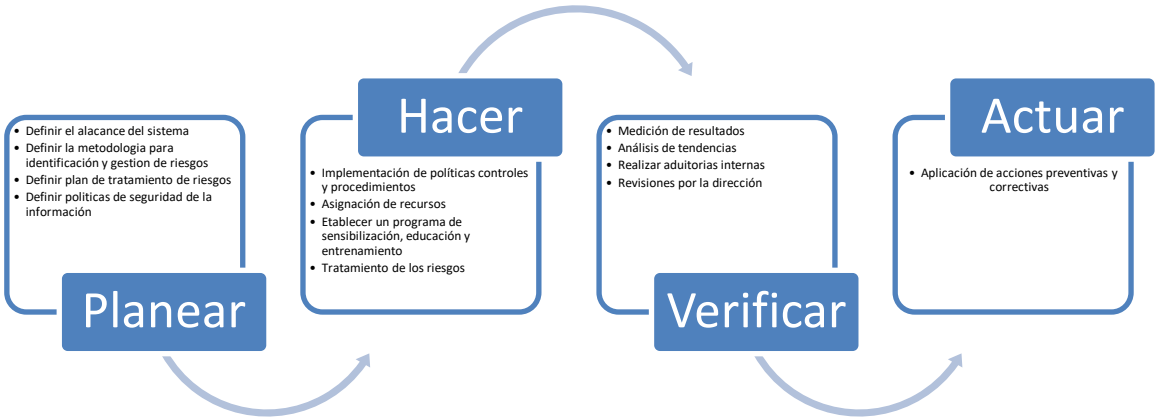
El organigrama vigente data del 2004, año en el que se suscribió el programa de reorganización y rediseño de la red pública de hospitales el cual se formalizó mediante la suscripción del convenio 0386 de diciembre de 2004 entre el Ministerio de Hacienda, Ministerio de la Protección Gobernación de Boyacá y la ESE Hospital regional de Duitama. En esta ocasión se suprimieron 154 empleos públicos y 50 de trabajadores oficiales.

El último plan de cargos aprobado es el que se encuentra previsto en el Acuerdo 11 del 22 de noviembre de 2019, en el cual se contempla una planta global con 59 cargos. En la actualidad

se cuenta con estudio de formalización laboral, en el cual se plantean diferentes fases para la vinculación progresiva del personal misional.

7. PLANEACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

El modelo del Sistema de Gestión de Seguridad de la Información (SGSI) de la E.S.E Hospital Regional de Duitama se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, verificar y actuar), el cual asegura que el SGSI esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo de mejoramiento continuo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.



7.1 Situación actual

Por situación actual se entiende el nivel de madurez que posee en este momento La E.S.E Hospital Regional de Duitama con relación a la seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina Instrumento de diagnóstico del MSPI de Mintic. Para poder realizar el PESI es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios con el fin de plantear prioridades sobre su implementación.

Diagrama radar por dominio

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	**INICIAL**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	20	100	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	20	100	**INICIAL**
A.8	GESTIÓN DE ACTIVOS	20	100	**INICIAL**
A.9	CONTROL DE ACCESO	20	100	**INICIAL**
A.10	CRIPTOGRAFÍA	20	100	**INICIAL**

A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	20	100	**INICIAL**
A.12	SEGURIDAD DE LAS OPERACIONES	20	100	**INICIAL**
A.13	SEGURIDAD DE LAS COMUNICACIONES	20	100	**INICIAL**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	20	100	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	20	100	**INICIAL**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	**INICIAL**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	**INICIAL**
A.18	CUMPLIMIENTO	20	100	**INICIAL**
PROMEDIO EVALUACIÓN DE CONTROLES		**20**	**100**	**INICIAL**

Resultados obtenidos por dominio

Al realizar la interpretación de los resultados obtenidos por la institución no alcanza el nivel inicial.

El avance del funcionamiento del ciclo PHVA muestra los siguientes resultados:

Año	**AVANCE PHVA**		
	COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
2020	Planificación	3%	40%
	Implementación	1%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
TOTAL		**4%**	**100%**

Por lo anterior se puede concluir que se observa una importante oportunidad de mejora frente a la implementación de la politica de seguridad y el plan estrategico de seguridad de la información basado en la norma ISO/IEC 27001:2013, por locual se hace necesario avancer en la construcción e implementación de un proyecto que permita establecer el sistema de gestión de la seguridad de la información para la entidad.

7.2 Análisis y priorización de iniciativas

La E.S.E Hospital regional de Duitama luego de analizar los resultados anteriores ha identificado las siguientes iniciativas buscando garantizar el avance de la institución en la construcción de una arquitectura de seguridad de la información.

Iniciativas	Descripción	Estrategia de Seguridad de la información			
		Modelo de seguridad de la información	**Gestión de riesgos de seguridad**	**Desarrollo y gestión del programa de seguridad de la información**	**Gestión de incidentes de seguridad de la información**
1	Documentar, Implementar, evaluar y mejorar el Plan estratégico de seguridad de la información	X			
2	Definir e integrar la seguridad de la información en los procesos institucionales buscando asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proceso	X			
3	Diseñar, documentar, implementar, evaluar y mejorar un programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores,	X			

	empleados, terceros y partes interesadas				
4	Actualizar los activos de información y realizar su valoración por criticidad para la entidad e identificar los riesgos de seguridad de la información asociados		X		
5	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.		X		
6	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad		X		
7	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes de continuidad por la alta dirección.		X		
8	Implementar arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core			X	
9	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger			X	

	la confidencialidad de la información.				
10	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.			X	
11	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.			X	
12	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web			X	
13	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la entidad.			X	
14	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información	X			

7.3 Definición del portafolio de proyectos

En esta etapa, después del análisis y priorización de iniciativas, se define el portafolio de proyectos del plan estratégico PESI, agrupados en proyectos relacionados con:

- Gobierno o modelo de seguridad de información.
- Gestión de riesgos de Seguridad.
- Desarrollo y gestión del plan de seguridad de la información.
- Gestión de incidentes de seguridad de la información.

Proyectos	Iniciativa	Proyectos		
		Descripción	**Avances**	**Requiere recursos financieros**
1	Documentar, Implementar, evaluar y mejorar el Plan estratégico de seguridad de la información	Implementar, evaluar y mejorar el Plan estratégico de seguridad de la información	En proceso	SI
2	Definir e integrar la seguridad de la información en los procesos institucionales buscando asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proceso	Integrar la seguridad de la información en los procesos institucionales	No iniciado	No
3	Diseñar, documentar, implementar, evaluar y mejorar un programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido	Diseñar y documentar programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores,	No iniciado	SI

	a los colaboradores, empleados, terceros y partes interesadas	empleados, terceros y partes interesadas		
		Implementar y evaluar el programa anual de capacitación y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas	No iniciado	SI
4	Actualizar los activos de información y realizar su valoración por criticidad para la entidad e identificar los riesgos de seguridad de la información asociados	Actualizar la matriz de activos de información y publicaciones por criticidad para la entidad e identificar los riesgos de seguridad de la información asociados	En proceso	No
5	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.	No iniciado	No
6	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad	No iniciado	No
7	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes	No iniciado	No

	de continuidad por la alta dirección.	de continuidad por la alta dirección.		
8	Implementar arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core	Gestionar la adquisición de herramientas para soportar la infraestructura del Datacenter, en esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.	No iniciado	SI
9	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.	No iniciado	NO
10	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que	No iniciado	NO

	requieren el uso de privilegios.	requieren el uso de privilegios.		
11	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.	No iniciado	NO
12	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web	No iniciado	NO
13	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la entidad.	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la entidad.	No iniciado	NO
14	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información	No iniciado	NO

7.4 Priorización de los proyectos

Priorización de los Proyectos

	Descripción	Prioridad (0) Año 2021	Prioridad (1) Año 2022	Prioridad (2) Año 2023	Prioridad (3) Año 2024
1	Implementar, evaluar y mejorar el Plan estratégico de seguridad de la información	X			
2	Integrar la seguridad de la información en los procesos institucionales	X			
3	Diseñar y documentar programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas		X		
	Implementar y evaluar el programa anual de capacitación y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas		X		
4	Actualizar la matriz de activos de información y publicaciones por criticidad para la entidad e	X			

	identificar los riesgos de seguridad de la información asociados				
5	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.		X		
6	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad		X		
7	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes de continuidad por la alta dirección.		X		
8	Gestionar la adquisición de herramientas para soportar la infraestructura del Datacenter, en esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de	X			

	comunicaciones Core.				
9	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.		X		
10	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.			X	
11	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios			X	

	privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.				
12	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web	X			
13	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la entidad.	X	X	X	X
14	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información	X			

El plan estratégico corresponde a la ejecución de los proyectos definidos en el portafolio de proyectos de seguridad de la información que aportan al cumplimiento de los objetivos de seguridad de la información y al Plan Estratégico de las Tecnologías de la Información y Comunicaciones PETI