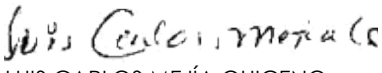
PLAN ESTRATEGICO DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE SISTEMA DE INFORMACIÓN Y GESTIÓN DOCUMENTAL

Documento integral que guía las acciones de una organización para proteger sus activos de información y mantener la confidencialidad, integridad y disponibilidad de los mismos.

Elaboro/Modificó:	Revisó:	Aprobó:
 ALEXANDER CASTAÑO BEDOYA Cargo: Analista de Sistemas	 CESAR VARGAS CARVAJAL Cargo: Jefe de Sistemas	 LUIS CARLOS MEJÍA QUICENO Cargo: Gerente
Fecha: Enero de 2024	Fecha: Enero de 2024	Fecha: Enero de 2024

CONTROL DE CAMBIOS

FECHA	ELABORÓ MODIFICÓ	REVISÓ	APROBÓ	CAMBIOS
Creación Enero de 2024	Alexander Castaño Bedoya	Cesar Vargas Carvajal	Luis Carlos Mejía Quiceno	Creación

Tabla de contenido

INTRODUCCIÓN

El Hospital San Juan de Dios E.S.E. Rionegro, a través de su Sistema de Gestión de Seguridad de la Información (SGSI), el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno en Línea (GEL) y teniendo en cuenta que la información es inherente a la misión de las instituciones y su correcta gestión debe apoyarse en tres atributos fundamentales:

- ✓ Confidencialidad: la información debe ser sólo accesible a sus destinatarios predeterminados.
- ✓ Integridad: la información debe ser correcta y completa.
- ✓ Disponibilidad: la información debe estar disponible en el momento y lugar que se requiera.

El plan general de seguridad de la información busca brindar seguridad, entendiéndola como la preservación de la confidencialidad, integridad y disponibilidad

Dichos atributos serán aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación de la ESE, por tal motivo, deberán ser conocidos y cumplidos por todo el recurso humano (servidores públicos, proveedores y terceros), que accedan a los sistemas de información e instalaciones físicas de la Institución.

OBJETIVOS

Objetivo General

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2024-2027, que debe seguir todo el personal del Hospital San Juan de Dios E.S.E. Rionegro.

Objetivos específicos

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la

• • •

Información. Definir un marco de referencia para direccionar el actuar del personal en el desarrollo de sus actividades, con miras a unificar la forma de realizar las tareas, propendiendo por el aumento de la productividad y la aplicación de las mejores prácticas de T.I.

- Mantener la confiabilidad, disponibilidad e integridad de la información, así como facilitar el mejor aprovechamiento de los recursos informáticos y las telecomunicaciones, que son propiedad o se encuentran a disposición del Hospital, para alcanzar la misión institucional.
- Utilizar los recursos tecnológicos de información y comunicación en forma responsable y apropiada, de conformidad con las disposiciones dadas en este documento y otras de carácter institucional, legal o emitido por otros órganos del Estado, que guarden relación con normativas aplicables a la materia.
- Minimizar las interrupciones de los servicios asociadas a los sistemas informáticos y comunicaciones, ocasionados por uso inapropiado o por daños causados en forma accidental o intencional.
- Adquirir tecnología acorde a las necesidades institucionales aprovechando al máximo las capacidades de los funcionarios y el presupuesto asignado para esta materia.
- Definir las directrices a seguir de los planes de contingencia referente a los eventos adversos.

MARCO LEGAL

- 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", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Resolución Institucional 189 de 2018
- Plan Estratégico de Tecnologías de Información institucional (PETI) vigente.

ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la entidad. Los lineamientos contenidos en el presente documento son de observancia obligatoria para todo el personal que labore en, o para, el Hospital, que por sus funciones tenga acceso a equipos de cómputo, sistemas y aplicaciones, bases de datos, instalaciones del centro de cómputo y en general, a todos los recursos informáticos de la organización.

Establecer un marco de gobierno para que el uso de las TIC de la institución, logre satisfacer las necesidades actuales y futuras derivadas de la estrategia de la Entidad, siguiendo los criterios de innovación, calidad, eficiencia, escalabilidad, y de arquitectura empresarial. Estas políticas son aplicables a todos los colaboradores, consultores, contratistas, terceras partes, que usen las tecnologías de información y la comunicación de la organización.

JUSTIFICACIÓN

El Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea, se encuentran basados, en el marco de lo establecido, en la norma internacional NTC-ISO-IEC 27001:2013 y las buenas prácticas contenidas en el componente Seguridad y Privacidad de la Información, de la estrategia GEL, este último desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia.

La norma ISO 27005:2011 es un estándar diseñado para la gestión de la seguridad de la información que contiene diferentes procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera.

Este plan de riesgos busca reducir las pérdidas de información y brindar protección de la misma, permitiendo conocer las debilidades que afectan, no solo en la prestación del servicio si no posterior a este durante la administración de la información recolectada.

DEFINICIONES

- ✓ **Activo:** 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).
- ✓ **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- ✓ **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- ✓ **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.
- ✓ **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- ✓ **Guía:** documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- ✓ **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- ✓ **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.
- ✓ **Parte interesada:** (Stakeholder) Persona u organización que puede afectar a, ser afectada por percibirse a sí misma como afectada por una decisión o actividad.
- ✓ **Política del SGSI:** Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la 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.
- ✓ **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).
- ✓ **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).

INFORMACIÓN GENERAL DE LA INSTITUCIÓN

El Hospital San Juan de Dios E.S.E. Rionegro es una entidad pública que en coherencia con su naturaleza y las diferentes normas que lo regulan da cumplimiento a los requerimientos de los entes de control.

La Alta Dirección de del Hospital San Juan de Dios E.S.E. Rionegro se compromete a la implantación, mantenimiento y mejora del SGSI, y el MSPI de GEL (Gobierno en Línea), dotándolos de aquellos medios y recursos que sean necesarios e instando a todos los empleados, proveedores y partes interesadas, para que asuman este compromiso. Para ello, el Hospital San Juan de Dios E.S.E. Rionegro implantará las medidas requeridas para la formación y concientización de los servidores públicos, proveedores y partes interesadas, en temas de seguridad de la información.

A su vez, cuando exista una violación de las políticas de seguridad de la información, la gerencia se reserva el derecho de aplicar las medidas disciplinarias, acordes a los compromisos laborales de los empleados públicos, proveedores y partes interesadas, dentro del marco legal aplicable y dimensionadas al impacto que tengan sobre el Hospital San Juan de Dios E.S.E. Rionegro.

La responsabilidad general de la seguridad de la información en el Hospital San Juan de Dios E.S.E. Rionegro recaerá sobre gerencia, subgerente administrativo y financiero, líder del área de sistemas y Analistas de Sistemas. Por otro lado, todos los empleados públicos, proveedores y partes interesadas, tendrán la obligación de reportar los incidentes, en materia de seguridad, haciendo uso de las directrices establecidas por el Hospital San Juan de Dios E.S.E. Rionegro.

CONTENIDO

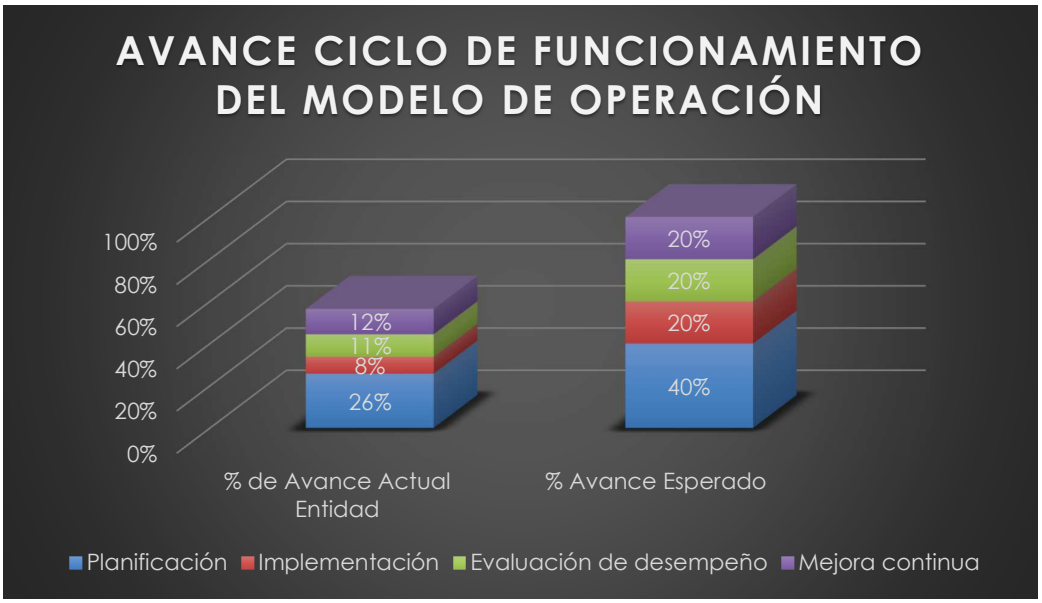
Estado actual de la entidad respecto al sistema de gestión de seguridad de la información

Entidad Evaluada	HOSPITAL SAN JUAN DE DIOS E.S.E RIONEGRO
Fechas de Evaluación	09/01/2024
Contacto	ING. CESAR ANDRES VARGAS CARVAJAL
Elaborado Por	ING. ALEXANDER DE JESUS CASTAÑO BEDOYA

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES

N°	Dominio	Calificación Actual	Calificación Objetivo	Evaluación de Efectividad de control
A.5	Políticas de seguridad de la información	50	100	**EFECTIVO**
A.6	Organización de la seguridad de la información	44	100	**EFECTIVO**
A.7	Seguridad de los recursos humanos	61	100	**GESTIONADO**
A.8	Gestión de activos	63	100	**GESTIONADO**
A.9	Control de acceso	68	100	**GESTIONADO**
A.10	Criptografía	20	100	**INICIAL**
A.11	Seguridad física y del entorno	66	100	**GESTIONADO**
A.12	Seguridad de las operaciones	64	100	**GESTIONADO**
A.13	Seguridad de las comunicaciones	70	100	**GESTIONADO**
A.14	Adquisición, desarrollo y mantenimiento de sistemas	56	100	**EFECTIVO**
A.15	Relaciones con los proveedores	80	100	**GESTIONADO**
A.16	Gestión de incidentes de seguridad de la información	34	100	**REPETIBLE**
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	60	100	**EFECTIVO**
A.18	Cumplimiento	60	100	**EFECTIVO**
Promedio evaluación de controles		57	100	**EFECTIVO**

AVANCE PHVA		
Componente	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	26%	40%
Implementación	8%	20%
Evaluación de desempeño	11%	20%
Mejora continua	12%	20%
Total	**56%**	**100%**



NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	SUFICIENTE
Definido	SUFICIENTE
Administrado	INTERMEDIO
Optimizado	CRÍTICO

Estrategia de seguridad digital

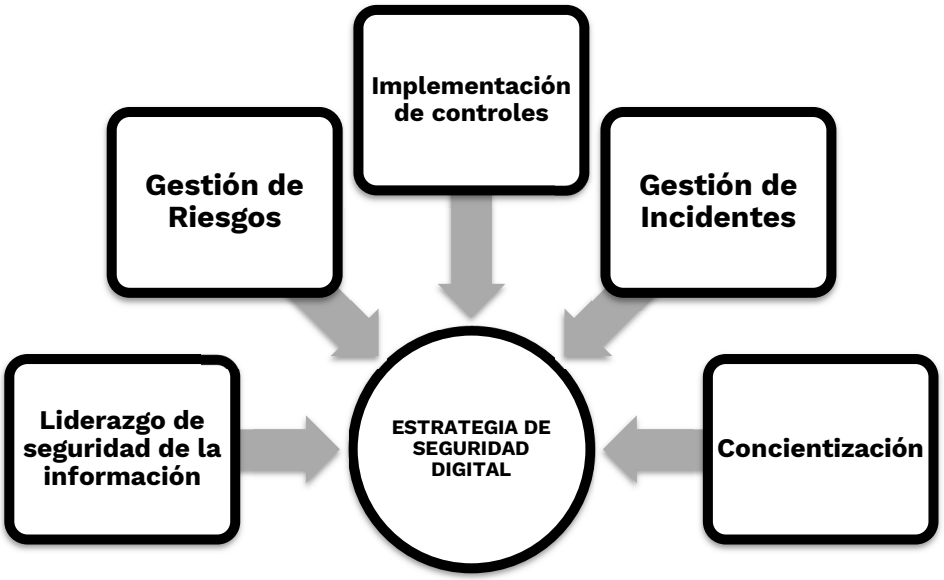
LA ENTIDAD establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y

• • •

Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse acorde a la Resolución 500 de 2021 MINTIC.

Por tal motivo, ***EL HOSPITAL SAN JUAN DE DIOS ESE RIONEGRO*** define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

Nota: Es fundamental que las entidades hagan la lectura de la resolución 500 de 2021 y del Anexo 1, que contiene la actualización del Modelo de Seguridad y Privacidad de la Información.



Descripción de las estrategias específicas (ejes)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.

• • •

Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

Portafolio de proyectos / actividades

Para cada estrategia específica, **EL HOSPITAL SAN JUAN DE DIOS ESE RIONEGRO** define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	PROYECTO 1: Desarrollar e implementar una política de seguridad PROYECTO 2: Definición de Roles y Responsabilidades de Seguridad de la Información.	Política de Seguridad Formalizada e Implementada. Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad.
Gestión de Riesgos	PROYECTO 1: Identificar, valorar y clasificar los riesgos asociados a los activos de información PROYECTO 2: Definir planes de tratamiento de riesgos de seguridad	Matriz de riesgos de seguridad digital Definir planes de tratamiento de riesgos

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Concientización	PROYECTO 1: Establecer desde el inicio de cada año la planeación de sensibilización para todo el año. PROYECTO 2: Realizar jornadas de sensibilización a todo el personal. PROYECTO 3: Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas. PROYECTO 4: Medir el grado de sensibilización a toda la Entidad.	1. Plan de Sensibilización 2. Evidencias de las actividades desarrolladas 3. Certificaciones de cursos 4. Resultado de las encuestas de medición
Implementación de controles	CONTROL 1 Política de respaldos de información. CONTROL 2 Procedimiento de Gestión de Cambios. CONTROL 3 Clasificación de la información. CONTROL 4 Políticas de Desarrollo Seguro	Política de respaldos de información. Procedimiento de Gestión de Cambios. Clasificación de la información. Políticas de Desarrollo Seguro
Gestión de incidentes	**PROYECTO 1:** Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. **PROYECTO 2:** Capacitar al personal en la gestión de incidentes de seguridad de la información.	1. Procedimiento de gestión de incidentes de seguridad formalizado. 2. Sesiones de capacitación desarrolladas.

• • •

Cronograma de actividades / proyectos

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

AÑO 2024				**AÑO 2025**	
TRIMESTRE 1	**TRIMESTRE 2**	**TRIMESTRE 3**	**TRIMESTRE 4**	**TRIMESTRE 1**	**TRIMESTRE 2**
Realizar diagnóstico seguridad y privacidad		Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.	Capacitar al personal en la gestión de incidentes de seguridad de la información.	Actualización Diagnóstico de Seguridad	Adoptar medidas correctivas y de control que reduzcan los riesgos hallados.
Identificación de activos procesos misionales	Implementación de solución WAF		Gestión de Riesgos de Seguridad	Adquisición e Implementación IPS	
Desarrollo Plan de Sensibilización 2024	Adquisición e implementación Sistema de Análisis de Vulnerabilidades			Desarrollo Sensibilización 2025	Implementación Estrategias de Capacitación en Seguridad

Nota: Al finalizar cada vigencia, EL HOSPITAL SAN JUAN DE DIOS ESE RIONEGRO, realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

• • •

Análisis presupuestal

Para este punto se tomará como referencia el presupuesto vigente para el área de sistemas del HOSPITAL SAN JUAN DE DIOS ESE RIONEGRO

DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- ✓ 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", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- ✓ Resolución 500 de 2021. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
- ✓ Manual de Gobierno Digital – MINTIC.
- ✓ Modelo de Seguridad y Privacidad de la Información – MINTIC.