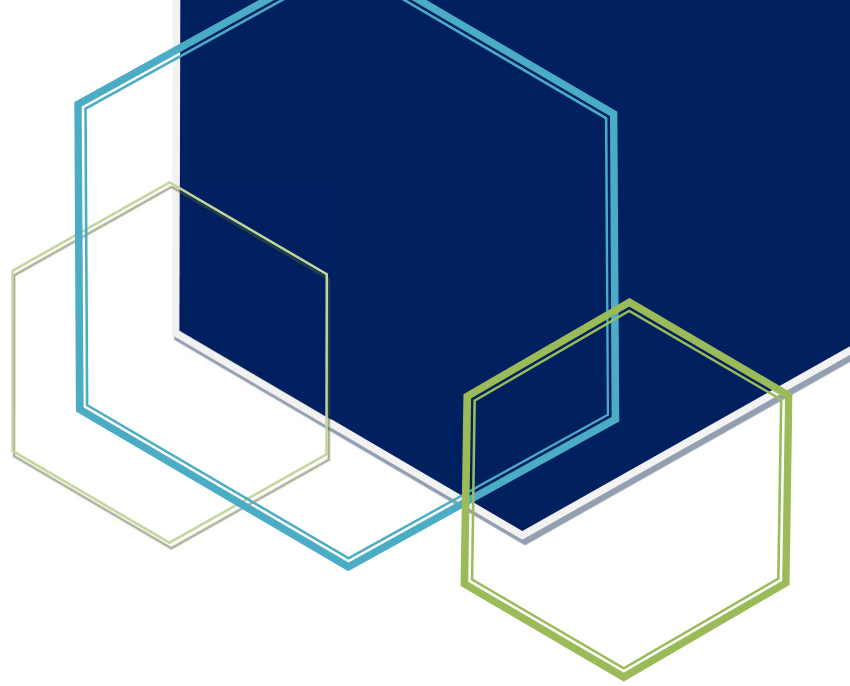
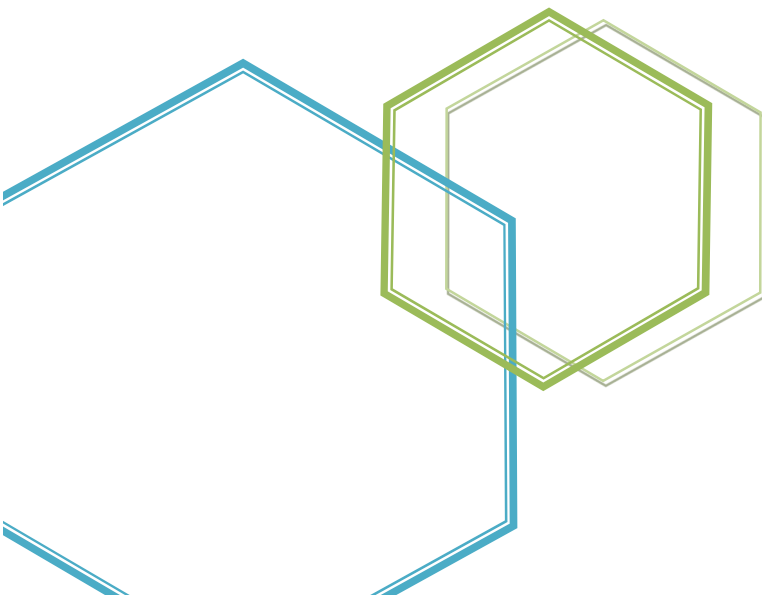




PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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.



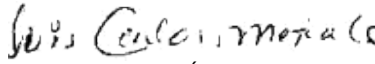


PROCESO DE SISTEMA DE INFORMACIÓN Y GESTIÓN DOCUMENTAL

PLAN DE TRATAMIENTO RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN 01

Código
LPA0203004

...

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

CONTROL DE CAMBIOS

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



• • •

Tabla de contenido

INTRODUCCIÓN	3
OBJETIVOS	5
MARCO LEGAL.....	6
ALCANCE	7
JUSTIFICACIÓN	7
DEFINICIONES	8
INFORMACIÓN GENERAL DE LA INSTITUCIÓN	12
CONTENIDO	13
Diagnóstico.....	13
Planificación	14
Fase 2: Operación.....	14
Fase 3: Evaluación de desempeño	15
Fase 4: Mejoramiento continuo	15
ANEXOS	15
Controles y objetivos de control.....	15
Declaración de Aplicabilidad	26
Formatos.....	27

INTRODUCCIÓN

El Hospital San Juan de Dios ESE Rionegro es consecuente con la realidad de que las entidades públicas están cada vez más expuestas a sufrir incidentes de seguridad digital, por lo que puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía. Razón por la cual, adopta las medidas que el ministerio MinTIC como entidad encargada de diseñar, adoptar y promover políticas, planes, programas y proyectos en el uso y apropiación de las TIC, así mismo, establece lineamientos con el objetivo de generar confianza en el uso del entorno digital, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.

La política de gobierno digital tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Además 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 y del entorno de las entidades públicas de orden nacional y territorial, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura crítica, 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 enmarcados en su modelo de operación por procesos.

Teniendo en cuenta lo anterior, el MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información:

Diagnóstico: Se debe iniciar con un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.

• • •

Planificación: Determina 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. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

Operación: La entidad implementa 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.

Evaluación de desempeño: la entidad determina de qué manera va a ser evaluado la adopción del modelo.

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

Cada una de las fases se dará por completada cuando se cumplan todos los requisitos definidos en cada una de ellas.



Ilustración 1: Ciclo del Modelo de Seguridad y Privacidad de la Información

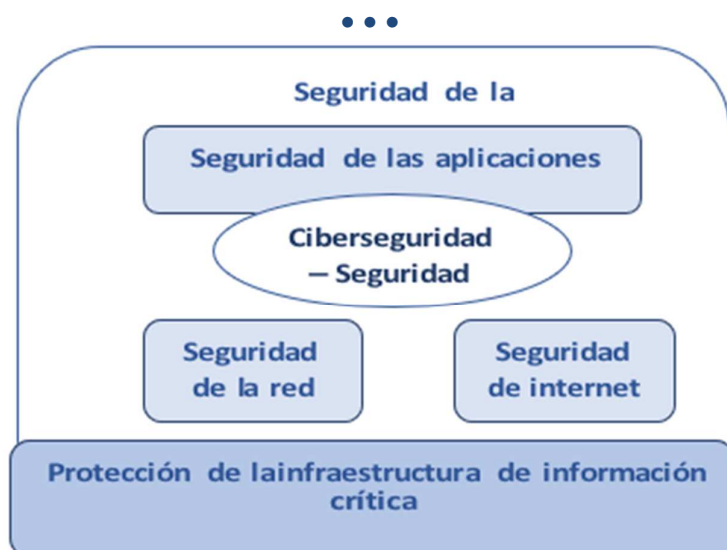


Ilustración 2. Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente ISO/IEC 27032)

OBJETIVOS

Proteger la información del Hospital San Juan de Dios ESE Rionegro, los mecanismos utilizados para el procesamiento de la información, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

Objetivos específicos

1. Establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información dentro de la entidad, que reporte a nivel central su estado de avance.
2. Fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información.
3. Garantizar la aplicación de medidas de seguridad adecuadas en los accesos a la información propiedad de la entidad.

MARCO LEGAL

Conforme con lo establecido en la normatividad vigente el Hospital San Juan de Dios ESE Rionegro, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la entidad:

- Constitución Política de Colombia. Artículo 15. Artículos 209 y 269 de la Constitución política
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- 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 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 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 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 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 1083 de 2015 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".
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades

• • •

- del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
 - Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
 - 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.
 - 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 públicas.
 - 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.
 - Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.

ALCANCE

El Modelo de Seguridad y Privacidad de la Información (MSPI) 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.

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

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. (CONPES 3854 de 2016).

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)

• • •

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).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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: 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.

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).

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: 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 este documento 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)

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)

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

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).

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

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

Diagnóstico

La fase de diagnóstico permite a las entidades establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un "Diagnóstico" utilizando el "instrumento de evaluación MSPI" con el que se identifica de forma específica los controles implementados y faltantes y así tener insumos fundamentales para la fase de planificación.

Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación, y actualizarlo posterior al término de la fase de evaluación de desempeño, esto con el fin de identificar los avances en la implementación del Modelo en la entidad, el resultado que se obtenga posterior a la fase de evaluación de desempeño será incluido como un insumo, en la fase de mejoramiento continuo.

Lineamiento: Propósito: Identificar a través de la herramienta de autodiagnóstico (Análisis GAP) el estado actual de la entidad respecto a la Seguridad y privacidad de la Información.

Propósito: Identificar el nivel de madurez de seguridad y privacidad de la información se encuentra la entidad, como punto de partida para la implementación del MSPI.

Entradas recomendadas	Salidas
Para la identificación del estado de implementación del MSPI, se debe utilizar la herramienta de autodiagnóstico del MSPI.	Documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del

• • •

Revisar aspectos internos tales como el talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional, entre otros.	MSPI en toda la entidad, y sus acciones de mejora.
--	--

Planificación

Para el desarrollo de esta fase se deben utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información con el objetivo de que la entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI.

Los documentos que se deben generar en esta fase son:

- Alcance MSPI
- Acto administrativo con las funciones de seguridad y privacidad de la información.
- Política de seguridad y privacidad de la información.
- Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información
- Procedimiento de inventario y Clasificación de la Información e infraestructura crítica
- Metodología de inventario y clasificación de la información e infraestructura crítica
- Procedimiento de gestión de riesgos de seguridad de la información
- Plan de tratamiento de riesgos de seguridad de la información • Declaración de aplicabilidad
- Manual de políticas de Seguridad de la Información
- Plan de capacitación, sensibilización y comunicación de seguridad de la información

Fase 2: Operación

Una vez culminada las actividades del MSPI de la fase de 7.3 Planificación, se llevará acabo la implementación de los controles, con el fin de dar cumplimiento con los requisitos del MSPI.

• • •

Los documentos que se deben generar en esta fase son:

- Plan de implementación de controles de seguridad y privacidad de la información
- 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 que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 "Protección de datos personales", Ley 1712 de 2014 "Ley de Transparencia y Acceso a la Información Pública", Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.

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.

ANEXOS

Controles y objetivos de control

La siguiente tabla muestra los controles de seguridad detallando cada uno de los dominios establecidos en el anexo **A** de la norma NTC: ISO/IEC 27001, los cuales tratan de los objetivos de control, y se estructurarán tal como lo muestra la Tabla 1:

Políticas específicas			
Núm.	Nombre	Seleccionado / Excepción	Descripción / Justificación
	Nombre	Control	

PLAN DE TRATAMIENTO RIESGO DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN
VERSIÓN 01

• • •

Cada uno de los campos de la tabla anterior se definen de la siguiente manera:

- Núm.: Este campo identifica cada uno de los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001.
- Nombre: Este campo hace referencia al nombre del control que se debe aplicar para dar cumplimiento a la política definida.
- Control: Este campo describe el control que se debe implementar con el fin de dar cumplimiento a la política definida.
- Dominio: Este campo describe si el control aplica para uno o múltiples dominios.
- Seleccionado / Excepción: El listado de controles además debe incluir un campo que permita ser utilizado para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado, lo cual ayuda a que la entidad tenga documentado y de fácil acceso el inventario de controles.
- Descripción / Justificación: El listado de controles cuenta con la descripción de cada control en la tabla. Adicionalmente, es posible utilizarlo para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado.

Tabla 1. – Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece

Núm.	Nombre	Selección / Excepción	Descripción / Justificación
1	Objeto y campo de aplicación		Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas		La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones		Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma		La norma ISO/IEC 27000, contiene 14 numerales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
A.5	Políticas de seguridad de la información		
A.5.1	Directrices establecidas por la dirección para la seguridad de la información		Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.5.1.1	Políticas para la seguridad de la información		Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad de la información		Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

• • •

A.6	Organización de la seguridad de la información		
A.6.1	Organización interna		Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1	Roles y responsabilidades para la seguridad de información		Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes		Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades		Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial		Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos		Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	Dispositivos móviles y teletrabajo		Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.6.2.1	Política para dispositivos móviles		Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo		Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	Seguridad de los recursos humanos		
A.7.1	Antes de asumir el empleo		Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A.7.1.1	Selección		Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo		Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	Durante la ejecución del empleo		Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la dirección		Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información		Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario		Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra

PLAN DE TRATAMIENTO RIESGO DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN
VERSIÓN 01

• • •

		empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	Terminación o cambio de empleo	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
A.8	Gestión de activos	
A.8.1	Responsabilidad por los activos	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deberían tener un propietario.
A.8.1.3	Uso aceptable de los activos	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	Clasificación de la información	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
A.8.2.1	Clasificación de la información	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.1	Gestión de medios removibles	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9	Control de acceso	

• • •

A.9.1	Requisitos del negocio para control de acceso		Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso		Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de red		Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios		Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios		Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios		Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado		Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios		Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios		Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso		Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	Responsabilidades de los usuarios		Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta		Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	Control de acceso a sistemas y aplicaciones		Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1	Restricción de acceso Información		Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro		Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas		Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados		Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.

• • •

A.9.4.5	Control de acceso a códigos fuente de programas		Control: Se debería restringir el acceso a los códigos fuente de los programas.
A.10	Criptografía		
A.10.1	Controles criptográficos		Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos		Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves		Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11	Seguridad física y del entorno		
A.11.1	Áreas seguras		Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
A.11.1.1	Perímetro de seguridad física		Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada		Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones		Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales		Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras		Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga		Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	Equipos		Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.11.2.1	Ubicación y protección de los equipos		Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro		Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado		Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos		Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.

PLAN DE TRATAMIENTO RIESGO DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN
VERSIÓN 01

• • •

A.11.2.5	Retiro de activos		Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos		Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos		Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia		Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12	Seguridad de las operaciones		
A.12.1	Procedimientos operacionales y responsabilidades		Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados		Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios		Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad		Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2	Protección contra códigos maliciosos		Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos		Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3	Copias de respaldo		Objetivo: Proteger contra la pérdida de datos.
A.12.3.1	Respaldo de información		Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4	Registro y seguimiento		Objetivo: Registrar eventos y generar evidencia.

• • •

A.12.4.1	Registro de eventos		Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro		Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador		Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4	sincronización de relojes		Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	Control de software operacional		Objetivo: Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operativos		Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	Gestión de la vulnerabilidad técnica		Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas		Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software		Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	Consideraciones sobre auditorías de sistemas de información		Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
A.12.7.1	Información controles de auditoría de sistemas		Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
A.13.1.1	Controles de redes		Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red		Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes		Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2	Transferencia de información		Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

PLAN DE TRATAMIENTO RIESGO DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN
VERSIÓN 01

• • •

A.13.2.1	Políticas y procedimientos de transferencia de información		Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información		Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica		Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación		Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14	Adquisición, desarrollo y mantenimientos de sistemas		
A.14.1.1	Requisitos de seguridad de los sistemas de información		Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información		Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas		Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones		Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2	Seguridad en los procesos de desarrollo y soporte		Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A.14.2.1	Política de desarrollo seguro		Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas		Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software		Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

• • •

A.14.2.5	Principios de construcción de sistemas seguros	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3	Datos de prueba	Objetivo: Asegurar la protección de los datos usados para pruebas.
A.14.3.1	Protección de datos de prueba	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2	Gestión de la prestación de servicios con los proveedores	Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.16	Gestión de incidentes de seguridad de la información	
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

PLAN DE TRATAMIENTO RIESGO DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN
VERSIÓN 01

• • •

A.16.1.1	Responsabilidad y procedimientos		Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información		Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información		Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información		Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información		Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia		Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio		
A.17.1	Continuidad de seguridad de la información		Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
A.17.1.1	Planificación de la continuidad de la seguridad de la información		Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información		Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2	Redundancias		Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.		Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18	Cumplimiento		

PLAN DE TRATAMIENTO RIESGO DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN
VERSIÓN 01

• • •

A.18.1	Cumplimiento de requisitos legales y contractuales		Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales		Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual		Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros		Control: Los registros se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales		Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos		Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2	Revisiones de seguridad de la información		Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
A.18.2.1	Revisión independiente de la seguridad de la información		Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad		Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico		Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Declaración de Aplicabilidad

La Declaración de Aplicabilidad, por sus siglas en inglés *Statement of Applicability* (SoA), es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.

La declaración de aplicabilidad se debe realizar luego del tratamiento de riesgos, y a su vez es la actividad posterior a la evaluación de riesgos.

• • •

La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe justificar por qué algunas medidas han sido excluidas (las innecesarias y la razón del por qué no son requerías por la Entidad).

Dentro de las actividades a seguir, después de la selección de los controles de seguridad, se procede a crear el plan de tratamiento de riesgos, esto con la finalidad de definir las actividades necesarias para la aplicación de los controles de seguridad.

A continuación, se presenta un ejemplo de formato de Declaración de aplicabilidad:

Tabla 2. Formato Ejemplo Declaración de Aplicabilidad.

		Objetivo de control o control seleccionado Si/No	Razón de la Selección	Objetivo de control o control Implementado Si/No	Justificación de exclusión	Referencia	Aprobado por la alta dirección Firma director de la entidad
Dominio	A.5 Políticas de seguridad de la información						
Objetivo de control	A. 5.1 Directrices establecidas por la dirección para la seguridad de la información						
Control	A. 5.1.1 Políticas para la seguridad de la información						
Control	A. 5.1.2 Revisión de las políticas para seguridad de la información						

Formatos

Se deben adaptar a las necesidades de la entidad las siguientes herramientas suministradas por MinTIC para la implementación y seguimiento del MSPI.

- [Instrumento de evaluación MSPI](#)
- [Seguridad en la nube](#)
- [Formato Reporte de Incidentes - CSIRT Gobierno \(Versión 3\)](#)
- [Reporte Eventos No Críticos](#)
- [Gestión de Incidentes de seguridad de la información](#)
- [Gestión inventario clasificación de activos e infraestructura critica](#)



PROCESO DE SISTEMA DE INFORMACIÓN Y GESTIÓN
DOCUMENTAL

PLAN DE TRATAMIENTO RIESGO DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN
VERSIÓN 01

Código
LPA0203004

• • •

- [Indicadores Gestión de Seguridad de la Información](#)