



**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE  
LA INFORMACIÓN.**

**HOSPITAL**  
**SAN JOSÉ DEL GUAVIARE**  
2024  
**EMPRESA SOCIAL DEL ESTADO**

*"El Hospital a su servicio"*



## TABLA DE CONTENIDO

INTRODUCCIÓN .....	3
1. OBJETIVOS.....	4
1.1. OBJETIVO GENERAL .....	4
1.2. OBJETIVOS ESPECIFICOS .....	4
2. ALCANCES Y LIMITACIONES .....	4
3. ALCANCES.....	4
3.1. LIMITACIONES.....	5
4. EJECUCIÓN DEL PLAN .....	5
4.1. IMPORTANCIA DE LA GESTIÓN DE RIESGOS .....	5
4.2. DEFINICIÓN GESTIÓN DEL RIESGO .....	7
4.3. IDENTIFICACIÓN DEL RIESGO.....	7
4.4. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN.....	8
4.5. IDENTIFICACIÓN DE LAS AMENAZAS .....	9
4.6. IDENTIFICACIÓN DE LAS VULNERABILIDADES.....	10
4.7. ANÁLISIS DEL RIESGO INHERENTE.....	11
5. IDENTIFICACIÓN DE CONTROLES .....	15
6. PLAN DE TRATAMIENTO DE RIESGOS .....	17
Bibliografía .....	19

## INTRODUCCIÓN

Teniendo en cuenta que la evolución de las comunicaciones y de la información digital genera nuevos riesgos y amenazas para garantizar la confidencialidad, integridad y disponibilidad de la información generada por los procesos de la E.S.E Hospital San José del Guaviare, se hace necesaria la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, que garantice la protección de la información ante la ocurrencia de eventos que pongan en peligro su integridad, realizando la identificación de los activos de información junto con sus posibles amenazas, vulnerabilidades, proporcionando controles para el manejo de los mismos, basados en el impacto de la probabilidad de ocurrencia.

## OBJETIVOS

### OBJETIVO GENERAL

Desarrollar el Plan de gestión de Seguridad y Privacidad de la Información que permita minimizar los riesgos de pérdida de activos de la información en la E.S.E Hospital San

*"El Hospital a su servicio"*



José del Guaviare

## **OBJETIVOS ESPECIFICOS**

Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana en materia de seguridad de la información.

Priorizar los riesgos según los criterios establecidos en el Mapa de Riesgos de Seguridad Digital.

Realizar la identificación de los principales Activos de Información presentes en la E.S.E.

Identificar las principales amenazas que afectan a los activos.

Definir el impacto de la ocurrencia de las amenazas.

Establecer controles, responsables y periodos de ejecución de las acciones de mitigación de las amenazas de los activos de la información.

Medir a través de indicadores, el manejo de los riesgos establecidos.

## **ALCANCES Y LIMITACIONES**

### **ALCANCES**

La E.S.E Hospital San José del Guaviare, con el propósito de realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la Información, debe lograr el compromiso para emprender la implementación de este plan en todos los procesos institucionales que se generen, mediante el uso de buenas prácticas y lineamientos nacionales, y locales, con el propósito que ello contribuya a la toma de decisiones y prevenir incidentes que puedan comprometer los activos de información, designando roles de liderazgo que apoyen y asesoren la implementación del Plan, capacitando al personal de la Entidad para su correcta ejecución.

### **1.1. LIMITACIONES**

No asignar los recursos necesarios en el presupuesto para apoyar la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de

*"El Hospital a su servicio"*



la Información en la E.S.E Hospital San José del Guaviare.

## 2. EJECUCIÓN DEL PLAN

### 2.1. IMPORTANCIA DE LA GESTIÓN DE RIESGOS

Debido a la evolución en el manejo de la información digital se hace prioritario salvar, proteger y custodiar los activos de la información de la E.S.E Hospital San José del Guaviare.



**Figura 1. Proceso de Administración del Riesgo**

Siguiendo los lineamientos trazados por el Gobierno Nacional en cumplimiento de la ley de transparencia 1712 del 2014 y Gobierno en Línea, que vienen impulsando

*"El Hospital a su servicio"*



actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información, con iniciativas como el concurso Máxima Velocidad, creado por el Ministerio de las TICs, la E.S.E da cumplimiento al Decreto 1078 de 2015, por medio del cual “Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Para la realización del plan de tratamiento de riesgos de seguridad y privacidad de la información se utilizó la Guía 7 Gestión de riesgos y la Guía 8 Controles de seguridad de la información.

## **2.2. DEFINICIÓN GESTIÓN DEL RIESGO**

Según la Organización Internacional de Normalización (ISO), la gestión del riesgo se define como: “Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (NTC ISO 31000:2011)”. Según la Cartilla de Administración de Riesgos del DAFP, la administración del riesgo se divide en los siguientes procesos:

## **2.3. IDENTIFICACIÓN DEL RIESGO**

Para la identificación de los riesgos, el Ministerio de las TIC, en su guía número 7 de Seguridad y Privacidad de la Información, establece la siguiente lista de clasificación de riesgos:

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta Gerencia.

*“El Hospital a su servicio”*



Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

Riesgos financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad de acuerdo a su misión.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

#### **2.4. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN**

El Mapa de Riesgos de Seguridad Digital, proporcionado por el Ministerio de Las TIC, define los siguientes tipos de Activo de Información:

Información y Datos de la Entidad: Datos e información almacenada o procesada física o electrónicamente, tales como: Bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.

Sistemas de información y aplicaciones de software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades

*"El Hospital a su servicio"*



relacionadas.

Dispositivos de tecnologías de información-hardware: Equipos de Cómputo que por su criticidad son considerados activos de información, no solo activos fijos.

Soporte para el saneamiento de información: Equipo para almacenamiento de información como: USB, Discos Duros, CDs, NAS.

Servicios: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e intranet.

Teniendo en cuenta los criterios mencionados, se identifican los siguientes activos de información.

Tipo de Activo de Información	Activo de Información
Servicios	Canal de datos
Información y datos de la entidad	Políticas de Seguridad Digital
Sistemas de Información y aplicaciones de software	Directorio Activo
Información y datos de la entidad	Copias de Respaldo
Información y datos de la entidad	Información Personal

**Tabla 1. Identificación de activos de información**

## 2.5. IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daños a la información, los procesos y los sistemas y, por lo tanto, a la E.S.E Hospital San José del Guaviare. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas, etc). A continuación, se describen las amenazas identificadas:

Activo de Información	Propiedad que afecta el riesgo	Amenazas
Canal de datos	Perdida de disponibilidad	Falla del equipo de telecomunicaciones
Políticas de Seguridad Digital	Perdida de integridad	Fallas humanas
Copias de Respaldo	Perdida de disponibilidad	Uso no autorizado de la información
Información Personal	Perdida de confidencialidad	Hurto de la Información

**Tabla 2. Identificación de Amenazas**

## 2.6. IDENTIFICACIÓN DE LAS VULNERABILIDADES

A continuación, se presentan las vulnerabilidades que podrían causar la materialización de las amenazas para cada activo de información:

Activo de Información	Amenazas	Vulnerabilidades
Canal de datos	Falla del equipo de telecomunicaciones	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)
Políticas de Seguridad Digital	Fallas humanas	Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información
Copias de Respaldo	Uso no autorizado de la información	Uso inadecuado o descuido del control de acceso físico a las edificaciones y los recintos
Información Personal	Hurto de la Información	Ausencia de políticas de control de acceso

**Tabla 3. Identificación de Vulnerabilidades**

## 2.7. ANÁLISIS DEL RIESGO INHERENTE

*"El Hospital a su servicio"*



Para cuantificar y clasificar el riesgo inherente, se toma como base la tabla de probabilidad, la tabla de impacto y la matriz de calificación.

**Tabla de Probabilidad:** La probabilidad es la medida para estimar la ocurrencia del riesgo y se mide con criterios de frecuencia

<b>RARO</b>	El evento puede ocurrir solo encircunstancias excepcionales	No se ha presentado en los últimos 5 años.
<b>IMPROBABLE</b>	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
<b>POSIBLE</b>	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
<b>PROBABLE</b>	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de 1 vez en el último año.
<b>CASI SEGURO</b>	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

**Figura 2. Tabla de Probabilidad**

**Tabla de Impacto:** Son las consecuencias potenciales que genera el hecho que sematerialice en el riesgo.

<b>TABLA DE IMPACTO</b>			
<b>TIPO</b>	<b>NIVEL</b>	<b>DESCRIPTOR</b>	<b>DESCRIPCIÓN</b>
<b>CONFIDENCIALIDAD EN LA INFORMACIÓN</b>	1	<b>INSIGNIFICANTE</b>	Se afecta a una persona en particular.
	2	<b>MENOR</b>	Se afecta a un grupo de trabajo interno del proceso.
	3	<b>MODERADO</b>	Se afecta a todo el proceso.
	4	<b>MAYOR</b>	La afectación se da a nivel estratégico.

*"El Hospital a su servicio"*



	5	<b>CATASTRÓFICO</b>	La afectación se da a nivel institucional.
<b>CREDIBILIDAD O IMAGEN</b>	1	<b>INSIGNIFICANTE</b>	Se afecta al grupo de funcionarios y contratistas del proceso.
	2	<b>MENOR</b>	Se afecta a todos los funcionarios y contratistas de la entidad.
	3	<b>MODERADO</b>	Se afecta a los usuarios de la Sede Central de la entidad.
	4	<b>MAYOR</b>	Se afecta a los usuarios de las Direcciones Territoriales.
	5	<b>CATASTRÓFICO</b>	Se afecta a los usuarios de la Sede Central y de las Direcciones Territoriales.
	<b>LEGAL</b>	1	<b>INSIGNIFICANTE</b>
2		<b>MENOR</b>	Se producen demandas para la entidad.
3		<b>MODERADO</b>	Se producen investigaciones disciplinarias.
4		<b>MAYOR</b>	Se producen investigaciones fiscales.
5		<b>CATASTRÓFICO</b>	Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control u otro Ente regulador.
	1	<b>INSIGNIFICANTE</b>	Se tendrían que realizar ajustes a una actividad

<b>OPERATIVO</b>			concreta del proceso.
	2	<b>MENOR</b>	Se tendrían que realizar ajustes en los procedimientos del proceso.
	3	<b>MODERADO</b>	Se tendrían que realizar ajustes en la interacción de procesos.
	4	<b>MAYOR</b>	Se presentarían intermitencias o dificultades en la operación del proceso
	5	<b>CATASTRÓFICO</b>	Se presentaría paro o no operación del proceso.

**Figura 2. Tabla de Impacto**

**Matriz De Calificación, Evaluación Y Respuesta A Los Riesgos:** Representa la Zona en la que se encuentra el riesgo a la que se enfrenta inicialmente un proceso o la Entidad en ausencia de controles.

CONCEPTO		IMPACTO				
		1	2	3	4	5
PROBABILIDAD		INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
	VALOR	1	2	3	4	5
RARA VEZ (1)	1	11	12	13	14	15
IMPROBABLE (2)	2	21	22	23	24	25
POSIBLE (3)	3	31	32	33	34	35
PROBABLE (4)	4	41	42	43	44	45
CASI SEGURO (5)	5	51	52	53	54	55



**Figura 4. Matriz de Calificación, Evaluación y Respuesta a los Riesgos**

Basados en las figuras presentadas anteriormente, se presenta el análisis del riesgo inherente para E.S.E Hospital San José del Guaviare:

Activo de Información	Probabilidad	Impacto	Zona de Riesgo
Canal de datos	Posible	Mayor	Zona De Riesgo Alta
Políticas de Seguridad Digital	Probable	Mayor	Zona De Riesgo Alta
Copias de Respaldo	Probable	Mayor	Zona De Riesgo Extrema
Información Personal	Casi Seguro	Mayor	Zona De Riesgo Extrema

**Tabla 4. Análisis del riesgo inherente**

### 3. IDENTIFICACIÓN DE CONTROLES

En esta etapa, se establecieron los controles que se realizan para mitigar el riesgo inherente, teniendo como referencia las opciones del manejo del riesgo, la descripción del mismo y el responsable de ejecutar su control:

Activo de Información	Opciones de manejo del Riesgo	Descripción del control	Responsable de ejecutar el control
Canal de datos	Reducir el riesgo	Monitorear el canal de datos de la entidad	Oficina de Sistemas
Políticas de Segu Digital	Reducir el riesgo	Socializar las políticas de seguridad con cada uno de los funcionarios de la entidad	Oficina de Sistemas
Copias de Respaldo	Reducir el riesgo	Se cuenta con la Política de Seguridad de la Información	Oficina de Sistemas
Información Personal	Reducir el riesgo	Bloqueo y control de acceso al personal en cada una de las máquinas	Oficina de Sistemas

DESCRIPCION	RESPONSABLE	TIEMPO
Sensibilización, socialización y capacitación a responsables de los activos de tecnologías información, sobre el proceso de identificación, valoración, tratamiento y gestión de riesgos frente a las Ciberamenazas.	OFICINA DE SISTEMAS	1 DE FEBRERO A 31 DE DICIEMBRE 2024
Evaluación de controles de seguridad informática implementados frente a las Ciberamenazas.	OFICINA DE SISTEMAS	10 DE FEBRERO A 31 DE DICIEMBRE 2024
Actualización el Plan de tratamientos de riesgos frente a Ciberamenazas.	OFICINA DE SISTEMAS	1 DE FEBRERO A 31 DE DICIEMBRE 2024

**Tabla 4. Identificación de Controles**

## PLAN DE TRATAMIENTO DE RIESGOS

Luego de elegir los controles más adecuados para tener un nivel de riesgo aceptable para los procesos, se diseñó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, en el cual se tienen en cuenta la reducción del riesgo, los controles, las actividades y los responsables de la ejecución, y así medir periódicamente la ejecución de los mismos mediante un indicador definido para cada activo de la información.

Activo de Información	Opciones de manejo del riesgo	Controles	Actividad	Objetivo del Control	Responsable de Ejecutar el control	Periodo / Fecha de ejecución	Indicador
Canal de datos	Reducir el riesgo	Mantenimiento de los equipos de red	Realizar seguimiento al mantenimiento de los equipos informáticos	Realizar un adecuado soporte a los dispositivos de red de la Entidad.	Oficina de Sistemas	Trimestral	No de mantenimientos realizados / No de mantenimientos programados
Políticas de Seguridad Digital	Reducir el riesgo	Sensibilización de las políticas de seguridad a los funcionarios de la entidad	Realizar campañas de sensibilización con el objetivo de apropiar las responsabilidades descritas en las políticas de seguridad de la información	Fortalecer la implementación de las políticas de seguridad	Oficina de Sistemas	Trimestral	No de sensibilizaciones realizadas / No de sensibilizaciones programadas

*"El Hospital a su servicio"*



Copias de Respaldo	Reducir el riesgo	Socializar el manual de seguridad de la información con los funcionarios de la Oficina de Informática	Plan de sensibilización del manual de seguridad de la información	Reducir la pérdida de información	Oficina de Sistemas	Trimestral	No de sensibilizaciones realizadas / No de sensibilizaciones programadas
Información Personal	Reducir el riesgo	Seguimiento a los roles y permisos del software hospitalario	Realizar seguimiento y actualizar los permisos de los usuarios del software hospitalario	Limitar el acceso a información de la entidad	Oficina de Sistemas	Trimestral	No de Actividades ejecutadas / No de Actividades planeadas

**Tabla 5. Plan de Tratamiento de Riesgos**

## Bibliografía

Guía 7 Gestión de riesgos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea. Guía 8 controles de seguridad y privacidad de la información. Modelode Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea. Guía para la administración del riesgo y el diseño de controles en entidades públicas. Función pública, octubre 2018, versión 4. Anexo 4, lineamiento para la gestión de riesgos de seguridad digital en entidades públicas. Ministerio de tecnologías de la información y las comunicaciones, 2018.