

# EMPRESA SOCIAL DEL ESTADO HOSPITAL DE LA VEGA



## PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

 <p>E.S.E. HOSPITAL De La Vega</p>	E.S.E. HOSPITAL DE LA VEGA LA VEGA - CUNDINAMARCA	Código: PLN-PL-08
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0
		Fecha: 26/01/2026
		Página 2 de 20

## Tabla de contenido

<b>INTRODUCCIÓN .....</b>	3
<b>ALCANCE .....</b>	3
<b>OBJETIVOS .....</b>	3
<b>OBJETIVO GENERAL .....</b>	3
<b>OBJETIVOS ESPECÍFICOS .....</b>	3
<b>DEFINICIONES.....</b>	4
<b>DESCRIPCIÓN DEL PLAN.....</b>	5
<b>IDENTIFICACIÓN DEL RIESGOS.....</b>	5
<b>CLASIFICACIÓN DEL RIESGO .....</b>	5
<b>CRITERIOS BASICOS.....</b>	6
<b>CRITERIOS DE EVALUACIÓN DEL RIESGO .....</b>	6
<b>CRITERIOS DE IMPACTO.....</b>	6
<b>CRITERIOS DE ACEPTACIÓN DEL RIESGO .....</b>	7
<b>ANÁLISIS DE RIESGO .....</b>	8
<b>IDENTIFICACIÓN DE LAS AMENAZAS Y VULNERABILIDADES .....</b>	8
<b>EVALUACIÓN DE RIESGOS .....</b>	15
<b>EJEMPLO DE EVALUACIÓN DE RIESGOS .....</b>	16
<b>APLICABILIDAD.....</b>	17
<b>COMUNICACIÓN Y SEGUIMIENTO .....</b>	17
<b>BIBLIOGRAFIA .....</b>	18
<b>CONTROL DE CAMBIOS .....</b>	18

 <p><b>E.S.E HOSPITAL De La Vega</b></p>	<b>E.S.E. HOSPITAL DE LA VEGA LA VEGA - CUNDINAMARCA</b>	<b>Código: PLN-PL-08</b>
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión: 0</b>
		<b>Fecha: 26/01/2026</b>
		<b>Página 3 de 20</b>

## INTRODUCCIÓN

El plan de tratamiento de riesgo de seguridad y privacidad de la información de la E.S.E Hospital de La Vega se basa en buscar estrategias que permitan desarrollar una cultura de carácter preventivo en la entidad, de manera que el cliente interno comprenda el concepto de riesgo, a través de herramientas que permitan reducir la afectación de la entidad en caso de materializarse un riesgo. La E.S.E Hospital de La Vega, busca desarrollar estrategias que permitan identificar, reducir y monitorear los riesgos asociados a la seguridad y privacidad de la información.

De acuerdo con lo mencionado anteriormente, la E.S.E Hospital de La Vega adopta estrategias y mecanismos proporcionado por el MINTIC y su Modelo de Seguridad y Privacidad de la Información – MSPI, tomando las buenas prácticas y lineamientos establecidos por el ente de control.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la ESE Hospital de la Vega se enmarca en los lineamientos de la política de seguridad digital establecida en el Modelo Integrado de Planeación y Gestión MIPG, y se encuentra alineado a la estructura organizacional vigente del Hospital, así como con sus objetivo, metas y proyectos.

## ALCANCE

La E.S.E Hospital de La Vega con el propósito de realiza una correcta gestión del riesgo, busca integrar los procesos de buenas prácticas y correcto uso de la información mediante estrategias que permitan la toma de decisiones ante un evento o riesgo que afecte la operación y los objetivos de la entidad.

Teniendo en cuenta lo anterior se definen lineamientos que permitan la gestión de riesgos de seguridad digital en la E.S.E Hospital de La Vega.

## OBJETIVOS

### OBJETIVO GENERAL

Gestionar un plan de tratamiento de riesgo de seguridad y privacidad de la información el cual permita ser una guía para el control y minimización de los riesgos con el fin de proteger la privacidad y seguridad de la información de la entidad.

### OBJETIVOS ESPECÍFICOS

- Establecer mecanismos que permitan proteger los activos de información mediante la implementación de estrategias para la mitigación del riesgo.
- Definir un diagnóstico que permita la identificación de posibles riesgos sobre los activos de

	E.S.E. HOSPITAL DE LA VEGA LA VEGA - CUNDINAMARCA	Código: PLN-PL-08
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0
		Fecha: 26/01/2026
		Página 4 de 20

información de la entidad.

- Sugerir estrategias que permitan a los clientes internos reconocer y mitigar los posibles riesgos asociados a la seguridad de la información.

## DEFINICIONES

Para conocer el plan de tratamiento de riesgos de seguridad y privacidad de la información, el cliente interno deberá conocer los términos y definiciones asociados al desarrollo del plan actual con el fin de proveer conocimientos previos al lector.

- **Confidencialidad:** Información que no debe ser puesta a disposición o ser relevada a individuos, entidades o terceros no autorizados.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Integridad:** Propiedad de la información referente a su exactitud y complejidad.
- **Control:** Medida que modifica el riesgo.
- **Activos de información:** Información o elemento de valor para operación de la organización.
- **Administración del riesgo:** Elementos de control que permiten a la entidad brindar estrategias para el correcto manejo de los eventos que puedan afectar las operaciones de la entidad.
- **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- **Riesgo:** Contingencia o proximidad de un posible daño.
- **Proceso:** Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- **Seguimiento:** Mesa de trabajo institucional la cual se encarga de revisar y validar el control de riesgos o eventos durante periodos establecidos por la entidad.
- **Vulnerabilidad:** Es aquella debilidad de un activo o grupo de activos de información.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y

 <p>E.S.E HOSPITAL De La Vega</p>	E.S.E. HOSPITAL DE LA VEGA LA VEGA - CUNDINAMARCA	Código: PLN-PL-08
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0
		Fecha: 26/01/2026
		Página 5 de 20

disponibilidad de la información.

- **MSPI:** Modelo de Seguridad y privacidad

## DESCRIPCIÓN DEL PLAN

### IDENTIFICACIÓN DEL RIESGOS

El propósito de la identificación del riesgo es determinar una visión general de los riesgos que pueden afectar el cumplimiento de los objetivos de la entidad, se establecen varias determinantes para la identificación del riesgo, el cómo, donde, y porque podría suceder un evento o el riesgo.

Una vez se identifica el riesgo, se debe establecer criterios de clasificación del riesgo, el criterio permitirá establecer acciones de solución o toma de decisiones.

### CLASIFICACIÓN DEL RIESGO

CLASIFICACIÓN DEL RIESGO	
<b>RIESGO ESTRATÉGICO</b>	Se asocia con la forma como 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.
<b>RIESGOS DE IMAGEN</b>	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
<b>RIESGOS OPERATIVOS</b>	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. De la articulación entre dependencias.
<b>RIESGOS FINANCIEROS</b>	Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
<b>RIESGOS DE CUMPLIMIENTO</b>	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.

<b>RIESGOS TECNOLOGICOS</b>	Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
---------------------------------	--

Se debe tener en cuenta que la entidad tiene la posibilidad de agregar diferentes tipos de riesgos de seguridad de la información, los riesgos se clasifican según la guía de El Modelo de Seguridad y Privacidad de la Información – MSPI.

### **CRITERIOS BASICOS**

Dependiendo del alcance y los objetivos del plan, se pueden aplicar diferentes enfoques, pero debe ser adecuado y que contenga criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo:

#### **CRITERIOS DE EVALUACIÓN DEL RIESGO**

Se recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la institución teniendo en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información para la entidad
- La criticidad de los activos de información involucrados en el proceso
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

#### **CRITERIOS DE IMPACTO**

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información del proceso
- Brechas en la seguridad de la información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- Operaciones deterioradas
- Perdida del negocio y del valor financiero

 <b>E.S.E HOSPITAL De La Vega</b>	<b>E.S.E. HOSPITAL DE LA VEGA LA VEGA - CUNDINAMARCA</b>	<b>Código: PLN-PL-08</b>
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión: 0</b>
		<b>Fecha: 26/01/2026</b>
		<b>Página 7 de 20</b>

- Alteración de planes y fechas límites
- Daños para la reputación
- Incumplimiento de los requisitos legales.

### **CRITERIOS DE ACEPTACIÓN DEL RIESGO**

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas

La organización debería definir sus propias escalas para los niveles de aceptación del riesgo. Durante el desarrollo, se deberían considerar los siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas.
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado.
- Los diferentes criterios de aceptación del riesgo pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual.
- Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga el riesgo y se podrían considerar los siguientes elementos:

- Criterios de negocio.
- Aspectos legales y reglamentarios.
- Operaciones.
- Tecnologías.
- Finanzas.
- Factores sociales y humanitarios.

### **ANÁLISIS DE RIESGO**

Para la E.S.E Hospital de La Vega, es muy importante documentar y especificar cada una de las etapas de los riesgos o eventos presentados. La entidad tendrá una bitácora de registro y seguimiento para el análisis de datos, el análisis se realiza según la guía de El Modelo de Seguridad y Privacidad de la Información – MSPI.

### **IDENTIFICACIÓN DE LAS AMENAZAS Y VULNERABILIDADES**

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. 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)

Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

A continuación, se describen una serie de amenazas comunes:

**D = Deliberadas, A = Accidentales, E = Ambientales**

TIPO	AMENAZA	ORIGEN
<b>Daño físico</b>	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
<b>Eventos naturales</b>	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
<b>Perdida de los servicios esenciales</b>	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Perdida de suministros de energía	E
	Falla en el equipo de telecomunicaciones	A, D, E
<b>Perturbación debida a la</b>	Radiación electromagnéticos	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnético	A, , E
	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D



<b>Compromiso de la información</b>	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D
<b>Fallas técnicas</b>	Fallas del equipo	A, D
	Mal funcionamiento del equipo	A, D
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A, D
	Incumplimiento en el mantenimiento del sistema de información.	A, D, E
<b>Acciones no autorizadas</b>	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
<b>Compromiso de las funciones</b>	Error en el uso	A, D
	Abuso de derechos	A, D
	Falsificación de derechos	A, D
	Negación de acciones	A, D
	Incumplimiento en la disponibilidad del	

Es importante tener en cuenta que las fuentes de amenazas humanas, estas amenazas se desglosan de la siguiente manera:

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto; Ego; Rebelión; Estatus; Dinero	<ul style="list-style-type: none"><li>• Piratería</li><li>• Ingeniería Social</li><li>• Intrusión, accesos forzados al sistema</li><li>• Acceso no autorizado</li></ul>



Criminal de la computación	Destrucción de la información; Divulgación ilegal de la información; Ganancia monetaria; Alteración no autorizada de los datos	<ul style="list-style-type: none"><li>• Crimen por computador</li><li>• Acto fraudulento</li><li>• Soborno de la información</li><li>• Suplantación de identidad</li></ul>
Terrorismo	Chantaje; Destrucción; Explotación; Venganza; Ganancia política; Cubrimiento de los medios de comunicación	<ul style="list-style-type: none"><li>• Bomba/Terrorismo</li><li>• Guerra de la información</li><li>• Ataques contra el sistema Dos</li></ul>
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva; Espionaje; económico	<ul style="list-style-type: none"><li>• Ventaja de defensa</li><li>• Ventaja política</li><li>• Explotación económica</li><li>• Hurto de información</li></ul>
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad; Ego; Inteligencia Ganancia monetaria Venganza; Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	<ul style="list-style-type: none"><li>• Asalto a un empleado Chantaje</li><li>• Observar información reservada</li><li>• Uso inadecuado del computador</li><li>• Fraude y hurto</li><li>• Soborno de información</li><li>• Ingreso de datos falsos o corruptos</li></ul>

Para la E.S.E Hospital de La Vega es importante tener en cuenta las posibles vulnerabilidades según el tipo de activo por esta razón se realiza la caracterización de las vulnerabilidades más conocidas y sus métodos de valoración.



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

<b>TIPO DE ACTIVO</b>	<b>EJEMPLOS DE VULNERABILIDADES</b>	<b>EJEMPLO DE POSIBLES AMENAZAS.</b>
<b>HARDWARE</b>	Mantenimiento insuficiente/Instalación	Incumplimiento en el mantenimiento del sistema de información.
	fallida de los medios de almacenamiento	
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.



<b>SOFTWARE</b>	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso



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

	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos



	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
RED	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos

 <p>E.S.E HOSPITAL De La Vega</p>	E.S.E. HOSPITAL DE LA VEGA LA VEGA - CUNDINAMARCA	Código: PLN-PL-08 Versión: 0
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Fecha: 26/01/2026
		Página 15 de 20

<b>PERSONAL</b>	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos

 <p>E.S.E HOSPITAL De La Vega</p>	E.S.E. HOSPITAL DE LA VEGA LA VEGA - CUNDINAMARCA	Código: PLN-PL-08
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0
		Fecha: 26/01/2026
		Página 16 de 20

## EVALUACIÓN DE RIESGOS

El análisis y la evaluación de los riesgos dependen de la información obtenida durante la clasificación e identificación de las amenazas, para ello la entidad debe tener en cuenta los criterios anteriormente descritos. La guía MSPI menciona cuales son los pasos claves en el análisis de riesgos, posibilidades e impactos.

Para facilitar la calificación y evaluación a los riesgos, se presenta una matriz donde contempla un análisis cualitativo, para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad).

PROBABILIDA D	IMPACTO				
	Insignifican te 1	Meno r 2	Moderad o 3	Mayo r 4	Catastrófic o 5
Raro 1	B	B	M	A	A
Improbable 2	B	B	M	A	E
Possible 3	B	M	A	E	E
Probable 4	M	A	A	E	E
Casi Seguro 5	A	A	E	E	E

Las categorías relacionadas con el Impacto son: insignificante, menor, moderado, mayor y catastrófico. Las categorías relacionadas con la Probabilidad son: raro, improbable, posible, probable, casi seguro.

ZONAS DE RIESGO			
B: Zona de riesgo baja:	M: Zona de riesgo Moderado:	A: Zona de riesgo alto:	E: Zona de riesgo Extremo:
Asumir el riesgo.	Asumir el riesgo, reducir el riesgo.	Reducir el riesgo, evitar, compartir o transferir.	Reducir el riesgo, evitar, compartir o transferir.

 <p>E.S.E. HOSPITAL De La Vega</p>	E.S.E. HOSPITAL DE LA VEGA LA VEGA - CUNDINAMARCA	Código: PLN-PL-08 Versión: 0
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Fecha: 26/01/2026
		Página 17 de 20

## EJEMPLO DE EVALUACIÓN DE RIESGOS.

A continuación, se realiza la demostración para el correcto análisis de los posibles riesgos que puede llegar a presentar la entidad.

ANÁLISIS DEL RIESGO					
PROCESO: ATENCIÓN AL USUARIO					
RIESGO	CALIFICACIÓN		Tipo Impacto	Evaluación Zona de Riesgo	Medidas de Respuesta
	Probabilidad	Impacto			
Cambio en los datos de contacto de los usuarios	3	4	confidencialidad de la información	extrema	Reducir el Riesgo Evitar Compartir o Transferir

PROBABILIDAD	IMPACTO				
	Insignificante 1	Menor 2	Moderado 3	Mayo 4	Catastrófico 5
Raro 1	B	B	M	A	A
Improbable 2	B	B	M	A	E
Possible 3	B	M	A	E	E
Probable 4	M	A	A	E	E
Casi Seguro 5	A	A	E	E	E

Para finalizar el análisis del riesgo se debe realizar la valoración y control final y se debe recordar que estos se clasifican en dos:

<b>PREVENTIVOS</b>	<b>CORRECTIVOS</b>
aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.	aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable, también permiten la modificación de las acciones que proporcionan su ocurrencia.

### **COMUNICACIÓN Y SEGUIMIENTO**

La oficina de sistemas debe realizar la comunicación activa de los riesgos presentados, es importante tener en cuenta que los puntos de vista entre el equipo de trabajo varía en cuanto a los conceptos técnicos y profesionales de cada uno, se debe tener presente que el área de sistemas debe exponer las necesidades, suposiciones del estudio o la evaluación realizada.

Posteriormente la información procesada deberá ser expuesta en comités administrativos, el área de control interno deberá llevar control y seguimiento de los riesgos presentados. Se debe contemplar un informe que exponga el proceso de mejora que debe llevar la institución para evitar posibles riesgos.

Por otra parte, se debe establecer un valor de desempeño que permita administrar la gestión de los riesgos de la entidad. Los indicadores de cumplimiento para un correcto manejo del riesgo se deben establecer de la siguiente manera

 <b>E.S.E. HOSPITAL De La Vega</b>	<b>E.S.E. HOSPITAL DE LA VEGA LA VEGA - CUNDINAMARCA</b>	<b>Código: PLN-PL-08</b>
		<b>Versión: 0</b>
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Fecha: 26/01/2026</b>
		<b>Página 19 de 20</b>

Indicador	Estructura del Indicador	Riesgo Identificado	Acción de Mejora	Meta	Responsable	Periodicidad	Resultado Esperado
Copias de seguridad	(Nº copias realizadas / Total de copias programadas) x 100	Pérdida de información crítica	Validar diariamente las copias de seguridad del sistema de	Cumplir ≥ 95 %	Área de Sistemas	Diaria	Disponibilidad e integridad de la información

			información				
Protección antivirus	(Equipo s con antivirus activo / Total de equipos) x 100	Infección por malware	Verificar y actualizar antivirus institucional	Cumplir 100 %	Área de sistemas	Mensual	Reducción de incidentes de seguridad
Sensibilización	(Funcionarios capacitados / Total funcionarios) x 100	Errores humanos y phishing	Realizar capacitaciones en seguridad de la información	≥ 90 %	Área de Sistemas	Semestral	Mayor cultura de seguridad

Durante la vigencia 2025, el Área de Sistemas realizó el seguimiento permanente a la gestión de los riesgos asociados a la seguridad de la información, conforme a lo establecido en el Plan de Tratamiento de Riesgos. Como resultado de este seguimiento, el indicador (número de riesgos gestionados / total de riesgos presentados) x 100 se mantuvo en 0, lo cual representa un resultado positivo para la institución, dado que no se presentaron riesgos de seguridad de la información durante el periodo evaluado.

Este resultado refleja la efectividad de los controles preventivos implementados, así como el adecuado manejo de los activos de información y la adopción de buenas prácticas por parte de los usuarios y del Área de Sistemas.

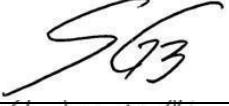
Así mismo, se deja establecido que los indicadores definidos en el Plan de Tratamiento de Riesgos de Seguridad de la Información serán ejecutados y evaluados durante la vigencia 2026, con el fin de continuar fortaleciendo los mecanismos de prevención, control y mitigación de posibles riesgos tecnológicos, garantizando la confidencialidad, integridad y disponibilidad de la información institucional.

 <p>E.S.E HOSPITAL De La Vega</p>	E.S.E. HOSPITAL DE LA VEGA LA VEGA - CUNDINAMARCA	Código: PLN-PL-08
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0
		Fecha: 26/01/2026
		Página 20 de 20

## BIBLIOGRAFIA

MSPI. (s. f.). Gobierno Digital Guía 7 - 8. Recuperado 3 de enero de 2022, de <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>

## CONTROL DE CAMBIOS

APROBACIÓN DE MODIFICACIÓN ÚLTIMA VERSIÓN				
	NOMBRE	CARGO	FECHA	FIRMA
ELABORÓ	Sebastián García Barbosa	Líder de Sistemas	14/01/2026	
REVISÓ	Gloria Alexandra Plazas	Asesora de Planeación	23/01/2026	
APROBÓ	Carlos Alberto Mantilla M.	Gerente	26/01/2026	

CONTROL DE CAMBIOS				
VERSION	FECHA DE APROBACIÓN	DESCRIPCIÓN DEL CAMBIO	SOLICITO	ESTADO
0	26 enero 2026	Plan de acción 2026	Asesora planeación	aprobado