HIDALGO
IEE
INSTITUTO ESTATAL ELECTORAL

Análisis de Riesgos de Seguridad de la Información en Infraestructura Tecnológica

Octubre 2025, Versión 1.0

Unidad de Tecnologías
de la Información y Comunicaciones

Contenido

GLOSARIO

Activo crítico	Recurso, sistema o información cuya interrupción o destrucción causaría un daño grave a la operación del Instituto.
Contingencia	Situación de riesgo o un suceso inesperado que puede interrumpir el funcionamiento normal de los sistemas informáticos.
IEEH / Instituto	Instituto Estatal Electoral de Hidalgo.
Incidencia	Evento inesperado que interrumpe o degrada el funcionamiento normal de un sistema, red o servicio, afectando la productividad.
Riesgo	Amenaza o vulnerabilidad que puede comprometer la seguridad de los sistemas y datos digitales, desde errores humanos hasta ataques de ciberdelincuentes y desastres naturales
UPS	Acrónimo en inglés de Uninterruptable Power Supply, Sistema de Alimentación Ininterrumpida, es un dispositivo permite tener flujo de energía eléctrica mediante baterías, cuando el suministro eléctrico falla.
UTIC	Unidad de Tecnologías de la Información y Comunicaciones

INTRODUCCIÓN

La información, como bien, es de importancia vital ya que a través de ella se toman decisiones, para la resolución de conflictos o necesidades, se tiene el conocimiento de hechos ocurridos y sienta las bases para innovaciones.

En este sentido, los sistemas de información adquieren su relevancia al eficientar los procesos y actividades encaminadas al logro de sus objetivos estratégicos del IEEH; estos, se pueden mantener, actualizar y mejorar teniendo una adecuada sistematización.

Es por esto, que los activos de información han pasado a formar parte de la actividad cotidiana del Instituto; los equipos de cómputo almacenan información, la procesan y la transmiten a través de redes y canales de comunicación, abriendo posibilidades y facilidades a las personas servidoras públicas; pero, se debe considerar nuevos paradigmas en estos modelos tecnológicos y tener muy claro que no existen sistemas cien por ciento seguros, porque el costo de la seguridad total es muy alto (aunque en la realidad no es alcanzable idealmente).

El manejo de la seguridad de la información digital abarca la protección de sistemas de información que se tienen en el Instituto y sistemas externos a los que esté obligado a reportar información, pasando por aspectos tan importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información y planes de contingencia o de continuidad del Instituto, claro está, incluyendo además los sistemas físicos de protección y accesibilidad a sitios o áreas restringidas.

Consecuencia de este documento, se ha de generar el Plan de Continuidad y Seguridad dirigido a determinar las acciones que garanticen el seguimiento y la continuidad en la ejecución de los procedimientos, en caso de que se suscite un evento adverso o incidencia y a la protección de los Activos para la operación del IEEH.

ANTECEDENTES

El 22 de septiembre del 2025, se aprobaron las Políticas y Lineamientos de Gestión de Sistemas de Información y Comunicaciones cuyo objetivo es establecer las políticas y lineamientos en materia de gestión de sistemas de información y comunicaciones en el Instituto para el cumplimiento de sus objetivos institucionales, la seguridad, el procesamiento y la detección de riesgos en la información y los activos informáticos.

Dentro de estas, la Política de Administración de Riesgos establece los lineamientos para la identificación, evaluación, mitigación, seguimiento y respuesta ante riesgos relacionados con la información, con el fin de garantizar la continuidad operativa, la protección de los activos de información y el cumplimiento de las obligaciones legales y normativas aplicables, como sigue:

6.1 Identificación y Evaluación de Riesgos

6.1.1 Se deberán realizar evaluaciones periódicas para identificar riesgos asociados al manejo de la información, tales como:

- Pérdida o destrucción de datos
- Acceso no autorizado
- Corrupción o alteración de datos
- Almacenamiento de información digital
- Fallos tecnológicos o humanos
- Riesgos derivados de terceros o proveedores
- Almacenamiento de equipamiento informático
- Capacitación continua en seguridad de la información para el personal del Instituto

6.1.2 Cada riesgo será evaluado en términos de probabilidad de ocurrencia e impacto potencial, clasificándose en niveles de criticidad (alto, medio, bajo).

6.1.3 Se utilizarán herramientas como matrices de riesgos, entrevistas, análisis de procesos y revisión de incidentes previos.

6.1.4 Las medidas serán revisadas y actualizadas conforme a los resultados de las evaluaciones de riesgo.

OBJETIVO

Identificar y evaluar las amenazas y vulnerabilidades que puedan afectar la seguridad, integridad y disponibilidad de los sistemas de información del IEEH, mediante el monitoreo continúo y evaluación; con el propósito de establecer medidas preventivas, correctivas y de mitigación que contribuyan a proteger los activos de información, garantizar la continuidad operativa de los procesos institucionales y asegurar el cumplimiento de las políticas y normativas aplicables en materia de seguridad de la información.

Alcance

- El presente análisis aplica a todas las unidades administrativas del IEEH.

- Para la identificación de Activos críticos, se clasificarán en Recursos Humanos, Infraestructura tecnológica, Software y Servicios.

- La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis, con criterios de riesgo establecidos en este documento.

    - Probabilidad de ocurrencia
    - Nivel de Impacto
    - Intensidad del riesgo
    - Tipo de amenaza
    - Tratamiento del riesgo

CRITERIOS DE RIESGO

Los criterios que se deberán tomar en cuenta para la valoración de los riesgos van relacionados con el nivel de impacto que el riesgo y la ocurrencia de este, en el desarrollo y funcionamiento de los sistemas informáticos. En su intensidad estará el grado de magnitud en el daño potencial que represente para el Instituto. Estos los valoraremos en la siguiente tabla:

Matriz de Riesgos				
Matriz de calificación, evaluación y respuesta de riesgo				
Probabilidad	**Alta**	**Zona de riesgo moderado** Prevenir el riesgo	**Zona de Riesgo Importante** Eliminar el riesgo Mitigar el riesgo Compartir riesgo Transferir el riesgo	**Zona de Riesgo Inaceptable** Eliminar el riesgo Mitigar el riesgo Compartir riesgo Transferir el riesgo
	Media	**Zona de Riesgo Tolerable** Prevenir el riesgo	**Zona de Riesgo Moderado** Prevenir el Riesgo Mitigar el Riesgo Compartir riesgo Transferir el Riesgo	**Zona de Riesgo Importante** Eliminar el Riesgo Mitigar el Riesgo Compartir riesgo Transferir el Riesgo
	Baja	**Zona de Riesgo Aceptable** Aceptar el Riesgo	**Zona de Riesgo Tolerable** Mitigar el Riesgo Compartir riesgo Transferir el Riesgo	**Zona de Riesgo Moderado** Mitigar el Riesgo Compartir riesgo Transferir el Riesgo
		Bajo	**Medio**	**Alto**
		Impacto		

Matriz de riesgo para la clasificación de riesgos.

A. **Zona Riesgo Bajo** (Zona verde de la tabla Matriz de riesgos)**:** Los elementos a los que afecte no detendrán el funcionamiento de las operaciones del IEEH; sin embargo, entorpecerán el desarrollo de estas. Al momento de determinar un Riesgo Bajo, es importante, considerar el daño que en su ocurrencia repetitiva pueda, por sí mismo, presentar el entorpecimiento del desarrollo de otras actividades, lo cual en cadena representaría un Riesgo Medio o Alto.

B. **Zona Riesgo Medio** (Zona amarilla de la tabla Matriz de riesgos)**:** Cuando el nivel de afectación puede ser mediado con la utilización de una medida emergente sin afectar el desarrollo de actividades del Instituto, será considerado que el elemento presente un nivel de riesgo medio. Para los elementos definidos en este nivel será necesario que se instrumente paralelamente la medida contingente para su atención.

C. **Zona Riesgo Alto** (Zona roja de la tabla Matriz de riesgos)**:** Los elementos que afecten este nivel de riesgo podrán poner en peligro la continuidad de la operación del IEEH y deberán tener la mayor prioridad en su inmediata atención.

Tratamientos de riesgo

A continuación, se definen los tratamientos de riegos que se emplearán para la identificación de los mismos:

Eliminar el riesgo

Evitar riesgos significa no participar en actividades que puedan afectar negativamente al IEEH.

Mitigar el riesgo

Acepta el riesgo, pero tiene como objetivo minimizarlo y sus impactos. La reducción del riesgo acepta el riesgo, pero se enfoca en evitar que cualquier pérdida se propague.

Transferir el riesgo

La transferencia de riesgos implica contratar a un tercero para que absorba el riesgo.

Aceptar el riesgo

No es posible eliminar todos los riesgos. Luego de tomar medidas para evitar, reducir, compartir o transferir el riesgo, el Instituto enfrenta cualquier preocupación restante (también conocida como riesgo residual). La aceptación y la retención de riesgos implican aceptar las posibles consecuencias del riesgo y preparar para gestionarlas si ocurren.

Para la determinación del nivel de riesgo, se deberá tomar en cuenta el tiempo que pudiese detener, en su eventual aparición, el funcionamiento del proceso. En igual manera se medirán los tiempos para solventar la situación una vez presentada, incluyendo los recursos requeridos para su atención, ya sean humanos, financieros o materiales.

ACTIVOS DEL IEEH

Los activos críticos del IEEH son los elementos clave para el funcionamiento y procesamiento de información, se tipificarán de acuerdo con su naturaleza para su focalización y continuo monitoreo. Acorde a lo anterior, se identificaron cuatro tipos de activos:

Recursos Humanos

Personal que labora en el Instituto, los Distritos Electorales Locales y la nube en internet.

A. Personal permanente
B. Personal temporal
C. Personal técnico

Infraestructura tecnológica

Se instala y opera en instalaciones del IEEH, los Consejos Distritales Electorales Locales.

A. Computadoras personales
B. Ruteadores
C. Switches
D. Telefonía análoga
E. Telefonía IP
F. Videovigilancia
G. Equipo Satelital
H. Servidores
I. Escáneres
J. Impresoras
K. UPS
L. Reguladores
M. Planta de energía
N. Aire acondicionado
O. Red cableada

Software

Programas informáticos por el cual se captura, procesa, trasmite, pública o almacenan datos.

A. Sistemas operativos
B. De productividad
C. Desarrollo del propio Instituto
D. Gestión de tareas
E. Uso en línea
F. Almacenamiento de archivos
G. De bases de datos
H. Sitios de internet
I. Correos electrónicos

J. Videoconferencia

Servicios

Para la construcción de la red estatal del Instituto se deberá realizar con las siguientes características.

A. Líneas Telefónicas
B. Enlaces
C. Internet
D. Energía eléctrica

TIPOS DE AMENAZAS

De acuerdo a la identificación de activos críticos y a su análisis se determinaron las siguientes amenazas o riesgos:

Amenazas:

1. Electrónico
    a. No intencionado
        i. Caída de red
        ii. Caída de Servidores
        iii. Fallos de equipo informático
        iv. Errores de programas informáticos
    b. Intencionado
        i. Robo de información
        ii. Manipulación de datos
        iii. Sabotaje de comunicaciones y equipo de computo
        iv. Virus informáticos
2. Físico
    a. No intencionado
        i. Terremoto
        ii. Inundación
        iii. Fallo de energía
        iv. Ausencia de personal
    b. Intencionado
        i. Robo de equipo informático
        ii. Sabotaje de equipo informático
        iii. Vandalismo
        iv. Ausencia de personal

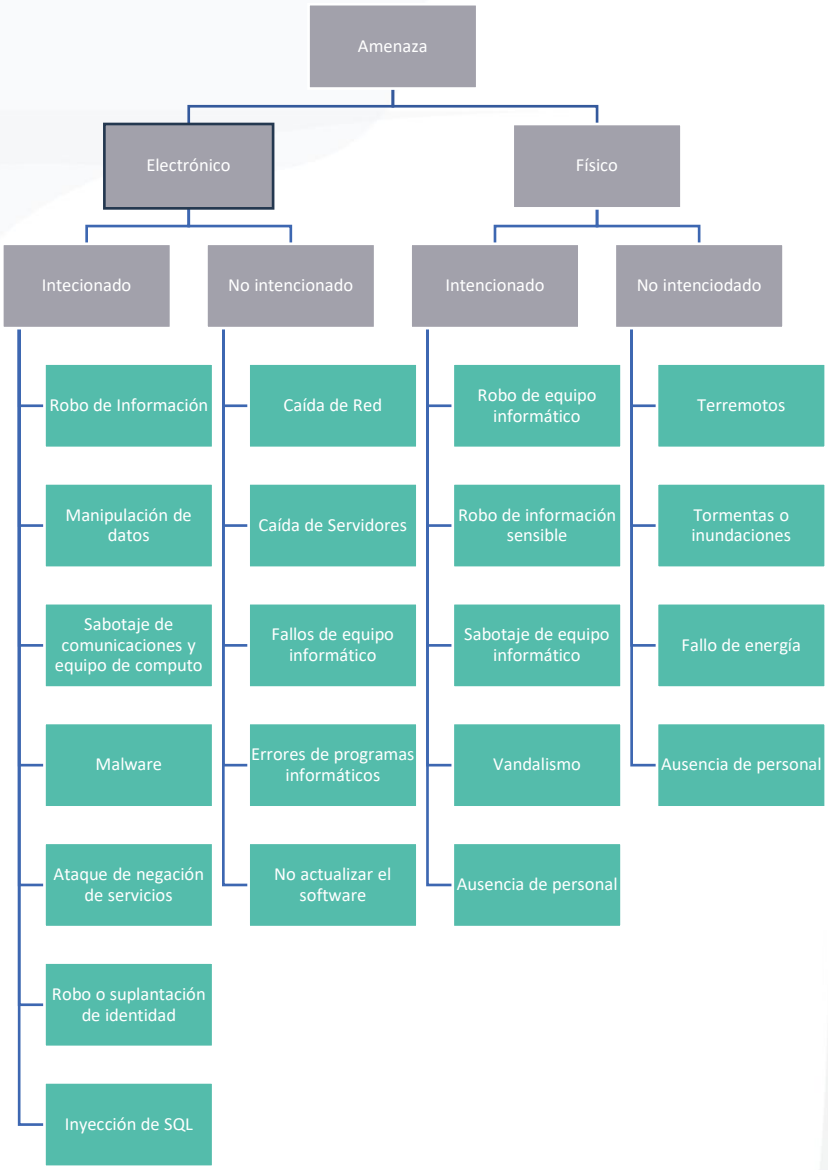
En este sentido se simplifican estas amenazas de la siguiente manera:

A. Amenazas Electrónicas Intencionadas (AEI).

B. Amenazas Electrónicas No Intencionadas (AEN).

C. Amenazas Físicas Intencionadas (AFI).

D. Amenazas Físicas No Intencionadas (AFN).



Identificación y clasificación de amenazas

IDENTIFICACIÓN DE AFECTACIONES Y RIESGOS

Para la identificación de las afectaciones y riesgos potenciales en el IEEH, se han tomado en cuenta los activos críticos previamente identificados de acuerdo con su área y los elementos que le componen. Así mismo, se detalló su nivel de riesgo en cuanto al grado de afectación en el desarrollo de las operaciones del Instituto.

Matriz de Identificación de Riesgos		
Activo Critico	**Tipo de Amenaza**	**Afectación**
Recursos Humanos	AEI	Aplica
	AEN	No aplica
	AFI	Aplica
	AFN	Aplica
Infraestructura tecnológica	AEI	Aplica
	AEN	Aplica
	AFI	Aplica
	AFN	Aplica
Software	AEI	Aplica
	AEN	Aplica
	AFI	No aplica
	AFN	No aplica
Servicios	AEI	Aplica
	AEN	Aplica
	AFI	Aplica
	AFN	Aplica

Recursos Humanos

Se detalla el personal por nivel que participa en las operaciones de proceso de información del Instituto.

Clasificación del activo	Activo crítico	Nivel de riesgo
Recursos humanos	Consejerías	Bajo
	Titular de área	Bajo
	Subdirectores	Medio
		Bajo
	Jefaturas de Departamento, Personal Operativo y Personal Temporal	Medio
		Bajo
	Personal Técnico	Alto
		Medio

1. **Consejerías. –** Las funciones que realiza son de toma de decisiones y de consulta. La falta de alguno no tendría repercusiones serias en la operación, por ello su nivel de Riesgo es bajo.

2. **Titular de área. –** Las funciones que desempeña son dirección, administrativas y de consulta. La falta de algún Titular no tendría repercusiones serias en el procesamiento de información; por ello, su nivel de Riesgo es bajo.

3. **Subdirectores. –** Dadas sus funciones de administración, supervisión y generación y conformación de información, la falta de alguno no tendría repercusiones serias en la operación; por ello, su nivel de Riesgo es bajo.

4. **Jefaturas de Departamento, Personal Operativo y personal temporal. –** Realizan procedimientos y operaciones, generan y procesan información interactuando con los Sistemas e infraestructura, la falta de alguno no tendría repercusiones serias en la operación, por ello su nivel de Riesgo es medio.

5. **Personal Técnico. -** Realizan procedimientos de administración y supervisión de Sistemas e infraestructura. Por esta situación, su nivel de riesgo es alto.

Infraestructura tecnológica

Se detalla el equipo tecnológico utilizado en las operaciones.

Clasificación del activo	Activo crítico	Nivel de riesgo
Infraestructura tecnológica	Computadoras personales	Bajo
	Ruteadores	Alto
	Switches	Medio
	Telefonía análoga	Bajo
	Telefonía IP	Bajo
	Videovigilancia	Bajo
	Equipo Satelital	Medio
	Servidores	Alto
	Escáneres	Bajo
	Impresoras	Bajo
	UPS	Bajo
	Reguladores	Bajo
	Planta de energía	Bajo
	Aire acondicionado	Medio
	Red cableada	Bajo

1. **Computadoras personales:** Son el medio principal de captura, procesamiento, y almacenamiento de información. Su Riesgo es bajo dado que solo procesan la información de una persona.

2. **Ruteadores:** Es el medio primario de comunicación de ahí que su función es de riesgo alto.

3. **Switches:** Se requieren diversos tipos de Switches para conectar los equipos de la Red Local del Instituto, siendo así su riesgo alto.

4. **Telefónica análoga:** Ya que existe cobertura de telefonía Celular, el nivel de riesgo se tipifica en bajo.

5. **Telefónica IP:** Ya que existe cobertura de telefonía Celular, el nivel de riesgo se tipifica en bajo.

6. **Videovigilancia:** Equipo cuya función es brindar seguridad, no entorpece la operación. Su nivel de riesgo es bajo.

7. **Equipo Satelital:** Equipo de respaldo para comunicación de voz, video y datos, por lo que su nivel de riesgo es alto.

8. **Servidores:** Unidades de procesamiento y almacenamiento “global” de información del Instituto, por lo que su nivel de riesgo es alto.

9. **Escáneres:** Equipos utilizados para la digitalización de información, nivel de riesgo bajo.

10. **Impresoras:** Utilizados para la impresión de información, su nivel de riesgo es bajo.

11. **UPS:** Unidades de energía ininterrumpida, por sus siglas en inglés; son equipos que en caso de falla entrará la planta de energía. Su nivel de riesgo es bajo.

12. **Reguladores:** Equipos para regular la corriente eléctrica, su nivel de riesgo es bajo.

13. **Planta de energía:** Equipo que provee respaldo de energía eléctrica en caso de que la energía pública falte, su nivel de riesgo es medio.

14. **Aire acondicionado:** Utilizado para asegurar el rango de temperatura requerido para que el equipo electrónico del Site funcione adecuadamente, su nivel de riesgo es medio.

15. **Red cableada:** Es el sistema de conexión de computadoras y otros dispositivos a través de cables físicos, dado que se emplea una topología de red tipo estrella. Su nivel de riesgo es medio.

Software

Se describe el software utilizado en los diferentes procesos de información del Instituto.

Clasificación del activo	Activo crítico	Nivel de riesgo
Software	Sistemas operativos	Bajo
	De productividad	Bajo
	Desarrollo del propio Instituto	Bajo
	Gestión de tareas	Bajo
	Uso en línea	Bajo
	Almacenamiento de archivos	Bajo
	De bases de datos	Bajo
	Sitios de internet	Medio/Bajo
	Correos electrónicos	Bajo
	Videoconferencia	Bajo

1. **Sistemas Operativos. –** Programa básico para interacción entre las personas usuarias y la computadora. Nivel de riesgo bajo.

2. **De productividad. -** Programas informáticos diseñados para mejorar la productividad y facilitar tareas de oficina. Nivel de riesgo bajo.

3. **Desarrollo del propio instituto**. – Aplicaciones para realizar tareas específicas y particulares del Instituto. Nivel de riesgo alto.

4. **Gestión de tareas. -** Aplicaciones para realizar tareas específicas de un área determinada del Instituto. Nivel de riesgo bajo.

5. **Programas de uso en línea**. - Se ejecuta en un servidor remoto y se accede a través de un navegador web, sin necesidad de instalarlo en un dispositivo. Nivel de riesgo bajo.

6. **Almacenamiento de archivos.** – Almacenamiento de archivos en la nube, para ser accesibles desde cualquier punto con acceso a Internet. Nivel de riesgo bajo.

7. **Programa de bases de datos**. - Permiten crear, organizar, gestionar, almacenar y recuperar información de una base de datos de manera estructurada y segura. Nivel de riesgo alto.

8. **Sitios de Internet.** – Publicación de información. Nivel de riesgo medio.

9. **Correo electrónico**. – Comunicación de información. Nivel de riesgo bajo.

10. **Videoconferencia**. – Comunicación visual entre personas con el fin de intercambiar información. Nivel de riesgo bajo.

Servicios

Se muestran los principales Activos críticos por área de localización.

Clasificación del activo	Activo crítico	Nivel de riesgo
Servicios	Líneas Telefónicas	Bajo
	Servicios de Internet	Medio
	Energía eléctrica	Alto
	Servidores	Alto

1. **Líneas Telefónicas. –** Ya que existe cobertura de telefonía Celular, el nivel de riesgo de este servicio se tipifica en bajo.

2. **Servicios de Internet. –** Conectividad que permite a dispositivos acceder a la red mundial de Internet. Este servicio, es proporcionado por empresas privadas o públicas. Su nivel de riesgo es alto.

3. **Energía eléctrica. -** El servicio de energía eléctrica es la actividad que permite la generación, transmisión, distribución y suministro de electricidad hasta los puntos de consumo, como hogares, oficinas e industrias. Su nivel de riesgo es medio.

4. **Servidores.** – Servicio de arrendamiento de servidores para el procesamiento y alojamiento de datos, sistemas y aplicaciones. Su nivel de riesgo es medio.

Con el objetivo de abordar los riesgos de manera proactiva y reactiva, en caso de un evento de contingencia; así como la protección de Activos de acuerdo con los niveles y tratamiento de riesgos identificados, se establece el Plan de Continuidad y Seguridad.

TRATAMIENTO DE RIESGOS

Medidas de control para eliminar, mitigar, transferir o aceptar los riesgos.

1. Eliminar el riesgo

- Descontinuar sistemas o procesos obsoletos que representen vulnerabilidades significativas.
- No implementar tecnologías o servicios cuya seguridad no pueda garantizarse.
- Restringir el uso de dispositivos externos (USB, almacenamiento portátil) en sistemas críticos.
- Bloquear accesos remotos no autorizados o innecesarios.

2. Mitigar el riesgo (medidas preventivas y correctivas)

- Implementar firewalls, antivirus y sistemas de detección de intrusos (IDS/IPS).
- Establecer copias de seguridad automáticas y cifradas de información crítica.
- Aplicar actualizaciones y parches de seguridad en sistemas y aplicaciones.
- Configurar control de accesos con autenticación multifactor (MFA) y privilegios mínimos.
- Utilizar cifrado de datos en tránsito y en reposo.
- Realizar auditorías de seguridad y pruebas de penetración periódicas.
- Definir políticas y procedimientos de seguridad de la información.
- Capacitar al personal en ciberseguridad y manejo responsable de la información.
- Establecer protocolos de respuesta ante incidentes y simulacros periódicos.
- Aplicar clasificación de la información y controles de acceso basados en niveles de sensibilidad.

3. Transferir el riesgo

- Contratar seguros cibernéticos o de responsabilidad tecnológica.
- Establecer acuerdos de nivel de servicio (SLA) con proveedores que incluyan cláusulas de seguridad.
- Delegar servicios críticos (como hosting o respaldo) a proveedores certificados (por ejemplo, ISO 27001 o SOC 2).

- Establecer contratos con cláusulas de confidencialidad (NDA) y gestión de riesgos compartidos.

4. Aceptar el riesgo

- Documentar formalmente la decisión de aceptación del riesgo con aprobación de la alta dirección.
- Incluir el riesgo en el registro institucional de riesgos para seguimiento periódico.
- Realizar monitoreo continuo para detectar cualquier cambio en su nivel o probabilidad.
- Establecer planes de contingencia por si el riesgo se materializa.

MONITOREO Y EVALUACIÓN

1. Establecimiento de indicadores de desempeño

Se definen métricas para medir la eficacia de los controles y la evolución de los riesgos.

- % de riesgos mitigados respecto al total de identificados.
- % de incidentes de seguridad detectados vs. no detectados.
- Tiempo promedio de respuesta ante incidentes.
- Cumplimiento del plan de continuidad y seguridad (% de acciones implementadas).

Responsable: Unidad de Tecnologías de la Información y Comunicaciones.

2. Revisión periódica del registro de riesgos

Mantener un registro de riesgos actualizado con estatus, responsables y medidas implementadas.

Revisar y revaluar los riesgos existentes ante cambios en:

- Infraestructura tecnológica, Recursos Humanos, Software y Servicios.

- Procesos institucionales o normativas.
- Detección de nuevas amenazas.
- Periodicidad: al menos una vez al año o ante cualquier cambio significativo.

Responsable: Unidad de Tecnologías de la Información y Comunicaciones.