COLOMBIA POTENCIA DE LA VIDA

Igualdad

# Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024

República de Colombia
Ministerio de Igualdad y Equidad

INSOR
Instituto Nacional para Sordos

República de Colombia
Ministerio de Igualdad y Equidad

INSOR

Instituto Nacional para Sordos

#InclusiónTotal
ParaLaPaz

Cra.: 89A #64c-30 - Bogotá
contacto@insor.gov.co
Tel.: (601) 439 12 21
**www.insor.gov.co**

# INSTITUTO NACIONAL PARA SORDOS – INSOR

**Geovani Andrés Meléndres Guerrero**

Director General

**Néstor Julián Rosas**

Secretario General

**Helena Patricia Hernández Aguirre**

Subdirectora de Promoción y Desarrollo

**Luz Mary López Franco**

Subdirectora de Gestión Educativa

**Diego Armando López Cely**

Asesor de Dirección

**Carolina Ramos Castellanos**

Jefe Oficina Asesora de Planeación y Sistemas

**Luis Hernán Cuellar**

Jefe Oficina Asesora Jurídica

**Cilia Guio**

Jefe Oficina con funciones de Control Interno

**Documento elaborado por**

**Oficina Asesora de Planeación y Sistemas**

**Bogotá D.C, Diciembre de 2023**

República de Colombia
Ministerio de Igualdad y Equidad
INSOR
Instituto Nacional para Sordos

## Contenido

## 1. OBJETIVOS.

- Cumplir con los requisitos legales, reglamentarios y regulatorios en cuanto a riesgos de Seguridad de la Información.
- Preservar la integridad, confidencialidad, disponibilidad, privacidad y de la información, contribuyendo al logro de los objetivos, la misión y la visión institucional.
- Realizar una adecuada gestión de riesgos de Seguridad y Privacidad de la información, teniendo en cuenta los lineamientos establecidos Instituto Nacional para Sordos-INSOR.

## 2. ALCANCE.

El presente plan aplica en todos los procesos y áreas del Instituto Nacional para Sordos-INSOR donde haya recolección, procesamiento, almacenamiento, recuperación, intercambio, tránsito y consulta de información, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

## 3. INTRODUCCION.

El Instituto Nacional para Sordos-INSOR mediante la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información busca establecer un conjunto de actividades que permitan garantizar la protección y privacidad de los datos; preservando la confidencialidad, integridad y disponibilidad de la información. A través de la gestión del riesgo en los activos de información del INSOR, se analiza la exposición a las amenazas para asegurar los procesos de recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información.

El plan de tratamiento de riesgos de seguridad de la información para la vigencia 2024, se elabora con el fin de evaluar las acciones que permitan mitigar los riesgos identificados en los procesos de la entidad, con acciones que permitan garantizar la protección y la privacidad de los datos, contribuyendo al cumplimiento de la misión y objetivos estratégicos de la Entidad.

Alineados con la Norma Técnica Colombiana ISO 27001:2022 y la ISO 27005 sobre el análisis de riesgos permitiendo identificar las amenazas en las que se

está expuestos todos los activos de información, la frecuencia en las que se pueden materializar las amenazas y valoración de impacto.

## 4. DEFINICIONES

**Activo:** 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 2016, pág. 56).

**Administración del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la entidad un aseguramiento razonable con respecto al logro de los objetivos. (DAFP 2018).

**Autenticación:** Provisión de credenciales (usuario y contraseña) para poder acceder a recursos protegidos en equipos de cómputo.

**Amenaza:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO/IEC 27000:2016)

**Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

**Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

**Confidencialidad:** garantizar que todos los recursos informáticos estén protegidos contra uso no autorizado o revelaciones accidentales. La información deberá ser considerada como privada y restringida. se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

**Disponibilidad:** garantizar que la información crítica y la capacidad de procesamiento puedan ser resguardadas y recuperadas rápida y completamente en caso de que ocurra alguna contingencia que interrumpa la continuación de las operaciones. se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

**Evaluación del riesgo:** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, también se fundamenta en comparar el riesgo estimado contra criterios de riesgo dados, para determinar

la importancia del riesgo, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

**Firewalls:** son dispositivos de seguridad, que permiten filtrar contenidos y proteger las aplicaciones de accesos no autorizados o ataques de tipo hacker.

**Impacto:** Se entiende como las consecuencias ocasionadas por la materialización del riesgo. (DAFP 2018).

**Integridad:** Propiedad de exactitud y completitud. (DAFP 2018)

**Incidente de seguridad**: Un incidente de seguridad es un evento adverso en un sistema de computadores, o red de computadores, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

**Integridad:** establecer mecanismos para garantizar que toda la información que se maneje se encuentre libre de errores y/o corrupción de cualquier índole. se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

**Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

**Lugar seguro:** Sitio físico o electrónico que protege la información de accesos no autorizados, perdida, robo, daño, fuga. Cuya recuperación es inmediata para personas autorizadas.

**No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

**Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el Objeto de simular múltiples peticiones del mismo remitente original.

**Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

**Responsable de Seguridad y privacidad de la información**: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

**Riesgo:** Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos del INSOR. Se expresa en términos de probabilidad y consecuencias.

**Riesgo de seguridad y privacidad:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de probabilidad y consecuencias.

**Tecnología de la Información:** Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

**Tercero:** Empresa con contrato temporal que presta servicios directos o indirectos, bien sea en las instalaciones del INSTITUTO NACIONAL PARA SORDOS, o en sus propias instalaciones y que emplea algunos de los recursos informáticos y de comunicaciones del INSTITUTO NACIONAL PARA SORDOS.

**Usuario:** funcionarios, contratistas o terceros que hacen uso de los servicios informáticos del Instituto Nacional para Sordos-INSOR.

**Vulnerabilidad:** Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas. (Basado en DAFP 2018)

## 5. GESTIÓN DEL RIESGO:

La gestión de riesgos del INSOR se lleva a cabo por los líderes de cada proceso gestionando la misión y la visión estratégica determinando el tratamiento de riesgos de cada uno de los activos identificados teniendo en cuenta la Guía de Gestión del Riesgo del Departamento Administrativo de la Función Pública - DAFP y la Guía de la Secretaría de Transparencia de la Presidencia de la República, denominada Guía para la Gestión de Riesgo de Corrupción y Modelo de Gestión de Riesgos de Seguridad Digital.

### 5.1 ANÁLISIS DE RIESGO:

Se realiza la identificación de causas, vulnerabilidades, amenazas, consecuencias y se determina la clase de riesgo (probabilidad e impacto), todo esto asociado a aquellos eventos o situaciones que afecten los activos de información que pueden entorpecer el normal desarrollo de los procesos, garantizando que los controles son eficaces y eficientes tanto en el diseño como la operación

## 5.2 TRATAMIENTO DE RIESGO:

El tratamiento del riesgo consiste en seleccionar y aplicar las medidas adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos, para lo cual se definen Medidas de Respuesta ante los Riesgos (asumir, reducir, compartir, transferir o evitar), luego se definen acciones de mitigación de riesgos (actividades o tareas, responsables, plazo de ejecución y seguimiento) para mejorar la validación del riesgo.

## 5.3 COMUNICACIÓN DEL RIESGO:

Participan todos los procesos e involucran a todos los colaboradores para el levantamiento de los mapas de riesgo, contando con el aporte de los colaboradores con mayor experticia tanto para la identificación como para el tratamiento de riesgos.

Cuando se identifica un riesgo el INSOR suministra, comparte u obtiene información a través de un diálogo con las partes involucradas con respecto a la gestión del riesgo. La información está relacionada con la existencia, la naturaleza, la forma, la probabilidad, el significado, la evaluación, la aceptabilidad y el tratamiento de la Gestión de riesgo.

## 5.4 MONITOREO:

Los riesgos identificados traen consigo controles que incluyen el monitoreo de los eventos correspondientes, invirtiendo los recursos de acuerdo a la criticidad del riesgo asociado, las responsabilidades del monitoreo comprenden todos los aspectos del proceso para la gestión del riesgo con el fin de:

- Garantizar que los controles son eficaces y eficientes tanto en el diseño como en la operación.
- Obtener información adicional para mejorar la valoración del riesgo.
- Analizar y aprender lecciones a partir de los eventos.
- Detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios de riesgo y en el riesgo mismo que puedan exigir revisión de los tratamientos del riesgo y las prioridades.

## 6. PLAN DE ACTIVIDADES TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El Plan de Tratamiento de Riesgos de Seguridad de la Información establece las actividades a desarrollar con el fin de mitigar los riesgos sobre los activos identificados por la entidad, de acuerdo con las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información establecida por la Función Pública

| Etapa | Actividad | Fecha Inicio | Fecha Final | Responsable | Producto |
|---|---|---|---|---|---|
| **GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** | | | | | |
| Actualización de lineamientos de riesgos | Actualizar la política, metodología y lineamientos de la gestión de riesgos, cuando se requiera. | Febrero | Marzo | Oficina Asesora de Planeación y Sistemas | Matriz de riesgos (guía) |
| Sensibilización | Socializar los lineamientos y Herramientas para la Gestión de los Riesgos de Seguridad y privacidad de la Información. | Abril | Mayo | Oficina Asesora de Planeación y Sistemas | Actas, correos electrónicos pieza de comunicación |
| Identificación de Riesgos de Seguridad y Privacidad de la Información. | Identificar o actualizar los activos de información de los procesos del INSOR.<br>Identificar, analizar y evaluar los riesgos de seguridad y privacidad de la información. | Junio | Julio | Líderes de Proceso | Matriz de riesgos |

| | | | | | |
|---|---|---|---|---|---|
| Tratamiento | Tratamiento de riesgos de seguridad de la información | Agosto | Septiembre | Líderes de Proceso | Actas, correos electrónicos auto seguimiento matriz de riesgos |
| Seguimiento y revisión de riesgos de seguridad | Realizar el seguimiento a la implementación de controles y planes de tratamiento para los riesgos identificados. | Octubre | Noviembre | Todas las líneas de defensa | Informe |
| Mejoramiento | Identificar oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento de los riesgos de seguridad y privacidad de la información. | Diciembre | Diciembre | Todos los procesos | Plan de mejoramiento |

COLOMBIA POTENCIA DE LA VIDA

Igualdad

Te invitamos a escanear este código, para conocer más sobre la **cultura sorda.**

República de Colombia
Ministerio de Igualdad y Equidad

INSOR
Instituto Nacional para Sordos