MINISTERIO DE EDUCACIÓN NACIONAL

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

Carrera 89A # 64C - 30 Álamos zona industrial
www.insor.gov.co /contacto@insor.gov.co
Tel. (57-1) 4391221

República de Colombia
Ministerio de Educación Nacional
INSOR
Instituto Nacional para Sordos

TABLA DE CONTENIDO

1. OBJETIVO.

Velar por la disponibilidad, integridad y disponibilidad de la información a través de la gestión del riesgo del 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 y consulta de información, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

INTRODUCCION.

El Instituto Nacional para Sordos-INSOR presenta a la ciudadanía y a los grupos de interés el plan de tratamiento de riesgos de seguridad de la información para la vigencia 2023, donde se establece un conjunto de actividades, que permiten garantizar la protección y la privacidad de los datos preservando la confidencialidad, integridad y disponibilidad de la información, contribuyendo al cumplimiento de la misión y objetivos estratégicos de la entidad. Basados en la Norma Técnica Colombiana ISO 27001:2022 y la ISO 27005 sobre el análisis de riesgos permitiendo identificar las amenazas en las que se esta expuestos todos los activos, la frecuencia en las que se pueden materializar las amenazas y valoración de impacto.

3. DEFINICIONES

Administración del riesgo: Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

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

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.

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.

4. 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.

4.1 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.

4.2 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).

4.3 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.

4.4 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.

5. PLAN DE ACTIVIDADES TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

N	Actividad	Fecha Inicio	Fecha Final	Responsable	Producto
RIESGOS DE SEGURIDAD DE LA INFORMACIÓN					
1	Actualización metodología riesgos seguridad	Febrero	Marzo	Oficina Asesora de Planeación y Sistemas	Matriz de riesgos (guía)
2	Identificación de análisis de riesgos de seguridad de la información	Julio	Agosto	Todas las áreas y procesos del INSOR	Matriz de riesgos
3	Comunicación de riesgos de seguridad de la información	Julio	Diciembre	Oficina Asesora de Planeación y Sistemas	Actas, correos electrónicos pieza de comunicación

N	Actividad	Fecha Inicio	Fecha Final	Responsable	Producto
RIESGOS DE SEGURIDAD DE LA INFORMACIÓN					
4	Tratamiento de riesgos de seguridad de la información	Julio	Diciembre	Todas las áreas y procesos del INSOR	Actas, correos electrónicos auto seguimiento matriz de riesgos
5	Seguimiento y revisión de riesgos de seguridad	Julio	Diciembre	Oficina Asesora de Planeación y Sistemas	Informe