|  |  |  |
| --- | --- | --- |
|  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Directriz rectora para la Administración de Riesgos |  | **MAAGTICSI** | | | Establecer la línea a seguir para planear, realizar, analizar y evaluar los riesgos asociados a los activos críticos del Instituto. | **Proyecto:**  **ID:** | | |  |  | | |

**CONTENIDO**

1. OBJETIVO DE LA DIRECTRIZ 2

2. ABREVIATURAS Y DEFINICIONES 2

3. Referencias 2

4. ALCANCE 3

5. JUSTIFICACIÓN 3

6. REQUERIMIENTOS REGULATORIOS 3

7. ROLES Y RESPONSABILIDADES 5

8. METODOLOGÍA 8

9. ELEMENTOS para la administración de riesgos 12

10. DIRECTRICES DE ADMINISTRACIÓN DE RIESGOS 13

11. MECANISMOS DE DIFUSIÓN 13

12. MECANISMOS DE REVISIÓN 13

13. Bitácora de Control de Cambios 14

1. OBJETIVO DE LA DIRECTRIZ

[Establecer la línea a seguir para planear, realizar, analizar y evaluar los riesgos asociados a los activos críticos del Instituto, sensibilizando al personal involucrado del nivel de riesgos al cual se está expuesto e identificar y planear las medidas adecuadas para mitigar, controlar, transferir o aceptar los riesgos con los menores daños y costos posibles.]

1. ABREVIATURAS Y DEFINICIONES

|  |  |
| --- | --- |
| **Abreviación o definición** | **Descripción** |
|  |  |
|  |  |
|  |  |

1. Referencias

|  |  |
| --- | --- |
| **Nombre del documento** | **Descripción del documento** |
| *[Nombre del o los documentos a los que se hace referencia a lo largo del llenado de este formato].* | *[Escriba una breve descripción del documento, así como su ubicación física o lógica].* |
|  |  |
|  |  |

1. ALCANCE

*[El presente documento aplica a cualquier activo de información que esté expuesto a las amenazas internas o externas definidas en el SGSIInstitucional y que pongan en riesgo la Confidencialidad, Integridad y/o Disponibilidad de la información de los procesos definidos por los involucrados de la STIC del Instituto, los cuales se mencionan a continuación:]*

| **Área** | **Proceso** | **Descripción** |
| --- | --- | --- |
| *[Nombre del área responsable]* | *[Nombre del proceso]* | *[Describa brevemente el proceso]* |
|  |  |  |

1. JUSTIFICACIÓN

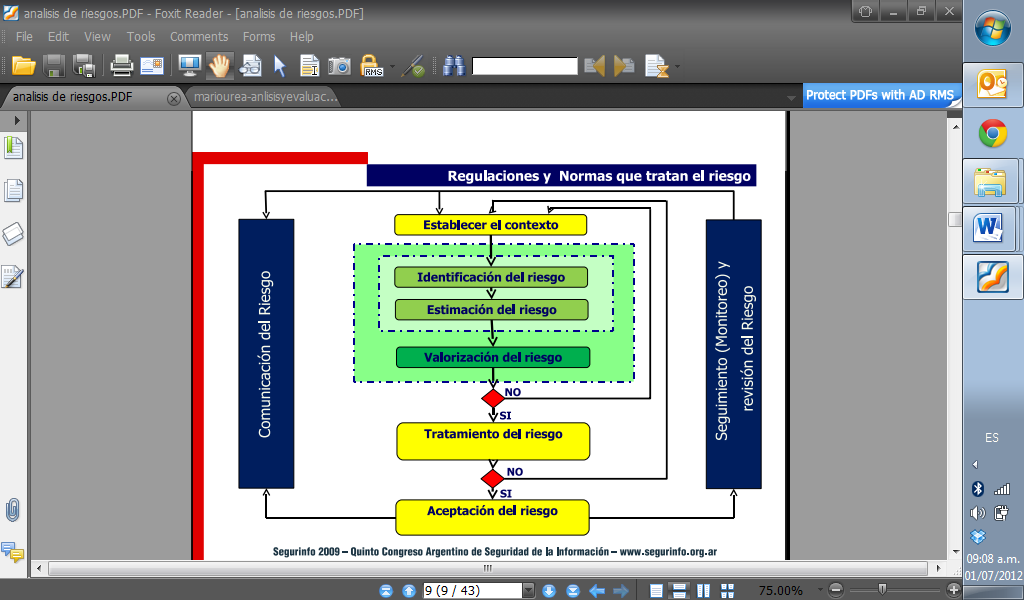
*[La presente directriz nos permitirá describir los elementos internos y externos que obligan al establecimiento de la Administración de riesgos, para evitar impactos negativos alaSTIC del Instituto en sus bienes y servicios, logrando asíbeneficios significativos.]*

1. REQUERIMIENTOS REGULATORIOS

Los estándares aplicables en materia de mitigación de riesgos son:

* **ISO/IEC 27001:** La cual especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
* **ISO/IEC 27005:** La cual proporciona las Directrices para la Gestión del Riesgo de Seguridad de la Información de cualquier organismo o institución.

La cual sebasa en el siguiente modelo:



1. ROLES Y RESPONSABILIDADES

| **Rol** | **Descripción** | **Responsabilidad** |
| --- | --- | --- |
| RSII | Responsable de la Seguridad de la Información en el Instituto | Coordinar los trabajos del equipo en la identificación, documentación, revisión periódica de los Procesos Críticos de la Institución, así como de las Infraestructuras Críticas y Activos de Información.  Impulsar la participación de los integrantes del GI-TIC.  Vigilar el desarrollo y cumplimiento de los trabajos desarrollados por el equipo de trabajo.  Dar seguimiento a los resultados de la implantación del SGSI.  Asegurar que los controles de seguridad se hayan implantado de acuerdo a lo previsto en el Documento de definición, implantación, evaluación y mejora del SGSI.  Dar seguimiento a las posibles desviaciones en la implantación y/o en la operación de los controles de seguridad.  Enviar el Documento de Definición, implantación, Evaluación y Mejora del SGSI al Grupo Integral de TIC.  Obtener los datos necesarios para verificar la eficiencia y eficacia de los controles implementados.  Medir la efectividad de los controles de seguridad implantados.  Efectuar, con base en el Documento de Definición, implantación, Evaluación y Mejora del SGSI, las evaluacionesal SGSI.  Registrar la información de los intentos, exitosos y no exitosos, de violaciones e incidentes de seguridad, así como efectuar el análisis y evaluación de dicha información.  Documentar las acciones de revisión del SGSI que hayan resultado de los factores críticos anteriores y enviarlas al GI-TIC.  Verificar el contenido del Documento de Definición, implantación, Evaluación y Mejora del SGSI; actualizarlo en caso aplicable y enviarlo al GI-TIC. |
| GI-TIC | Grupo Integral de TIC | Realizar la identificación y clasificación de Infraestructuras Críticas, supervisar las actividades de identificación de Infraestructuras críticas y activos clave, así como la integración del Documento respectivo y su actualización anual.  Realizar el Análisis de riesgos, supervisar el proceso de administración de riesgos, el Documento de Identificación, Evaluación y Resultados del Análisis de Riesgos generado por el responsable y vigilar que éste análisis se realice cuando sea necesario o al menos anualmente.  Autorizar el Documento de Definición, implantación, Evaluación y Mejora del SGSI.  Autorizar la Directriz rectora para la administración de riesgos y verificar que dicha directriz permanezca actualizada.  Asegurarse de que se observe lo establecido en le Ley de Seguridad Nacional, en la Ley de Transparencia y Acceso a la Información Pública Gubernamental, su reglamento y demás disposiciones aplicables, para la clasificación y resguardo de la información de la infraestructura crítica y activos de información.  Autorizar la Directriz rectora para la Administración de riesgos.  Autorizar la integración y operación del Equipo de Respuesta a Incidentes de Seguridad de TIC (ERISC), en las que se preverán los mecanismos de coordinación del ERISC al interior de la Institución o con otros ERISC o entidades externas, en concordancia con la Directriz rectora de respuesta a incidentes.  Identificar los procesos críticos y las interdependencias que existen entre los mismos, así como los activos de información de la Institución, incluyendo aquellos vinculados con la estabilidad y permanencia del Estado Mexicano, de acuerdo a los artículos 3 y 5 de la Ley de Seguridad Nacional.  Elaborar el Documento de Identificación de Procesos, Activos e Infraestructuras Criticas y efectuar la valoración de activos de información, en términos de la posible pérdida de confidencialidad, integridad o disponibilidad, identificando los Activos clave y registrando los resultados en el documento: Matrices de infraestructuras críticas y Activos clave. |
| ERISC | Equipo de Respuesta a Incidentes de Seguridad de TIC del Instituto. | Bajo la coordinación y supervisión del GI-TIC, elaborar y mantener actualizada una Directriz rectora de respuesta a incidentes.  En coordinación con el GI-TICy de acuerdo a lo establecido en la Directriz rectora de respuesta a incidentes: Definir acciones de resolución de incidentes e integrar una Guía técnica de atención a Incidentes de acuerdo a la criticidad de los activos de TIC afectados.  Reportar al Responsable de seguridad de la información, los incidentes que se presenten y el resultado de su gestión.  Ejecutar las acciones necesarias para atender un incidente de seguridad de la información.  El ERISC, en coordinación con el Responsable del GI-TIC, deberá:   * Definir las acciones de atención a los incidentes con apoyo de la Guía técnica, respecto del Incidente que se haya presentado. * Ejecutar la solución necesaria. * Registrar los datos del Incidente y su solución.   Asegurar que se comunique el Incidente y su solución, al GI-TIC y a los Responsables de los dominios tecnológicos involucrados, así como a los usuarios afectados. |

1. METODOLOGÍA

La administración de riesgos es el proceso realizado por la STCI del Instituto, que tiene como propósito identificar los riesgos a que está expuesta en el desarrollo de sus actividades y analizar los distintos factores que pueden provocarlos, con la finalidad de definir las estrategias que permitan controlarlos y, por lo tanto, contribuir al logro de las metas y objetivos de una manera razonable.

Esta metodología es aplicable para identificar y medir el grado de impacto y probabilidad de ocurrencia de los riesgos dentro de un área, operación, función, programa o proceso específico. Una vez que el riesgo se ha identificado y evaluado, el Mapa de Riesgos permite visualizar los riesgos en relación con otros, valorar su impacto y planear la revisión de los controles para asegurar su efectividad y en su caso, recomendar su fortalecimiento para mitigarlos; todo este proceso y sus elementos, se consolidarán por medio del formato de Matriz de Administración de Riesgos.

La metodología tiene por objeto contribuir al cumplimiento de la misión institucional, asegurar la eficacia, eficiencia y economía de las operaciones, programas y proyectos, proteger contra daños o pérdidas los activos de la STIC, cumplir con el marco jurídico aplicable, salvaguardar, preservar y mantener los recursos públicos en condiciones de integridad, transparencia y disponibilidad para los fines a que están destinados y establecer los mecanismos para la administración de riesgos en la STIC del INR.

La Metodología se divide en 6 etapas principales como a continuación se describe:

**EVALUACIÓN DE RIESGOS.**

**Identificación, selección y descripción de riesgos.** La identificación de riesgos se realizará con base en las estrategias, objetivos y metas de los proyectos, programas, áreas y/o procesos del Instituto, lo cual constituirá el inventario de riesgos; el proceso de identificar y analizar riesgos debe ser una práctica sistemática, ya que es un componente relevante dentro de un sistema de control interno efectivo. Es por ello, que la STIC debe enfocarse prioritariamente a la atención de los riesgos en los ámbitos y niveles relevantes, alineados en forma directa a los objetivos y metas, con el propósito de tomar las acciones preventivas necesarias para minimizar su posibilidad de ocurrencia y, en su caso, poder controlar y administrar adecuadamente sus efectos, la identificación, selección y descripción de riesgos.

La identificación de riesgos debe hacerse en forma preventiva, documentando aquellos que potencialmente pueden incurrir de darse determinadas circunstancias durante la consecución de las metas y objetivos institucionales.

**Clasificación de los riesgos.** Se realizará en congruencia con la descripción del riesgo, considerando el origen más representativo del riesgo identificado:

**Sustantivo:** Aquellos que se determinen como prioritarios en las áreas sustantivas.

**Administrativo:** Son los relacionados con los servicios proporcionados por el área administrativa de la Secretaria, y se pueden detectar tanto en las áreas sustantivas o de apoyo.

**Legales:** Son aquellos que tienen implicaciones legales.

**Financiero:** Son los riesgos detectados en el ejercicio de los recursos financieros utilizados para el logro de los objetivos. Se vinculan con las actividades desarrolladas en el área financiera.

**Presupuestal:** Son los riesgos detectados en el ejercicio del presupuesto.

**Servicios:** Se refiere a los que se vinculan con los servicios generales proporcionados por el área de recursos materiales y servicios.

**Recursos Humanos:** Se refiere a aquellos que se vinculan con los servicios proporcionados por el área de recursos humanos.

**TIC’s:** Son los detectados en el desarrollo, implantación y mantenimiento de los sistemas de información y son determinados en la DGTI.

**Identificación de factores de riesgo.** Atenderá a los factores internos y externos que indican la presencia de un riesgo o tiendan a aumentar la probabilidad de materialización del mismo.

**Identificación de los posibles efectos de los riesgos.** Se describirán las consecuencias que, de materializarse el riesgo identificado, incidirán en el cumplimiento de los objetivos y metas que en su caso se afectarían;

Valoración inicial del grado de impacto.

Valoración inicial de la probabilidad de frecuencia.

En esta etapa los riesgos deberán valorarse sin considerar los controles existentes para administrar el riesgo, tanto en el Grado de Impacto como en la Probabilidad de Ocurrencia.

**EVALUACIÓN DE CONTROLES.**

Se realizará conforme a lo siguiente:

Descripción de los controles existentes para administrar el riesgo. Se deberán describir los principales controles identificados, por factor, que tiene laSTIC para administrar el riesgo identificado.

Descripción de los factores que sin ser controles promueven la aplicación de éstos.

Descripción del tipo de control preventivo, correctivo y/o detectivo.

Determinación de la suficiencia o deficiencia del control para administrar el riesgo.

**VALORACIÓN FINAL DE RIESGOS RESPECTO A CONTROLES.**

Se deberán tener presente las características de los Controles definidos para administrar cada riesgo identificado. La Valoración Final del riesgo nunca podrá ser superior a la Valoración Inicial.

Se realizará conforme a lo siguiente:

Se dará valor final al Grado de Impacto y a la Frecuencia/Probabilidad de Ocurrencia del riesgo con la confronta de los resultados de las etapas de evaluación de riesgos y de controles, y

Se deberá determinar la valoración final del Grado de Impacto y Frecuencia/Probabilidad de Ocurrencia del riesgo.

Para la valoración inicial y final del impacto y de la frecuencia/probabilidad de ocurrencia, se podrán utilizar metodologías, modelos y/o teorías basados en cálculos cualitativos o cuantitativos, lo cual se definirá entre los responsables de la Administración de Riesgos y Seguridad de la Información del Instituto.

**RESULTADO DE RIESGOS.**

Los riesgos se evaluarán de acuerdo al límite máximo permitido de acuerdo al MAAGTICSI, considerando para su tratamiento los riesgos que se identifiquen como Altos, y los identificados como Medio y Bajos se monitorearán para asegurar que no se incrementen a Altos, en función del grado de impacto y la frecuencia/probabilidad de ocurrencia.

**DEFINICION DE ESTRATEGIAS Y ACCIONES PARA SU ADMINISTRACIÓN.**

Las estrategias constituirán las opciones para administrar los riesgos basados en su valoración respecto a controles, permiten tomar decisiones y determinar las acciones de control.

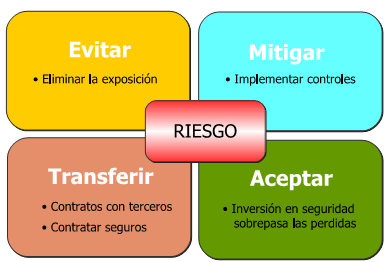
Algunas de las estrategias que pueden considerarse independientemente, interrelacionadas o en su conjunto, son las siguientes:

**Evitar el riesgo.-** Se aplica antes de asumir cualquier riesgo. Se logra cuando al interior de los procesos se generan cambios sustanciales por mejora, rediseño o eliminación, resultado de controles suficientes y acciones emprendidas.

**Mitigar el riesgo.-** Se aplica preferentemente antes de optar por otras medidas más costosas y difíciles. Implica establecer acciones dirigidas a disminuir la probabilidad de ocurrencia (acciones de prevención) y el impacto (acciones de contingencia), tales como la optimización de los procedimientos y la implementación de controles.

**Aceptar el riesgo.-** Se aplica cuando el riesgo se encuentra en un nivel que puede aceptarse sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

**Transferir el riesgo.-** Implica que el riesgo se controle mediante la responsabilidad de un tercero que tenga la experiencia y especialización necesaria para asumirlo.



A partir de las estrategias definidas, se describirán las acciones viables jurídica, técnica, institucional y presupuestalmente, tales como la implementación de políticas, optimización de programas, proyectos, procesos, procedimientos y servicios, entre otras.

**SEGUIMIENTO DE ESTRATEGIAS, ACCIONES Y ANÁLISIS COMPARATIVO DE RIESGOS**

Para la implementación y seguimiento de las estrategias y acciones, se dará seguimiento a la Administración de Riesgos, considerando análisis, estrategias y acciones de la Matriz de Administración de Riesgos; así como, las áreas responsables de la implementación, fechas de inicio y de término, resultados esperados.

Se realizará un análisis anual del comportamiento de los riesgos, con relación a los determinados en la Matriz de Administración de Riesgos del año inmediato anterior, que considerará al menos los aspectos siguientes:

Comparativo del total de riesgos.

1. Variación del total de riesgos.
2. Riesgos identificados y cuantificados con cambios en la valoración final de 3.
3. probabilidad de ocurrencia y grado de impacto, así como los modificados en su conceptualización.

Conclusiones sobre los resultados cualitativos de la administración de riesgos.

Fecha de autorización, nombre y firma del RSII.

El resultado anterior, se informará en la sesión ordinaria del Grupo Integral de TIC.

1. ELEMENTOS para la administración de riesgos

|  |  |  |
| --- | --- | --- |
| **Elemento** | **Grupo de riesgos sobre los que incide** | **Escenario** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. DIRECTRICES DE ADMINISTRACIÓN DE RIESGOS

|  |  |  |  |
| --- | --- | --- | --- |
| **Necesidad en la STIC** | **Requerimiento** | **Escenarios** | **Impacto** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. MECANISMOS DE DIFUSIÓN

*[La STICdel Instituto establecerá el mecanismo y sus elementos para asegurar la difusión de la Directriz rectora y procurará su entendimiento en la totalidad de los involucrados del Instituto e instancias externas para los aspectos que les atañan.]*

1. MECANISMOS DE REVISIÓN

*[Los periodos de revisión y evaluación del mecanismo y sus elementos para asegurar el cumplimiento de la Directriz por parte de los involucrados y/o responsables de la procuración de su seguimiento se ha acordado con las áreas involucradas en periodos anuales (al menos una vez al año). Si fuera necesario, se revisará por medio de una petición formal de los responsables de su implementación y monitoreo.]*

1. Bitácora de Control de Cambios

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Revisión** | **Descripción del Cambio** | **Fecha de evaluación** | **Aprobador** | **Aceptado /Rechazado** | **Fecha de aplicación** |
| 01 | Actualización de la Imagen Institucional | JUN 15 | Mtra. Ma. De Lourdes Zaldívar Martínez | Aceptado | JUN 15 |
| 02 | Transición del SGC de la Norma ISO 9001:2008 a la Norma ISO 9001:2015  Revisión de contenidos y actualización de encabezados | MAY 18 | M. en I. María Isabel Garrido Galindo | Aceptado | MAY 18 |
| 03 | Actualización de Imagen Institucional | DIC 20 | M. en I. María Isabel Garrido Galindo | Aceptado | DIC 20 |