**Objetivo:**

El presente documento pretende establecer el plan de tratamiento de riesgos de seguridad de y privacidad de la información.

**Alcance:**

El presente plan define el tratamiento adecuado de los riesgos asociados a los activos de información y recursos informáticos del proceso de gestión tecnología Instituto distrital de las artes - Idartes.

| Fecha de Aprobación | Responsable del Documento | Ubicación |
|---|---|---|
| 25 de Julio de 2018 | Área de TIC | Página Intranet: http://comunicarte.idartes.gov.co/idartes |

| HISTÓRICO DE CAMBIOS | | |
|---|---|---|
| **Versión** | **Fecha de Emisión** | **Cambios realizados** |
| 01 | 25/07/2018 | Emisión Inicial |
| **Oficinas Participantes** | | |
| Subdirección Administrativa y Financiera<br>Área de TIC | | |

| Elaboró: | Aprobó: | Validó | Aprobó |
|---|---|---|---|
| ORIGINAL FIRMADO<br>**Luis Albeiro Cortés**<br>Contratista<br>Área de Tecnología | ORIGINAL FIRMADO<br>**Juan Carlos Cubillos**<br>Profesional Universitario Área de Tecnología<br><br>ORIGINAL FIRMADO<br>**Liliana Valencia Mejía**<br>Subdirectora Administrativa y Financiera | ORIGINAL FIRMADO<br>**Camila Crespo Murillo**<br>Contratista<br>Oficina Asesora de Planeación | ORIGINAL FIRMADO<br>**Luis Fernando Mejía Castro**<br>Jefe Oficina Asesora de Planeación |

## CONTENIDO

INTRODUCCIÓN ..... 3
1. OBJETIVO DEL DOCUMENTO ..... 3
2. ALCANCE ..... 3
3. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ..... 3
4. IDENTIFICACIÓN DE RIESGOS ..... 4
5. IDENTIFICACIÓN DE CONTROLES ..... 7
6. TRATAMIENTO DEL RIESGO ..... 9
7. NORMATIVA ..... 13
8. DEFINICIONES ..... 13

## LISTA DE FIGURAS

Figura 1. Proceso de gestión del riesgo de la seguridad de la información ..... 5
Figura 2. Actividades tratamiento del riesgo ..... 10
Figura 3. Tratamiento del riesgo ..... 12

## INTRODUCCIÓN

Es responsabilidad del Instituto Distrital de las Artes, implementar medidas que permitan mitigar y tratar los riesgos de seguridad y privacidad de la información.

El personal del IDARTES, contratistas, funcionaros y terceros, en cumplimiento de sus funciones, están sometidos a riesgos que pueden ocasionar el no cumplimiento de los objetivos misionales y administrativos del instituto; por lo tanto, es necesario tomar los controles necesarios, para identificar las causas y consecuencias de la materialización de dichos riesgos.

El presente plan tiene como objetivo orientar y facilitar la implementación y tratamiento eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta la implementación de controles.

## 1. OBJETIVO DEL DOCUMENTO

El objetivo es diseñar un plan de contingencia con las herramientas y procedimientos necesarios que permitan la recuperación de las actividades normales en el menor lapso de la información y servicios informáticos tales como los sistemas de información, los equipos, la infraestructura y el personal, ante eventuales sucesos internos o externos que produzcan su pérdida total o parcial, en el Instituto Distrital de la Artes.

## 2. ALCANCE

El plan de tratamiento de riesgos está limitado solo a los activos de información que tienen una clasificación como ALTA dentro del inventario de activos de información.

## 3. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El objetivo de gestión de riesgo de seguridad de la información es proteger la organización de las posibles consecuencias de las pérdidas de confidencialidad, integridad, disponibilidad, no-repudio, accountability (Responsabilidad y Rendición de Cuentas), autenticidad, o confiabilidad de los activos

De acuerdo con lo anterior y en el marco de la Política Nacional de Seguridad Digital, define la gestión de riesgos de seguridad digital como el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades.

Referente a los riesgos de privacidad se refiere a los que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

## 4. IDENTIFICACIÓN DE RIESGOS

El proceso de gestión de riesgo en la seguridad de la información está basado en las normas NTC-ISO/IEC 27005 y la NTC-ISO 31000

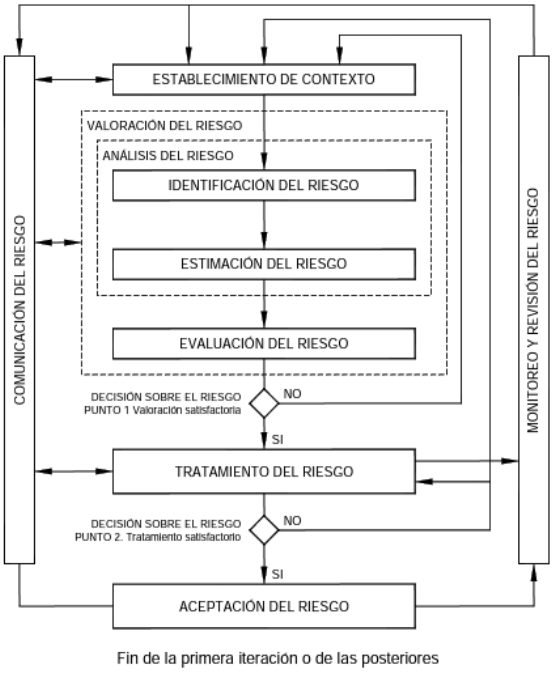
El objetivo de la identificación de riesgos es determinar que podría suceder que cause una perdida potencial y llegar a comprender el cómo, dónde y por qué podría ocurrir pérdida. Las causas pueden ser internas o externas, según lo que haya identificado la Entidad a través del Contexto estratégico.

Es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible y revisar los procesos según la clasificación.

**Ver:** *Matriz de riesgos de SGSI*

*Metodología de gestión de riesgos - SGSI*

*Figura 1. Proceso de gestión del riesgo de la seguridad de la información*




*Fuente: NTC-ISO/ IEC 27005*

El primer paso para el plan de tratamiento de riesgos es tomar como base el análisis de los riesgos de los activos de información.

| ID Riesgo | Escenario de riesgo |
|---|---|
| R1 | Acceso no autorizado de personas a equipos y servidores debido a la mala gestión de configuraciones de seguridad |
| R2 | Daño a los equipos y servidores parte de funcionarios y/o terceros. |
| R3 | Destrucción o daño físicos debido a exposición de temperaturas extremas y uso incorrecto de los mismos. |
| R4 | Fallas parciales o totales de equipos debido a no realizar jornadas de mantenimiento |
| R5 | Pérdida parcial o total del servicio o equipo causado por inundaciones o incendio. |

| | |
|---|---|
| R6 | Indisponibilidad en la prestación de servicio tanto a usuarios internos como externos debido a problemas o cortes en los servicios públicos primarios |
| R7 | Manipulación de los equipos de manera indebida, debido a la mala gestión de activos, control de cambios y políticas de dispositivos móviles. |
| R8 | Fallas parciales o totales en el funcionamiento de los equipos y servidores debido no contar con la implementación de controles ambientales en el área donde se encuentran alojados. |
| R9 | Divulgación de información por falta de procedimientos para el manejo de medios y devolución de activos de TI. |
| R10 | Manipulación del software o aplicativo de manera indebida, debido a falta de gestión de versiones, actualizaciones, mala gestión de contraseñas y por falta de pistas de auditoría (logs) |
| R11 | Degradación y/o problemas en la prestación del servicio por fallos o mal funcionamiento de aplicaciones por configuración errónea, desarrollos incompletos, cambio de versión, falta de pruebas y falta de pistas de auditoría (logs). |
| R12 | Descarga, instalación y uso de Software no licenciado o no autorizado en los equipos de computo |
| R13 | Acceso no autorizado al sistema debido a una ausencia de mecanismos de identificación y autenticación de usuario |
| R14 | Daño, perdida de datos e información de la base de datos debido a falta de controles de acceso, copias de seguridad y documentación. |
| R15 | Incumplimiento en la prestación del servicio por deficiencia en el servicio asociado al dominio contratado o por falta claridad en los acuerdos de calidad de servicio (SLA). |
| R16 | Falla, interferencia en el servicio de datos e Internet debido a conexión deficiente en el cableado y falta de mantenimiento de los dispositivos por parte de la empresa prestadora del servicio. |
| R17 | Abuso, falsificación, divulgación de la información por falta de pistas de auditoría (logs) falta de mecanismos de monitoreo y tablas de contraseñas sin protección. |
| R18 | Daño o perdida de datos e información por no contar con controles ante infecciones de malware |
| R19 | Manipulación de la información de manera indebida, divulgación de la información debido a la ausencia de controles de acceso de usuarios, mala gestión de contraseñas y a no contar con una clasificación de información adecuada |
| R20 | Robo de información debido a la ausencia de controles de acceso de usuarios, falta de protección de código malicioso mala gestión de contraseñas y falta de procedimientos para baja de usuarios. |
| R21 | Ataques a los portales de la entidad y publicación de contenidos con información confidencial o no autorizada. Debido a configuraciones de seguridad débiles. |
| R22 | Publicación de correo con contenidos de información confidencial o no autorizada. |
| R23 | Error de acceso a sistemas bancarios y Financieros debido a perdida de conectividad de Intranet y/o red |
| R24 | Robo de información debido a la ausencia de controles de acceso de usuarios, conexiones de red desprotegidas, falta de protección contra código malicioso y uso de medios removibles no controlado. |

| | |
|---|---|
| R25 | Escuchas encubiertas (sniffing) debido a tráfico sin protección, arquitecturas inseguras, envió de contraseñas sin cifrar y falta de protección ante código malicioso. |
| R26 | Manipulación de la información de manera indebida, divulgación de la información debido a la ausencia de controles de acceso de usuarios, mala gestión de contraseñas y a no contar con una clasificación de información adecuada |
| R27 | Mal funcionamiento de los dispositivos o activos de gestión de red debido a inadecuada configuración. |
| R28 | Debido no contar con una adecuada instalación eléctrica, se podría presentar el daño de los equipos tecnológicos en general. |
| R29 | Saturación de red debido a una inadecuada gestión de la red |
| R30 | Errores en el uso del sistema debido a la ausencia de un eficiente control de cambios en la configuración, entrenamiento insuficiente del personal, falta de conciencia acerca de seguridad de la información. |
| R31 | Errores en el uso de hardware y software debido a falta de capacitación técnica de personal de soporte técnico. |
| R32 | Falta de disponibilidad del personal de tecnología debido a contratación ineficiente, falta de separación de funciones y la falta de capacidad de personal. |
| R33 | Incumplimiento de compromisos debido a acciones deliberadas de los funcionarios causada por el inconformismo laboral de los mismos, ausentismo y/o por contar con funcionarios sin la competencia requerida. |
| R34 | Acciones legales en contra de la entidad por abuso de autoridad por parte de funcionarios |
| R35 | Suplantación o uso de personal no autorizado a los sistemas debido a gestión de acceso ineficiente y política de puestos de trabajo. |
| R36 | Hurto, fraude o sabotaje de equipos, medios, información o documentos, debido a la falta de protección de cables y dispositivos, una inadecuada protección de la información en lugares no apropiados o inseguros y por no contar con una práctica de clasificación de información que proponga los niveles de protección de la misma |
| R37 | Accesos no autorizados a oficinas debido a uso inadecuado o descuidado del control de acceso físico a oficinas y áreas protegidas. |
| R38 | Perdida de los servicios por perdida de suministro de energía. |
| R39 | Pérdida parcial o total del servicio causado por inundaciones, radiación, incendio y movimientos telúricos. |

## 5. IDENTIFICACIÓN DE CONTROLES

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas.

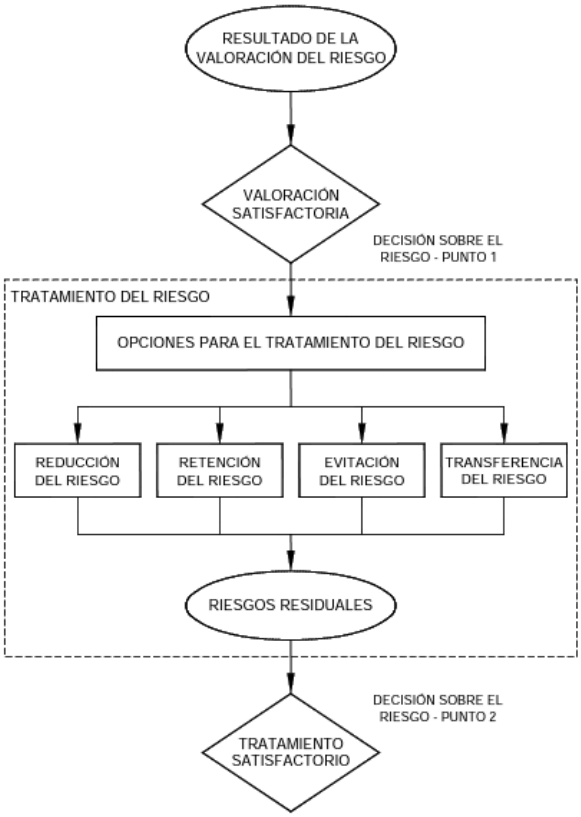
| ID Control | Controles Existentes |
|---|---|
| 1 | Acceso restringido a personal del área de sistemas. |
| 2 | Políticas de seguridad de la información. |
| 3 | Compromiso del funcionario con las políticas de seguridad de la información. |
| 4 | Sistema de aire acondicionado. |
| 5 | Plan de mantenimiento de equipos informáticos |
| 6 | Planes de contingencia TIC |
| 7 | Funcionamiento de las UPS y planta eléctrica en las sedes y escenarios del IDARTES, que brinda Equipo de protección de UPS una autonomía de 20 minutos aproximadamente. |
| ID Control | Controles Existentes |
| 8 | Inventarios de activos de TI. |
| 9 | Plan de emergencias y contingencias de la entidad. |
| 10 | Segmentación de red |
| 11 | Revisión del Firewall |
| 12 | Monitoreo firewall |
| 13 | Monitoreo canales herramienta de ETB |
| 14 | Revisión de equipos activos de red |
| 15 | Bitácora de registro de eventos. |
| 16 | Separación de los ambientes de desarrollo, pruebas y operación |
| 17 | Procedimiento “Administración de Cuentas de Usuario”. |
| 18 | Se cuenta con el listado de software autorizado y solo lo instalan los técnicos o ingenieros autorizados del área de sistemas. |
| 19 | Se cuenta con copia de seguridad de la base de datos Oracle. |
| 20 | Acuerdos de Calidad del servicio por parte del proveedor y obligaciones contractuales. |
| 21 | Contrato de servicio de proveedor del servicio |
| 22 | Acceso privilegiado solo a administradores. |
| 23 | Antivirus |
| 24 | Control de acceso de usuarios |
| 25 | Contrato de servicio de proveedor hosting garantizando la disponibilidad e integridad. |
| 26 | Copias de seguridad |
| 27 | Registros en el sistema ORFEO |
| 28 | Registros del Sistema SICAPITAL |

| | |
|---|---|
| 29 | Calidad del servicio del proveedor de Internet. |
| 30 | Restricción de acceso a las oficinas y áreas restringidas. |
| 31 | Contrato de servicio de proveedor Codensa |
| 32 | Restricción de acceso a las oficinas y áreas restringidas. |
| 33 | Capacitación en la utilización de los sistemas y seguridad de la información |
| 34 | Verificación de perfiles personal. |
| 35 | Revisión documentos precontractuales y verificación de perfil. |
| 36 | Asignación de presupuesto para cubrir la falta de recurso humano. |
| 37 | Documento de roles y responsabilidades. |

## 6. TRATAMIENTO DEL RIESGO

La implementación del tratamiento de riesgo inicia con la determinación de la actividad de tratamiento (mitigar, aceptar, evitar o transferir) a seguir para cada uno de los riesgos identificados en la Plantilla de análisis de riesgos, siguiendo el proceso planteado en la norma NTC-ISO-IEC27005. Se deben establecer controles para reducir, retener, evitar o transferir los riesgos.

*Figura 2. Actividades tratamiento del riesgo*




*Fuente: NTC-ISO/ IEC 27005*

A partir del tipo de riesgo, existen 4 alternativas de tratamiento:

**Evitar el riesgo:** evitar la actividad o la acción que da origen al riesgo particular, esta alternativa de tratamiento ocurre cuando su probabilidad es alta y representa un alto peligro para el instituto. Se debe tener si los costos para implementar los controles exceden los beneficios se puede tomar la decisión de evitar por completo el riesgo.

**Transferir o compartir el riesgo**: transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular. La transferencia se puede realizar mediante un seguro. Al transferir el riesgo a un tercero le damos la responsabilidad para su administración, pero no significa que eliminamos el riesgo.

**Mitigar el riesgo**: reducir mediante la implementación de controles, de manera tal que el riesgo residual se pueda revaluar como aceptable.

**Aceptar o asumir el riesgo**: retener el riesgo sin acción posterior. Los riesgos se aceptan cuando la frecuencia es baja e impacto leve, y no coloca en peligro la estabilidad del instituto.

Una vez definidas las alternativas de tratamiento de riesgos identificadas en la matriz, se fabricará el Plan para el Tratamiento de Riesgos con una serie de Controles que permitirán reducir el nivel de riesgo teniendo en consideración:

- Que sean adecuados y justificados
- Costo y tiempo esperado de implementar estas opciones
- Beneficios esperados
- Presupuestos
- Requisitos de negocio (cumplimiento de política y normas de seguridad)

A continuación, se describe el esquema de diligenciamiento:

**ID Riesgo:** Identificador que identifica el escenario de riesgo.

**Escenario de riesgo:** posibles consecuencias, daños temporales o permanentes a causa de ocurrencia de un incidente donde una amenaza explote una vulnerabilidad o conjunto de vulnerabilidades.
**Tratamiento del riesgo:** Actividades de tratamiento la cuales pueden ser evitar, transferir, mitigar y/o aceptar el riesgo.

**Controles/acciones a implementar:** Acciones establecidas desde el área o dependencia responsable para mitigar el riesgo.

**Controles asociados a NTC 27001:2013:** controles sugeridos de acuerdo al anexo A de la norma Técnica 27001:2013 para mitigar los riesgos.

**Recursos tecnicos:** Recursos necesarios para mitigar o disminuir los riesgos.

**Fecha maxima de implementación:** fecha limite para implementar las actividades de tratamiento propuesto.

**Responsables:** Área, dependencia o personal responsable de liderar la ejecucion y seguimiento de las actividades o controles del tratamiento.

En la siguiente figura se presenta modelo del plan de tratamiento de riesgos de seguridad y privacidad de la información el cual pertenece a la matriz de riesgos – SGSI.

*Figura 3. Tratamiento del riesgo*

Matriz de Riesgos - SGSI

| | | Plan de Tratamiento del riesgo | | | | | |
|---|---|---|---|---|---|---|---|
| ID Riesgos | Escenario de riesgo | Tratamiento del Riesgo | Controles / acciones a implementar | Controles asociados a NTC 27001:2013 | Recursos Técnicos | Fecha maxima de implementación | RESPONSABLES |
| R1 | Acceso no autorizado de personas a equipos y servidores debido a la mala gestión de configuraciones de seguridad | Asumir, Reducir Riesgo | Revisión continua de acceso personal del Área de tecnología. | A.11.1.1 | Sistema Biométrico | 31/12/2018 | Área de tecnología |
| R2 | Daño a los equipos y servidores por parte de funcionarios y/o terceros. | Reducir el riesgo, Evitar, Compartir o Transferir | Divulgación de políticas de seguridad | | | | Área de tecnología |
| R3 | Destrucción o daño físicos debido a exposición de temperaturas extremas y uso incorrecto de los mismos. | Reducir el riesgo, Evitar, Compartir o Transferir | Mantenimiento aire acondicionado. | | | | Área de tecnología |

*Fuente: Autor*

## 7. NORMATIVA

Guía de gestión de Riesgos (MSPI-MinTIC).

Décimo segundo lineamiento – Gestión del Riesgo (Sistema Integrado de Gestión Distrital).

Norma Técnica Distrital NTD-SIG 001-2011

NTC-ISO-IEC27001:2013: Sistemas de Gestión de la Seguridad de la información.

NTC-ISO-IEC27002:2013: Código de Buenas Prácticas en Gestión de la Seguridad de la Información

NTC-ISO 27005: Gestión del riesgo en la seguridad de la información.

NTC-ISO/IEC 31000: La gestión de riesgos, principios y directrices.

## 8. DEFINICIONES

**Activo de información:** Cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO 27000:2013)

**Activos primarios:** actividades, información y procesos del negocio (ISO 27005).

**Amenaza:** causa potencial de un incidente no deseado, que puede provocar daños a los activos, aplicativos, sistema de información o a la organización

**Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo

**Confidencialidad**: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (ISO 27000:2013)

**Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida.

**Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (ISO 27000:2013)

**Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

**Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

**Impacto:** El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales

**Información**: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. **(**ISO 27000:2013)

**MSPI:** Modelo de Seguridad de privacidad de la información.

**Riesgo en la seguridad de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

**Riesgo inherente:** riesgo intrínseco de cada actividad, proceso o trabajo, que no puede ser eliminado del sistema.

**Riesgo residual:** El riesgo que permanece tras el tratamiento del riesgo.

**Vulnerabilidad:** debilidad de un activo o control que puede ser explotada por una o más amenazas

***(Fuente ISO 27000)***