




# **PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

<b>ELABORADO POR</b>	<b>REVISADO POR</b>	<b>APROBADO POR</b>
LIDER DEL PROCESO	REPRESENTANTE DE LA DIRECCIÓN	GERENTE GENERAL

	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>		
<b>Código:</b> OD-407-02	<b>Versión:</b> 01	<b>Fecha de aprobación:</b> 08/05/2018	<b>Página:</b> 2 de 11

## 1. PRESENTACIÓN:

Realizar un plan de tratamiento de riesgos de seguridad de la información es la parte más compleja de la implantación de la norma ISO 27001. A la vez la evaluación del riesgo es un paso más importante al comienzo de su proyecto de seguridad de la información, se establecen las bases para la seguridad de la información en el Instituto.

La pregunta sería ¿por qué es tan importante? Es simple, pero no se entiende por muchas personas, la principal filosofía de ISO 27001 es encontrar los incidentes que puede ocurrir y la forma más apropiada para evitar los incidentes. No sólo eso, también tiene que evaluar la importancia de cada riesgo para que pueda enfocarse en los más importantes. Resulta interesante la lectura ISO 27005: ¿Cómo identificar los riesgos?.

## 2. DEFINICIONES:


- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.
- Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como

fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000). Análisis de Riesgo Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Cyberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **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. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades

públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6). Datos Personales Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación

	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>		
<b>Código:</b> OD-407-02	<b>Versión:</b> 01	<b>Fecha de aprobación:</b> 08/05/2018	<b>Página:</b> 5 de 11

y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000). Derecho a la Intimidad Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- 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. (ISO/IEC 27000).
- Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e

implantar los controles necesarios para proteger la misma. (ISO/IEC 27000). Privacidad En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- Responsabilidad Demostrada Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- Responsable del Tratamiento de Datos Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- Riesgo 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. (ISO/IEC 27000).
- Seguridad de la información Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Sistema de Gestión de Seguridad de la Información SGSI Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- Titulares de la información Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3). Trazabilidad  
Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

### 3. OBJETIVO

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en el INSTITUTO DE FINANCIAMIENTO PROMOCIÓN Y DESARROLLO DE TULUA – INFITULUA EICE. con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

### 4. MAPA DE RIESGO

PROCESO	IDENTIFICACIÓN DEL RIESGO				
	CAUSAS	CAUSAS	TIPO DE RIESGO	RIESGO	EFFECTOS
GESTIÓN INFORMÁTICA	No se tiene establecido una metodología dentro de la elaboración del presupuesto	No se tiene en cuenta el PETI dentro de la elaboración del presupuesto	Operativo	Ejecución inoportuna a las políticas que se plantean en el Plan Estratégico de Tecnología e Informática del instituto	Obsolescencia de equipos y vulnerabilidad a ataques informáticos
GESTIÓN INFORMÁTICA	No se tiene establecida una metodología para el seguimiento y control del cronograma de mantenimiento	Falta de coordinación entre sistemas y el mantenimiento general de la empresa	Operativo	No contar con un cronograma de mantenimiento preventivo aprobado	Daño de equipo, reprocesos, pérdida de información, demora de procesos
GESTIÓN INFORMÁTICA	No renovación de licencias de antivirus oportunamente	Antivirus desactualizado	Operativo	Ataque efectivo de un virus	Pérdida de información
GESTIÓN INFORMÁTICA	Falta de ética	Incumplimiento a las políticas de seguridad informática	Operativo	Manipulación sin autorización a la base de datos del sistema de información	Daño o pérdida de información Detrimiento patrimonial
GESTIÓN INFORMÁTICA	No tener una metodología para la realización de back ups	No tener una frecuencia de realización de back ups	Operativo	No realizar back up a intervalos planificados	Pérdida de Información
GESTIÓN INFORMÁTICA	No tener políticas de seguridad informática	No tener un control a la instalación de software a través de internet	Operativo	Tener software no legalizado en los equipos de cómputo del instituto	Sanciones por derecho de autor

## 5. EVALUACIÓN DEL RIESGO



<b>RIESGO</b>	<b>EFFECTOS</b>	<b>Zona de riesgo</b>	<b>Medidas de respuesta</b>	<b>CONTROLES</b>
Ejecución inoportuna a las políticas que se plantean en el Plan Estratégico de Tecnología e Informática del instituto	Obsolescencia de equipos y vulnerabilidad a ataques informáticos	Zona de riesgo moderada	Reducir el riesgo	Seguimiento trimestral al PETI
No contar con un cronograma de mantenimiento preventivo aprobado	Daño de equipo, reprocesos, pérdida de información, demora de procesos	Zona de riesgo moderada	Reducir el riesgo	Revisión de mantenimientos Se cuenta con procedimientos
Ataque efectivo de un virus	Pérdida de información	Zona de riesgo baja	Asumir el riesgo	Tener actualizado el antivirus
Manipulación sin autorización a la base de datos del sistema de información	Daño o pérdida de información Detrimiento patrimonial	Zona de riesgo alta	Compartir o transferir el riesgo	Autorización restringida y autorizada para la manipulación de la base de datos.  Copia de Seguridad Automática (Task manager)
No realizar back up a intervalos planificados	Perdida de Información	Zona de riesgo moderada	Reducir el riesgo	Automatización del sistema de información
Tener software no legalizado en los equipos de cómputo del instituto	Sanciones por derecho de autor	Zona de riesgo baja	Asumir el riesgo	Políticas de seguridad por directorio activo

## 6. ADMINISTRACIÓN DEL RIESGO

RIESGO	Medidas de respuesta	ACCIONES	RESPONSABLE	FECHA LÍMITE	INDICADOR	FRECUENCIA
Ejecución inoportuna a las políticas que se plantean en el Plan Estratégico de Tecnología e Informática del instituto	Asumir el riesgo	Validar cumplimiento de las acciones incluidas en el PETI en el periodo evaluado.	Director Administrativo y Financiero y Técnico Administrativo en Sistemas	Al cierre de cada trimestre	Porcentaje de ejecución trimestral del PETI	trimestral
No contar con un cronograma de mantenimiento preventivo aprobado	Asumir el riesgo	Seguimiento y control al cronograma de mantenimientos preventivos.	Director Administrativo y Financiero	30/06/2018 31/12/2018	Cumplimiento del cronograma de mantenimiento preventivo	semestralmente
Ataque efectivo de un virus	Asumir el riesgo	Actualizar licencias. Seguimiento al cronograma de Actualización de Licencias.	Técnico Administrativo de Sistemas. Director Administrativo y Financiero	30/06/2018 31/12/2018	Cantidad de licencias actualizadas / total Licencias	semestralmente
Manipulación sin autorización a la base de datos del sistema de información	Reducir el riesgo	Capacitación en Código de Ética Socializar las Políticas e Seguridad Informática. Inducción y	Técnico Administrativo de Sistemas	30/06/2018 31/12/2018	Cumplimiento del plan de Inducción y reinducción.	semestralmente
No realizar back up a intervalos planificados	Asumir el riesgo	Realizar seguimiento al Backup automático diario	Técnico Administrativo de Sistemas	30/06/2018 31/12/2018	Carpeta Virtual "400.5 Backup" en el equipo del técnico de Sistemas	Mensual
Tener software no legalizado en los equipos de cómputo del instituto	Asumir el riesgo	Verificar la instalación de software ilegal	Director de Control Interno	30/06/2018 31/12/2018	Cumplimiento del cronograma de mantenimiento preventivo	Semestral

## 7. CONCLUSIONES

De acuerdo al mapa de riesgos, la evaluación y administración de los riesgos en INIFITULUA EICE. Podemos deducir que anualmente hay que revisar los siguientes documentos:

- a. Plan Estratégico de Tecnología e Informática PETI.
- b. Manual de políticas informáticas

- c. Cronograma de mantenimiento preventivo y correctivo de los equipos informáticos del Instituto.
- d. Plan de contingencia informática.

Es importante también que anualmente se renueven los contratos de:

- e. Licenciamiento de antivirus.
- f. Alquiler de espacio en la nube para realizar las copias de seguridad del Instituto
- g. Actualización del firewall del Instituto.

El personal de sistemas debe de tener capacitación en la implementación de la norma técnica ISO 27001.

Mayo 08 de 2018

:  
MANUEL GUILLERMO AREIZA Y.  
Técnico Administrativo de Sistemas

RODOLFO RAMIREZ ALVAREZ  
Gerente General