Plan de Tratamiento de

Riesgos de Seguridad y Privacidad de la Información

2024

IDEAM

Tabla de contenido

Introducción

Este plan define el análisis, evaluación y tratamiento de los riesgos de seguridad y Privacidad de la información, tomando como base la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP) y la "Guía de Gestión de Riesgos" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), realizando la identificación análisis, valoración, tratamiento de los riesgos e identificación de las vulnerabilidades y amenazas asociadas a los riesgos conforme a la norma ISO/IEC 27005:2011 Tecnologías de la información- Técnicas de Seguridad- Administración de riesgos de Seguridad de la Información.

Objetivo principal

Realizar el tratamiento de riesgos de seguridad y privacidad de la información alineada con la guía metodológica para la gestión del riesgo del DAFP adoptada por el IDEAM

Objetivos específicos

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que el IDEAM pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.
- Evaluar las medidas existentes a fin de determinar cuáles otras podrán ser adoptadas por el IDEAM.
- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en el Instituto
- Identificar los responsables de la aplicación de las medidas de tal forma que esto facilite su implementación.

Alcance

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016) se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el IDEAM.

El plan de tratamiento de riesgos evaluará las opciones de manejo y tratamiento para los riesgos identificados y evaluados en el análisis de riesgos, cuyos niveles de riesgo para cualquiera de las áreas de impacto resultaron como “Extremo” y “Alto”, en el marco de la operación por procesos de IDEAM y dando alcance al Modelo de Seguridad y Privacidad de la información regido por MINTIC.

Definiciones

- **Activos de Información.** Todo aquel elemento de información, recibido, gestionado o producido, que posee valor para la entidad y, por lo tanto, debe protegerse para el logro de la misión. Serán activos de información críticos aquellos que son imprescindibles o su valor es clave para la operación de la entidad. Cuando se trate de activos informáticos, se entenderán como aquellos dispositivos tecnológicos que permiten la emisión, transmisión, procesamiento y recepción de información.
- **Acuerdo de confidencialidad.** Conocido también como acuerdo de no divulgación, es un documento formal entre al menos dos partes interesadas, para compartir información considerada como confidencial, pero restringida para el uso público.
- **Acuerdo de Nivel de Servicio (ANS).** Documento que contiene las especificaciones o características de un servicio que se será entregado por un proveedor y su cliente o usuario. Entre dos o más áreas de una entidad, se conoce como Acuerdo de Nivel Operacional (OLA).
- **Agente de amenaza.** Entidad humana o no humana que explota una vulnerabilidad.
- **Anti Rootkits.** Aplicativo de software que busca bloquear un rootkits o código malicioso que permite el acceso privilegiado a una computadora de manera oculta al administrador, buscando dañar el funcionamiento normal del sistema operativo y algunas aplicaciones.
- **Bluetooth.** Especificación tecnológica para redes inalámbricas, permite transmisión de voz y datos entre dispositivos.
- **Cibernético.** Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas.
- **Cifrado.** Método que permite aumentar la seguridad de la información de un archivo o mensaje mediante la codificación de su contenido, para que sólo pueda leerlo por el usuario autorizado y que posea la contraseña de cifrado para descodificarlo.
- **Cloud Computing.** Concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos están ubicados en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente, a través de “la Nube” de Internet (Guía 12 Seguridad en la Nube, MinTIC).
- **Confidencialidad.** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27001).
- **Custodia.** Acción de guardar con cuidado y vigilancia una información o mensaje.
- **Disponibilidad.** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (ISO/IEC 27001).
- **Hardware.** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

- **IoT.** Sigla en inglés para Internet de las Cosas, que comprende la tecnología en la que se interconectan dispositivos u objetos cotidianos, mediante internet.
- **Infraestructura.** Conjunto de activos o recursos técnicos, servicios o instalaciones que se consideran necesarios para el desarrollo normal de procesos o actividades.
- **Integridad.** Propiedad de salvaguardar la exactitud y estado completo de los activos. (ISO/IEC 27001).
- NFC (Near Field Communication). Tecnología de comunicación inalámbrica de corto alcance que facilita el intercambio de información entre dispositivos como smartphones y tablets.
- **No Repudio.** Es la garantía de que no puedan ser negados los mensajes en una comunicación electrónica (Guía 3 Cero papeles, MinTIC). Esto permite vincular al autor con la responsabilidad derivada de sus actuaciones y certificar que los datos o información provienen de la fuente que dice ser.
- **OT.** Sigla en inglés para Tecnología Operacional y comprende los dispositivos, redes y software asociados a procesos industriales, como tareas robotizadas, redes inteligentes, entre otros. Al software que permite controlar y supervisar estos procesos industriales, se le conoce como SCADA.
- **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, ISO 22301 de 2012 y la NTC 5722 de 2009).
- **Privacidad.** 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, que genera la obligación de proteger dicha información en observancia del marco legal vigente.
- **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).
- **Riesgo de corrupción.** Posibilidad que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo inherente.** Es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Riesgo institucional.** Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:
    - Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
    - Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
    - Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
    - Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de

corrupción serán considerados como riesgos de tipo institucional.

- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización.
- **Seguridad de la información.** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Software.** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.
- **T.I.** Tecnología de la Información, generalmente se conoce así al área o dependencia que administra la tecnología en una entidad. Para el presente documento, OTI o TI hacen referencia a la Oficina de informática del IDEAM
- **Wifi.** Tecnología que permite la interconexión inalámbrica de dispositivos electrónicos a internet.

Metodología riesgos de seguridad de la información

El análisis del riesgo de seguridad de la información busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, evaluándolos con el fin de obtener información para calificar su nivel. Se han establecido dos aspectos: probabilidad e impacto, para tener en cuenta en el análisis de los riesgos identificados.

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo y puede ser medida con criterios de frecuencia si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos, que pueden propiciarlo, aunque éste no se haya materializado. El impacto se mide por las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. Los pasos para el análisis de los riesgos son:

CALIFICACIÓN DEL RIESGO

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

EVALUACIÓN DEL RIESGO

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.
Con la evaluación del riesgo, previa a la formulación de controles, se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina evaluación del riesgo inherente.

DESARROLLO PRÁCTICO – ANÁLISIS

Formato de Análisis de riesgos, el cual hace parte del proceso Administración del Sistema Integrado de Gestión de Calidad, donde se debe relacionar la siguiente información:

- Riesgo: Relacionar el riesgo redactado en el mapa de riesgos.
- Calificación de probabilidad: de acuerdo con la información cuantitativa y cualitativa generada por el análisis de los Riesgos.
- Calificación de impacto: de acuerdo con la información cuantitativa y cualitativa generada por el análisis de los Riesgos.
- Clasificación del riesgo: Ver componentes de la identificación del riesgo, en el apartado de clasificación de los riesgos.
- Evaluación: surge del cruce de los resultados cuantitativos de la calificación para probabilidad e impacto.

VALORACIÓN DE LOS RIESGOS

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

SEGUIMIENTO DE RIESGOS

La Oficina de Control Interno, realizará seguimiento a todo el componente de administración de ciber riesgos y verificará aspectos como:

- Cumplimiento de las políticas y directrices para la administración del riesgo en seguridad y privacidad de la información.
- Administración de los riesgos de seguridad y privacidad de la información por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Los resultados de la evaluación y las observaciones serán presentados a la Dirección General, en el momento que lo considere pertinente, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de

la Administración de estos riesgos en el IDEAM.

Responsabilidades

El IDEAM deberá definir los roles y responsabilidades de todas las partes interesadas en lo concerniente a la gestión de riesgos, promoviendo el monitoreo y revisión a la gestión en sus etapas, con el propósito de asegurar el cumplimiento de los planes de tratamiento proyectados, ejecutando los controles y acciones definidos, desarrollando e implementado procesos de control y gestión con el propósito de asegurar la efectividad y el cumplimiento de los objetivos institucionales.

Dichas responsabilidades son acordes a línea estratégica y las tres líneas de defensa del Modelo Integrado de Planeación y Gestión (MIPG), donde se aprueban las directrices para la gestión del riesgo en la entidad y la revisión y/o mejora de las políticas establecidas.

Mapa de riesgos de seguridad de la información

Riesgos de Gestión

Proceso	Descripción del riesgo / oportunidad	Fecha de identificación	Análisis Inherente	Controles	Análisis Residual
Gestión de Tecnología de Información y Comunicaciones	Posibilidad de pérdida reputacional por desalineación e incumplimientos de Planes, metas y objetivos institucionales, debido a la inoportuna comunicación en la definición de proyectos de TI entre las dependencias con la oficina de informática y recortes presupuestales que afectan a las necesidades de TI.	26/10/2023	moderado	1. Un funcionario y/o contratista de la Oficina de Informática realizará la actualización del Plan Estratégico de Tecnologías de la Información - PETI, que contemple las necesidades de la Entidad y la articulación con objetivos y metas institucionales, fortaleciendo la transformación digital de la entidad y el correcto uso y aprovechamiento de TI, mínimo una vez al año 2. Un funcionario y/o contratista de la oficina de Informática realizar un ejercicio de arquitectura empresarial que contribuya al mejoramiento de la infraestructura tecnológica, sistemas de información, gobernabilidad de la información y seguridad de la misma que permita el cumplimienyo de los objetivos institucionales, mínimo una vez al año.	Moderado
Gestión de Tecnología de Información y Comunicaciones	Posibilidad de pérdida Económica y Reputacional por degradación o afectación en la prestación de los servicios institucionales que soportan la operación de TI. Debido a obsolescencia tecnológica, carencia de mantenimientos preventivos y correctivos, daños de la infraestructura tecnológica, vencimiento soporte de garantía, errores humanos, desconocimiento en el manejo y gestión de las plataformas y desactualización de componentes y licenciamiento.	26/10/2023	Extremo	1. El contratista o proveedor de la Oficina de Informática debe realizar el mantenimiento preventivo y correctivo, mínimo una vez al año, conforme a las especificaciones de la entidad a nivel central, dejando como evidencia el informe de mantenimiento. Para las áreas operativas, dicho proceso debe ser realizado por los funcionarios de la dependencia que sean designados 2. Un funcionario y/o contratista de la Oficina de Informática debe renovar los servicios de Nube en el IDEAM, mínimo una vez al año, conforme a las especificaciones de la entidad, dejando como evidencia la adquisición de servicios en la nube. 3. Un funcionario y/o contratista de la Oficina de Informática debe brindar soporte tecnológico al IDEAM diariamente, a través del personal designado que presta el soporte mediante la herramienta definida para tal fin, y como resultado quedan los reportes mensuales de la gestión de casos. 4. Un funcionario y/o contratista de la Oficina de Informática debe gestionar la adquisición del hardware y software en el IDEAM, conforme a la programación del Plan Anual de Adquisiciones y a las necesidades de la Entidad, quedando como evidencia los contratos suscritos. 5. Un funcionario y/o contratista de la Oficina de Informática debe garantizar la transferencia de conocimiento en temas tecnológicos con jornadas de inducción y/o capacitación, como mínimo una vez al año..	Alto
Gestión de Tecnología de Información y Comunicaciones	Posibilidad de pérdida Económica y reputacional por afectación de la confidencialidad, integridad y disponibilidad de los servicios institucionales brindados al ciudadano debido a posible daño, fuga o pérdida de información física o digital, Inadecuado custodia de la información, no realización de respaldo información, ataques cibernéticos, descuido por parte de los colaboradores y acciones de personal mal intencionado.	26/10/2023	Extremo	1. Un funcionario y/o contratista de la Oficina de Informática programará y realizará los backups a través de la herramienta correspondiente, con una frecuencia diaria, semanal y mensual. Como evidencia, se dejará un reporte mensual. 2. El contratista de la Oficina de Informática realiza un informe sobre el análisis del estado actual de la seguridad y privacidad de la información, respecto a la normatividad vigente, una vez al año. 3. El contratista de la Oficina de Informática realizará el seguimiento y control al plan de tratamiento de riesgos y seguridad de la información, dependiendo de la periodicidad definida en los controles y planes de acción. Como evidencia, se dejará un reporte o reunion de seguimiento. 4. El contratista de la Oficina de Informática debe realizar la gestión de incidentes y eventos de seguridad reportados por los canales de la mesa de servicios, de acuerdo con la demanda de incidentes presentados. Como evidencia, quedará un informe o reporte de incidente 5. El contratista de la Oficina de Informática realiza un diagnóstico del estado actual y/o recomendaciones para la construcción del BIA (Análisis del impacto del negocio) y del BCP (Plan de continuidad del negocio) del Instituto, una vez al año, dejando como evidencia un documento	Alto

Riesgos de Corrupción

Proceso	Descripción del riesgo / oportunidad	Fecha de identificación	Controles	Análisis Residual
Gestión de Tecnología de Información y Comunicaciones	Posibilidad de afectación reputacional y económica por la estructuración de proyectos de TI para beneficio específico de un tercero o propio mediante la manipulación deliberada de fichas técnicas y documentos contractuales, adaptándolos a medida con el propósito de favorecer intereses personales o de terceros.	23/08/2023	El contratista y/o funcionario de la oficina de Informática realizará los estudios previos de acuerdos con las necesidades expuestas por las diferentes dependencias del IDEAM para la gestión del proceso contractual, como evidencia el documento de estudios previos..	Moderado
			El jefe de la oficina de Informática revisará y validará la información continuidad en los estudios previos proyectados, como evidencia quedará el respectivo estudio previo firmado.	
			El jefe de la dependencia solicitante realizara revisión y validación de los estudios previos remitidos desde la oficina de Informática, como evidencia estará los correos electrónicos y el respectivo estudio firmado.	

Plan de implementación del tratamiento de riesgos de seguridad y privacidad de la información

El Plan de implementación el tratamiento de riesgos de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento trimestral.

FASE I: IDENTIFICACIÓN	
ACTUALIZACIÓN DE MATRIZ DE RIESGOS	
Objetivo	Actividades
Realizar la Actualización de los riesgos de gestión, corrupción y ciber riesgos	Realizar un análisis de la efectividad de los controles y la identificación de nuevos riesgos de seguridad y privacidad de la información.
	Realizar la actualización de la matriz de riesgos.

FASE II: SEGUIMIENTO	
SEGUIMIENTO A LA EFECTIVIDAD DE LOS CONTROLES DISEÑADOS	
Realizar Seguimiento y monitoreo a los riesgos	Actualizar procedimientos y lineamientos técnicos sobre la gestión de los riesgos de seguridad de la información.

FASE II: SEGUIMIENTO	
SEGUIMIENTO A LA EFECTIVIDAD DE LOS CONTROLES DISEÑADOS	
identificados.	Realizar monitoreo mensual con reporte trimestral de los riesgos de seguridad de la información

Hoja de ruta

Para cada una de las fases planteadas para la vigencia 2024 se establecen las fechas de culminación de la misma con la cantidad de entregables.

	2024											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
FASE I							1					
FASE II			1			1			1			1

VERSIÓN	FECHA	DESCRIPCIÓN
01	29/10/2015	Actualización documento para SGI
02	26/06/2018	Actualización del documento y para dar cumplimiento al decreto 415
03	18/12/2019	Actualización del documento – contenido en cumplimiento al decreto 612 de 2018
04	18/01/2021	Actualización del documento – contenido en cumplimiento al CONPES 3995
05	17/01/2022	Actualización del documento.
06	01/08/2022	Actualización cronograma Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del IDEAM debido a la sentencia de la corte suprema que tumbo los contratos de tercerización interrumpiendo el que se venía ejecutando.
07	03/01/2023	Actualización del cronograma del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del IDEAM.
08	29/12/2023	Actualización del documento en su estructura y cronograma

ELABORÓ:	REVISÓ:	APROBÓ
Omar Villarreal Osorio Profesional Especializado Grupo GAESI	Juan David García Castaño Jefe Oficina Informática	Juan David García Castaño Jefe Oficina Informática