Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Dirección de Tecnología

2024

IU Digital de Antioquia

INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA

Historial de cambios

Versión	Fecha	Descripción del Cambio
01	31/01/2023	No aplica para la primera versión
02	26/01/2024	Se adecuaron las metas e indicadores al Plan de Desarrollo 2022-2026. Se actualizaron todos los componentes del plan

Contenido

1. Introducción

La Institución Universitaria Digital de Antioquia presenta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2023, en él se instaura un conjunto de actividades para crear requisitos de uso confiable en el entorno híbrido de la información a través de un enfoque basado en la gestión de riesgos, conservando la confidencialidad, integridad, privacidad y disponibilidad de la información de la entidad para moderar las posibles afectaciones a los activos que apoyan la evaluación de la educación y las investigaciones sobre factores que inciden en la calidad educativa.

El análisis de riesgos de los activos de información le permite a la IU Digital entender de una manera efectiva y eficiente los riesgos de afectación en la pérdida de confidencialidad, integridad, privacidad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis. Los escenarios de riesgo obligan a que las entidades como la IU Digital de Antioquia contemplen procesos integrales de gestión de riesgos enfocados en facilitar la confianza necesaria a las partes interesadas a través de una institución apta, confiable y que tiene capacidad de actuar frente a los diferentes factores externos causantes de inestabilidad en los procesos, afectación de la información y conflictos digitales.

2. Objetivos

2.1 Objetivo General

Definir las actividades necesarias para garantizar la integridad, confidencialidad y disponibilidad de la información a través de la gestión de los riesgos de Seguridad y Privacidad de la información, Seguridad digital, ciberseguridad y Continuidad de la Institución Universitaria Digital de Antioquia.

2.2 Objetivos específicos

- Involucrar a la Alta Dirección en la gestión proactiva, pertinente y oportuna de los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad, que apoyan el cumplimiento de los objetivos estratégicos de la Institución.

- Identificar y gestionar los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de manera articulada con los riesgos de corrupción y gestión, de acuerdo con el Modelo Integrado de Planeación y Gestión (MIPG).
- Realizar un efectivo análisis de los riesgos que afectan los activos más críticos de la Institución en cuanto a confidencialidad, integridad, privacidad y disponibilidad de la información.
- Hacer seguimiento a la implementación y cumplimiento de los controles y planes de tratamiento definidos, documentando las evidencias y resultados de las acciones realizadas.

3. Generalidades

3.1 Contexto estratégico

El presente plan está alineado y contribuye al logro de la misión, visión y demás elementos del direccionamiento estratégico de la Institución Universitaria Digital de Antioquia, los cuales se estipulan en el Plan Estratégico Institucional, PETI y el Plan de Seguridad de la Información.

Articulación con el contexto estratégico	
Objetivo estratégico al que aporta	• Fortalecer análisis y divulgación de información relevante para grupos de interés. • Mejorar los procesos administrativos. • Generar una cultura de calidad e innovación en todos los niveles de la organización. • Fortalecer el uso de la tecnología.
Gestión y Desempeño Institucional - MIPG	• Política Gobierno Digital • Política de Seguridad Digital • Política de Gestión Documental • Política de Transparencia, acceso a la información pública y lucha contra la corrupción • Gestión del conocimiento y la innovación

4. Alcance

El presente plan aplica en los procesos de la Institución Universitaria Digital de Antioquia que impliquen almacenamiento, procesamiento, recolección, intercambio, recuperación y consulta de información, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

5. Contexto normativo

La formulación e implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información están fundamentadas principalmente en el siguiente sustento legal:

- Ley 527 de 1999: "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
- Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- CONPES 3854 de 2016: "Política de Seguridad Digital del Estado Colombiano".
- Decreto 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Dirección de Gestión y Desempeño Institucional, (diciembre de 2020). Guía para la administración del riesgo y el diseño de controles en entidades públicas.
- Decreto 612 de 2018: "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado".
- Ley 1273 de 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- ICONTEC, (22/03/2006). NTC-ISO\IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
- ICONTEC, (19/10/2022). GTC-ISO\IEC 27002: Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.

- ICONTEC, (16/12/2020). NTC-ISO\IEC 27005: Tecnología de la información. Técnicas de seguridad. Gestión de riesgos para la seguridad de la información.
- ICONTEC, (18/07/2018). NTC-ISO 31000: Gestión del riesgo. Directrices.

6. Definiciones

- **Vulnerabilidad:** es una debilidad, deficiencia o falta de control en los procesos, tecnología o administración.
- **Amenaza:** peligro latente de que un evento pueda causar un incidente no deseado, presentando daños y/o pérdidas a los activos de información.
- **Riesgo residual:** el riesgo que permanece tras el tratamiento del riesgo después de aplicar los controles.
- **Privacidad**: es el aspecto que se ocupa de la capacidad que una organización o individuo tiene para determinar el tratamiento que se les da a los datos de recolecta o produce.
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia**: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Control**: acción o medida que modifica el nivel del riesgo.
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.
- **Gestión de riesgos:** proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.
- **Incidente de seguridad de la información**: resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.
- **Información:** conjunto organizado de datos que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.
- **Integridad:** propiedad de exactitud y completitud.
- **Impacto**: efecto negativo o positivo que resultaría en caso de materializarse un riesgo.
- **Nivel de riesgo:** magnitud de un riesgo o de una combinación de riesgos, es la combinación del impacto y posibilidad.

- **Activo de información:** la información imprescindible o de alto valor para la Institución se llama Activo de Información, su protección es uno de los objetivos del SGSI. (Ej.: Información, sistemas de información, servicios, *hardware, software* y personas).
- **Probabilidad**: posibilidad de materialización del riesgo analizado. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Riesgo:** es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos. Se expresa en términos de probabilidad y consecuencias (impacto).
- **Riesgo Inherente**: es el nivel de riesgo sin implementar controles.
- **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.

7. Desarrollo del Plan de Seguridad y Privacidad de la Información

La metodología para la evaluación y gestión de riesgos de los sistemas de gestión vigentes de la IU Digital de Antioquia se basa en la NTC-ISO 31000, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública – DAFP, principalmente en lo dispuesto en su Anexo 4 - Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, la cual se encuentra definida en la política de gestión de riesgos de la entidad.

Esta política tiene como objetivo generar un lineamiento para la gestión del riesgo de la IU Digital de Antioquia, que permita la mejora continua y el cumplimiento de los objetivos institucionales mediante el tratamiento de controles, fortaleciendo el desempeño de los procesos y la transparencia en la gestión institucional y aplica para todos los procesos institucionales.

Por lo anterior se realiza la gestión de todos los riesgos en la IU Digital de Antioquia , ya sean de gestión, corrupción, seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad, las actividades de identificación y análisis de los riesgos se realizan con los líderes de cada proceso como propietarios de los activos, por lo cual deben velar porque los custodios de la información cumplan con los controles establecidos para procurar la confidencialidad, integridad, privacidad y disponibilidad de la información institucional. El objetivo del análisis es identificar los

riesgos, evaluar la pertinencia de los controles y determinar el tratamiento del riesgo que lo lleve a un nivel aceptable, teniendo en cuenta el siguiente orden:

7.1 Establecimiento de contexto

Se establece un contexto del proceso con los siguientes aspectos:

- **Contexto del proceso:** se determinan las características o aspectos esenciales del proceso y sus interrelaciones.
- **Diseño del proceso:** claridad en la descripción del alcance y objetivo del proceso.
- **Interrelación con otros procesos:** relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
- **Transversalidad:** procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
- **Procedimientos asociados:** pertinencia en los procedimientos que desarrollan los procesos.
- **Responsables del proceso:** grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- **Comunicación entre los procesos:** efectividad en los flujos de información determinados en la interacción de los procesos.

Y luego se establece el tipo de proceso: Misional, Estratégicos, de Apoyo y Evaluación y Control.

7.2 Valoración y análisis del riesgo

Se realiza la identificación de los riesgos, sus causas, vulnerabilidades, amenazas (identificación, descripción, tipo), consecuencias y se determina la clase de riesgo basados en la probabilidad e impacto, todo esto asociado a aquellos eventos o situaciones que puedan afectar los activos de información interrumpiendo el normal desarrollo de los procesos.

7.3 Tratamiento del riesgo

El tratamiento del riesgo consiste en seleccionar y aplicar las medidas adecuadas, con el fin de 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), y luego se definen acciones de mitigación de riesgos (actividades o tareas, responsables, plazo de ejecución y seguimiento).

7.4 Comunicación de riesgos

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, la Institución 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.

7.5 Información de riesgos y revisión

Los riesgos identificados traen consigo controles que incluyen el monitoreo de los eventos correspondientes, invirtiendo los recursos de acuerdo con 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.

8. Mapa de ruta y seguimiento

La implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene lugar a partir del desarrollo de actividades y la ejecución de esfuerzos encaminados a su consecución, comprendiendo indicadores que facilitan la medición de las acciones e identificando plenamente la descripción de los productos y/o resultados alcanzados y esperados, de la siguiente manera:

No	Actividad	Meta establecida	Unidad de medida	Producto o resultado esperado
1	Socialización de la estrategia para el análisis de riesgos, ciberseguridad y seguridad informática.	2	Unidad	Evidencias de campañas sensibilización
2	Actualización de la matriz de riesgos de seguridad y privacidad de la información.	2	Unidad	Matriz de riesgos actualizada
3	Publicación de riesgos, ciberseguridad y seguridad informática.	1	Unidad	Enlace de transparencia
4	Informe de seguimiento y gestión de riesgos, ciberseguridad y seguridad informática.	1	Unidad	Informe final de la gestión de riesgos
5	Socialización de la gestión de riesgos.	1	Unidad	Acta de reunión de socialización de la gestión de riesgos.

En ese sentido, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información será objeto de **un (1) seguimiento semestral**, conforme a los formatos dispuestos para tal fin en el Modelo de Operación por Procesos institucional.

Acción	Nombre	Fecha
Proyectó y Elaboró:	César Alexander Zapata Jiménez	19/01/2024
Revisó y Aprobó:	Jhonatan Arroyave Jaramillo	23/01/2024
Los anteriores, declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales y, por lo tanto, bajo nuestra responsabilidad presentamos para firma.		

IU Digital de Antioquia

INSTITUCIÓN UNIVERSITARIA
DIGITAL DE ANTIOQUIA