Universidad Industrial de Santander

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

Planes Institucionales y Estratégicos del Decreto 612 de 2018

División de Tecnologías de la Información y la Comunicación
Enero de 2025

Tabla de Contenido

1. INTRODUCCIÓN

La seguridad de la información es un pilar fundamental para garantizar la continuidad de las operaciones, la protección de los activos de información y el cumplimiento de las normativas vigentes en la Universidad Industrial de Santander. En un entorno cada vez más digital y conectado, la identificación y el tratamiento de riesgos asociados a la seguridad de la información son actividades esenciales para prevenir incidentes que puedan comprometer la confidencialidad, integridad y disponibilidad de la información institucional.

Mediante la definición del Plan de Tratamiento de Riesgos de Seguridad de la Información, la Universidad busca mitigar los riesgos presentes en el Mapa de Riesgos de Seguridad Digital, enfocados especialmente en aquellos ubicados en zona de riesgo residual alta y extrema. Este plan tiene como fin evitar situaciones que puedan impedir el logro de los objetivos institucionales, garantizando la continuidad y confiabilidad de los servicios ofrecidos.

El presente plan establece las acciones específicas a tomar para reducir los riesgos existentes, organizando estas medidas de seguridad de manera estructurada. Para cada una de las acciones se define claramente la tarea, el responsable y la fecha límite de realización, cubriendo el periodo de vigencia 2025. Estas medidas fueron definidas tras un análisis exhaustivo de los riesgos, proporcionando las herramientas necesarias para asegurar la protección adecuada de los activos de información críticos de la Universidad.

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información está alineado con los principios del Modelo de Seguridad y Privacidad de la Información emanado por el MinTIC, el MSE.01 Manual para la administración del riesgo y la Guía para la gestión del riesgo de seguridad de la información (estos últimos dos, documentos institucionales) y refleja el compromiso de la Universidad con la mejora continua en materia de seguridad de la información. Está basado en una orientación estratégica que promueve el desarrollo de una cultura preventiva; al comprender y contextualizar los riesgos, la Universidad puede planear acciones efectivas que minimicen las afectaciones potenciales en caso de materialización de los mismos.

2. OBJETIVO

Preservar la integridad, confidencialidad y disponibilidad de los activos de información críticos de la Universidad, mediante la definición de acciones concretas y la asignación clara

de responsables para el tratamiento de los riesgos de seguridad y privacidad de la información de la institución.

3. ALCANCE

De acuerdo a los lineamientos definidos por la Universidad en el MSE.01 Manual para la administración del riesgo, los riesgos residuales deben tratarse de la siguiente manera:

- Zona de riesgo bajo (verde): NO requiere Plan de Acción
- Zona de riesgo moderada (amarillo): plantear acciones encaminadas a mantener y fortalecer los controles existentes o crear nuevos, según análisis del proceso eventualmente puede requerir Plan de Acción.
- Zona de riesgo alta (naranja): Requiere de Plan de Acción, plantear acciones encaminadas a fortalecer los controles existentes o crear nuevos controles, a través de acciones de mitigación, reducción o transferencia.
- Zona de riesgo extrema (rojo): Requiere de Plan de Acción, plantear acciones encaminadas a reemplazar, rediseñar o eliminar la actividad que origina el riesgo.

Este plan, por lo tanto, se centra en dar tratamiento a los riesgos residuales de seguridad de la información ubicados en las zonas de riesgo extrema y alta, así como a los riesgos en zona moderada, según el análisis realizado.

4. DEFINICIONES

- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- **DTIC:** División de Tecnologías de la Información y la Comunicación.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Probabilidad:** es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. (NTC ISO 31000:2011).
- **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. (NTC ISO 31000:2011).

- **Riesgo residual:** Remanente después del tratamiento del riesgo. (NTC ISO 31000:2011).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

5. MARCO NORMATIVO

- Manual de gobierno digital
- Guía del MinTIC de seguridad y privacidad de la información para la gestión del riesgo (guía # 7)
- Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - MinTIC 2018.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 6 – noviembre 2022.
- Guía para la gestión del riesgo de seguridad de la información – DTIC UIS.
- Manual para la administración del riesgo. MSE.01 – Universidad Industrial de Santander – Versión 06 - enero 2024.
- Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas Anexo Técnico V 4.0 - Ministerio de Tecnologías de la Información y las Comunicaciones. - octubre 2021
- Anexo A de la ISO/IEC 27001.

6. GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Las siguientes son las etapas que hacen parte de la gestión de riesgos de seguridad de la información:

1. Identificar o actualizar los activos de información de la UAA.
2. Identificar los riesgos de seguridad de la información asociados a los activos.
3. Analizar los riesgos inherentes.
4. Valorar los controles.
5. Evaluar los riesgos residuales.
6. Planear el tratamiento de los riesgos.
7. Monitorear y revisar la gestión de los riegos.

En el MSE.01 Manual para la administración del riesgo y la Guía para la gestión del riesgo de seguridad de la información se dan los lineamientos completos para ejecutar cada una de estas etapas.

7. PLAN DE ACCIÓN

La gestión de los riesgos de seguridad de la información es un proceso dinámico y en constante evolución. No obstante, el presente plan de acción se basa en el análisis del mapa de riesgos de seguridad de la información correspondiente a enero de 2025. En este análisis, se ha identificado que el riesgo de **pérdida de confidencialidad** se encuentra clasificado en la zona de riesgo residual moderada. A partir de esta evaluación, se definen acciones concretas para mitigar los riesgos identificados, fortaleciendo los controles actuales y estableciendo nuevas medidas que garanticen la protección de los activos de información institucionales.

Ítem	Descripción de la actividad	Responsable	Fecha de finalización	Producto o entregable
1	Divulgar y socializar la política de seguridad de la información a las UAA involucradas en su cumplimiento (Fase II).	DTIC	30-nov-25	Plan de socialización y divulgación ejecutado.
2	Publicar y socializar el procedimiento de control de acceso físico a las instalaciones de procesamiento de información crítica.	DTIC	30-jun-25	Procedimiento publicado y socializado
3	Implementar múltiple factor de autenticación para las cuentas de correo electrónico funcionales institucionales.	DTIC	30-jun-25	Lista de cuentas de correo a las que se les activó el MFA.
4	Solicitar contraseñas de calidad para los correos electrónicos institucionales.	DTIC	30-jun-25	Cambio implementado
5	Ejecutar un simulacro de incidente como phishing o ingeniería social, para sensibilizar al personal sobre las amenazas más comunes y cómo reaccionar ante ellas.	DTIC	30-nov-25	Simulacro realizado
6	Implementar un SOC (Centro de operaciones de seguridad) que permita actuar proactivamente en la identificación de incidentes de seguridad *(Sujeto a asignación de recursos por parte de Rectoría).*	DTIC	30-nov-25	SOC implementado

Ítem	Descripción de la actividad	Responsable	Fecha de finalización	Producto o entregable
7	Realizar un análisis de vulnerabilidades para los activos de información críticos, para identificar y mitigar posibles puntos débiles en la infraestructura tecnológica.	DTIC	30-nov-25	Análisis de vulnerabilidades ejecutado.

8. TABLA DE CONTROL DE CAMBIOS

Versión	Fecha de aprobación del cambio	Descripción de cambios realizados
1	19/01/2021	Creación del documento.
2	19/01/2022	Actualización del documento.
3	17/01/2023	Actualización del documento.
4	30/01/2024	Actualización del documento.
5	29/01/2025	Actualización general del documento siguiendo los lineamientos de estructura sugeridos.