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 2026

Tabla de Contenido

1. INTRODUCCIÓN

La seguridad de la información constituye un pilar fundamental para garantizar la continuidad de las operaciones, la protección de los activos de información y el cumplimiento de la normativa vigente en la Universidad Industrial de Santander. En un entorno cada vez más digital e interconectado, la identificación, análisis y tratamiento de los riesgos asociados a la seguridad de la información se convierten en actividades esenciales para prevenir incidentes que puedan comprometer la confidencialidad, integridad y disponibilidad de la información institucional.

Mediante la formulación del Plan de Tratamiento de Riesgos de Seguridad de la Información, la Universidad busca gestionar y mitigar los riesgos identificados en el Mapa de Riesgos de Seguridad de la Información, con énfasis en aquellos clasificados en zona de riesgo residual alta y extrema. Este plan tiene como propósito reducir la probabilidad y el impacto de eventos que puedan afectar el cumplimiento de los objetivos institucionales, garantizando la continuidad y confiabilidad de los servicios ofrecidos.

El presente plan define las acciones específicas orientadas a la reducción de los riesgos existentes, organizando las medidas de seguridad de forma estructurada. Para cada acción se establecen claramente los entregables, responsables y los plazos de implementación, cubriendo el periodo de vigencia 2026. Estas medidas fueron definidas a partir del análisis de los riesgos identificados, con el fin de disponer de mecanismos efectivos para la protección de los activos de información críticos de la Universidad.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se encuentra alineado con los principios del Modelo de Seguridad y Privacidad de la Información del MinTIC, el MSE.01 Manual para la Administración del Riesgo y la GSI.04 Guía para la Gestión del Riesgo de Seguridad de la Información, estos últimos documentos institucionales, y refleja el compromiso de la Universidad con la mejora continua en materia de seguridad de la información. Asimismo, se fundamenta en una orientación estratégica que promueve una cultura preventiva, de manera que, al comprender y contextualizar los riesgos, la Universidad pueda planear acciones efectivas que minimicen las posibles afectaciones derivadas de su materialización.

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, requiere Plan de Acción para riesgos de corrupción, para los demás riesgos según análisis del proceso.
- 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.
- GSI.04 Guía para la gestión del riesgo de seguridad de la información – UIS – Versión 1.
- MSE.01 Manual para la administración del riesgo – UIS – Versión 8.
- 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 GSI.04 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 2026. En este análisis, se ha identificado que los siguientes riesgos se encuentran clasificados en zona de riesgo final moderada:

- Posibilidad de pérdida de integridad por ataque de malware o ransomware debido a ausencia de actualizaciones de seguridad en base de datos de sistemas de información.
- Posibilidad de perdida de integridad por fallas en el firware y hardware debido a hardware obsoleto sin mantenimiento o piezas de repuesto no disponibles o manipulación indebida en servidores físicos, centro de datos principal o alterno, infraestructura LAN y WIFI, sistema de almacenamiento, librería de cintas de backup, switches de distribución - nucleo - ToR, centros de cableado estructurado, firewall perimetral, controladoras.

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	Gestionar ante el Sistema General de Regalías – Gobernación de Santander la aprobación del proyecto "Adquisición de infraestructura para la actualización de la red LAN institucional de la Universidad Industrial de Santander".	DTIC	30-jun-2026	Proyecto aprobado
2	Dar continuidad a la implementación del Centro de Operaciones de Seguridad (SOC), orientando las actividades a la apropiación de las herramientas, la realización de pruebas, la implementación de ajustes y el análisis permanente de eventos de seguridad.	DTIC	30-nov-26	Informe de operación del SOC

Ítem	Descripción de la actividad	Responsable	Fecha de finalización	Producto o entregable
3	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-26	Análisis de vulnerabilidades ejecutado

Como complemento a las acciones de carácter técnico, se propone un plan de fortalecimiento de controles orientado a consolidar la cultura de seguridad de la información, mejorar los mecanismos de control de acceso físico y lógico, y reforzar las prácticas de autenticación y gestión de credenciales en la Universidad:

Ítem	Descripción de la actividad	Responsable	Fecha de finalización	Producto o entregable
4	Socializar de forma permanente de la Política de Seguridad y privacidad de la información de la Universidad.	DTIC	30-nov-26	INFOTIPS enviados, publicaciones y/o capacitaciones.
5	Publicar y socializar el procedimiento de control de acceso físico a las instalaciones de procesamiento de información crítica.	DTIC	30-jun-26	Procedimiento publicado y socializado
6	Continuar con la implementación de múltiple factor de autenticación para las cuentas de correo electrónico institucionales.	DTIC	30-nov-26	Lista de cuentas de correo a las que se les activó el MFA.
7	Solicitar contraseñas de calidad para los correos electrónicos institucionales.	DTIC	30-nov-26	Cambio implementado

8. TABLA DE CONTROL DE CAMBIOS

Versión	Fecha de aprobación	Descripción de cambios realizados
1	28/01/2026	Creación del documento.