Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones

PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2025

Tabla de Contenido

1. INTRODUCCIÓN 3
2. OBJETIVOS 4
a. General 4
b. Específicos 4
3. ALCANCE DEL SGSI 5
4. NORMATIVA APLICADA 5
5. POLÍTICA ADMINISTRACIÓN DEL RIESGO 6
a. Tratamiento de riesgos 6
b. Criterios de aceptación del riesgo 7
6. POLÍTICA DE ACEPTACIÓN DEL RIESGO 7
a. Principios generales 8
b. Criterios de aceptación del riesgo 8
c. Proceso de aceptación 9
d. Revisión y actualización 9
7. METODOLOGIA 9
8. DESARROLLO 11
a. Establecimiento Del Contexto Y Valoración Del Riesgo 11
b. Definición y Aprobación de Planes de Tratamiento 13
c. Materialización del Riesgo 13
d. Identificación de nuevos riesgos 14
e. Riesgos Priorizados 15
f. Plan de Acción 16
g. Oportunidades de Mejora 16
9. RECURSOS 17
10. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE CONTROLES 20
11. MEDICION 21
a. Indicadores de Seguimiento 21
REFERENCIAS BIBLIOGRÁFICAS 22

INTRODUCCIÓN

Las empresas hoy día, nos encontramos inmersas en la denominada revolución digital, en donde se reconoce el protagonismo de la información en sus procesos productivos, por tanto la importancia de tener su información adecuadamente identificada y protegida, como también la proporcionada por sus partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

La UPTC decide vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información aprobada por la Alta Dirección, y como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

1. OBJETIVOS

a. General

Proporcionar a la Universidad Pedagógica y Tecnológica de Colombia una herramienta que brinde las pautas necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información. Esto permitirá una toma de decisiones informada para reducir la probabilidad de que se materialice una amenaza, así como para disminuir la vulnerabilidad del sistema y el posible impacto en la entidad.

b. Específicos

- Consolidar una administración de riesgos acorde con las necesidades de la Universidad
- Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.

2. ALCANCE DEL SGSI

La gestión de riesgos de seguridad de la información y su tratamiento, podrá será aplicada sobre cualquier proceso de la Universidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

3. NORMATIVA APLICADA

Guía de Gestión de riesgos. Guía No.7 (Seguridad y Privacidad de la Información) de MINTIC. “Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2022.

4. POLÍTICA ADMINISTRACIÓN DEL RIESGO

Establecer los principios y lineamientos institucionales para la administración integral del riesgo de la información, como eje fundamental para la protección de los activos institucionales, el aseguramiento de la continuidad del servicio y el cumplimiento normativo. Esta política articula la gestión de riesgos con los Sistemas de Gestión implementados, incluyendo el SGSI (ISO/IEC 27001), el Sistema de Gestión de Riesgos (ISO 31000), la Gestión de Continuidad del Negocio (ISO 22301), y la Gestión de Servicios (ISO/IEC 20000-1).

a. Tratamiento de riesgos

En la UPTC, las acciones frente al riesgo se enmarcan en las siguientes categorías, conforme a las buenas prácticas establecidas en ISO 31000 y la normativa nacional:

- **ACEPTAR EL RIESGO:** Se admite el riesgo sin tomar acciones que alteren su probabilidad o impacto. Esta opción sólo es válida para riesgos clasificados como bajos, o cuando no existan medidas eficaces disponibles. La aceptación debe ser documentada y sujeta a seguimiento continuo.

- **REDUCIR EL RIESGO:** Se implementan controles para disminuir la probabilidad de ocurrencia y/o el impacto. Esto incluye medidas técnicas, organizativas, físicas o administrativas que minimicen la exposición al riesgo.

- **EVITAR EL RIESGO:** Se eliminan las actividades, procesos o situaciones que originan el riesgo. Esta medida es aplicable cuando el riesgo es inaceptable y no es posible mitigarlo adecuadamente mediante controles.

- **TRANSFERIR O COMPARTIR EL RIESGO:** Se transfiere total o parcialmente el riesgo a un tercero (por ejemplo, mediante seguros, acuerdos de nivel de servicio, o contratación de proveedores), sin que esto implique renunciar a la responsabilidad institucional. Esta opción es válida para riesgos operativos o tecnológicos específicos, pero no aplica para riesgos legales o éticos.

Todas las decisiones sobre tratamiento de riesgos deben quedar registradas formalmente en el plan de tratamiento correspondiente y estar alineadas con los criterios de aceptación definidos por la Dirección de Tecnologías.

b. Criterios de aceptación del riesgo

RIESGO	CRITERIO DE ACEPTACIÓN	TRATAMIENTO
Riesgos “Bajos”	Aceptar el riesgo Transferir o compartir el riesgo	pueden ser aceptados.
Riesgos “Medios”	Reducir el Riesgo	requieren mitigación y revisión
Riesgos “Altos o Extremos”	Evitar el riesgo	son inaceptables y deben tratarse obligatoriamente.

Ilustración 1 Criterios de aceptación del riesgo

5. POLÍTICA DE ACEPTACIÓN DEL RIESGO

La UPTC se compromete a adoptar los lineamientos institucionales para la aceptación de riesgos de seguridad y privacidad de la información, con el fin de apoyar decisiones informadas, responsables y trazables dentro del proceso de gestión del riesgo del SGSI, asegurando que estas decisiones se encuentren alineadas con la política de seguridad de la información, los objetivos institucionales y las normas internacionales aplicables.

a. Principios generales

- Todo riesgo debe ser identificado, analizado y valorado antes de tomar una decisión de aceptación.
- La aceptación del riesgo debe realizarse solo cuando:
  - El nivel de riesgo residual sea bajo o moderado y se considere tolerable.
  - No existan controles viables técnica o financieramente.
  - Los costos de mitigación superen los beneficios.
  - Existan planes de contingencia documentados.
- Los riesgos clasificados como altos o extremos no podrán ser aceptados sin la aprobación escrita del representante a Alta Dirección de las normas ISO 27001:2022, ISO 20000-1:2018, e ISO 22301:2015.
- Toda aceptación de riesgo debe ser documentada, revisada periódicamente y sujeta a reevaluación si las condiciones cambian.

b. Criterios de aceptación del riesgo

Nivel de riesgo residual	Aceptación permitida	Requisitos adicionales
Bajo	Sí	Documentación mínima
Moderado	Condicional	Aprobación del responsable del proceso + evidencia de justificación
Alto	No, salvo justificación técnica	Requiere aprobación formal del Director de DTIC
Extremo	Prohibido	Debe tratarse obligatoriamente

Ilustración 2 Aceptación permitida riesgo residual

Basado en la Guía A-RI-P35-G01 guía para la identificación, clasificación, gestión de riesgos y etiquetado de activos servicios y seguridad de la información para determinar el impacto y la probabilidad del riesgo.

c. Proceso de aceptación

El responsable del activo o proceso presenta una solicitud de aceptación documentada, incluyendo:

- Nivel de riesgo
- Controles existentes
- Justificación de no mitigación
- Análisis de impacto

El Grupo de Infraestructura revisa la solicitud y emite concepto técnico.

La solicitud es aprobada por:

- El responsable del proceso (riesgos bajos o moderados)
- El director de DTIC (riesgos altos)

d. Revisión y actualización

Esta política será revisada anualmente o cuando se modifique el contexto del SGSI, la matriz de riesgo, la declaración de aplicabilidad, o la normativa aplicable.

6. METODOLOGIA

El Plan de Tratamiento de Riesgos contempla la definición de actividades para mitigar los riesgos identificados sobre los activos de información institucional, y se estructura de acuerdo con las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC, 2016). Las actividades se desarrollan en las siguientes etapas:

ACTIVIDADES	TAREAS	RESPONSABLES	FECHA INICIAL	FECHA FINAL
Sensibilización	Socializar lineamientos de seguridad y privacidad de la información	Equipo de gestión	jul-25	dic-25
Definición de medidas de control	Selección de controles técnicos, administrativos, físicos o legales según el Anexo A de ISO/IEC 27001:2022.	lideres de servicios de TI equipo de gestión	jul-25	dic-25
Asignación de responsables	Identificación del propietario del activo, custodio o líder de proceso encargado del tratamiento.	Equipo de gestión	jul-25	dic-25
Identificación de riesgos de seguridad y privacidad de la información	Identificación y verificación de los riesgos de seguridad y privacidad de la información.	lideres de servicios de TI equipo de gestión	jul-25	dic-25
Registro de actividades en el formato A-RI-P35-F01	Documentación de las acciones planificadas, responsables, fechas, estado y observaciones.	Equipo de gestión	jul-25	dic-25
Seguimiento y evaluación	Verificación del cumplimiento de actividades y efectividad de los controles implementados.	lideres de servicios de TI equipo de gestión	jul-25	dic-25
Mejoramiento	Identificación de planes de mejoramiento	Equipo de Gestión	jul-25	dic-25
Monitoreo y revisión	Envío de avances e informes director de Tecnología.	lideres de servicios de TI equipo de gestión	jul-25	dic-25

Ilustración 3 Metodología

7. DESARROLLO

a. Establecimiento Del Contexto Y Valoración Del Riesgo

El contexto para la gestión del riesgo de la información en la UPTC contempla aspectos externos (normativos, regulatorios y del entorno tecnológico nacional), internos (procesos institucionales, estructuras de TI, cultura organizacional), y del proceso (tecnologías específicas, roles y responsabilidades), como base para identificar riesgos que puedan comprometer la seguridad y privacidad de la información, la seguridad digital y la continuidad de los servicios ofrecidos.

La definición del contexto se realiza con base en los lineamientos establecidos en los documentos institucionales: GUIA PARA LA IDENTIFICACION, CLASIFICACION, GESTION DE RIESGOS Y ETIQUETADO DE ACTIVOS SERVICIOS Y SEGURIDAD DE LA INFORMACION (A-RI-P35-G01), IDENTIFICACION, CLASIFICACION Y GESTION DE RIESGOS DE ACTIVOS DE INFORMACIÓN Y ETIQUETADO DE LA INFORMACIÓN (A-RI-P35) y las políticas del Sistema Integrado de Gestión (SIG-UPTC). Estos documentos permiten caracterizar los procesos, identificar interdependencias, y determinar escenarios de amenaza.

Identificación del Riesgo: La UPTC desarrolla este proceso considerando el inventario de activos institucionales, sus clasificaciones por criticidad y confidencialidad, y los factores de exposición definidos en el Catálogo de Amenazas del MinTIC. Esta identificación considera elementos como:

- Infraestructura física, tecnológica y lógica.
- Áreas de trabajo, entornos académicos y administrativos.

- Vulnerabilidades asociadas a procesos, sistemas o personas.
- Potenciales consecuencias de la materialización del riesgo.

Se documentan en el formato IDENTIFICACION, CLASIFICACION, GESTION DE RIESGOS Y ETIQUETADO DE ACTIVOS SERVICIOS Y SEGURIDAD DE LA INFORMACION A-RI-P35-F01 los siguientes elementos:

- Atributo afectado (Confidencialidad, Integridad, Disponibilidad).
- Activo relacionado.
- Amenazas y vulnerabilidades.
- Responsable del activo y del proceso.
- Consecuencias probables.

Valoración del Riesgo: La valoración se realiza aplicando la metodología establecida por la Guía para la Administración del Riesgo y el Diseño de Controles del DAFP, así como lo dispuesto por la Guía MinTIC de Gestión de Riesgos SPI (2016). Cada riesgo identificado es evaluado para determinar:

- Nivel de probabilidad y nivel de impacto.
- Riesgo inherente.
- Controles existentes y su diseño (preventivo, detectivo o correctivo).
- Naturaleza (manual o automatizado), periodicidad y propósito del control.
- Evidencia y seguimiento del desempeño del control.
- Impacto residual
- Probabilidad residual
- Riesgo residual ¿Aceptable según criterios? (Sí/No)

Los controles deben estar alineados con el Anexo A de la Norma ISO/IEC 27001:2022 y considerar la segregación de funciones, asignación de responsabilidades y mecanismos de evidencia para cada actividad. En el caso de activos cuya custodia pertenezca a un tercero o a otra dependencia, la definición y tratamiento del riesgo debe realizarse de forma conjunta.

Esta fase cierra con la elaboración de los Planes de Tratamiento por cada proceso responsable, su integración al Plan Institucional y seguimiento.

b. Definición y Aprobación de Planes de Tratamiento

Una vez concluida la valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios, los líderes de procesos de la UPTC, con el apoyo del equipo de gestión y gobierno de la DTIC y el Oficial de Seguridad y Privacidad de la información, deberán consolidar los respectivos planes de tratamiento.

Estos documentos serán aprobados por el director de tecnologías, asegurando la trazabilidad de las decisiones y la asignación formal de responsabilidades sobre cada actividad definida para mitigar riesgos con nivel de riesgo residual moderado, alto o extremo.

c. Materialización del Riesgo

En caso de que un riesgo se materialice, este deberá ser reportado de manera inmediata mediante el procedimiento A-RI-P07 “PROCEDIMIENTO PARA LA GESTION DE INCIDENTES”. Una vez registrado, se evaluará su impacto real, se actualizará el mapa de riesgos y se documentará la nueva valoración. Si el riesgo no estaba previamente identificado, se iniciará su proceso de caracterización e inclusión en el inventario institucional.

d. Identificación de nuevos riesgos

- **Riesgo emergente**: amenaza o vulnerabilidad no contemplada previamente en el inventario institucional de riesgos.
- **Mapa de riesgos**: herramienta que consolida la evaluación y priorización de riesgos activos en la institución.
- **Evento gatillo**: situación operativa que genera la necesidad de evaluar un riesgo no registrado.

Paso	Actividad	Responsable	Evidencia
1	Detectar el riesgo nuevo (incidente, hallazgo, observación, etc.)	Personal TI / Líder de proceso	Registro de evento / informe técnico
2	Notificar formalmente al equipo de gestión de riesgos DTIC	Responsable del activo / área afectada	Formato A-RI-P35-F01 (versión abreviada para reactividad)
3	Analizar el contexto del nuevo riesgo	Grupo de gestión de riesgos	Caracterización del riesgo
4	Valorar el riesgo según probabilidad e impacto	Grupo de gestión + área afectada	Nivel de riesgo inherente y residual
5	Proponer controles y plan de tratamiento reactivo	Grupo de gestión + responsable del proceso	Plan de acción (fechas, responsables, controles)
6	Incluir el riesgo en el Mapa de Riesgos institucional	Responsable SGSI	Mapa de riesgos actualizado y versionado
7	Registrar el seguimiento y resultado	Responsable SGSI y DTIC	Bitácora / seguimiento de eficacia

Ilustración 4 Plan al identificar nuevos riesgos

Plazos máximos sugeridos

Actividad	Plazo máximo
Notificación tras la detección	24 horas
Análisis y valoración	3 días hábiles
Inclusión en el mapa actualizado	5 días hábiles

Ilustración 5 Plazos máximos sugeridos

Criterios de prioridad

Riesgos detectados reactivamente serán clasificados como:

- **Críticos:** cuando afectan servicios vitales o información sensible → tratamiento inmediato.
- **Moderados:** atención en el siguiente comité de gestión.
- **Bajos:** pueden ser aceptados con documentación de justificación.

Revisión y mejora del protocolo

Este protocolo será revisado anualmente o tras la materialización de un riesgo crítico no identificado, para asegurar su eficacia y adaptabilidad.

e. Riesgos Priorizados

ID	Riesgo identificado	Nivel de riesgo	Activo afectado	Clasificación C-I-D	Control Asociado	Tratamiento propuesto
R1	Acceso no autorizado a información sensible	Alto	Motor base de datos institucional	Alta C, Alta I, Alta D	A.5.18 Autenticación de usuario	Control de autenticación multifactor, políticas de acceso mínimo
R2	Pérdida de datos por fallo de energía	Alto	Servidores críticos	Media C, Alta I, Alta D	A 8.13 Copia de seguridad de la información	Plan de respaldo, UPS y pruebas de recuperación periódicas
R3	Exposición de información por errores de configuración	Medio	Aplicaciones Web	Media C, Alta I, Media D	A 8.31 Separación de los entornos de desarrollo, prueba y producción A 8.29 Pruebas de seguridad en desarrollo y aceptación.	Auditorías técnicas, revisión de permisos, hardening

Ilustración 6 riesgos priorizados

f. Plan de Acción

Riesgo	Control propuesto	Responsable	Costo estimado	Fecha inicio	Fecha fin	Estado	Evidencia requerida
R1	Implementación de autenticación multifactor (MFA)	DTIC	$12.000.000	10/07/2025	20/08/2025	Pendiente	Registro de configuración y prueba funcional
R2	Simulación de recuperación de datos	Grupo soporte infraestructura	$25.000.000	15/08/2025	15/09/2025	Programado	Bitácora de pruebas, informes técnicos
R3	Revisión de configuraciones críticas	Responsable de aplicaciones	$18.000.000	01/07/2025	01/08/2025	En curso	Informe de revisión y plan de ajustes

Ilustración 7 Plan de Acción

g. Matriz de priorización de controles

Riesgo	Control sugerido	Nivel de riesgo residual	Impacto esperado del control	Costo estimado	Esfuerzo requerido	Prioridad
Fuga de datos sensibles	Implementar DLP + políticas de uso aceptable	Alto	Alto	Alto	Medio	**Alta**
Acceso indebido a servidores	MFA + bloqueo por IP	Medio	Medio	Bajo	Bajo	**Alta**
Daño físico a infraestructura TI	Adquirir gabinetes ignífugos	Bajo	Bajo	Medio	Medio	**Baja**
Ataques de phishing	Campaña de concienciación + simulacros	Medio	Alto	Bajo	Alto	**Media**
Pérdida de registros por apagón	Adquisición de UPS	Alto	Alto	Medio	Bajo	**Alta**
Saturación de red interna	Segmentación VLAN + monitoreo	Medio	Medio	Alto	Medio	**Media**

Ilustración 8 Matriz de priorización de controles

h. Oportunidades de Mejora

La administración de riesgos no sólo debe centrarse en la mitigación de amenazas, sino también en la identificación de oportunidades derivadas del tratamiento de los mismos. La UPTC entiende la oportunidad como el resultado positivo asociado al fortalecimiento de los controles, a la mejora de procesos y a la prevención de incidentes futuros.

A través de los planes de tratamiento y la ejecución eficaz de controles, la Universidad avanza en la madurez de su Sistema de Gestión de Seguridad de la Información (SGSI), mejora su postura institucional ante auditorías externas, y consolida una cultura organizacional orientada a la protección de la información y la continuidad de sus servicios.

8. RECURSOS

En el marco de su compromiso institucional con la gestión del riesgo de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, la UPTC dispone de los siguientes recursos clave:

RECURSO HUMANO CALIFICADO:

Conformado por el Equipo de Gestión, el Oficial de Seguridad de la Información, líderes de procesos, responsables de activos y grupos de apoyo interdisciplinario.

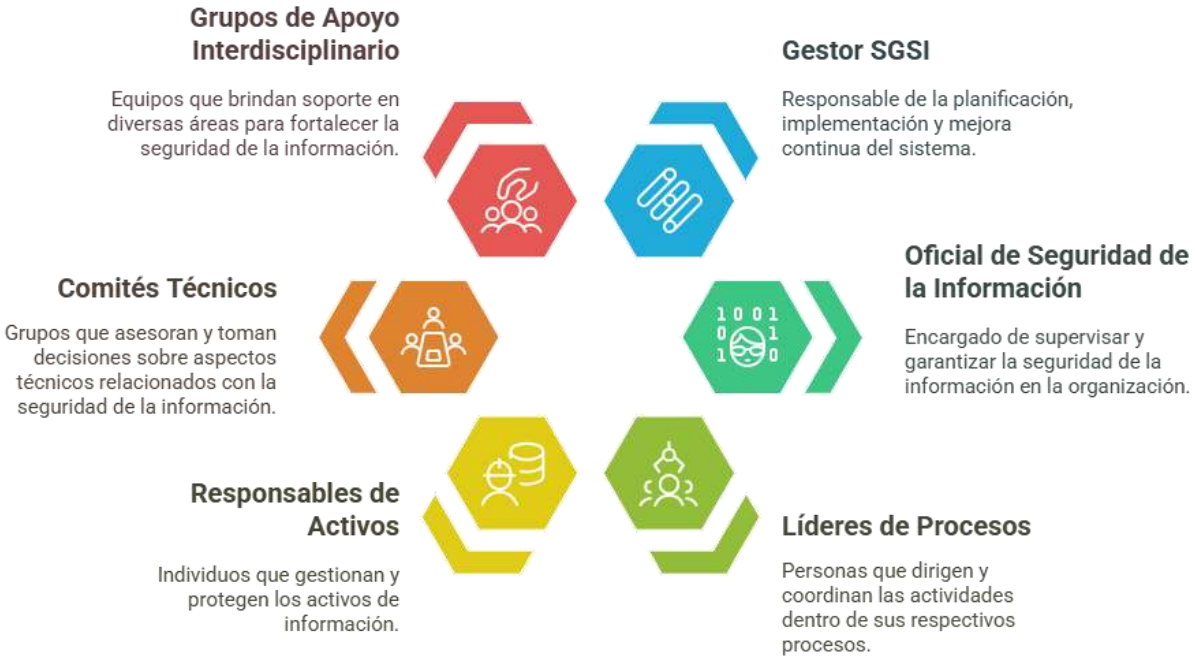

Ilustración 9 recurso humano para la gestión de riesgo

HERRAMIENTAS DE GESTIÓN:

Formatos normalizados como el A-RI-P35-F01 para la identificación, análisis y tratamiento de riesgos; inventario institucional de activos; y herramientas de seguimiento en el SIG-UPTC.

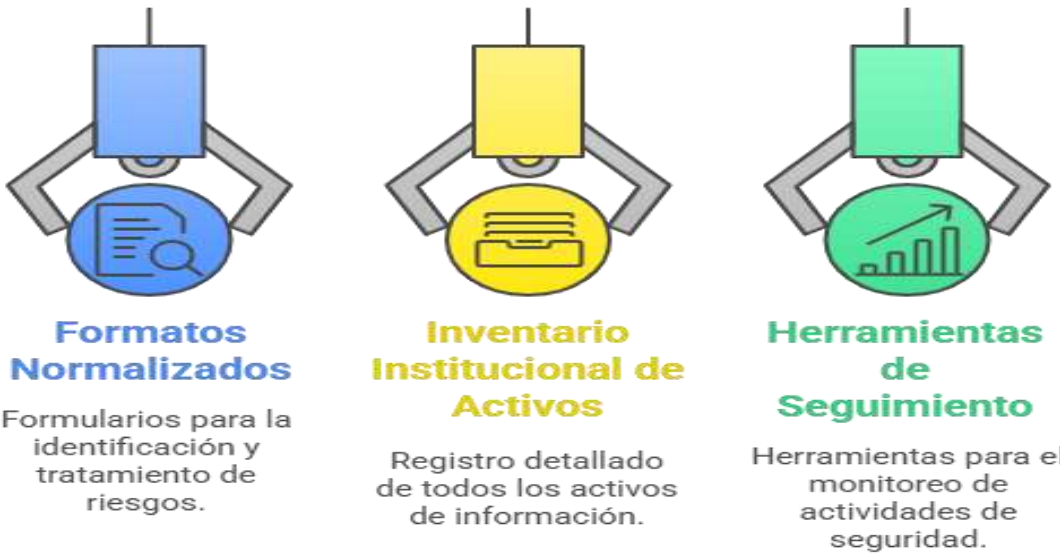

Ilustración 10 Herramientas de gestión para determinar el riesgo

INFRAESTRUCTURA TECNOLÓGICA:

Soluciones de protección perimetral, respaldo, monitoreo, cifrado, continuidad, control de accesos y autenticación, entre otras.

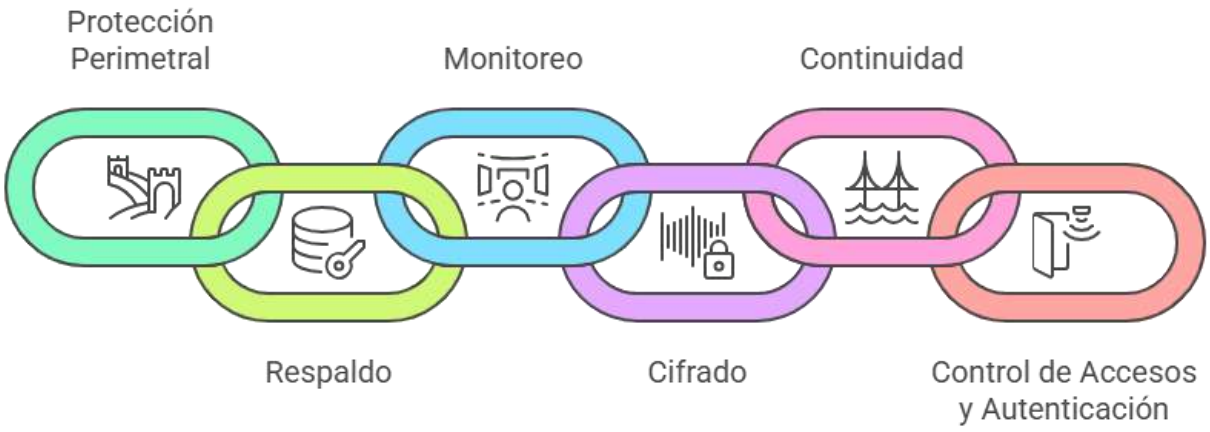

Ilustración 11 Recurso tecnológico

NORMATIVA Y LINEAMIENTOS:

Documentos institucionales, políticas, manuales y procedimientos internos alineados con ISO/IEC 27001:2022, ISO 31000, ISO 22301, ISO/IEC 20000-1 y el MSPI del MinTIC.

Ilustración 12 Normatividad

Estos recursos permiten a la Universidad garantizar un enfoque sistemático, colaborativo y efectivo frente a los riesgos que puedan afectar la información y la operación de los servicios institucionales.

9. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE CONTROLES

La estimación y asignación del presupuesto para la implementación de los controles definidos en los planes de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en la UPTC será responsabilidad del dueño del riesgo (líder del proceso), quien deberá gestionar los recursos necesarios dentro del marco del presupuesto institucional.

Cada líder de proceso deberá:

- Incluir las actividades de tratamiento de riesgos en su planificación operativa anual.
- Justificar los requerimientos técnicos y financieros ante la Vicerrectoría Administrativa y Financiera.
- Coordinar con la Dirección de Tecnologías y Sistemas de Información (DTIC) y el Oficial de Seguridad y privacidad de la Información la priorización de inversiones en infraestructura y soluciones tecnológicas.

El director de tecnología podrá emitir recomendaciones sobre la pertinencia y oportunidad de los controles definidos, buscando optimizar los recursos y asegurar su alineación con los objetivos estratégicos institucionales y con las disposiciones del Sistema Integrado de Gestión (SIG-UPTC).

10. MEDICION

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios (riesgos de interrupción) aprobados por la dirección de tecnologías, así como de sus controles y planes de tratamiento, será realizado por el Equipo de Infraestructura y el director de DTIC, en coordinación con los líderes de proceso.

Esta actividad se ejecutará conforme a la periodicidad definida en el cronograma institucional del SGSI, validando los resultados obtenidos por cada dependencia y el cargue de evidencias y soportes de cumplimiento de los controles establecidos.

Una vez se reporte el cumplimiento de los planes de tratamiento, la DTIC realizará la revisión y validación de la información para alimentar los indicadores de gestión de incidentes, cuyo objetivo es comparar año a año la disminución que debería presentarse en estos indicadores definidos para mitigar los riesgos de seguridad, privacidad y continuidad en los sistemas de gestión de la universidad.

Los resultados de este seguimiento no sólo permiten fortalecer la madurez del SGSI, sino que también constituyen un insumo estratégico para los procesos de auditoría, mejora continua y evaluación de desempeño institucional, en el marco del Sistema Integrado de Gestión (SIG-UPTC).

a. Indicadores de Seguimiento

Indicador	Fórmula	Frecuencia	Responsable	Fuente
% incidentes resueltos dentro del RTO	(Incidentes resueltos dentro del RTO / Total de incidentes) * 100	Semestral	Coordinador BCP	Bitácora de incidentes

Ilustración 13 Indicadores de Seguimiento

REFERENCIAS BIBLIOGRÁFICAS

- Norma técnica colombiana NTC-ISO /IEC 27005
- Norma técnica colombiana NTC-ISO /IEC 27005
- Metodología para la evaluación del desempeño de controles en sistema de gestión de seguridad de la información sobre la norma ISO/IEC 27001 de la Universidad Nacional, 2016
- Guía de gestión de riesgos, seguridad y privacidad de la información, MINTIC
- Manual integrado de gestión, SIG-UPTC, versión 31
- Procedimiento elaboración y control de documentos, SIG-UPTC, versión 13
- Plan de tratamiento de riesgos de seguridad y privacidad de la información, MINTIC, versión 5
- Guía aspectos generales de la documentación, SIG-UPTC, versión 3
- Guía para la gestión de riesgos de activos de información, SIG-UPTC, versión 7

Proyectó: Equipo de Gestión y Gobierno DTIC