PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PRSI)

Tecnológico de Antioquia
Institución Universitaria

Coordinación TIC

TABLA DE CONTENIDO

CONTROL DE CAMBIOS

Versión	Fecha de aprobación	Descripción del cambio
1.0	Marzo 2022	Creación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PRSI), Vigencia 2022
2.0	Abril 2023	Actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PRSI), Vigencia 2023

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PRSI)

OBJETIVOS

Objetivo General

Definir una metodología para la implementación del Plan de Tratamiento del Riesgo de Seguridad y privacidad de la Información del Tecnológico de Antioquia, institución Universitaria (TdeA), de ahora en adelante PRSI.

Objetivos específicos

- Identificar los riesgos de seguridad de la información del Tecnológico de Antioquia, institución Universitaria y establecer los controles que permitan minimizar y fortalecer la seguridad de los sistemas de información y de su infraestructura de TIC.
- Alinear el plan de tratamiento de riesgos de seguridad y privacidad con los planes institucionales y la normatividad prevista por el Min Tic y la ISO 27001.
- Elaborar un PRSI que permita preservar la confidencialidad, integridad y disponibilidad de la información del Tecnológico de Antioquia, institución Universitaria.

DEFINICIONES

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Activos Críticos de información: Sistema Administrativo y Financiero, Sistema Académico y sistema educación virtual (Moodle).

Activos críticos de tecnología: Centro de Datos institucional.

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).

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

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.

Centro de Datos: Instalación que alberga servidores, almacenamiento, firewall, equipos de comunicaciones, internet, aplicaciones y datos de toda la institución.

Debilidad de controles: Falta de credenciales, claves débiles, cambio de contraseñas limitado, sin control de acceso físico o lógico.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Procesos misionales: Docencia, Investigación y Extensión.

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Sistema de Seguridad Integral: Protección de acceso lógico y físico, a través de controles de acceso en puertas, servidores, PC, sistemas de información y detección de ataques con antivirus y firewall, uso de credenciales.

Sistema de protección eléctrico: Protección ante fallas de energía, a través de UPS, plantas de energía.

UPS (Uninterruptable Power Supply): Dispositivo que permite tener flujo de energía eléctrica mediante baterías de forma temporal, cuando el suministro eléctrico falla.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

ALCANCE

Adoptar los lineamientos y recomendaciones previstas por el MinTic y la ISO 27001, permitiendo definir, implementar y documentar el PRSI de una forma ordenada y de acuerdo a una

metodología establecida que permita minimizar los riesgos informáticos.

RECURSOS

El Tecnológico de Antioquia Institución Universitaria para la gestión del PRSI dispone de los siguientes recursos para desarrollar el PRSI:

Humanos

La definición e implementación del PRSI será liderado por la Coordinación TIC, acompañada por la oficina de gestión de Calidad Institucional

Físicos

Para lograr los objetivos trazados dentro de la implementación del PRSI se hace necesario contar con el acceso a los diferentes espacios físicos y digitales, a través de los lideres técnicos y funcionales de los sistemas de información, así mismo que los líderes de los procesos, para evidenciar los incidentes y definir su tratamiento.

Financieros

Para estimar y asignar los recursos financieros para el PRSI, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento de riegos. Si el establecimiento de los controles implica la adquisición de herramientas tecnológicas bajo la responsabilidad de la Coordinación de TIC, los recursos de inversión se asignarán de las diferentes bolsas de mantenimiento con que cuentan los contratos de servidos tecnológicos de acuerdo a la relación del incidente con el objeto de cada contrato.

FASES DE DESARROLLO

Acogiendo lo planteado en el modelo de seguridad y privacidad de la información del Min TIC (MSPI), se plantean cuatro (4) fases que sirven de ruta para el desarrollo de dicho modelo y permite gestionar de una forma adecuada la seguridad y la privacidad de la información como componente fundamental de los procesos institucionales, se definen las siguientes fases:

Ilustración 1 Fases del modelo de tratamiento de riesgos y seguridad de la información.

Planeación

Contexto

El Tecnológico de Antioquia Institución Universitaria, cuenta con tres (3) sedes ubicadas en el área metropolitana del Valle de Aburra: Medellín (sede principal), Copacabana e Itagüí, con una población educativa de aproximadamente 56.000 miembros, entre estudiantes, graduados, docentes, administrativos y contratistas.

Sus Sistemas de Información están alojados tanto en sitio (Centro de Datos Institucional) como en nube pública operados por proveedores de servicio tipo Saas (Software como servicio). Todos estos sistemas operan 24 horas – 365 días al año.

Roles y responsabilidades

Se definen los roles y responsabilidades para la gestión y control del riesgo, teniendo en cuenta la participación integral de la Comunidad Educativa y está compuesto por las siguientes líneas:

Primera línea de defensa: Identificación y tratamiento de riesgos en los procesos a su cargo en el día a día. Están los coordinadores y líderes de áreas y procesos, responsables de planes, programas y proyectos y en general la Comunidad Educativa.

Segunda línea de defensa: Tratamiento de riesgos, socialización y seguimiento, tratamiento y aplicación de controles. Responsables: Coordinación TIC, Supervisores e interventores de contratos Dirección de Planeación, Secretaría General y representantes de la Alta Dirección.

Tercera línea de defensa: Monitorea de manera independiente el manejo y tratamiento de los riesgos en la Institución. Está a cargo de Control Interno.

Identificación de medidas de seguridad

Identificar medidas de seguridad apropiadas para mitigar los riesgos identificados en la evaluación de riesgos. Estas medidas pueden incluir políticas y procedimientos de seguridad, controles de acceso, controles de autenticación y autorización, controles de seguridad física y controles de seguridad lógica:

- ✓ Control de acceso físico: Ingreso Institución, salones, oficinas (carnet)
- ✓ Control de Acceso lógico: Credenciales, roles y perfiles. (Directorio Activo, aplicaciones)
- ✓ Políticas de Seguridad Digital – "Seguridad y Privacidad de la Información"
- ✓ Pólizas de cumplimiento
- ✓ Contratos de soporte y garantía
- ✓ Licenciamiento de software
- ✓ Sistema de respaldo (Eléctrico, internet, copias de seguridad)

Actividades

Se realizan varias actividades tendientes a identificar y tratar los riesgos en tecnología de la Institución:

- ✓ Identificación de riesgos
- ✓ Definición de criterios para definir el nivel de probabilidad
- ✓ Definición de criterios para definir el nivel de impacto
- ✓ Definición para la evaluación del riesgo
- ✓ Definición para la valoración del riesgo
- ✓ Definición para la evaluación de controles
- ✓ Definición para la valoración del control
- ✓ Análisis de los riesgos
- ✓ Mapa de riesgos
- ✓ Definición de indicadores

Identificación de riesgos en Tecnología

- Riesgo1: Posibilidad de indisponibilidad de los activos críticos de información o de tecnología
- Riesgo2: Posibilidad de pérdida, alteración o robo de información digital
- Riesgo3: Posibilidad de acceso no autorizado a los activos críticos de información o de tecnología

Criterios para definir el nivel de probabilidad

Para Tecnología se toma como criterio de tiempo un (1) año - 365 días. (1 día = 1 Vez)

Criterio	*Frecuencia de la actividad*	*Probabilidad*
Muy Baja	La actividad que conlleva el riesgo se ejecuta o está disponible como máximos 19 veces por año y tiene el 5% o más sin supervisión.	20%
Baja	La actividad que conlleva el riesgo se ejecuta o está disponible de 20 a 99 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta o está disponible de 100 a 299 veces por año y tiene el 5% o más sin supervisión.	60%
Alta	La actividad que conlleva el riesgo se ejecuta o está disponible entre 300 y 360 veces por año y tiene el 5% o más sin supervisión.	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta o está disponible más de 361 veces por año y tiene el 5% o más sin supervisión.	100%

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 (DAFP)

Criterios para definir el nivel de impacto

Criterio	*Indisponibilidad del servicio TIC*	*Retrasos y/o reprocesos*	*Afectación de índole legal, operativo o de pérdida de imagen Institucional*	*Perdida o alteración de información*
Leve 20% (0-20)	La afectación total acumulada en el último año de los recursos tecnológicos críticos fue por menos de 24 horas.	Afectación en tiempo de un proceso operativo específico de corto plazo que no repercute institucionalmente.	Afectación de índole operativo de solo un área específica de la Institución de forma temporal	Afectación por errores de usuario, hardware y/o software que no compromete la integridad de la información, ni su calidad y que se corrige inmediatamente
Menor 40% (21-40)	La afectación total acumulada en el último año de los recursos tecnológicos críticos fue entre 24 y 48 horas	Afectación de procesos operativos de corto plazo de un área específica que no repercuten institucionalmente.	Afectación de índole operativo de varias áreas de la Institución de forma temporal.	Afectación de algún dato específico que no compromete más del 99.9 % de la información contenida en las Bases de Datos

Criterio	Indisponibilidad del servicio TIC	Retrasos y/o reprocesos	Afectación de índole legal, operativo o de pérdida de imagen Institucional	Perdida o alteración de información
Moderado 60% (41-60)	La afectación total acumulada en el último año de los recursos tecnológicos críticos fue entre 49 y 96 horas	Afectación de varios procesos operativos institucionales que no repercuten en procesos críticos o misionales.	Afectación de índole operativo, de imagen o legal de solo un área específica de la Institución de forma temporal que no tiene repercusiones sancionatorias.	Afectación por errores de usuario, hardware y/o software que no compromete la integridad de la información, ni su calidad, pero que se corrigen después de una auditoría o revisión de control.
Mayor 80% (61-80)	La afectación total acumulada de los recursos tecnológicos críticos en el último año fue entre 97 y 168 horas	Afectación de procesos académicos en época de inscripciones y matrículas o pagos de compromisos.	Afectación de índole operativo, imagen o legal de forma temporal que puede tener repercusiones sancionatorias internas	Afectación por alteraciones o robo de información sensible
Catastrófico 100% (81-100)	La afectación total acumulada de los recursos tecnológicos críticos en el último año fue mayor a 168 horas	Afectación de procesos académicos en época de inscripciones y matrículas o pagos de compromisos, que pueden tener repercusiones sancionatorias	Afectación de índole operativo, imagen o legal a nivel externo, de forma sostenida y con repercusiones sancionatorias.	Afectación por ataques con pérdidas financieras y/o indisponibilidad permanente de las bases de datos

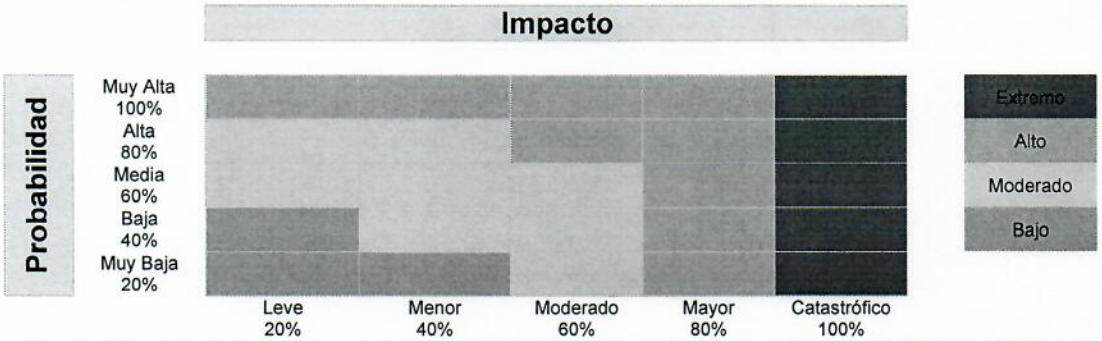
Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 (DAFP)

Definición para la evaluación del riesgo.

- **Análisis preliminar (riesgo inherente):** Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto inicial.
- **Análisis final (riesgo residual):** es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Se definen 4 zonas en la matriz de calor



Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 (DAFP)

Definición para la valoración del riesgo.

Se realiza un análisis de riesgos donde se estable la probabilidad de ocurrencia del riesgo y sus

consecuencias o impacto.

- **Valoración**: Impacto en la entidad.
- **Frecuencia de la actividad**: Número de ocurrencias en un rango de tiempo.
- **Probabilidad**: se entiende como la posibilidad de ocurrencia del riesgo en un rango de tiempo.

Definición para la evaluación de los Controles

Los controles permiten reducir o mitigar el riesgo y para el caso del TdeA se utilizarán dos (2) tipologías de controles:

- **Control Preventivo**: Control en la entrada del proceso y antes de que se realice la actividad originadora del riesgo. Estos afectan la Probabilidad.
- **Control Correctivo**: Control en la salida del proceso y después de que se materializa el riesgo. Estos afectan el Impacto.

Así mismo, de acuerdo con la forma como se implementan los controles tenemos:

- **Control Manual**: Control que es accionado por personas.
- **Control Automático**: Control accionado por un sistema.

Definición para la valoración del Control

Para poder determinar el grado de eficiencia de los Controles se da un peso de acuerdo a los atributos que tenga cada Control y ese valor se traslada a la matriz de calor, teniendo presente la afectación del Control sobre la Probabilidad o el Impacto.

Control			Peso
Tipo	Preventivo		30%
	Correctivo		20%
Implementación	Automático		30%
	Manual		20%
Documentación	Políticas y procedimientos actualizados (Procedimiento de Mantenimiento preventivo y correctivo de Hw y Sw (equipos de escritorio, portátiles e impresoras), Políticas de seguridad digital "Seguridad y privacidad de la información")		

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 (DAFP)

Análisis de los Riesgos

Factor de Riesgo: Tecnología

Riesgo1: Posibilidad de indisponibilidad de los activos críticos de información o de tecnología

Probabilidad

Actividad	Frecuencia de la Actividad	Probabilidad frente al riesgo
Infraestructura TIC, Sistemas de información. (Disponibilidad de aplicativos, recursos tecnológicos, control de acceso)	Diario	100%

Teniendo en cuenta lo anterior, el nivel de Frecuencia de la actividad del Riesgo1 en un año es de 365 veces y la probabilidad frente al riesgo es "Muy alta" por ejecutarse 365 días al año y estar más del 5% de ese tiempo sin supervisión (Tiempo de vacaciones, fin de semana y horario nocturno).

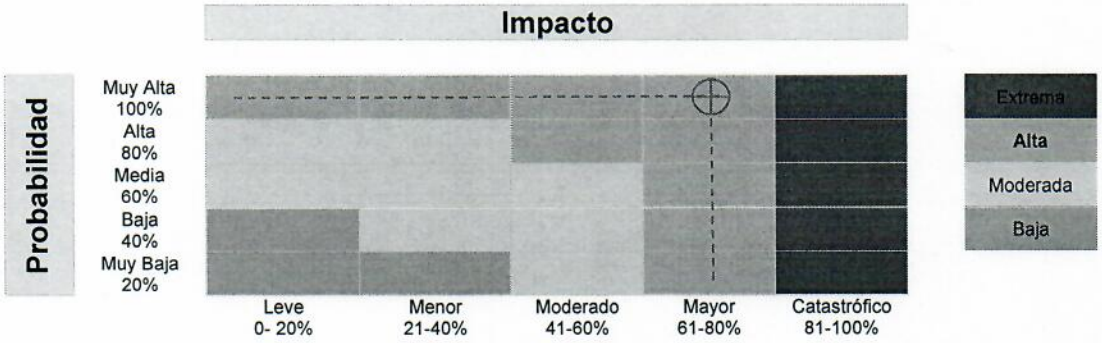
Impacto

Actividad	Criterios	Impacto del riesgo (%)
Infraestructura TIC, Sistemas de información. (Disponibilidad de aplicativos, recursos tecnológicos, control de acceso)	La afectación total de los recursos tecnológicos críticos en el último año fue entre 97 y 168 horas	80%
	Afectación de procesos académicos en época de inscripciones y matrículas o pagos de compromisos.	80%
	Afectación de índole operativo, de imagen o legal de solo un área específica de la Institución de forma temporal que no tiene repercusiones sancionatorias.	60%
	Impacto promedio del Riesgo1	Moderado 73.33%

Teniendo en cuenta las consecuencias asociadas al Riesgo1 y promediando su Impacto, el nivel de Impacto de la actividad del Riesgo1 en un año es "Moderado"

Nivel de severidad (Zona inicial)

Se cruza la probabilidad (100%) con el impacto (73,33%) generado por el Riesgo1 y se ubica en la zona inicial "Alta".



Controles Existentes

Al tener claro la zona de riesgo inicial y las causas, se identifican los controles existentes para minimizar el Riesgo1:

- Contratos vigentes (soporte y garantía)
- Sistema de respaldo (Eléctrico, internet, Copias de seguridad)
- Pólizas de cumplimiento (contratos)

Valoración del Control

Control 1 – Riesgo 1			Peso
Contratos vigentes (soporte y garantía)	Preventivo		30%
	Correctivo	X	20%
	Documentación	X	
Afecta Impacto	Automático	-	30%
	Manual	X	20%

Control 2 – Riesgo 1			Peso
Sistema de respaldo (Eléctrico, internet, Copias de seguridad)	Preventivo	X	30%
	Correctivo		20%
	Documentación	X	
Afecta la Probabilidad	Automático	X	30%
	Manual	-	20%

Control 3 – Riesgo 1			Peso
Pólizas de cumplimiento (Contratos)	Preventivo		30%
	Correctivo	X	20%
	Documentación	X	
Afecta el Impacto	Automático	-	30%
	Manual	X	20%

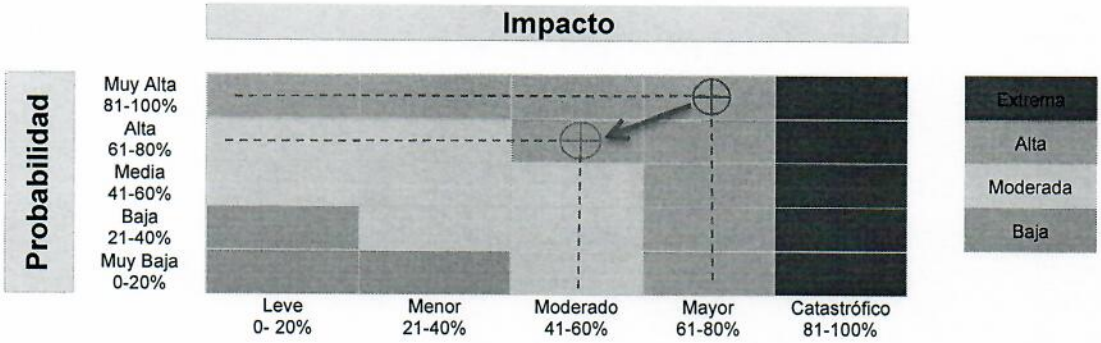
Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos
Riesgo 1	Probabilidad inherente	100%	Valoración control 2 preventivo	30%	100% x 30% = 30% 100% - 30% = 70%
	Probabilidad Residual	**70%**			
	Impacto Inherente	73.33%	Valoración control 1 Correctivo	20%	73.33% * 20% = 14.67% 73.33% - 14.67% = 58.66%
	Valor probabilidad para aplicar al control 3	58.66%	Valoración control 3 Correctivo	20%	58.66% * 20% = 11.73% 58.66% - 11.73% = 46.93%
	Impacto Residual	**46.93%**			

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 (DAFP)

Nivel de severidad (Zona Final)

Se cruza la probabilidad (70%) con el impacto (46.93%) generado por el Riesgo1 después de aplicados los controles y se ubica en la zona Final "Alta".



Riesgo2: Posibilidad de pérdida, alteración o robo de información digital

Probabilidad

Actividad	Frecuencia de la Actividad	Probabilidad frente al riesgo
Infraestructura TIC, Sistemas de información. (Acceso de aplicativos, recursos tecnológicos, control de acceso)	Diario	100%

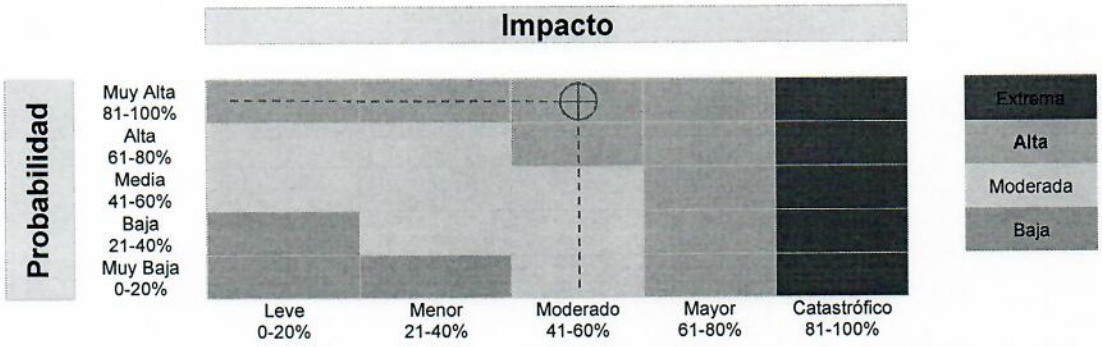
Teniendo en cuenta lo anterior, el nivel de Frecuencia de la actividad del Riesgo2 en un año es de 365 veces, por lo tanto, la probabilidad frente al riesgo es "Muy alta" por ejecutarse y estar disponible 365 días al año y estar más del 5% de ese tiempo sin supervisión (Tiempo de vacaciones y horario nocturno).

Impacto

Actividad	Criterios	Impacto del riesgo (%)
Infraestructura TIC, Sistemas de información. (Acceso de aplicativos, recursos tecnológicos, control de acceso)	Afectación de varios procesos operativos institucionales que no repercuten en procesos críticos o misionales.	60%
	Afectación por errores de usuario, hardware y/o software que no compromete la integridad de la información, ni su calidad, pero que se corrigen después de una auditoría o revisión de control.	60%
	Afectación de índole operativo o de imagen de varias áreas de la Institución de forma temporal que no tiene repercusiones sancionatorias.	40%
	Impacto promedio del Riesgo2	Moderado 53.33%

Teniendo en cuenta las consecuencias asociadas al Riesgo2 y promediando su Impacto, el nivel de Impacto de la actividad del Riesgo2 en un año es "Moderado"

Nivel de severidad (Zona inicial)



Se cruza la probabilidad (100%) con el impacto (53.33%) generado por el Riesgo2 y se ubica en la zona inicial "Alta".

Controles Existentes

Al tener claro la zona de riesgo inicial y las causas, se identifican los controles existentes para minimizar el Riesgo2:

- Sistema de seguridad integral
- Contratos vigentes (soporte y garantía)
- Pólizas de cumplimiento (contratos)

Valoración del Control

Control 1 – Riesgo 2			Peso
Sistema de seguridad integral	Preventivo	X	30%
	Correctivo		20%
	Documentación	X	
Afecta la Probabilidad	Automático	X	30%
	Manual	-	20%

Control 2 – Riesgo 2			Peso
Contratos vigentes (soporte y garantía)	Preventivo		30%
	Correctivo	X	20%
	Documentación	X	
Afecta el Impacto	Automático	-	30%
	Manual	X	20%

Control 3 – Riesgo 2			Peso
Pólizas de cumplimiento (contratos)	Preventivo		30%
	Correctivo	X	20%
	Documentación	X	
Afecta el Impacto	Automático		30%
	Manual	X	20%

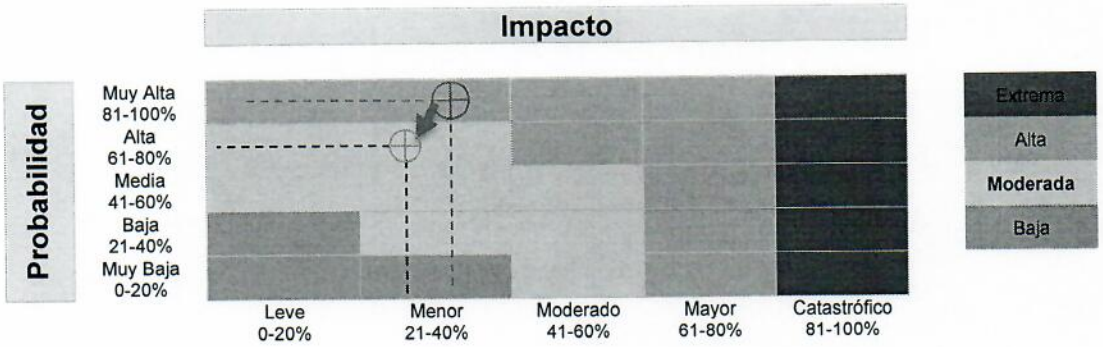
Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos
Riesgo 2	Probabilidad inherente	100%	Valoración control 1 predictivo	30%	100% x 30% = 30% 100% - 30% = 70%
	Probabilidad Residual	**70%**			
	Impacto Inherente	53.33%	Valoración control 2 Correctivo	20%	53.33% * 20% = 10.67% 53.33% - 10.67% = 42.66%
	Valor probabilidad para aplicar al control 3	45.05%	Valoración control 3 Correctivo	20%	45.05% * 15% = 6.76% 45.05% - 6.76% = 32.32%
	Impacto Residual	**32.32%**			

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 (DAFP)

Nivel de severidad (Zona Final)

Se cruza la probabilidad (70%) con el impacto (32.32%) generado por el Riesgo1 después de aplicados los controles y se ubica en la zona Final "Moderada".



Riesgo3: Posibilidad de acceso no autorizado a los activos de información o de tecnología

Probabilidad

Actividad	Frecuencia de la Actividad	Probabilidad frente al riesgo
Infraestructura TIC, Sistemas de información. (Acceso indebido de aplicativos, recursos tecnológicos, control de acceso)	Diario	100%

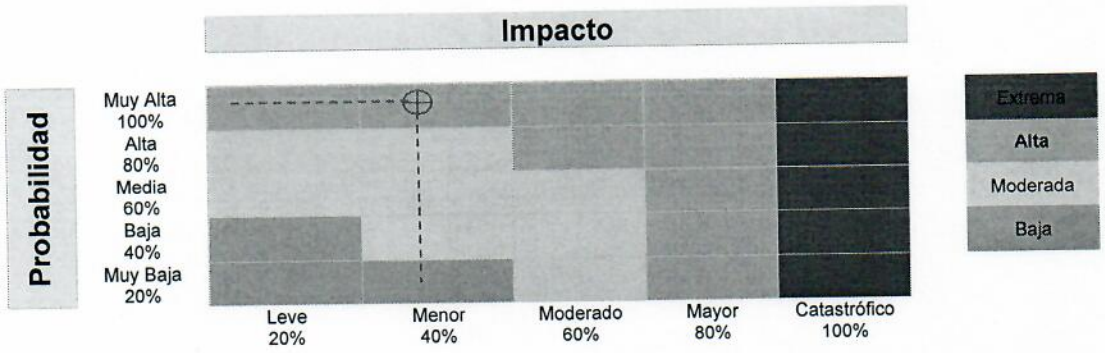
Teniendo en cuenta lo anterior, el nivel de Frecuencia de la actividad del Riesgo3 en un año es de 365 veces, por lo tanto, la probabilidad frente al riesgo es "Muy alta" por ejecutarse y estar disponible 365 días al año y estar más del 5% de ese tiempo sin supervisión (Tiempo de vacaciones y horario nocturno).

Impacto

Actividad	Criterios	Impacto del riesgo (%)
Infraestructura TIC, Sistemas de información. (Acceso indebido de aplicativos, recursos tecnológicos, control de acceso)	Afectación de varios procesos operativos institucionales que no repercuten en procesos críticos o misionales.	60%
	Afectación por errores de usuario o hardware y/o software que no compromete la integridad de la información, ni su calidad y que se corrige inmediatamente	20%
	Afectación de índole operativo o de imagen de varias áreas de la Institución de forma temporal que no tiene repercusiones sancionatorias.	40%
	Impacto promedio del Riesgo3	Menor 40%

Teniendo en cuenta las consecuencias asociadas al Riesgo3 y promediando su Impacto, el nivel de Impacto de la actividad del Riesgo3 en un año es "Alta"

Nivel de severidad (Zona inicial)



Se cruza la probabilidad (100%) con el impacto (40%) generado por el Riesgo3 y se ubica en la zona inicial "Alta".

Controles Existentes

Al tener claro la zona de riesgo inicial y las causas, se identifican los controles existentes para minimizar el Riesgo3:

- Sistema de seguridad integral
- Pólizas de cumplimiento (contratos)

Valoración del Control

Control 1 – Riesgo 3			Peso
Sistema de seguridad integral	Preventivo	X	30%
	Correctivo		20%
	Documentación	X	
Afecta la Probabilidad	Automático	X	30%
	Manual	-	20%

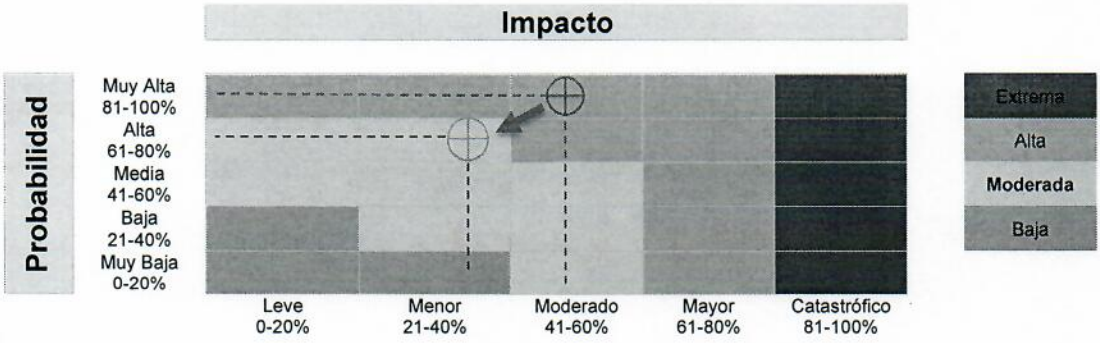
Control 2 – Riesgo 3			Peso
Pólizas de cumplimiento (contratos)	Preventivo		30%
	Correctivo	X	20%
	Documentación	X	
Afecta el Impacto	Automático		30%
	Manual	X	20%

Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos
Riesgo 3	Probabilidad inherente	100%	Valoración control 1 predictivo	30%	100% x 30% = 30% 100% - 30% = 70%
	Probabilidad Residual	**70%**			
	Impacto Inherente	40%	Valoración control 2 Correctivo	20%	40% * 20% = 8% 40% - 8% = 32%
	Impacto Residual	**32%**			

Nivel de severidad (Zona Final)

Se cruza la probabilidad (70%) con el impacto (32%) generado por el Riesgo1 después de aplicados los controles y se ubica en la zona Final "Moderada".



Después de realizado el tratamiento de riesgos en tecnología se puede apreciar que los controles implementados logran una mejora tanto en la probabilidad como en el impacto de los tres (3) riesgos. No obstante, es responsabilidad de la Institución hacer seguimiento y mejorar o implementar nuevos controles que mitiguen los riesgos residuales.

Administración del riesgo

Riesgo	Administración del Riesgo (Asumir, Evitar, Reducir, Mitigar, Compartir o Transferir)
Posibilidad de indisponibilidad de los activos críticos de información o de tecnología	✓ **Mitigar:** Se disminuye la probabilidad de ocurrencia del riesgo con el control: Sistema de respaldo (Eléctrico, internet, copias de seguridad) ✓ **Compartir:** Se comparte la aplicación del control correctivo con el proveedor responsable del servicio, disminuyendo el impacto del riesgo: Contratos vigentes (soporte y garantía) ✓ **Transferir:** Se transfiere la aplicación del control correctivo al proveedor responsable del servicio, disminuyendo el impacto del riesgo: Pólizas de cumplimiento
Posibilidad de pérdida, alteración o robo de información digital	✓ **Mitigar:** Se disminuye la probabilidad de ocurrencia del riesgo con el control: Sistema de Seguridad Integral ✓ **Compartir:** Se comparte la aplicación del control correctivo con el proveedor responsable del servicio, disminuyendo el impacto del riesgo: Contratos vigentes (soporte y garantía) ✓ **Transferir:** Se transfiere la aplicación del control correctivo al proveedor responsable del servicio, , disminuyendo el impacto del riesgo: Pólizas de cumplimiento
Posibilidad de acceso no autorizado a los activos de información o de tecnología	✓ **Mitigar:** Se disminuye la probabilidad de ocurrencia del riesgo con el control: Sistema de Seguridad Integral ✓ **Transferir:** Se transfiere la aplicación del control correctivo al proveedor responsable del servicio, disminuyendo el impacto del riesgo: Pólizas de cumplimiento.

Mapa de Riesgos

Riesgo	Posibles Causas	Consecuencias	Zona Inicial			Controles	Zona Final			Administración del Riesgo (Asumir, Evitar, Reducir, Mitigar, Compartir o Transferir)
			P	I	S		P	I	S	
Posibilidad de indisponibilidad de los activos críticos de información o de tecnología	✓ Fallas en el fluido eléctrico ✓ Fallas de Conectividad (Red, Internet) ✓ Fallas del hardware y/o software ✓ Vencimiento de licencias ✓ Fallas en los procesos de mantenimiento o falta de soporte y/o garantía de la infraestructura	✓ Indisponibilidad del servicio ✓ Retrasos y/o reprocesos ✓ impacto negativo de índole legal, operativo o de pérdida de imagen Institucional	Muy Alta (100%)	Moderado (73,33%)	Alta	✓Contratos vigentes (soporte y garantía) ✓Sistema de respaldo (Eléctrico, internet, copias de seguridad) ✓Pólizas de cumplimiento	Alta (70%)	Moderado (46.93%)	Alta	✓Mitigar ✓Compartir ✓Transferir
Posibilidad de pérdida, alteración o robo de información digital	✓ Acceso no autorizado a los sistemas de información ✓ Hurto de equipos ✓ Virus informático ✓ Errores humanos ✓ Fallas en el sistema de seguridad integral ✓ Mecanismos de control débiles respecto a la identificación, clasificación y uso de activos de información	✓ Retrasos y/o reprocesos ✓ Perdida o alteración de información ✓ impacto negativo de índole legal, operativo o de pérdida de imagen Institucional	Muy Alta (100%)	Moderado (53,33%)	Moderada	✓Sistema de seguridad integral ✓Contratos vigentes (soporte y garantía) ✓Pólizas de cumplimiento (contratos)	Media (40.1%)	Menor (34.34%)	Moderada	✓Mitigar ✓Compartir ✓Transferir
Posibilidad de acceso no autorizado a los activos de información o de tecnología	✓ Virus informático ✓ Debilidad en los controles ✓ Incumplimiento de las Políticas de seguridad digital "Seguridad y privacidad de la información"	✓ ✓ Perdida o alteración de información ✓ Retrasos y/o reprocesos ✓ impacto negativo de índole legal, operativo o de pérdida de imagen Institucional	Muy Alta (100%)	Menor (40%)	Alta	✓Sistema de seguridad integral ✓Pólizas de cumplimiento (contratos)	Alta (70%)	Menor (32%)	Moderada	✓Mitigar ✓Compartir ✓Transferir

Riesgos, impacto y controles actuales

P Probabilidad
I Impacto
S Nivel de Severidad

Implementación

En esta fase se debe llevar a cabo todo lo planteado como control en la etapa de Planeación y garantizar su implementación, incluyendo los recursos necesarios para poder iniciar el tratamiento de riesgos. Es de anotar que en esta etapa la Institución liderada por la Coordinación TIC debe revisar que todos los controles establecidos estén o sean implementados y ajustados a los requerimientos de cada sistema y se cumpla con todo lo estipulado en las Políticas de Seguridad Digital para dar cumplimiento a lo planteado en el PRSI, incluyendo la ejecución de actividades en los tiempos pactados.

Actividades de implementación y evidencias

Actividad	Meta	Responsable	Fecha	Evidencia
Presentar Plan de tratamiento de riesgos de seguridad y privacidad de la información (PRSI)	Aprobación del PRSI por parte del Comité de Informática	Coordinador TIC Comité de Informática	Abril 2023	Acta Comité de Informática (Carpeta OneDrive:)
Publicar Plan de tratamiento de riesgos de seguridad y privacidad de la información (PRSI)	Publicación del PRSI en la página WEB Institucional	Coordinador TIC Coordinador de Comunicaciones	Mayo 2023	Link www.tdea.edu.co
Publicar Políticas de Seguridad Digital "Seguridad y Privacidad de la Información"	Publicar las Políticas en la página WEB Institucional	Coordinador TIC Coordinador de Comunicaciones	Mayo 2023	Link www.tdea.edu.co
Socializar Plan de tratamiento de riesgos de seguridad y privacidad de la información (PRSI)	Socialización del PRSI	Seguridad TIC	Mayo- Junio 2023	(Carpeta OneDrive:)
Socializar Políticas de Seguridad Digital "Seguridad y Privacidad de la Información"	Socialización de las Políticas	Seguridad TIC	Mayo- Junio 2023	(Carpeta OneDrive:)
Elaborar procedimiento de reporte incidentes	Procedimiento aprobado	Seguridad TIC Coordinación de Calidad	Mayo 2023	(Carpeta OneDrive:)
Socializar el procedimiento de reporte incidentes	Socialización del procedimiento	Seguridad TIC	Mayo 2023	(Carpeta OneDrive:)
Realizar auditorías internas	Monitoreo sobre los riesgos y controles	Seguridad TIC	Trimestral	(Carpeta OneDrive:)
Seguimiento a indicadores	Monitoreo sobre los riesgos y controles	Seguridad TIC	Trimestral	(Carpeta OneDrive:)

Evaluación de desempeño

Monitorear y revisar continuamente la efectividad de las medidas de seguridad implementadas, así como los cambios en el entorno de riesgos, para asegurar que la seguridad de la información se mantenga adecuadamente.

La Institución a través de las tres (3) líneas de defensa definidas en este documento en el ítem: Roles y Responsabilidades, debe hacer seguimiento del PRSI, para determinar su efectividad y cada línea es responsable de acuerdo a su incidencia dentro del proceso y se debe realizar como mínimo las siguientes actividades:

- ✓ Realizar seguimiento y monitoreo a la etapa de implementación del PRSI, para

determinar el cumplimiento de las acciones planteadas.

- ✓ Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- ✓ Realizar monitoreo de los riesgos y controles tecnológicos, a través de los indicadores y auditorías internas.
- ✓ Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos. De ser necesario dar recomendaciones para mejorar o implementar nuevos controles que mejoren su eficiencia y eficacia.
- ✓ La Institución debe valorar nuevamente los riesgos, comparando los resultados con el último nivel de riesgo residual y así determinar la efectividad de los planes de tratamiento y de los controles propuestos, de acuerdo con lo definido en PRSI.

Formato Indicadores propuestos

Indicador ## –		
Definición		
Objetivo		
Tipo de indicador		
Indicador de eficacia/Eficacia		
Variables	**Fórmula**	**Fuente de información**
Metas		
Mínima	**Satisfactoria**	**Sobresaliente**
Observaciones		
VI## = VI: Variable Indicador, ##: Consecutivo		

Fuente: Adaptado de la Guía de indicadores de gestión para la seguridad de la información – MIN TIC (Guía No. 9)

Definición de Indicadores

Indicadores Riesgo1

Para medir la eficacia de los Controles implementados para el Riesgo1: Posibilidad de indisponibilidad de los activos críticos de información o de tecnología, se definieron 2 indicadores:

- ✓ Indicador R101 - Continuidad del servicio del Centro de Datos Institucional
- ✓ Indicador R102 - Continuidad del servicio de los Activos críticos de información

Indicador R101 – Continuidad del servicio del Centro de Datos Institucional
Definición
El indicador permite determinar y hacer seguimiento al número de veces en el año que el Centro de Datos Institucional suspendió servicios de forma total por fallas en el fluido eléctrico.
Objetivo
Hacer un seguimiento a la operación normal del Centro de Datos y la eficacia de los controles implementados.
Tipo de indicador

Indicador R101 – Continuidad del servicio del Centro de Datos Institucional		
Indicador de eficacia		
Variables	**Fórmula**	**Fuente de información**
VI01: Número de veces de suspensión total de servicios del Centro de Datos Institucional durante un año por fallas eléctricas	Número de incidencias = V101	Informe de incidentes de activos críticos de información o de tecnología durante el año.
Metas		
Mínima	**Satisfactorio**	
1 vez	0 veces	
Observaciones		
Toda incidencia total por fallas de fluido eléctrico que afecta el Centro de Datos		

Indicador R102 – Continuidad del servicio de los activos críticos de información		
Definición		
El indicador permite determinar y hacer seguimiento al número de horas en el año que los activos críticos de información prestaron servicio.		
Objetivo		
Hacer un seguimiento a la operación normal de los sistemas de información críticos (Académico, Moodle, Administrativo y Financiero)		
Tipo de indicador		
Indicador de eficacia		
Variables	**Fórmula**	**Fuente de información**
VI02: Número de horas que presta servicio el activo crítico de durante un año (8.760). VI03: Número de horas que dejaron de funcionar los activos críticos de información durante el año.	((VI03 – V04) * 100) / VI03)	Informe de incidentes de activos críticos de información o de tecnología durante el año.
Metas		
Mínima	**Satisfactoria**	**Sobresaliente**
99% (8.672,4)	99.9 - 99,9999% (8.681,16 - 8.751,24)	99.9999 - 100% (8.760)
Observaciones		
Se debe tener en cuenta toda falla o suspensión total o parcial del servicio de los activos críticos de información, tanto por causas al interior de la institución como en la nube.		

Indicadores Riesgo2

Para medir la eficacia de los Controles implementados para el Riesgo2: Posibilidad de pérdida, alteración o robo de información digital, se definió 1 indicador:

Indicador PSD06 – Uso de contraseñas		
Definición		
El indicador permite determinar y hacer seguimiento al control que se hace dentro de cualquier sistema de información crítico institucional.		
Objetivo		
Hacer un seguimiento a la existencia de perfiles para el acceso a contenido de los activos críticos de información.		
Tipo de indicador		
Indicador de Cumplimiento		
Variables	**Fórmula**	**Fuente de información**
VIP02: ¿El líder técnico asigna perfiles dentro de cada uno de los activos críticos de información limitando el acceso solo a los procesos	Cumplimiento= Si se evidencia - 1 No se evidencia - 0	Informe de incidentes de activos críticos de información o de tecnología durante el año.

Indicador PSD06 – Uso de contraseñas		
autorizados para cada usuario?		
Metas		
Cumple	**No Cumple**	
Observaciones		
Manejo de credenciales para ingreso		

Indicadores Riesgo3

Para medir la eficacia de los Controles implementados para el Riesgo3: Posibilidad de acceso no autorizado a los activos de información o de tecnología, se definió 1 indicador:

Indicador R301 – Control de ingreso a los activos críticos de información		
Definición		
El indicador permite determinar y hacer seguimiento al control que se hace al ingreso de cualquier sistema de información crítico institucional.		
Objetivo		
Hacer un seguimiento a la existencia de credenciales para el acceso a los activos críticos de información.		
Tipo de indicador		
Indicador de Cumplimiento		
Variables	**Fórmula**	**Fuente de información**
VI04: ¿Los activos críticos de información cuentan con control de acceso a través de credenciales?	Cumplimiento= VI04 Si se evidencia - 1 No se evidencia - 0	Activos críticos de información
Metas		
Cumple	**No Cumple**	
Observaciones		
Manejo de credenciales para ingreso y gestión de estas.		

Mejora Continua

En esta fase se deben tomar acciones para mitigar las debilidades encontradas, de acuerdo a los resultados obtenidos en la fase de evaluación de desempeño y se realizan como mínimo las siguientes acciones:

Se analizan los resultados de las acciones implementadas y si estas no cumplen los objetivos definidos, se analizan las causas de las desviaciones y se generan los respectivos ajustes. Adicionalmente la Institución debe definir las acciones para mejorar continuamente la gestión de riesgos de seguridad de la información:

- ✓ Revisar y evaluar los hallazgos encontrados en las diferentes auditorías.
- ✓ Establecer las posibles causas y consecuencias del hallazgo y revisar si existen hallazgos similares, para determinar las acciones correctivas que eviten su materialización.
- ✓ Se deben realizar revisiones continuas que permitan gestionar el riesgo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado y la aparición de nuevos

riesgos.

- ✓ Documentar los hallazgos y las acciones para mitigar su impacto.

Es importante tener en cuenta que el plan de tratamiento de riesgos de seguridad y privacidad de la información debe ser una responsabilidad de toda la Institución, no solo de la Coordinación TIC. Además, es importante garantizar la colaboración y coordinación con otras entidades gubernamentales y del sector público y privado que tengan relación con la Institución, para garantizar la seguridad de la información en el ecosistema digital.