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

2018-2021

Tecnológico de Antioquia
Institución Universitaria

TABLA DE CONTENIDO

LISTA DE TABLAS

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

1. OBJETIVOS

Objetivo General

Elaborar un documento que permita desarrollar las pautas para la implementación y socialización del *Plan de Tratamiento del Riesgo de Seguridad de la Información del Tecnológico de Antioquia, institución Universitaria (TdeA*), de ahora en adelante PRSI, el cual busca Identificar las vulnerabilidades y amenazas cibernéticas a las que el TdeA puede estar expuesto y desarrollar controles que permitan minimizar y fortalecer la seguridad de los sistemas de información y de su infraestructura de TIC.

Objetivos específicos

- Definir la metodología y etapas de implementación del PRSI del TdeA.
- Realizar el plan de trabajo para la implementación del PRSI del TdeA.
- Identificar los riesgos actuales, las posibles causas y los controles existentes.

2. ALCANCE DEL DOCUMENTO

Este documento busca identificar la metodología, los documentos y procesos que permitan desarrollar el PRSI de la Institución, definiendo las tareas generales en cada una de las etapas de implementación.

De esta forma la institución puede comenzar a definir, implementar y documentar el PRSI de una forma ordenada y de acuerdo a una metodología establecida que garanticen minimizar los riesgos informáticos.

3. RECURSOS

Aquí se definen los recursos tanto humanos, físicos y financieros que soportan la implementación del PRSI.

Humanos

La definición e implementación del PRSI será liderado por el coordinador de las TIC del TdeA, apoyado por los profesionales que lideran los procesos de Sistemas de información, Soporte e Infraestructura y telecomunicaciones y acompañados por la oficina de gestión de calidad de la institución.

Físicos

Para lograr los objetivos trazados dentro de la implementación del PRSI se hace necesario el acceso a los equipos de control perimetral con que cuenta la Institución (Firewall, IDS/IPS), al equipo de análisis de tráfico que permitirá una visión más real de lo que está pasando en el perímetro de la red de datos, además el acceso a los centros de cableado, switches CORE y de borde.

Financieros

Para desarrollar el PRSI se requiere un presupuesto estimado de diez millones de pesos ($ 10.000.000).

4. METODOLOGÍA DE IMPLEMENTACIÓN

Para la implementación el PRSI Institucional se acoge el modelo del Ministerio de Tecnologías de la Información y las Comunicaciones (Min-TIC), para estar acorde con las buenas prácticas de seguridad y teniendo en cuenta las normas ISO 27001 del 2013, entre otras.

5. FASES DE IMPLEMENTACIÓN

Acogiendo lo planteado en el modelo de seguridad y privacidad de la información del Min-TIC (MSPI), donde se plantean cinco (5) 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:

Diagnóstico

En esta fase se realiza un levantamiento de información que pretende identificar los riesgos que tiene la Institución en su infraestructura y sistemas de información.

Planificación

Partiendo de los resultados de la fase de diagnóstico, se procede a la elaboración del PRSI, definiendo las acciones a implementar y los alcances de dicho plan.

Implementación

Se implementan todas las acciones planteadas en la fase de planificación, teniendo en cuenta indicadores de riesgos y tratamiento de la seguridad y privacidad de la información.

Gestión

A través de auditorías internas, monitoreo, medición y evaluación de controles y los resultados que arrojan los indicadores de la seguridad de la información se puede verificar la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Mejora continua

En esta fase se define el plan de mejoramiento continuo donde se toman acciones para mitigar las debilidades encontradas, de acuerdo a los resultados obtenidos en la fase de evaluación de desempeño.

Tabla 1. Desarrollo de fases del PRSI

Fase	Actividad	Meta	Entregable	Plazo	Avance
Diagnostico	Realizar diagnóstico del estado actual del manejo de Riesgos de la información en el TdeA.	Determinar el grado de madurez del PRSI	Documento con levantamiento de Riesgos identificados en la actualidad	Jul-18	100%
	Realizar un diagnóstico de riesgos de la nueva solución de infraestructura TIC adquirida	Elaborar documento con los nuevos hallazgos y actualizados los existentes	Formato de manejo de riesgos actualizado	Mar-19	0%
Planeación	Realizar revisión y valoración de los Riesgos actuales.	Actualizar el formato con los riesgos actuales, identificando el nivel de riesgo actual	Formato de Riesgos actualizado	Ago-18	20%
	Establecer Los periodos y actividades a desarrollar para el seguimiento de los	Elaborar documento con directrices de	Documento con políticas de	Mar-19	0%

Fase	Actividad	Meta	Entregable	Plazo	Avance
	riesgos	control y seguimiento de riesgos	manejos de riesgos.		
Implementación	Revisión del PRSI en grupo primario	Presentación del PRSI al comité de informática	Documento de PRSI Aprobado por la alta dirección	Jun-19	0%
	Elaboración de estrategias de control de riesgos	Establecer cronograma de actividades y control de riesgos	Cronograma de seguimiento y control de riesgos	Jul-19	0%
	Configurar en los equipos de seguridad las reglas de anti-spam, anti-virus y prevención de intrusos.	Implementación de controles la infraestructura informática	Controles establecidos y en operación	Jul-19	0%
	Llevar al formato de gestión de riesgos, todos las amenazas y vulnerabilidades que requieren control	Formato actualizado con nivel de riesgos.	Formato entregado y aprobado por la oficina de Gestión de la calidad.	Dic-19	0%
Gestión	Revisar el comportamiento de los controles establecidos.	Determinar el grado de efectividad de los controles establecidos	Documento con acciones a realizar para mejorar controles a los riesgos	Sep-20	0%
Mejora continua	Realizar pruebas de penetración tanto a la infraestructura, como a los sistemas de información	Análisis de vulnerabilidades	Documento con resultado del análisis de vulnerabilidades y posibles acciones correctivas.	NA	0%
	Realizar revisiones de las actividades y acciones establecidas dentro del PRSI	Auditorías internas al PRSI	Documento con resultados de las auditorias y definición de mejoras.	NA	0%
	Definir estrategias para mejorar la cultura cibernética en la institución.	Involucrar a los usuarios en la mejora de la seguridad informática	Manuales capacitación de usuario final. Envío de Tips a través de correo electrónico.	NA	0%

6. SEGUIMIENTO Y EVALUACIÓN

Periódicamente se debe realizar una avaluación con el grupo primario, que permita establecer acciones de mejora y que el grupo conozca y participe de primera mano de las soluciones y nuevos retos en materia de control y aseguramiento de la infraestructura y sistemas de información de la institución.

7. MAPA DE RIESGOS

Tabla 2. Riesgos, impacto y controles actuales

Riesgo	Posibles Causas	Probabilidad (1-5)	Consecuencias	Impacto (1-5)	Zona Inicial	Controles Existentes	Zona Final			Políticas de Administración del Riesgo (Asumir, Evitar, Reducir, Mitigar, Compartir o Transferir)
1. Vencimiento de licencias, contratos de soporte y garantías.	*Retrasos en la gestión interna. *Descuido del supervisor del contrato *No autorización de la alta dirección. *Falta de presupuesto. *Ley de garantías	Posible (3)	*Demandas por el uso indebido del licenciamiento. *Inoperancia de la infraestructura. tecnológica *Suspensión de servicios críticos. *Insatisfacción de la comunidad educativa.	Catastrófico (5)	Extrema	Ninguno	Posible (3)	Catastrófico (5)	Extrema	**Evitar**: Parametrizar el sistema de control de fechas para las licencias y contratos de soporte. (AP) **Reducir**: Incluir los presupuestos de las licencias y contratos de soporte en los planes de acción y de adquisiciones del área. **Mitigar**: No aplica. **Compartir**: Iniciar proceso disciplinario al supervisor del contrato por incumplimiento de obligaciones. **Transferir**: No aplica.
2. No continuidad del negocio	*Falta fluido eléctrico. *Daño en la infraestructura tecnológica. *Mantto inadecuados *Vencimiento de licencias o contratos. *Incumplimiento de proveedores. *Ausencia de planes de contingencia. *Obsolescencia tecnológica	Probable (4)	*No prestación del servicio *Insatisfacción de la comunidad educativa *Procesos disciplinarios administrativos *Extemporaneidad en el cumplimiento de obligaciones	Catastrófico (5)	Extrema	*Sistema de UPS *Contratos suscritos para el mantto. *Pólizas de cumplimiento *Backup's de información TdeA	Probable (4)	Moderado (3)	Alta	**Evitar**: Documentar e implementar planes de contingencia. **Reducir**: Documentar e implementar procedimientos para el mantenimiento preventivo. **Mitigar**: Asegurar la continuidad en la contratación. **Compartir**: No aplica. **Transferir**: Hacer efectivas las pólizas de cumplimiento.

Riesgo	Posibles Causas	Probabilidad (1-5)	Consecuencias	Impacto (1-5)	Zona Inicial	Controles Existentes	Zona Final			Políticas de Administración del Riesgo (Asumir, Evitar, Reducir, Mitigar, Compartir o Transferir)
3. Acceso no autorizado a la Infraestructura Tecnológica	*Hackers *Debilidad en los controles. *No actualización del sistema de seguridad integral. *Incumplimiento a las políticas de seguridad de la información.	Posible (3)	*Pérdida o alteración de información. *Pérdida del control del sistema. *Daños en el sistema *Pérdida de imagen institucional. *Procesos disciplinarios	Mayor (4)	Extrerma	*Sistema de seguridad integral. *Políticas de seguridad de las TIC's *Capacitación usuarios. *Actualización de plataformas. *Contratos de soporte y garantía.	Posible (3)	Moderado (3)	Alta	**Evitar**: Continuidad del sistema de seguridad integral **Reducir**: Realizar seguimiento trimestral al cumplimiento de las políticas de seguridad de TIC's. **Reducir**: Documentar e implementar el proced para la sensibilización y capacitación a usuarios. **Mitigar**: Asegurar la continuidad en la contratación. **Compartir**: Iniciar proceso disciplinario o sancionatorio al funcionario o usuario. **Transferir**: Hacer efectivas las pólizas de cumplimiento por falta de controles del proveedor.
4. Pérdida de Información	*Fallas o desactualizac del sistema de seguridad integral. *No actualización de backups. *Borrado indiscriminado de información. *Errores humanos. *Fallas técnicas en los equipos. *Accesos no autorizados. *Hurto del equipo. *Virus informático.	Posible (3)	*Pérdida de capital intelectual. *Fuga de información confidencial. *Uso indebido de información. *Pérdida de imagen institucional. *Retrasos o reprocesos en la gestión.	Mayor (4)	Extrerma	*Backup's semanal de la infraestructura tecn. *PR: Entrega de puestos de trabajo. *Sistema de seguridad integral. *Capacitación a usuarios. *PR: Mantto correctivo y preventivo.	Posible (3)	Menor (2)	Moderada	**Evitar**: Continuidad del sistema de seguridad integral **Reducir**: Documentar e implementar el proced para la sensibilización y capacitación a usuarios. **Mitigar**: Asegurar la continuidad en la contratación. **Compartir**: Iniciar proceso disciplinario o sancionatorio al funcionario o usuario. **Transferir**: No aplica.