PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TECNOLOGÍA Y SISTEMAS DE LA INFORMACIÓN

2021

OBJETIVO

Dar inicio con la implementación del Plan para el Tratamiento Integral de los Riesgos asociados con la seguridad y privacidad de la información desarrollado en 2020, que permita su adecuada gestión, alineado con la Política de Seguridad de la Información y el Manual de Administración de Riesgos de la Institución Universitaria ITSA.

ALCANCE

El presente plan aplica a los activos de información y los riesgos que sean identificados en los procesos y valorados como prioritarios a través de los principios básicos y metodológicos para la gestión de los riesgos de Seguridad y Privacidad de la Información.

VALORACIÓN DE LOS RIESGOS

Para la valoración de los riesgos, se debe identificar previamente un inventario de activos de información, el cual constituye la base del enfoque de la valoración de los riesgos asociados con seguridad y privacidad de la información.

La valoración de los riesgos de seguridad y privacidad de la información comprende las siguientes actividades:

- Análisis del riesgo. En primer lugar, se deberán identificar los activos de información institucionales, de acuerdo con los procesos o actividades de la institución, cuya pérdida o daño afectan la prestación del servicio, o que son requeridos para el cumplimiento de requisitos contractuales, legales o reglamentarios. También se deberán identificar aquellos activos relacionados con el hardware, software, redes, personal, sitios y estructura organizativa, que contienen, soportan o utilizan la información.

  Una vez identificados todos los activos, se deben determinar las amenazas que pueden afectar la información, los procesos y los soportes, para luego revisar las vulnerabilidades (debilidades) que podrían aprovechar las amenazas y causar daños a los activos de información institucionales. Finalmente se identificarán cómo podrían afectar estas amenazas y vulnerabilidades la confidencialidad, integridad y disponibilidad de los activos de información.

- Estimación del riesgo. Aquí se busca establecer la probabilidad de que ocurra el riesgo y el impacto de sus consecuencias, asignándole una calificación con la finalidad de determinar el nivel del riesgo, su importancia y la estrategia para su tratamiento.

  La probabilidad indica el número de veces que el riesgo se ha presentado o que se puede presentar en un periodo de tiempo determinado. El impacto se refiere a las consecuencias que puede ocasionar en la institución la materialización del riesgo.

Una vez realizado el análisis de los riesgos determinados por su probabilidad e impacto, se obtendrá una evaluación del riesgo en un escenario sin controles y el grado de exposición al riesgo que tiene la Institución. Esta exposición no es más que la ponderación de la probabilidad e impacto y que se puede observar gráficamente en la matriz de riesgos, la cual nos permite analizar de forma global los riesgos que deben priorizarse, de acuerdo con la zona donde se encuentren ubicados, facilitando organizar los riesgos, indicar su importancia para determinar su tratamiento e implementar los planes de acción correspondientes.

Las zonas de riesgo se representan con los siguientes colores:

Zona de Riesgo Bajo	
Zona de riesgo Moderado	
Zona de riesgo Alto	
Zona de riesgo Extremo	

La matriz de riesgo contiene el impacto, la probabilidad y la zona de acuerdo con la importancia del riesgo.

MAPA DE CALOR

PROBABILIDAD DE OCURRENCIA	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi seguro	Alto	Alto	Extremo	Extremo	Extremo
Probable	Moderado	Alto	Alto	Extremo	Extremo
Posible	Bajo	Moderado	Alto	Extremo	Extremo
Improbable	Bajo	Bajo	Moderado	Alto	Extremo
Rara vez	Bajo	Bajo	Moderado	Alto	Extremo

IMPACTO

Diagrama general de Matriz de Riesgo

ESTRATEGIAS EN EL TRATAMIENTO DE RIESGOS

Una vez realizada la etapa de evaluación del riesgo, se tendrá una lista o una matriz de riesgo con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, para lo cual de deberán indicar las estrategias para el tratamiento del riesgo, con el fin de minimizar la probabilidad de materialización de este.

En virtud del nivel de los riesgos evaluados, se seleccionará una de las siguientes opciones de tratamiento por cada uno de los riesgos identificados.

- **Evitar**. Esta opción busca abandonar la actividad que origina el riesgo o escoger otras alternativas para la actividad que no incorpore el riego detectado.
- **Compartir o Transferir.** Con este procedimiento se busca entregar la gestión del riego a un tercero, para reducir la probabilidad y/o el imparto del mismo.
- **Reducir.** Establecer controles para reducir la probabilidad de ocurrencia del riesgo y/o reducir su impacto.
- **Aceptar.** No se implementarán medidas de control adicionales y se le hará frente al riesgo, verificando constantemente que este no se incrementa.

Es importante que, para la selección de los controles, se consideren posibles restricciones que impidan su elección como pueden ser: tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, uso, de personal, entre otras.

MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El seguimiento y monitoreo al Plan de Tratamiento de Riesgos, se debe hacer periódicamente revisando el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades, debido a que los riesgos son dinámicos y pueden cambiar en cualquier momento; razón por la cual es necesario una supervisión continúa para detectar nuevos activos o modificación de estos, nuevas amenazas, cambios o nuevas vulnerabilidades, cambios en las consecuencias de impactos, incidentes de seguridad, entre otros.

Para determinar el cumplimiento de la gestión de los riesgos de seguridad y privacidad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de seguridad y privacidad de la información, como las auditorías internas, que permitan en cualquier momento conocer el estado actual del cumplimiento de los objetivos y tomar decisiones de forma oportuna.

RECURSOS

Los recursos requeridos por el plan de Seguridad y privacidad de la información son los siguientes:

- Humano: Líderes de procesos, Persona encargada de Planeación estratégica, Jefe de Control Interno, responsable del Sistema de Gestión de Calidad, responsable del Proceso de Tecnologías y Sistemas de la Información, Ingeniero encargado de la administración de la infraestructura de servidores, Ingeniero encargado de la administración de networking, Ingeniero especialista en seguridad informática (Recomendado).
- Físicos: Firewall, equipos de red, servidores, equipos de escritorio.
- Software. Sistemas de información.
- Financieros: A definir.

ACTIVIDADES

El Plan de Tratamiento de Riesgos de Seguridad y privacidad de la información contempla las siguientes actividades con el fin de mitigar los riesgos sobre los activos de información institucionales:

Gestión	Actividad	Tarea	Responsable	Gestión
Tratamiento de Riesgos	Identificación	Actualizar la información de 10 activos de información pertenecientes al inventario de activos de 2 proceso misionales.	Responsable TSI / Líderes o encargados de los 2 procesos misionales	Marzo-Junio/2021
	Identificación	Revisar los listados de amenazas pueden afectar la información, los procesos y los soportes de acuerdo a los documentos, estudios, papers relacionados con la identificación de riesgos y amenazas.	Responsable TSI / Ingeniero de Planta TSI / Responsables encargados Proceso misionales	Julio-Octubre/2021
	Identificación	Revisar las vulnerabilidades (debilidades) que podrían aprovechar las amenazas y causar daños a los activos de información institucionales.	Responsable TSI / Ingeniero de Planta TSI / Responsables encargados Proceso misionales	Marzo-Junio/2021
	Identificación	Ubicar los riesgos inherentes asociados de los 15 activos identificados en el mapa de calor.	Responsable TSI / Ingeniero de Planta TSI	Julio-Septiembre/2021
	Sensibilización	Crear un curso en Aula Virtual para la concientización de la gestión de riesgos.	Personal involucrado de los procesos misionales / Ingeniero de Planta TSI	Febrero-Junio/2021

Los controles seleccionados para el tratamiento de los riesgos serán alineados con los estándares de la norma ISO 27001 y la Política de Seguridad y Privacidad de la Información institucional.