Plan de Tratamiento de Riesgos de Seguridad y privacidad de la información

Presentado Por:
Coordinador Recursos Informáticos

UNIDADES TECNOLOGICAS
DE SANTANDER

BUCARAMANGA, ENERO DE 2021

TABLA DE CONTENIDO

INTRODUCCION

El presente Plan de Tratamiento de Riesgos busca mitigar los riesgos identificados en la Matriz de Riesgo de SI (en la perdida de confidencialidad, de integridad y disponibilidad de los activos) con el fin de evitar situaciones que impidan el cumplimiento de los objetivos institucionales de Las UTS.

Este plan de tratamiento de riesgos está enfocado en evaluar las posibles acciones que sirvan para la mitigación de riesgos existentes, como medida de seguridad al resultado obtenido del análisis de los riesgos (Matriz de Riesgo de SI), el cual genero información importante sobre las necesidades del proceso de Seguridad de la información y así suministrando las herramientas adecuadas para la ejecución de las acciones planteadas.

Adoptando las buenas prácticas y los lineamientos de los estándares de la norma ISO 27001:2013, ISO 31000:2018.

1. TERMINOS Y DEFINICIONES

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Confidencialidad:** Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000).

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Disponibilidad:** Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000)

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000)

- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Vulnerabilidad:** Debilidad de un activo o de un control que puede ser explotada por una o más amenazas (ISO/IEC 27000).

2. OBJETIVO

Mitigar los riesgos asociados en Seguridad de la información a los procesos existentes de Las UTS con el fin de proteger los activos de información, el manejo de medios, el control de acceso, la gestión de los usuarios y preservando la confidencialidad, integridad, disponibilidad de la información.

2.1. OBJETIVOS ESPECIFICOS

- Implementar Políticas de la seguridad de la información para la protección de la información de acuerdo con el contexto de la organización.
- Gestionar la adecuada administración del riesgo como elemento integrador en el sistema de gestión de calidad y seguridad de la información de acuerdo con los lineamientos de la organización.
- Fortalecer el conocimiento referente a la gestión de los riesgos, su análisis y las acciones a tomar para su mitigación.

3. ALCANCE

Realizar una gestión de riesgos, que permita integrar los procesos de la organización con las buenas prácticas que contribuyan a la toma de decisiones para la prevención de incidentes que puedan afectar la continuidad del negocio.

A través de los principios básicos y metodológicos para la administración de los riesgos, así como los controles que permitan el fácil desarrollo de las fases de reconocimiento del contexto, de la identificación de los riesgos, del análisis y evaluación, las opciones de tratamiento o manejo del riesgo según la valoración.

4. RECURSOS

Para la gestión de los riesgos Las UTS dispone de los siguientes recursos:

- **Humano**: Gerente y director de operaciones, El responsable TI y/o comité TI, líderes de los procesos, Gestor estratégico TI y demás partes interesadas
- **Físico:** Los activos relacionados en la Matriz de activos **F GSI 02 Identificación y valoración de los activos**
- **Financiero:** Presupuesto asignado para Seguridad de la información
- **Técnico:** El procedimiento documentado para la gestión del riesgo **PC SGI 01 PROCEDIMIENTO GESTIÓN DE RIESGOS**

5. RESPONSABLES

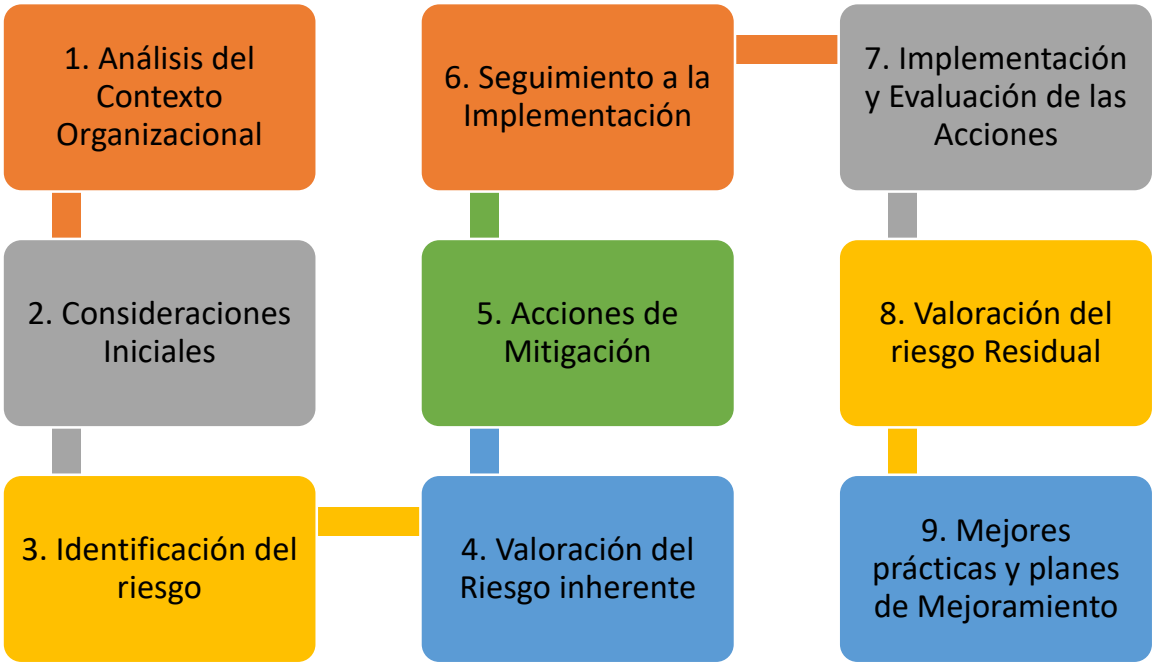
El éxito de la gestión del riesgo depende de diversos factores, aun así la participación de la gerencia y de los lideres permitirán que el proceso se desarrolle con una mayor fluidez es por ello que en la identificación de los roles no solo se observa el equipo técnico que hará las labores de análisis y tratamiento del riesgo.

- **Gerente y/o director de operaciones:** Aprueba los lineamientos para la gestión de los riesgos

- **Líderes de los procesos:** Apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos.
- **Trabajadores o terceros:** Ejecutar los controles y acciones definidas para la gestión de los riesgos aportando en la identificación de posibles riesgos que puedan afectar la gestión de los procesos, de los activos y/o la organización.
- **Responsable Ti y/o Comité de SI:** Realizar evaluación y seguimiento a las políticas, los procedimientos y los controles propios de la gestión de los riesgos.

6. VISION GENERAL DEL PROCEDIMIENTO DE GESTION DEL RIESGO

El modelo de gestión de riesgos de seguridad de la información es diseñado y adaptado con base a la norma ISO 31000 y la metodología Magerit para la adecuada gestión de los riesgos en la seguridad de la información; estructurado de la siguiente manera:



7. GENERALIDADES PARA LA GESTION DEL RIESGO

Se identifica las opciones para tratar y manejar los riesgos basados en su valoración, permitiendo la toma de decisiones y la definición de lineamientos para el control de estos; a su vez, se comunican las acciones necesarias a todos los colaboradores y demás partes interesadas para la mitigación de los riesgos.

Lo cual se definió dentro de la organización de la siguiente forma:

OPCIONES DE TRATAMIENTO DE RIESGOS	
Evitar el Riesgo	Implica tomar medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Cuando los escenarios de riesgo identificado se consideran demasiados extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.
Mitigar el riesgo	Implica tomar medidas encaminadas a disminuir tanto la probabilidad, como el impacto, a través de la optimización de los procedimientos y la implementación de controles eficientes y eficaces. El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.
Compartir o Transferir el Riesgo	Implica reducir su efecto a través del traspaso de posibles impactos a otras organizaciones, como el caso de los seguros o a través de otros medios que permitan distribuir una porción del riesgo con otra empresa. Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionarlo, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.
Asumir el riesgo	Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de

	riesgo bajo. Una vez el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el comité de seguridad de la información puede aceptar el riesgo residual.

8. METODOLOGÍA DE IMPLEMENTACIÓN

El Plan de Tratamiento de Riesgos contempla de las acciones a desarrollar en aras de mitigar los riesgos sobre los activos de TI, fueron seleccionados y validados con los estándares de la ISO 27001:2013 y su anexo A y dichas actividades se estructuraron de la siguiente manera:

No.	ACTIVIDAD	RESPONSABLE
1	Actualizar política y metodología de gestión del riesgo Actualización de los lineamientos definidos dentro de la política y el procedimiento de gestión del riesgo	Responsable TI y/o Comité SI
2	Realizar jornadas de socialización Incluir dentro del plan de capacitación una jornada para la socialización de las políticas de gestión del riesgo y la metodología a implementar dentro de la organización.	Responsable TI y/o Comité SI
3	Identificación de Riesgos Se realiza la identificación de los riesgos gestión en el formato **de Matriz de riesgos.** Una vez realizada la revisión y verificación de los riesgos identificados se realizará una jornada de retroalimentación con los líderes de los procesos para sus respectivos ajustes.	Responsable TI y/o Comité SI
4	Aprobación de los Riesgos Una vez ajustado los riesgos identificados	Responsable TI y/o Comité SI

No.	ACTIVIDAD	RESPONSABLE
	dentro de la matriz de riesgo se procederá a su aprobación y cambio de versión.	
5	Publicación de la Matriz de Riesgos SI La matriz de riesgo de SI debe quedar publicada en el repositorio organizacional de Las UTS.	Responsable TI y/o Comité SI
6	Seguimiento de las acciones Las acciones de seguimiento se harán en la matriz de riesgos de SI en la sección de Acciones de mitigación como parte del tratamiento que se le harán a los riesgos.	Responsable TI y/o Comité SI
7	Valoración de riesgo residual Realizado el seguimiento a los controles propuesto para su mitigación se procederá a valorar el riesgo residual en la sección de seguimiento a las acciones.	Responsable TI y/o Comité SI
8	Acciones de mejora Identificación de oportunidades de mejora acorde a los resultados obtenidos durante el seguimiento de las acciones en la valoración del riesgo residual	Responsable TI y/o Comité SI
9	Reporte Terminado el proceso de identificación del riesgo, de la formulación de las acciones y del seguimiento de los controles se generará un reporte de indicadores para el proceso de Seguridad de la información.	Responsable TI y/o Comité SI

8.1. DESARROLLO METODOLOGICO

Fase 1: Análisis de la información

En esta etapa se evaluarán los resultados obtenidos de las mesas de trabajo realizadas con los colaboradores y demás partes interesadas en el proceso de SI, descritas de la siguiente manera: -

- Socializar y aplicar la política de Gestión del Riesgo.
- Determinar los controles para la mitigación de los riesgos identificados e incluirlos en el Plan de tratamiento de riesgos.

Fase 2: Desarrollo de los controles

En esta fase se realizarán las actividades que permitirán la estructuración de las acciones para la mitigación de los riesgos.

- Determinar el estado del riesgo
- Determinar los controles a implementar (acciones)
- Definir los responsables
- Definir tiempos de ejecución.

Fase 3: Análisis de los controles

En esta fase se analizarán los controles propuestos para la mitigación del riesgo.

- Validar los riesgos mitigados por cada control propuesto
- Análisis de la aplicabilidad de los controles (Anexo A)
- Análisis de la priorización de los controles

Fase 4: Definición del organigrama de responsabilidad

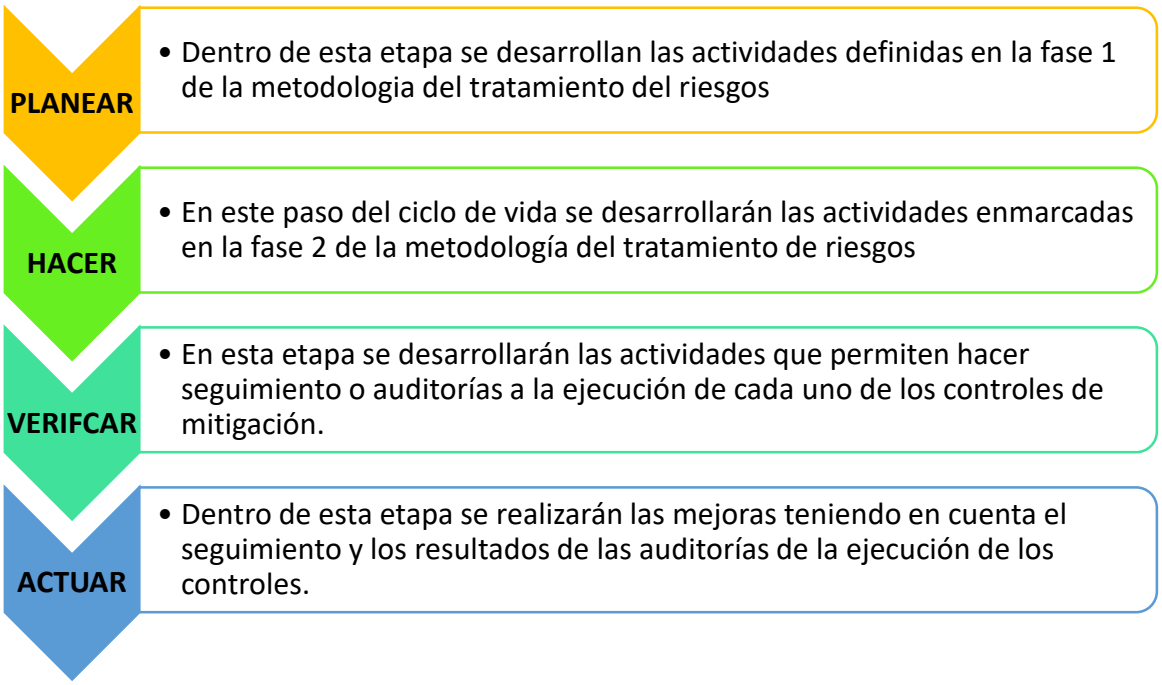
En esta fase se realizará la asignación de responsabilidades respecto a la gestión del riesgo, esta etapa deberá ser definida por el comité de SI teniendo en cuenta la estructura organizacional

- Identificación de las actividades en función de la Seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte de Las UTS para la aplicación de las políticas y demás lineamientos.

Fase 5: Ciclo de vida del tratamiento de riesgos

En esta fase se define las actividades a realizar para el cumplimiento de cada uno de los elementos que conforman el Plan de tratamiento de Riesgos.

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):



Dentro de este plan de tratamiento de riesgo se hace la aclaración que no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para la identificación oportunidades. Entendiéndose como oportunidad la consecuencia positiva de alguna acción.

9. CRONOGRAMA

Para dar cumplimiento al plan de tratamiento de riesgos, el cronograma se establecerá anualmente y serán identificados en la matriz de riesgos, donde se establecerán las acciones de control y las fechas para implementar dichos

controles, el responsable de TI y/o el comité de SI apoyarán en el proceso de definición de los controles con los líderes de los procesos.

10. SEGUIMIENTO Y EVALUACIÓN

Cuando sea solicitado se presentarán avances sobre el funcionamiento y el manejo de los riesgos en cuanto al cumplimiento de las políticas y las directrices para la gestión del riesgo. Los resultados de la evaluación y las observaciones deben ser posteriormente solucionados para que se tomen las decisiones pertinentes garantizando la Gestión del Riesgo dentro de la organización.

11. MEDICION

La medición se realizará con un indicador de gestión que este orientado principalmente en determinar el porcentaje de cumplimiento en la implementación de los controles definidos dentro de la matriz de riesgos y lo dispuesto en el plan de tratamiento de riesgos.