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

Presentado Por:

Coordinador Recursos Informáticos

UNIDADES TECNOLOGICAS DE SANTANDER

BUCARAMANGA, DICIEMBRE DE 2019.

Tabla de contenido

1. DEFINICIÓN

El presente documento establece los lineamientos para la administración, revisión, modificación y evaluación del tratamiento de riesgos de seguridad y privacidad de la información en las Unidades Tecnologías de Santander. En el mismo, se incluyen los principios y obligaciones que asume la institución con el fin de garantizar la protección de la información personal en razón a su tratamiento.

2. OBJETIVO GENERAL

Definir los lineamientos para la estructuración de una política donde se reflejen los criterios sobre la obtención, recolección, uso, tratamiento, intercambio, transferencia, transmisión, vigencia y supresión de los datos personales en las bases de datos de la institución, así como las responsabilidades de los directivos y trabajadores, encargados del tratamiento de datos personales en las Unidades Tecnológicas de Santander.

3. OBJETIVOS ESPECIFICOS

- Orientar en la implementación del Sistema de Gestión de Seguridad de Datos Personales en la operación y funcionamiento de la institución.
- Establecer los lineamientos para la conformación del gobierno del Sistema de Gestión de la Seguridad de Datos Personales y para la adjudicación de nuevas responsabilidades a los miembros que lo compongan.
- Asegurar la sostenibilidad del Sistema de Gestión de Seguridad de Datos Personales, a partir de la gestión de mecanismos de revisión y evaluación de dicho sistema y de la Política de Tratamiento de Información de la institución.
- Asegurar una cultura de protección de datos personales, mediante el reforzamiento cognitivo periódico, de temas asociados a la seguridad de la información.
- Realizar un seguimiento y control a la eficacia del plan tratamiento de riesgos de seguridad y privacidad de la información

4. MARCO LEGAL

	NORMA	DESCRIPCION
1	NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices
2	NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
3	Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

5. DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la institución.

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Activos de información: Los activos de información son los recursos del Sistema de Seguridad de la Información, relacionados con el procesamiento, almacenamiento y salvaguarda de la información de la institución y que soportan los procesos necesarios para la continuidad de las operaciones.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a destinatarios no autorizados. La información debe ser accedida sólo por aquellas personas a las que se ha concedido acceso como una necesidad legítima para la realización de sus funciones.

Control: Las políticas, los procedimientos, las prácticas y las estructuras institucionales concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Hallazgo: situación, evento o falla de las salvaguardas identificados de una condición de un sistema, servicio o red, que indica probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información, también se consideran la fuente o causa del riesgo y establecen la justificación de su valoración cualitativa.

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.

Privilegios: son los permisos de acceso otorgados a un usuario a una o varias funcionalidades de un activo de información tal como: red, sistemas de información, internet, aplicaciones web, recursos compartidos, servicios de impresión/escáner, telefonía, equipos de cómputo, etc.

Incidente de seguridad de la información: se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos.

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.

Impacto: Las consecuencias para la institución de la materialización de un riesgo.

Probabilidad: Medida porcentual para estimar la posibilidad de que el riesgo ocurra en las circunstancias expuestas en el hallazgo.

Integridad: Propiedad de la información relativa a su exactitud y completitud. La falta de integridad de la información puede exponer a la institución a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas económicas.

Riesgo Absoluto: Valoración del riesgo, sin la ejecución de ningún control.

Riesgo Controlado: El riesgo que permanece tras el tratamiento del riesgo mediante la implementación de los controles del sistema de gestión de seguridad de la información

Selección de controles: Proceso de elección de las salvaguardas que aseguren la reducción de los riesgos a un nivel aceptable.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo en términos de la probabilidad de su materialización y el impacto en caso de materializarse.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. ROLES Y RESPONSABILIDADES DEL PLAN

Con el propósito de garantizar la implementación y cumplimiento del presente plan se deben definir al interior de la institución, se presenta las actividades generales para la implementación del plan, el grupo de trabajo con sus respectivas funciones.

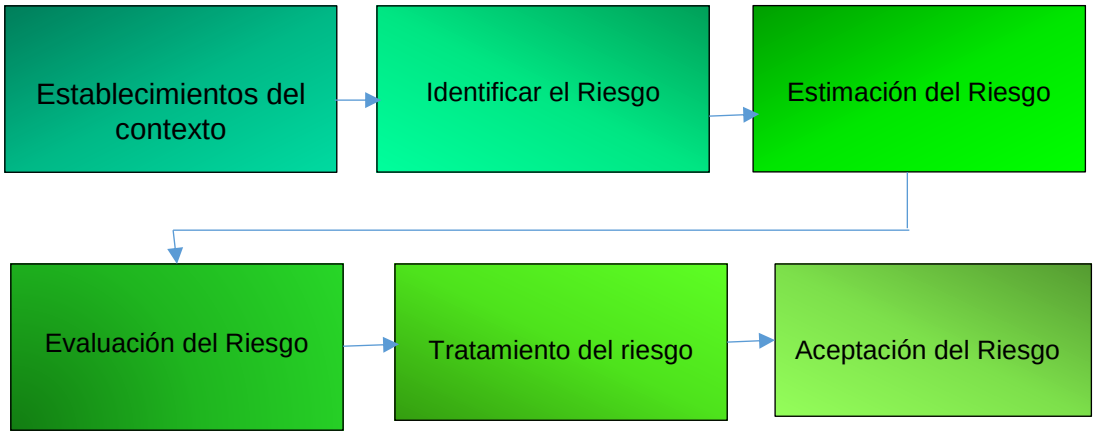

Imagen 1 Estructura General de la Metodología del Riesgo

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)

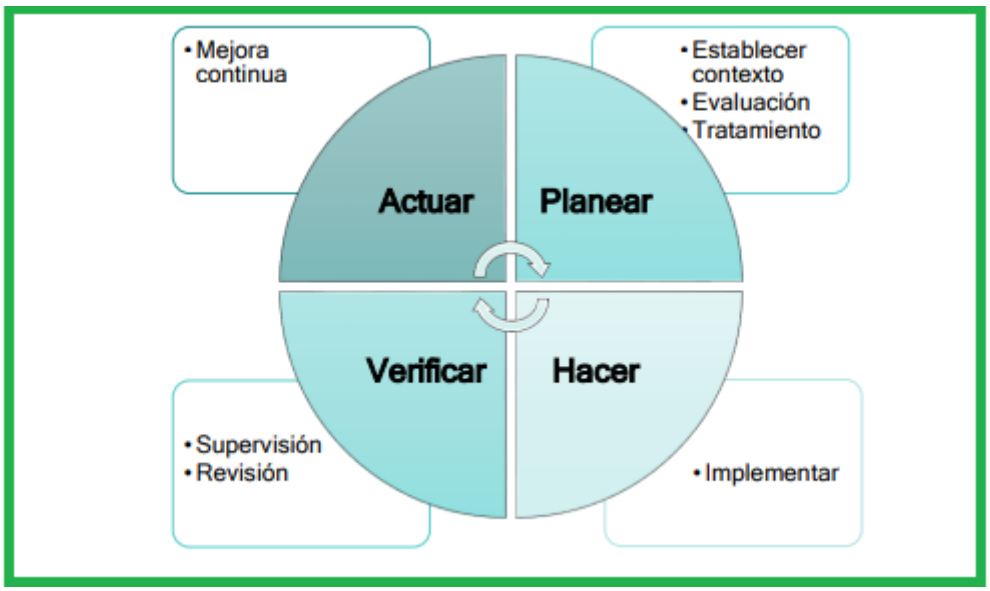

Imagen 2. Ciclo PHVA y la gestión de riesgos

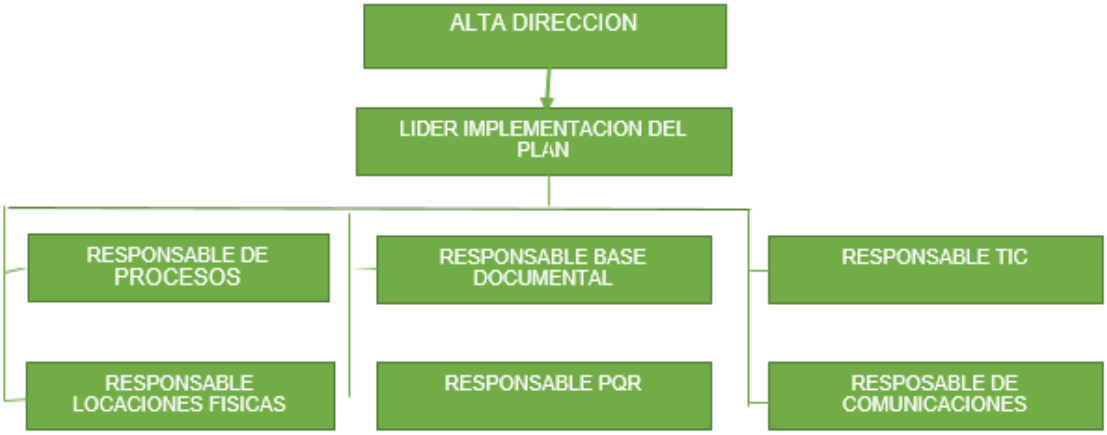

Imagen 3. Organigrama Roles

- **Alta Dirección:** Tomará las decisiones fundamentales para la implementación del plan y supervisará los resultados del funcionamiento del mismo.

- **Líder de la implementación del plan:** Al cargo designado para ejercer este rol, se le adscriben las siguientes funciones, supervisar la implementación de la Política de Tratamiento de la Información. De igual forma deberá coordinar y supervisar el cumplimiento de la implementación y funcionamiento del plan.

- **Responsable de Procesos:** Velar por la implementación, cumplimiento y actualización de los protocolos del ámbito de procesos descritos en el plan. Deberá gestionar los cambios en los elementos del plan, en el evento que existan modificaciones de procesos, procedimientos, documentos y normativas en la institución.

- **Responsable de Base Documental:** Al cargo designado para ejercer este rol, se le adscriben las siguientes funciones: Velar por la implementación, cumplimiento y actualización de la Política de Tratamiento de la Información y protocolos del ámbito de bases documentales, de igual forma deberá conservar y actualizar el normograma asociado a la seguridad de los datos personales.

- **Responsable de TIC:** Velar por la implementación, cumplimiento y actualización de las políticas y protocolos del ámbito TIC, de igual manera deberá gestionar los incidentes de seguridad de la información, para lo cual deberá implementar un Protocolo de Gestión de Incidentes de Seguridad.

Así mismo deberá llevar una medición de los Incidentes de seguridad asociados al tratamiento de datos personales.

- **Responsable de Locaciones Físicas:** Al cargo designado para ejercer este rol, se le adscribe la función de velar por la implementación, cumplimiento y actualización de las políticas y protocolos del ámbito de locaciones físicas de la institución.

- **Responsable de PQRS:** Atender y documentar la gestión de políticas de seguridad relacionadas con el tratamiento de datos personales. En los eventos de reclamos, reportar al Responsable de TIC para efectos del registro correspondiente en los indicadores de gestión.

- **Responsable de Comunicaciones:** Coordinar espacios de socialización del plan, políticas y protocolos de seguridad: Socializar al nuevo talento humano de la institución, el tema de protección de datos personales y el presente Documento de Privacidad de Información. Coordinar la realización de conferencias de reforzamiento cognitivo en seguridad de la información y de datos personales.

7. VALORACION DE RIESGOS

La valoración del riesgo y oportunidades utiliza las variables:

7.1. Probabilidad:

PROBABILIDAD	DESCRIPCIÓN	CALIFICACIÓN
Casi cierta	Es casi un hecho y/o ha ocurrido varias veces en el pasado	5
Muy probable	Alta posibilidad de que el evento ocurra y/o ha ocurrido en el último trimestre	4
Moderada	Alguna posibilidad de que el evento ocurra y/o ha ocurrido en el último semestre	3
Poco probable	Insignificante posibilidad de que el evento ocurra y/o ha ocurrido en el último año	2
Rara	Solo puede ocurrir en circunstancias excepcionales	1

7.2. Severidad o impacto:

IMPACTO	IMPACTO EN OPERACIÓN INSTITUCIÓNIAL	IMPACTO IMAGEN	CALIFICACIÓN
Catastrófico	Impacta completamente elementos indispensables para la operación misional y/o activos de alta confidencialidad	Altamente perjudicial, muy negativo con inminente cese de operaciones, efecto publicitario a nivel nacional, pérdida de clientes y/o intervención de ente regulador	5
Mayor	Impacta parcialmente procesos misionales de negocio y/o activos de alta confidencialidad	Tiene un gran impacto con repercusión muy negativa y efecto publicitario a nivel del sector, pérdida de clientes, requerimiento formal y/o sanción de ente regulador	4
Moderado	Impacta procesos no misionales y/o activos de media confidencialidad o información reservada	De mediano impacto, es relevante para la imagen de la institución con efecto publicitario local, incremento de reclamos de clientes, requerimiento informal y/o sanción del ente regulador	3
Menor	Impacta procesos no misionales y/o activos de baja confidencialidad o información interna	De poca importancia, con impacto leve, sin efecto publicitario, incremento de reclamos de clientes con posibles perdidas	2
Insignificante	No afecta activos, ni la operación, únicamente elementos de apoyo	De poca importancia sin efecto publicitario y/o posibles reclamos de clientes	1

7.3. El análisis del riesgo

Busca establecer la probabilidad de ocurrencia de los riesgos y la severidad o impacto de ellos, calificándolos y evaluándolos para establecer el nivel de riesgo y las acciones que conformarán el plan de tratamiento a implementar.

7.4. El efecto

Define las consecuencias o efectos que pueden perjudicar a la organización si se materializa el riesgo.

7.5. La calificación del riesgo

Se logra a través de la multiplicación de la probabilidad de ocurrencia y la severidad (impacto de la materialización del riesgo).

PROBABILIDAD	IMPACTO				
	INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
RARO (1)	1	2	3	4	5
IMPROBABLE (2)	2	4	6	8	10
MODERADA (3)	3	6	9	12	15
PROBABLE (4)	4	8	12	16	20
CASI SEGURO (5)	5	10	15	20	25

E EXTREMA A ALTA M MODERADA B BAJA

Imagen 4. Valoración del Riesgo

8. TRATAMIENTO DEL RIESGO

Deberá seleccionar las opciones de manejo o tratamiento en las siguientes categorías:

- **Evitar el Riesgo**: deberá seleccionar esta opción si es posible generar mejoras en los procesos o rediseños en los mismos encaminados a evitar la actividad que genera el riesgo.

- **Reducir el Riesgo**: deberá seleccionar esta opción si el riesgo se materializó en el pasado, o si su valor está en alguna de las siguientes zonas: moderada, alta o extrema y es posible implementar acciones encaminadas a reducir su probabilidad de ocurrencia o el impacto en caso de materializarse. También se puede seleccionar si, aunque la zona de riesgo en la que se encuentra es baja, se pueden generar acciones de mejora para reducirlo aún más.

- **Compartir o transferir el riesgo**: deberá seleccionar esta opción si se cuenta con controles que reduzcan el efecto a través del traspaso del impacto a otras organizaciones.

- **Asumir el riesgo**: una vez analizadas las opciones a, b y c y si no es aplicable ninguna, el responsable del riesgo puede seleccionar esta opción siempre y cuando el riesgo haya quedado en zona de riesgo “Baja” o “Moderada” asumiendo las responsabilidades y posibles consecuencias que pueda traer su materialización. En caso de que un riesgo se encuentre en una zona de riesgo alta o extrema y no exista la posibilidad de reducirlo, el riesgo debe permanecer en constante monitoreo y debe contar con planes de contingencia para actuar en caso de materializarse.

Los siguientes criterios, sirven para identificar como categorizar el tratamiento del riesgo:

8.1. Estrategias de evasión:

Se trata de minimizar la probabilidad de que el riesgo se presente. Para ello existen 4 opciones principales: transferencia, reducción, elusión y diversificación.

- **Transferencia:** representa el conjunto de procedimientos cuyo objetivo es eliminar el riesgo transfiriéndolo de un lugar a otro. Consiste, por ejemplo, en vender un activo dudoso, asegurar una actividad con importantes riesgos, etc
  .
- **Reducción:** esta estrategia busca, bien reducir la probabilidad de ocurrencia de un riesgo, bien reducir sus consecuencias, o bien lograr ambos objetivos a la vez. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, arreglos organizacionales, y procedimientos encaminados a reducir la frecuencia o la oportunidad de que ocurra un error.

- **Elusión:** existen dos opciones para intentar eludir un riesgo: no proceder con el proyecto o la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad, que logren el mismo resultado y no incorporen el riesgo detectado.

- **Diversificación:** consiste en intentar extender el riesgo de un área en concreto, a diferentes secciones, con el fin de impedir la pérdida de todo el negocio.

8.2. Estrategias de minimización:

Se trata de reducir el impacto del riesgo en el producto o proyecto. Las estrategias de minimización se platean cuando han fallado las estrategias de evitación, y por tanto, el riesgo pasa a ser un hecho. En estos casos, deberá plantearse un Plan de contingencia, que intentará paliar los efectos negativos del riesgo, una vez éste ya se ha producido.

9. SEGUIMIENTO Y EVALUACIÓN DEL PLAN

Establecer y ejecutar el Plan de auditoría del Sistema de Gestión de Seguridad de Datos Personales, para lo cual se sugiere la incorporación del siguiente cronograma de actividades:

CRONOGRAMA DE SEGUIMIENTO Y EVALUACIÓN DEL PLAN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN												
Actividad	**2020**											
	ENE	**FEB**	**MAR**	**ABRIL**	**MAYO**	**JUNII**	**JUL**	**AGOST**	**SEP**	**OCT**	**NOV**	**DIC**
Sensibilización Institutional												
Revisión y Evaluación del funcionamiento del Plan												
Revisión de actualizaciones de la PTI												
Revisión externa del funcionamiento del Plan												

Imagen 5. Cronograma

10. ASEGURAMIENTO DE LOS DATOS PERSONALES.

Para mitigar los riesgos de pérdida o consulta indebida de información crítica de la institución educativa tanto para los dispositivos corporativos, como los propios de los docentes y alumnos; deben seguirse las siguientes medidas básicas de seguridad:

- Activar la opción de copias de seguridad en los dispositivos.
- Desactivar la instalación de aplicaciones que no provengan de una tienda oficial.
- Implementación de un esquema de control de dominio sobre los equipos que se encuentren en la red de la institución para el manejo de acceso y control de perfiles de usuarios.
- Establecer contraseña de acceso seguras en los equipos de la institución.
- Evitar utilizar las redes Wifi públicas cuando se vaya a acceder a información sensible o crítica.
- Manejar contraseñas diferentes para el entorno laboral y para el personal.
- Desactivar la función de Auto-completado de formularios y credenciales de acceso.
- No descuidar los teléfonos móviles, tablets o laptops en lugares públicos, o abandonarlos adentro de los vehículos para evitar robos o accidentes que pongan en riesgo la información de la institución.
- Obliga a adoptar todas las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal, y las tendentes a la disminución de su alteración, pérdida, tratamiento o acceso no autorizado, entre otras, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que pueden estar almacenados y los riesgos a los que pueden estar expuestos, ya provengan de acción humana, o se trate de un hecho físico o natural.

11. EVALUACIÓN DE LA GESTIÓN DE RIESGOS

La evaluación de la efectiva gestión del riesgo se puede evidenciar a través de:

- La disminución de la valoración de los riesgos identificados.
- El aumento del número de controles existentes.
- Los resultados de la evaluación de efectividad de los controles.
- La ejecución de los planes de tratamiento determinados.
- La (in)materialización del Riesgo.
- Los resultados asociados al desempeño de los procesos.
- El Cumplimiento de los objetivos organizacionales