

	PROCESO TECNOLOGÍA DE LA INFORMACIÓN	CÓDIGO: PRTC-PC-03
	PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN	FECHA: 19/12/2023
		VERSIÓN: 1

1. OBJETIVO

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

- Involucrar a todas las áreas en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

2. DEFINICIONES

Acciones asociadas: son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.

Administración de riesgos: conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

Amenaza: situación externa que no controla la entidad y que puede afectar su operación

Análisis del riesgo: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

Asumir el riesgo: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

Causa: medios, circunstancias y/o agentes que generan riesgos.

Calificación del riesgo: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Compartir o transferir el riesgo: opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

Consecuencia: efectos que se pueden presentar cuando un riesgo se materializa.

Contexto estratégico: son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una entidad.

Control: acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

	PROCESO TECNOLOGÍA DE LA INFORMACIÓN	CÓDIGO: PRTC-PC-03
	PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN	FECHA: 19/12/2023
		VERSIÓN: 1

Control preventivo: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

Control correctivo: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

Debilidad: situación interna que la entidad puede controlar y que puede afectar su operación.

Evaluación del riesgo: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

Evitar el riesgo: opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.

Frecuencia: ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

Identificación del riesgo: etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

Impacto: medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

Mapa de riesgos: documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

Materialización del riesgo: ocurrencia del riesgo identificado

Opciones de manejo: posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

Plan de contingencia: conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio

Probabilidad: medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

Procedimiento: conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

Proceso: conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

	PROCESO TECNOLOGÍA DE LA INFORMACIÓN	CÓDIGO: PRTC-PC-03
	PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN	FECHA: 19/12/2023
		VERSIÓN: 1

Riesgo: eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

Riesgo de corrupción: posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

Riesgo inherente: es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

Riesgo institucional: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

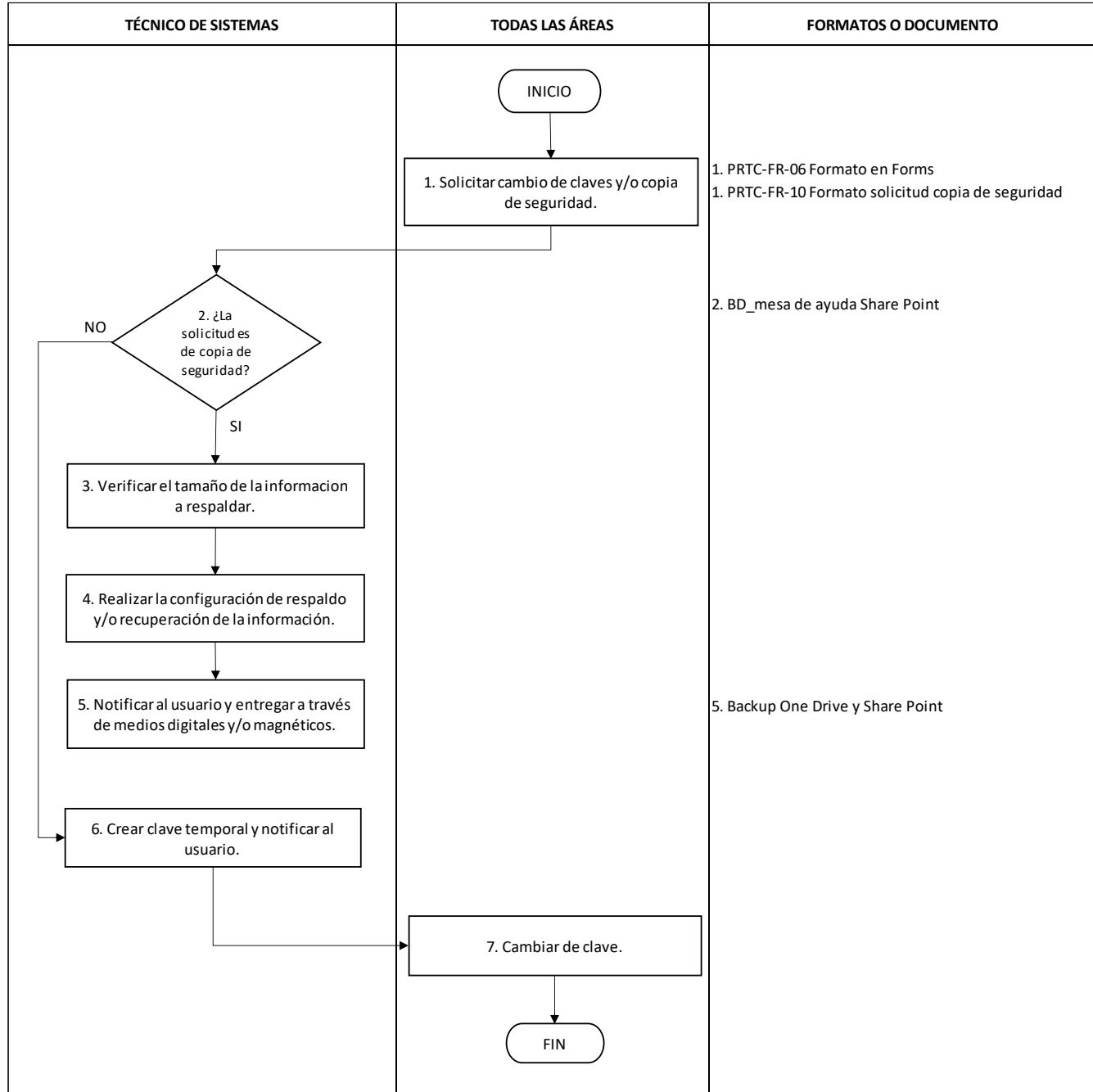
- **Los riesgos que han sido clasificados como estratégicos:** en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
- **Los riesgos que se encuentran en zona alta o extrema:** después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
- **Los riesgos que tengan incidencia en usuario o destinatario final externo:** en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa. Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción serán considerados como riesgos de tipo institucional.
- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

3. GENERALIDADES

Este procedimiento es el conjunto de medidas y técnicas para controlar y salvaguardar todos los datos que se manejan dentro de la organización y asegurar que los datos no salgan del sistema que ha establecido la organización.

Es la pieza clave para que la entidad pueda llevar a cabo sus operaciones, ya que los datos que se manejan son esenciales para la misionalidad. De forma mayoritaria, los sistemas de la organización se basan en las nuevas tecnologías, Es importante comprender que la entidad cuenta con datos sensibles, y que por ello se tienen que establecer las medidas de seguridad en protección de datos necesarios para garantizar el correcto tratamiento de estos.

4. DESCRIPCIÓN DE ACTIVIDADES



	PROCESO TECNOLOGÍA DE LA INFORMACIÓN	CÓDIGO: PRTC-PC-03
	PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN	FECHA: 19/12/2023
		VERSIÓN: 1

5. DOCUMENTOS RELACIONADOS

PRTC-FR-06 Formato en Forms

PRTC-FR-10 Formato solicitud copia de seguridad

Base de datos - mesa de ayuda

6. CONTROL DE CAMBIOS DEL DOCUMENTO

VERSION	FECHA	DESCRIPCION DE LA MODIFICACION
Versión 1	19/12/2023	Primer documento.

Elaboró: Cesar Alfredo Sanabria Méndez - Técnico en Sistemas
 Jeisson Leonardo Gil – Profesional de Planeacion y Calidad
 Deisy Viviana Triviño – Técnica de Apoyo Administrativo
 Revisó: Hugo Alberto Vega – Director de Desarrollo Administrativo