Supersolidaria

Superintendencia de la Economía Solidaria

"Super-Visión" para la transformación

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

El emprendimiento es de todos

Minhacienda

Contenido

DEFINICIONES

Administración del riesgo: Conjunto de elementos de control que al interrelacionarse brindan a la entidad la capacidad para emprender la acción necesaria que le permita el manejo de los eventos que pueden afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de información: Cualquier información o elementos de valor para los procesos de la entidad.

Análisis de riesgo: Método sistemático de recopilación, evaluación, registro y difusión de la información necesaria para formular recomendaciones orientadas a la adopción de una posición o medida de respuesta a un peligro determinado.

Amenaza: Causa potencial de una situación de incidente y no deseada por la organización.

Causa: Son todo aquello que se puede considerar fuente generadora de eventos - riesgos.

Confidencialidad: Propiedad en la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Control: Acción o mecanismo que se implementa para prevenir o reducir el riesgo.

Criterios del riesgo: Los términos de referencia frente a los cuales la importancia de un riesgo será evaluada.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis de riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Factores de riesgo: Situaciones, manifestaciones o características medibles observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, puede ser internos o externos a la entidad.

Gestión de riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de evaluación y el tratamiento de riesgo.

Identificación del riesgo: Proceso para encontrar enumerar y caracterizar los elementos de riesgo.

Impacto: consecuencias generadas por la materialización de un riesgo.

Incidente de la seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer la operación del negocio y amenaza a la seguridad de la información, confidencialidad, integridad y disponibilidad.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgo, expresa en términos de la combinación de la consecuencia y su probabilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Probabilidad: Es la posibilidad que de ocurrencia de un evento.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Riesgo: De acuerdo con la norma técnica ISO 31000, se define el riesgo como “El efecto de la incertidumbre sobre los objetivos” (ISO31000 ICONTEC, 2011, Pág.4).

Riesgo inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgos en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupo de activos causando así daño en la organización.

Reducción de riesgo: Acciones que se toman para disminuir la probabilidad, las consecuencias negativas o ambas, asociadas con un riesgo.

Retención de riesgo: Aceptación de la pérdida proveniente de un riesgo particular.

Valoración del riesgo: Proceso global de identificación del riesgo, análisis de riesgo y evaluación de los riesgos.

Vulnerabilidad: falencia o debilidad asociada a la tecnología, las personas, políticas o procedimientos (controles).

Seguridad de la información: Preservación de la confidencialidad integridad y disponibilidad de la información.

1. INTRODUCCION

La importancia de la seguridad y privacidad de la información va más allá de contar con herramientas y modelos que permitan trazar una ruta de acción para brindar los servicios digitales de las entidades de una manera adecuada y por supuesto asegurando la confiabilidad de los usuarios. Existen en el camino eventos que pueden llegar a perturbar el quehacer y las funciones propias de la entidad, tratados estos como riesgos que pueden ser previsibles y que, por su naturaleza, desde la administración se establezcan actividades que trabajen en función de la mitigación de los mismos, a través de acciones, en su mayoría preventivas que permitan ofrecer los servicios de una manera estable y persistente bajo las premisas de continuidad que cada uno de los activos tecnológicos que lo ameritan.

El presente documento se basa en la gestión sobre aquellos riesgos vigentes que puedan representar una potencial amenaza frente al manejo de los activos e información digital, bajo lineamientos de seguridad y privacidad de la información de la entidad para mantener un ambiente seguro de la información, de acuerdo con las directrices para el manejo adecuado, enmarcado en un plan de acción para el correspondiente tratamiento.

La seguridad de la información en las entidades debe tener como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales, como son la confidencialidad, integridad y la disponibilidad, adoptando e implementando medidas de control de seguridad de la información, que faciliten gestionar y reducir los riesgos e impactos a que está expuesta.

La SUPERSOLIDARIA vincula el modelo de administración de los riesgos de la seguridad de la información y las actividades de valoración de los mismos, en cumplimiento de la política de seguridad de la información, como medio para mantener la seguridad de la información de la entidad, preservando sus principios a saber:

- **Confidencialidad:** Propiedad que la información sea conocida únicamente a quien esté autorizado.
- **Integridad:** Propiedad que la información se mantenga exacta y completa.
- **Disponibilidad:** Propiedad que la información sea accesible y utilizable en el momento que se requiera.

2. OBJETIVO

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que la Supersolidaria pueda estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

Contar con una herramienta que proporcione los lineamientos requeridos para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información.

3. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a prevenir incidentes que puedan afectar el logro de los objetivos

La gestión de riesgos de seguridad de la información y su tratamiento, será aplicada a los procesos de la Supersolidaria, a los sistemas de información, mediante los principios establecidos para la administración de los riesgos de seguridad de la información, así como las técnicas y actividades que permitan y faciliten la identificación de los riesgos de seguridad de la información, análisis, evaluación, tratamiento, manejo y monitoreo del riesgo.

4. OBJETIVOS ESPECIFICOS

- Definir lineamientos y principios para la administración de los riesgos de seguridad de la información de la Supersolidaria.
- Fortalecer el sistema de gestión de riesgos de la entidad, a través de los controles y medidas de seguridad de la información, acordes con el marco estratégico y el quehacer institucional.
- Establecer mecanismos de protección de los activos de información, propendiendo por la mitigación del riesgo.
    - Fomentar la cultura y apropiación encaminada a la identificación, manejo y mitigación de los riesgos de seguridad de la información.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

5. PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN

La gestión de riesgos de seguridad de la información deberá ser iterativa para la actividad de valoración de riesgos o tratamiento de estos.

Como criterios para la gestión de riesgos de seguridad de la información se pueden establecer.

- El valor estratégico de la información en la Supersolidaria.
- La Criticidad de los activos de información.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- El nivel de importancia de los principios de seguridad de la información en la entidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la SUPERSOLIDARIA.

La Gestión para los riesgos asociados a la seguridad y privacidad de la información de la SUPERSOLIDARIA se debe basar en la **Política para la Administración de Riesgos de la Supersolidaria (PO-PLES-002)**, **Metodología para la Gestión de Riesgos (MT-PLES-001)**, y en las recomendaciones de la **norma ISO 27001**, buscando que haya una integración a lo que se ha desarrollado dentro de la Entidad como parte de los modelos de Gestión. Así mismo, para la evaluación de riesgos en seguridad de la información la Entidad debe preservar la Confidencialidad, Integridad y Disponibilidad de la información.

6. IDENTIFICACIÓN DEL RIESGO

El propósito de la identificación del riesgo es determinar qué pasaría en el caso de una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida. Se tiene un enfoque para la identificación del riesgo es basado en procesos y cuya responsabilidad es del dueño de proceso. Para ello se debe al menos definir el riesgo, activos de información asociados, así como el responsable de gestionarlo.

7. IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas institucionales; éstas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Por lo tanto, se deben identificar los orígenes de las amenazas accidentales como deliberadas.

8. IDENTIFICACIÓN DE CONTROLES EXISTENTES

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios; así mismo, mientras se identifican los controles es recomendable hacer una verificación del funcionamiento de los existentes y establecer las acciones para mejorar su implementación. Si no existen controles asociados a un riesgo, se debe establecer los mecanismos para la adopción del control que permita darle el adecuado y aceptable tratamiento al riesgo.

9.IDENTIFICACIÓN DE VULNERABILIDADES

Es importante identificar y conocer la lista de amenazas comunes, inventario de activos y controles existentes, para llevar a cabo una identificación de vulnerabilidades eficiente y generar las acciones para su mitigación.

10. CONTROL DE CAMBIOS

Fecha	Descripción del cambio
Diciembre 26 de 2021	Actualización del Plan por cambio de vigencia 2021