PLAN DE TRATAMIENTO DE RIESGOS

SERVICIUDAD E.S.P

DOSQUEBRADAS, AÑO 2021

INTRODUCCIÓN

La Seguridad de la Información en las empresas tiene como foco la protección de los activos de información en cualquiera de sus estados ante posibles amenazas o brechas que generen riesgos sobre principios fundamentales de confidencialidad, integridad, disponibilidad de la información, es por eso que, a través de la identificación, análisis e implementación de controles sobre estos, se permite gestionar y reducir los riesgos e impactos a que están expuestos en la Entidad. De este modo SERVICIUDAD ESP presenta el plan de acción para el tratamiento de riesgos con matriz de identificación análisis y controles en cumplimiento de la política de seguridad de la información aprobada por la Gerencia, y como herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible.

1. OBJETIVO

Establecer una herramienta con enfoque holístico que proporcione las pautas necesarias para identificar, implementar y fortalecer una efectiva gestión de los riesgos de seguridad de la información.

2. ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso, sistema de información o aplicación de SERVICIUDAD ESP, a través de la gestión y administración de los riesgos de seguridad de la información.

3. DEFINICIONES

Riesgo: Posibilidad de ocurrencia de un evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Administración del riesgo: Conjunto de elementos de control que brindan a la Entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: Cualquier información de valor para los procesos de la Organización.

Disponibilidad: Propiedad de la información para su acceso y uso cuando lo requiera una Entidad o usuario autorizados.

Confidencialidad: Propiedad de la información para disposición de uso de usuarios o Entidades autorizados.

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.

Valoración del Riesgo: Procedimiento de identificación, análisis y evaluación de los riesgos.

4. MARCO LEGAL

Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

5. TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el marco del Modelo de Seguridad y Privacidad de la Información se busca prevenir los impactos no deseados que se puedan presentar en afectación a la seguridad de la información, por lo cual es importante identificar, analizar, controlar y establecer los riesgos de seguridad de la información.

5.1. VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En esta actividad se identifica el inventario de activos de información que intervienen en los procesos de la Entidad, que será base del enfoque de la valoración de los riesgos de seguridad de la información. Definido el inventario, se describe cuantitativamente o cualitativamente, según el enfoque de la Oficina de Tecnologías de la Información y el activo correspondiente, para priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para SERVICIUDAD ESP

5.2. IDENTIFICACIÓN DEL RIESGO

Como se expuso en la fase anterior, para la evaluación de riesgos de seguridad de la información, primero debe identificarse los activos de información por proceso en evaluación.

Los activos de información se clasifican en dos tipos:

Primarios:

- **Procesos o Subprocesos y actividades del Negocio:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.
- **Información:** información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.
- **Actividades y procesos de negocio:** que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

De Soporte:

- **Hardware:** Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
- **Software:** Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
- **Redes:** Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)

- **Personal:** Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- **Sitio:** Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
- **Estructura organizativa:** responsables, áreas, contratistas, etc.

La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisan las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la Entidad.