PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024

Personería Distrital de Cartagena de Indias

Personería Auxiliar

PERSONERIA
DE CARTAGENA DE INDIAS

INTRODUCCION

El presente Plan de Tratamiento de Riesgos se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno digital en el Eje Temático de la Estrategia en **seguridad y privacidad de la información**, el cual busca proteger los datos de los ciudadanos garantizando la seguridad de la información.

OBJETIVOS

Tratar y Monitorear los riesgos asociados a los procesos existentes de la Personería Distrital de Cartagena de Indias con el fin de proteger los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

OBJETIVOS ESPECIFICOS

- Elaborar un plan de trabajo para la implementación del plan de seguridad y privacidadde la información.

- Aplicar las metodologías del DAFT o de la ISO respectivamente en seguridad de la información.

ALCANCE

La Personería Distrital de Cartagena es una entidad orientada al mejoramiento continuo, através de su plan de acción de seguridad y privacidad de la información, se aplicara a todaslas áreas de la entidad, con el compromiso día a día en la satisfacción de las necesidades de sus usuarios (comunidad) a través de la prestación de servicios de calidad, atendidos oportunamente y con respeto a la dignidad humana, enmarcados en los parámetros de ley;los cuales se soportan en procesos óptimos, un equipo de colaboradores competentes y en mecanismos de comunicación efectivos.

TERMINOS Y DEFINICIONES

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la informaciónpública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

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 dañosa un sistema o a la organización. (ISO/IEC 27000).

Confidencialidad: Propiedad que determina que la información no está disponible nisea 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.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentranen formatos estándar e interoperables que facilitan su acceso y reutilización, los cualesestán bajo la custodia de las entidades públicas o privadas que cumplen con funcionespúblicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivadosde los mismos (Ley 1712 de 2014, art 6).

Disponibilidad: Propiedad que la información sea accesible y utilizable porsolicitud 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/IEC27000).

Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos(2.36ISO 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 protegerla misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derechoque tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizary que generan en las entidades destinatarias del Manual de GEL la correlativa obligación

Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidadpara 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).

RECURSOS

- **Humano**: Personero y secretaria, Líderes de los Proceso, Funcionario y/o contratista encargado de las TICS
- **Físico:** PC y equipos de comunicación

RESPONSABLES

- Personero y Secretaria
- Líderes de los Proceso
- Profesional Universitario encargado de las TICS

METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la Personería Distrital de Cartagena de Indias, se toma referencia la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos porel Manual de implementación versión 3.02 del Ministerio de Tecnologías de la Información y las Comunicaciones.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar

Fuente: Manual Modelo de seguridad y Privacidad de la Información - MinTIc

CRONOGRAMA

No	ACTIVIDAD	RESPONSABLE	FECHA IMPLEMENTACIÓN	VALORACIÓN
1	Realizar Diagnostico	Área de Sistemas	Febrero 2024	10%
2	Elaborar el alcance del plan de seguridad y privacidad de la información	Área de Sistemas	Febrero 2024	10%
3	Realizar inventario de los activos de información con los lideres de proceso	Área de Sistemas	Febrero 2024	10%
4	Realizar la valoración de los activos de información con los lideres de proceso	Área de Sistemas	Febrero 2024	10%
5	Realizar el plande tratamiento de riesgos de seguridad y privacidad de la información	Área de Sistemas	Febrero 2024	20%
6	Socializar el plan de tratamiento de riesgos de seguridad y privacidad de la información	Área de Sistemas	Marzo 2024	10%
7	Realizar seguimiento al plan de seguridad y privacidad de la información.	Área de Sistemas	Mayo, Agosto, noviembre 2024	30%