Empresa Distrital de Desarrollo y Renovación Urbano Sostenible de

Santa Marta

PLAN DE SEGUIRDAD DE LA INFORMACION

Versión 1.0

ENERO del 2025

Contenido

1. OBJETIVO

Gestionar el plan de Seguridad de la Información para la Empresa distrital de desarrollo y renovación urbano sostenible –EDUS y seguridad privada, definiendo la estrategia y acciones a seguir para desarrollar, mantener y brindar mejor protección de la información.

2. ALCANCE DEL PLAN

El presente plan tiene como alcance llegar a alcanzar nivel de seguridad de la información para el desarrollo óptimo de la empresa

- Diagnóstico de situación actual de Seguridad de la Información
- Sensibilización en Seguridad de la Información
- Recuperación ante desastres
- Migración IPV4 IPV6

El presente plan se genera para lograr mantener estándares en seguridad y enmarca las principales acciones que se deben llevar a cabo para el desarrollo de la política de seguridad de la información y que se alinee al cumplimiento normativo de gobierno digital.

3. DIAGNÓSTICO DE SITUACIÓN EN SEGURIDAD

Debido a la dinámica que se presenta en la actualidad y la creciente actividad de las amenazas que pueden afectar a las TIC, es necesario mantener actualizado los niveles de seguridad con el fin determinar con precisión las acciones para el tratamiento de nuevos riesgos en materia de seguridad de la información. Las acciones necesarias desarrollar durante el periodo en mención incluyen:

4. ANÁLISIS DE VULNERABILIDADES

Durante el periodo y mediante el uso de herramientas de software libre se realizarán pruebas de detección de vulnerabilidades a los servidores y aplicaciones web definidas. En los casos en que la criticidad de la plataforma sea calificada como alta se intentará la explotación de la vulnerabilidad para proponer tareas concretas de remediación.

5. ASEGURAMIENTO DE PLATAFORMAS

Con el acompañamiento del ingeniero encargado del área se verificarán las plataformas se iniciará un programa anual de aseguramiento de servidores usando los resultados de las pruebas de detección de vulnerabilidades y el uso de plantillas de aseguramiento de servidores y plataformas como tomando como base los documentos de CIS (Center for Information Security).

6. SENSIBILIZACIÓN EN SEGURIDAD

La principal herramienta en materia de protección y gestión de la seguridad de la información es el usuario, una cadena es tan fuerte como el más débil de sus eslabones, es por esta razón que durante el periodo en mención se debe reforzar al usuario la necesidad de identificar oportunamente los riesgos de seguridad, aplicar las políticas de seguridad de la información y adoptar las medidas de seguridad de la información necesarias para reducir las posibilidades de pérdida de confidencialidad, integridad y disponibilidad de la información de la Superintendencia de Vigilancia y Seguridad de la Información.

7. RECUPERACIÓN ANTE DESASTRES

Para fortalecer las capacidades de respuesta antes contingencias de orden mayor y preparar a la empresa distrital de desarrollo renovación urbano sostenible -edus y Seguridad Privada para la certificación de su sistema de gestión de seguridad de la información, durante el periodo en mención se realizarán las siguientes acciones:

8. ACTUALIZACIÓN DE PANORAMA DE RIESGOS

Como ya se había mencionado, por lo menos semestralmente es obligación normativa realizar una revisión y actualización de los mapas de riesgos institucionales

9. MIGRACIÓN IPV4 IPV6

Dada el cambio inminente del protocolo IPV4 a su nueva versión IPV6, debido a obsolescencia y brechas de seguridad, la Superintendencia de Vigilancia y Seguridad Privada debe adelantar las acciones necesarias para planificar el cambio en la configuración de los dispositivos en el año 2019. Esta primera etapa del proceso de migración implicará:

10. INVENTARIO DE INFRAESTRUCTURA DE COMUNICACIONES

Se debe documentar el conjunto de dispositivos y plataformas tecnológicas, incluidos sistemas de información y aplicaciones que estén haciendo uso las funcionalidades del protocolo IPV4 para poder determinar el alcance y requerimientos del plan de migración a IPV6 en el año 2019

11. CIBERSEGURIDAD Y CIBERDEFENSA

Implementación de la estrategia de gestión de riesgo, ciberseguridad y ciberdefensa definida en el documento CONPES 3854 de ciberseguridad.

12. BACUKPS:

Este espacio se almacenará la información de la EDUS en discos duros físicos con el fin de salvaguardar la información de la EDUS en caso de daños robo cibernético desastre y demás

13. DIVULGACIÓN DE POLÍTICAS DE SEGURIDAD

Socializar a todas las áreas las políticas de seguridad de la información diseñadas dentro del marco del PETI de la Superintendencia de Vigilancia y Seguridad Privada y realizar sesiones de trabajo para identificar mecanismos para mejorar la Seguridad de la Información.

14. BITÁCOTA DE ACTUALIZACIÓN

Versión	Fecha	Descripción
01	ENERO de 2023	Primera elaboración del documento para implementación.

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	**Jaime Guerrero Urieles**	**Carlos Marchena**	**Jorge Luis Sarmiento Peñeranda**
Cargo:	**Asesor Tic´s**	**Jefe de Control Interno**	**Gerente General**