SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

Objetivo

Gestionar el plan de Seguridad de la Información para la Superintendencia de Vigilancia y seguridad privada, definiendo la estrategia y acciones a seguir para desarrollar, mantener y mejorar el SGSI vigente que se encuentra aprobado mediante resolución No. 20171400016907 del 31/03/2017.

Alcance del Plan

El alcance del presente plan de gestión del SGSI está definido para el periodo comprendido entre los años 2018-2022 y cubre los aspectos necesarios para mantener y mejorar el SGSI de la Superintendencia de Vigilancia y Seguridad Privada de forma que, al finalizar el periodo, la SVSP esté preparada para lograr la certificación ISO27001:2013 de su SGSI. Para cumplir con el alcance mencionado se tendrán en cuenta las tareas que se describen a continuación:

1. Diagnóstico de situación actual de Seguridad de la Información
2. Sensibilización en Seguridad de la Información
3. Recuperación ante desastres
4. Preparación para certificación del SGSI y mantenimiento de la misma
5. Migración IPV4 IPV6

El presente plan se genera para lograr mantener el SGSI 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.

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 el estado del SGSI con el fin determinar con precisión las acciones para el tratamiento de nuevos riesgos en materia de seguridad de la información. Las acciones necesarias a desarrollar durante el periodo en mención incluyen:

Nivel de riesgo en seguridad de la información en la SVSP

Realizar sesiones de trabajo con todos los procesos y dependencias para actualizar el proceso de gestión de riesgos de Seguridad de la Información, el particular en aquellos aspectos relacionados con los riesgos de seguridad de la información asociados a la disponibilidad, integridad y confidencialidad de la información y la plataforma tecnológica que la soportan.

Las sesiones de trabajo se programarán con el acompañamiento del dueño del proceso de cada una de las áreas de la SVSP.

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 como críticas para la SVSP.

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.

Aseguramiento de plataformas

Con el acompañamiento de los administradores de plataforma 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.

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

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.

Capacitación

Se ejecutará una charla de preparación para incidentes de Seguridad de la información, con el fin de mejorar las competencias de los funcionarios de la Superintendencia de Vigilancia y Seguridad Privada.

Sensibilización funcionarios

Mediante charlas en sitio y elementos didácticos se buscará mejorar el nivel de conciencia en seguridad de la información en los siguientes aspectos:

- Política general de la seguridad de la información
- Procedimientos de seguridad de la información
- Clasificación de la información
- Gestión de Riesgos de seguridad de la información

Recuperación ante desastres

Para fortalecer las capacidades de respuesta antes contingencias de orden mayor y preparar a la Superintendencia de Vigilancia 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:

Actualización de DRP: Verificar la documentación de procedimientos de recuperación de plataformas informáticos y mecanismos de respuesta ante incidentes tecnológicos que impidan a prestación continua de servicios de las plataformas críticas.

Probar el DRP: Una vez actualizado el plan de recuperación ante desastres se programarán y realizarán dos pruebas en las modalidades de:

1. Inspección y pruebas de escritorio
2. Verificación en sitio paso a paso del plan
3. De acuerdo con la disponibilidad de recursos se planificará una prueba de operación real en contingencia de algunos servicios críticos.

Preparación para certificación del SGSI

El objetivo principal del plan de seguridad de la información para en el periodo mencionado es preparar a la Superintendencia de Vigilancia y Seguridad Privada para optar por la certificación de su SGSI en la versión ISO 27001:2013. Este objetivo principal requiere:

Actualización documental

Aunque la documentación del SGSI ha estado en permanente actualización y revisión, es necesario mejorar aspectos como estándares, procedimientos formatos, evidencias, nuevos procedimientos y divulgación de procedimientos del SGSI.

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

Inventario de información clasificada y reservada

Para dar cumplimiento a las obligaciones del decreto 103 de 2015, que reglamenta parcialmente la ley 1712 de 2014 sobre transparencia y acceso a la información pública, es necesario realizar un acompañamiento a todas las áreas de la Superintendencia de Vigilancia y Seguridad Privada para que construyan, documenten y mantengan actualizado el inventario de información clasificada y reservada de todos los procesos misionales y de apoyo.

Modelo de Referencia de Arquitectura Empresarial (MRAE)

La estrategia de gobierno en línea requiere de la adopción de diversos lineamientos en materia de seguridad de la información que deben ser preparados por el SGSI a fin de cumplir las metas del Decreto 1078 de 2015.

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.

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.

Autoevaluación del SGSI

Con miras a la certificación ISO27001:2013 y a realización de la primera auditoria interna al SGSI, durante el segundo semestre de 2021, se realizará un ejercicio de autoevaluación del estado de la seguridad de la información para preparar a los colaboradores y dueños de los procesos de la Superintendencia de Vigilancia y Seguridad Privada para recibir formalmente la auditoria interna por parte de un tercero especializado.

Auditoria interna SGSI

De acuerdo con la programación se ha planteado una auditoría interna, en el tercer trimestre de 2021, se procederá con la contratación de este servicio por parte de un tercero especializado.

Migración IPV4 a 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 2021. Esta primera etapa del proceso de migración implicará:

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 2021.

Plan de Migración de IPV a IPV6

Con la información de diagnóstico de situación en materia de IPV4, se preparará una estrategia y plan de acción para realizar ajustes y cambios en la

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

infraestructura actual de comunicaciones y ejecutar las adecuaciones en el año 2021.

Relacionamiento Interinstitucional

Un aspecto fundamental en materia de seguridad de la información es establecer vínculos permanentes con grupos de interés y organizaciones dedicadas a la seguridad de la información, se fortalecerán los vínculos con el Comando Conjunto de Operaciones Cibernéticas y las entidades del sector.

Otras acciones concretas incluyen:

Ciberseguridad y Ciberdefensa

Implementación de la estrategia de gestión de riesgo, ciberseguridad y ciberdefensa.

Divulgación de políticas de seguridad

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

Fortalecimiento de seguridad de servicios y aplicaciones en la nube

Aunque la SuperVigilancia cuenta con seguridad perimetral, Firewall y otros mecanismos de seguridad, es necesario implementar un WAF (Web Application Firewall) para filtrar el contenido de aplicaciones web especificas

Control de Cambios

Versión	Control de Cambios	Fecha
1	Creación del documento Plan de Gestión de Privacidad y Seguridad de la Información	Mayo de 2018
2	Revisión y actualización del documento Plan de Gestión de Privacidad y Seguridad de la información. Actualización de logos. Se incluye Fortalecimiento de seguridad de servicios y aplicaciones en la nube.	Enero de 2021

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co