Oficina de Tecnología

Plan de Comunicación, Sensibilización y Capacitación en Seguridad de Información

Versión 1.0
Mayo 12 de 2020

Tabla de contenido

Introducción

Como parte del Sistema de Gestión de Seguridad de Información -SGSI en la USPEC, se han establecido diversos lineamientos a través de políticas, manuales, procedimientos y guías que describen el cómo implementar controles para asegurar la disponibilidad, integridad y confidencialidad de la información institucional. Esta documentación se ha elaborado de acuerdo a lo establecido en el Modelo de Seguridad y Privacidad de Información - MSPI establecido por MINTIC y la Norma ISO 27001:2013.

El incumplimiento a estos lineamientos se puede derivar en incidentes de seguridad de información que afecten los activos de información de la Entidad o incluso pueden llegar a generar sanciones de acuerdo a la normatividad legal vigente. Sin embargo, para mitigar este tipo de situaciones es importante que el personal vinculado a la USPEC conozca de manera oportuna todas las directrices del SGSI.

Por lo anterior surge la necesidad de establecer un plan que establezca tanto estrategias como actividades dirigidas a los diferentes roles de la Entidad que hacen parte del SGSI y que permitan comunicar, sensibilizar y crear conciencia frente a la adopción de medidas necesarias para proteger la información institucional y de esta manera apoyar en la disminución de incidentes de seguridad de información.

Glosario

- **Administradores de Sistema.** Administradores funcionales de aplicativos, sistemas de información o servicios provistos por otras Entidades.

- **Confidencialidad.** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Comparendo.** Es una medida correctiva en la cual se busca de manera focalizada oriental al personal que comente un incidente de seguridad de información, orientarlo frente a las buenas prácticas y lineamientos establecidos por la Entidad para proteger la información institucional.
- **Disponibilidad.** propiedad de la información de estar accesible y utilizable cuando lo requiera un usuario autorizado.
- **Integridad.** propiedad de la información relativa a su exactitud y completitud.

- **Sensibilización.** Proceso que tiene como objetivo impactar sobre el comportamiento de un grupo de usuarios o reforzar buenas prácticas sobre un tema específico.
- **SGSI.** Sistema de Gestión de Seguridad de Información. Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Usuarios**. Personal hacia el cual está dirigido el presente plan, entre los cuales se encuentran directivos y jefes de oficina, funcionarios y contratistas, administradores de sistemas, Administradores de infraestructura tecnológica y personal de soporte, partes interesadas.
- **Partes interesadas**. Asociado a proveedores, entidades del sector justicia u otras entidades interesadas

1. Objetivos

1.1 Objetivo General

Establecer estrategias para sensibilizar, comunicar y capacitar al personal de la USPEC con el fin de reforzar lineamientos y buenas prácticas establecidas a través del Sistema de Gestión de Seguridad de Información que permitan proteger la información institucional.

1.2 Objetivos Específicos

- Identificar las necesidades de información según el rol desempeñado por los usuarios de la Entidad, con el fin de focalizar la estrategia de sensibilización, comunicación y capacitación establecidas para la vigencia 2020.

- Ejecutar las estrategias establecidas a través del presente plan con el fin de fortalecer los controles de seguridad de información establecidos por los diferentes procesos en el marco del SGSI.

- Realizar seguimiento trimestral al plan de comunicación, sensibilización y capacitación en seguridad de información con el fin de identificar las actividades ejecutadas.

2. Alcance

El presente plan aplica para todo el personal vinculado a la Unidad de Servicios Penitenciarios y Carcelarios, es decir funcionarios y contratistas, así como para las partes interesadas.

3. Usuarios y Necesidades

Para efectos del presente plan se establecieron 5 grupos de usuarios en la Entidad y por cada uno de ellos objetivos especiales de conocimiento, lo cual permitirá enfocar el esfuerzo de las actividades de comunicación, sensibilización y capacitación. A continuación se detallan estos grupos:

USUARIOS	OBJETIVOS DE CONOCIMIENTO
Directivos y Jefes de Oficina	Deben conocer las leyes y directrices que forman la base del Sistema de Gestión de Seguridad de Información en la Entidad, también deben comprender el liderazgo que su rol tiene y que su ejemplo permitirá orientar las actuaciones del personal a su cargo.
Funcionarios y Contratistas	Deben conocer todas los lineamientos de seguridad de información y las reglas de comportamiento adecuados para proteger tanto los sistemas como la información institucional que tienen a su cargo.
Administradores de Sistemas	Deben conocer todas las políticas de seguridad y especialmente aquellos controles de seguridad relacionados con sistemas de información.
Administradores de infraestructura tecnológica y personal de soporte	Deben conocer a profundidad leyes, políticas, procedimientos asociados al SGSI, para soportar las operaciones críticas de la Entidad de manera apropiada, adicionalmente deberán estar en capacidad de orientar y hacer cumplir estos lineamientos en toda la Entidad.
Partes Interesadas	Deben conocer las directrices que la Entidad establece para acceder a su información, así como aquellas requeridas para proteger la información que en el cumplimiento de sus funciones requieran conocer.

Tabla 1. Grupos y necesidades de comunicación y sensibilización

4. Estrategias de comunicación, sensibilización y capacitación

4.1 Socialización de documentación.

Cada vez que una dependencia cree o actualice un documento que haga parte del Sistema de Gestión de Seguridad de Información, deberá realizar la gestión requerida para dar a conocer al personal de la Entidad, los lineamientos contenidos en el mismo. Se deberán tener en cuenta las siguientes actividades:

A. Publicar el documento en la página web de la Entidad y en la Intranet Institucional

B. Diseñar piezas gráficas alusivas al documento para promocionar su difusión a través de los canales de comunicación interna establecidos por la Entidad, tales como correo electrónico, intranet, pantallas institucionales, periódico interno, reuniones internas, redes sociales, etc.

C. Adicionalmente si el personal responsable del SGSI lo determina se realizarán reuniones virtuales o presenciales con el fin de dar mayor claridad sobre el documento.

Periodicidad: Depende de la publicación de documentación del SGSI.

4.2 Participación Ciudadana.

Con el fin de promover la participación ciudadana por parte de los grupos de interés y la ciudadanía en general, la USPEC ha dispuesto de una sección a través de su portal web con el fin de publicar entre otros, proyectos relacionados con seguridad de información. A través de estos ejercicios se busca dar a conocer nuevos lineamientos y escuchar la opinión de los ciudadanos, contestar oportunamente sus inquietudes, tener en cuenta sus propuestas y de ser posible llevarlas a la implementación. A través del correo seguridaddigital@uspec.gov.co se lleva a cabo la gestión de los temas asociados a participación ciudadana y relacionados con el SGSI. Para aplicar este tipo e estrategias se tendrán en cuenta las siguientes actividades:

A. Definición del documento en versión borrador con la propuesta de los lineamientos de seguridad de información

B. Publicación del documento en la portal web en la sección dispuesta por la Entidad.

C. Promoción del documento a través del portal web, redes sociales institucionales y correo electrónico.

D. Recepción de comentarios, inquietudes y/o propuestas al documento por parte de los interesados.

E. Respuestas a los ciudadanos y grupos de interés que participaron.

F. Ajustes a que haya lugar según la información recibida por los grupos de interés y la ciudadanía en general.

G. Aprobación del documento según lineamientos de la Entidad

H. Publicación del documento

I. Informe que contenga el resumen de la gestión realizada a través del ejercicio de participación ciudadana.

Periodicidad: Depende de la creación del borrador del documento que se requiera publicar para participación ciudadana.

4.3 Inducción y reinducción en seguridad de información.

A través de los canales de comunicación establecidos por el Grupo de Talento Humano de la Entidad, se publicará un resumen de los lineamientos del SGSI, adicionalmente se hará énfasis en los objetivos de conocimiento por cada grupo de usuarios (Ver sección 4. Usuarios y Necesidades) Para desarrollar esta estrategia se tendrán en cuenta las siguientes actividades:

A. La Oficina de Tecnología desarrollará el contenido de los resúmenes de inducción y reinducción en seguridad de información.

B. Prensa apoyará con el diseño de las piezas gráficas requeridas.

C. Grupo de Talento Humano apoyará con la distribución de la información al personal de la Entidad y el seguimiento al personal que ha participado en estas actividades.

D. Posteriormente Oficina de Tecnología tomará los resultados de este proceso de inducción y reinducción con el fin de determinar si se requiere reforzar algún tema con cada usuario.

Nota: Cada vez que nuevo personal se vincule a la Entidad, se remitirá a través de correo electrónico un mensaje de bienvenida para darle a conocer los lineamientos de seguridad de información, así como los demás aspectos a tener en cuenta para un adecuado uso de los servicios tecnológicos con que cuenta la USPEC.

Periodicidad: En el caso de los nuevos usuarios la inducción se debe realizará máximo dentro de la primera semana posterior a su ingreso, en el caso de los usuarios antiguos la reinducción se llevará a cabo de forma semestral.

4.4 Comparendo pedagógico en seguridad de información.

Este tipo de sanciones se aplicarán para aquellos usuarios que una vez conociendo las políticas de seguridad de información, generen en el desarrollo de sus labores incidentes de seguridad que puedan llegar a afectar la información institucional. A través de herramientas especializadas de seguridad de información que permiten monitorear la plataforma tecnológica, se realizará monitoreo periódico con el fin de determinar eventos anómalos por parte de los usuarios, adicionalmente se tendrán en cuenta los incidentes registrados a través de la herramienta HELPTIC, asociados con la afectación de confidencialidad, integridad o disponibilidad de información institucional.

Una vez que se identifique el personal que incurrió en estos incidentes, este deberá participar en cursos virtuales con el fin de reforzar los lineamientos del SGSI. A continuación se resumen las actividades que permiten dar cumplimiento a esta estrategia:

A. Identificar el personal vinculado con incidentes de seguridad de información

B. Reportar al usuario a través de correo, la información respecto al incidente presentado, notificando adicionalmente a su jefe inmediato o supervisor de contrato. Así mismo se compartirá el enlace del curso virtual al cual debe asistir el usuario.

C. La Oficina de Tecnología realizará seguimiento a los cursos tomados por los usuarios con el fin de determinar, si las respuestas dadas en el proceso de evaluación fueron satisfactorias. De lo contrario se procederá a generar una acción personalizada.

Nota: El usuario objeto del comparendo debe asistir a las sesiones que se programen por la OTEC. Estas serán coordinadas con la Subdirección Administrativa o el Supervisor del Contrato.

Periodicidad: Depende de los usuarios que incurran en incidentes de seguridad de información.

4.5 Noticias de Seguridad de Información

Teniendo en cuenta que continuamente se están presentando nuevos ataques informáticos , o incidentes de seguridad de información a nivel mundial y así mismo se toman nuevas medidas para fortalecer controles para su mitigación, la Oficina de Tecnología publicará este tipo de noticias de seguridad de información y controles internos que permitan sensibilizar al personal de la USPEC frente a las necesidades de proteger la información institucional así mismo se generará un valor agregado que le permita a los usuarios cuidar también su información personal. A continuación se relacionan la actividades a desarrollar:

A. Diseñar piezas con contenido de noticias en seguridad de información

B. Publicarla a través de los canales de comunicación internos establecidos por la Entidad.

C. De ser requerido contestar inquietudes de los usuarios.

Periodicidad: Se debe realizar por lo menos una publicación cada mes.

4.6 Capacitación en seguridad de información.

Por parte entidades como MINTIC o el SENA entre otros, se realizan diversas convocatorias para cursos en temáticas relacionadas con seguridad de información , en este sentido es importante publicitar entre el personal de la Entidad este tipo de actividades, con el fin de propiciar espacios para enriquecer los conocimientos.

A. El Grupo de Talento Humano y la Oficina de Tecnología de la Entidad canalizarán las convocatorias de diferentes entidades relacionadas con seguridad de información.

B. A través del correo thumano@uspec.gov.co se remitirá a los diferentes grupos de interés la información para participar en los cursos.

C. Una vez el funcionario culmine el curso deberá remitir al Grupo de Administración de Personal copia del certificado con el fin de archivarlo en su hoja de vida. Nota: Se deberán tener en cuenta los parámetros de dicho grupo para la recepción de documentos.

Periodicidad: Depende de las capacitaciones programadas por otras Entidades.

4.7 Encuestas de seguridad de información.

A través de las encuestas se busca recopilar información para medir el grado de conocimiento del personal de la Entidad o de las partes interesadas frente al SGSI. Estas se aplicarán teniendo en cuenta los grupos de usuarios y las necesidades de conocimiento con el fin de validar la efectividad de las sensibilizaciones realizadas. A continuación se enuncian las actividades a tener en cuenta:

A. La Oficina de Tecnología será la encargada de diseñar las encuestas de seguridad de información y remitirlas a través del correo a los diferentes grupos de usuarios.

B. Posteriormente se realizará seguimiento a los usuarios que atendieron la encuesta con el fin evaluar los resultados y determinar las necesidades de reforzar conocimientos entre el personal invitado.

Nota: Todo el material de sensibilización se publicará en la intranet institucional con el fin de acceder a ella en el momento requerido.

Periodicidad: Como mínimo se aplicará una encuesta semestral.

4.8 Usuario del SGSI

Teniendo en cuenta la participación de los usuarios de la USPEC en las actividades programadas por el SGSI se llevará a cabo un reconocimiento a través de los canales de comunicación internos exaltando las mejores gestiones, otorgando un certificado de reconocimiento por la participación.

Periodicidad: Se llevará a cabo este reconocimiento de manera bimestral.

4.9 Promoción de Actividades Externas

Entidades como MINTIC, MinJusticia, DNP entre otras realizan periódicamente actividades que permiten fortalecer las capacidades en seguridad digital tales como:

- Jornadas de socialización y promoción en tópicos del MSPI.
- Ejercicios de simulación para desarrollar habilidades y destrezas en materia de seguridad digital.
- Actividades para el intercambio de información para fomentar la investigación, la innovación y el desarrollo en temas relacionados con seguridad de información.
- Convocatorias para el fortalecimiento de capacidades en seguridad (posgrados, maestrías, etc)

Con el fin de darlas a conocer a todo el personal de la Entidad, la OTEC compartirá este tipo de actividades a través de los canales de comunicación internos establecidos por la Entidad. Será responsabilidad de los usuarios informar oportunamente a través del correo seguridaddigital@uspec.gov.co los eventos en los cuales han participado con el propósito de recopilar la respectiva evidencia y la posibilidad de compartir el conocimiento adquirido con el personal de la USPEC.

Periodicidad: Depende de las actividades programadas por otras Entidades.

5. Efectividad del plan

Fase 1. La efectividad del presente plan es proporcional al resultado de la meta tendiente a fortalecer la gestión pro activa de correos maliciosos y el reporte de incidentes de seguridad en los funcionarios y contratistas de la Unidad. La meta tiene un horizonte de aplicación de seis meses, contados a partir de la publicación del presente documento.

Fase 2. En concordancia con los resultados obtenidos en la Fase 1, se analizará la variación estadística que resulte de la gestión del reporte de incidentes reportados en comparación con la ejecución de las actividades de sensibilización, socialización y capacitación en seguridad de información; el resultado esperado debe dar cuenta en la disminución de los incidentes de seguridad.

6. Sanciones.

El incumplimiento de las actividades establecida en el presente plan generarán sanciones disciplinarias acorde a los lineamientos establecidos por la Entidad.

7. Seguimiento

El seguimiento al plan de comunicación, sensibilización y capacitación en seguridad de información se realizará de manera trimestral a través de un informe que incluirá las actividades ejecutadas por cada una de las estrategias definidas en el presente documento y se incluirá dentro del informe de revisión por la dirección que se elabora por la OTEC de manera semestral.

Aprobó:
Luis Ernesto Tapia
Subdirector Administrativo

Revisó:
Oscar Javier Suárez Ramos
Jefe Oficina de Tecnología

Diana Paola Cárdenas Huertas
Profesional Universitario

Elaboró:
Mayra Agudelo
Profesional Especializado