TABLA DE CONTENIDO

Introducción

La concienciación en seguridad de la información es básica para el éxito de un Sistema de Gestión de Seguridad de la Información SGSI. Por ello es necesario involucrar a los servidores públicos, judicantes, pasantes y practicantes del INPEC en la búsqueda de la creación de una Cultura de Seguridad de la información que servirá para establecer bases de protección, tanto de la información confidencial del Instituto como la de los clientes y proveedores, supervisando que se cumplen las buenas prácticas en seguridad establecidas; realizando acciones de sensibilización y concienciación en seguridad de manera continua.

El presente plan aplica los lineamientos de la Guía No. 14 Plan de Capacitación, sensibilización y comunicación de seguridad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones. MINTIC

Objetivo del Plan

Orientar y establecer buenas prácticas de seguridad, que permita tomar conciencia sobre la importancia de la Seguridad de la Información en los servidores públicos, judicantes, pasantes y practicantes del INPEC.

Objetivos Específicos

- Definir la estrategia de divulgación y sensibilización en seguridad de la información.
- Fomentar el desarrollo de buenas prácticas de seguridad de la información en los funcionarios, teniendo presente las políticas, normativas y procedimientos de seguridad establecidas en el INPEC.
- Evaluar la eficacia de las actividades de concienciación en seguridad de la información a los servidores públicos, judicantes, pasantes y practicantes de la Entidad para determinar el grado de formación que han alcanzado.

Glosario

- **Amenaza**: de acuerdo a la norma ISO/IEC 27000, es la causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Concienciación**: educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad de la información.
- **Ciberseguridad**: conjunto de técnicas o procedimientos que velan por la seguridad de los usuarios que comparten información entre sistemas de información.
- **Confidencialidad**: de acuerdo a la norma ISO/IEC 27000 es la propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Criptografía**: arte y la técnica de crear mensajes codificados con procedimientos o claves secretas con el objeto de que no pueda ser descifrado salvo por la persona a quien está dirigido o que detenta la clave.
- **Integridad**: de acuerdo a la norma ISO/IEC 27000 es la propiedad de la información relativa a su exactitud y completitud.
- **Disponibilidad**: de acuerdo a la norma ISO/IEC 27000 es la propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **ERON**: sigla usada para denominar a los Establecimientos de Reclusión del Orden Nacional.
- **Funcionario**: persona natural vinculada a la Planta de Personal del Instituto para prestar sus servicios de acuerdo con unas funciones previamente asignadas, sea en labores administrativas o del Cuerpo de Custodia y Vigilancia.
- **Malware**: abreviatura de “Malicious software”, término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.
- **Pasante**: estudiante que está cursando como mínimo octavo semestre en cualquier programa académico ofrecido por una Institución de Educación Superior, reconocida oficialmente, y que realiza en el instituto la práctica profesional voluntaria o exigida por el pensum académico de la respectiva disciplina profesional.
- **Phishing**: método más utilizado por delincuentes informáticos para estafar y obtener información confidencial de forma fraudulenta.
- **Practicante**: es el estudiante que realiza una práctica profesional, con el fin de poner en práctica sus conocimientos y facultades.
- **Privilegio de usuario**: gestión de derechos y niveles de acceso a un sistema de información.
- **Responsabilidad**: de acuerdo a la Guía No 4 Roles y Responsabilidades MINTIC es la cualidad de la persona responsable. "para cubrir ese puesto buscan a una persona con responsabilidad".
- **Riesgo en la seguridad de la información**: de acuerdo a la Norma ISO/IEC 27005:2018, es el potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- **Rol**: de acuerdo a la Guía No 4 Roles y Responsabilidades MINTIC es el papel, función que alguien o algo desempeña.
- **Sensibilización**: proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- **Servidor público**: persona con una vinculación laboral con el Instituto Nacional Penitenciario y Carcelario, que ejerce funciones públicas que están al servicio del estado y de la comunidad.
- **SGSI**: Sistema de Gestión de Seguridad de la Información.
- **TI**: Tecnología de la Información.

- **Vector de ataque**: formas o medios que permiten el acceso de piratas informáticos a un sistema de información o red de datos para transmitir códigos maliciosos, con el propósito expreso de obtener algún beneficio a cambio.
- **Vulnerabilidad**: de acuerdo a la norma ISO/IEC 27000 es la debilidad de un activo o control que puede ser explotada por una o más amenazas.

Marco Legal

• Ver Normograma del Instituto Nacional Penitenciario y Carcelario

1. Alcance

El Plan de sensibilización y comunicación de seguridad de la información, tiene el alcance establecido en la PA-TI-PL01 Política de Seguridad de la Información versión oficial.

2. Recursos

- **Humanos:** funcionarios de la Oficina de Sistemas de Información, con apoyo de la Oficina Asesora de Comunicaciones y la Dirección Escuela de Formación.
- **Tecnológico:** se dispone del correo electrónico institucional, Intranet, equipos de cómputo.
- **Canales de comunicación**: las campañas serás permanentes y se utilizarán los medios de comunicación internos del Instituto, los cuales serán entre otros:
    - Correo electrónico Institucional
    - Intranet
    - Boletín digital interno.
    - Vídeo Conferencia
    - Charlas

Los anteriores medios se determinaron teniendo en cuenta que:

- Facilita la comunicación a distancia.
- Fomenta la participación y reacción de quien los lee
- Medios de comunicación o canales disponibles en la infraestructura de comunicaciones del INPEC, lo cual no implica costos adicionales.
- Difusión masiva de la comunicación.
- PA-DO-PL01 Política de eficiencia Administrativa y Cero Papel, versión oficial.

3. Descripción general del plan de sensibilización y comunicación.

Un plan efectivo de sensibilización y comunicación en seguridad de la información debe exponer de manera apropiada las reglas de comportamiento adecuadas para el uso de la información y los sistemas y la información en relación a su confidencialidad, integridad y disponibilidad, reglas de comportamiento plasmados en la PA-TI-PL01 Política de Seguridad de la Información versión oficial y la PA-TI-G02 Guía de Normas y Buenas Prácticas de la Seguridad de la Información versión oficial, como a la norma ISO/IEC 27001:2013 en su capítulo **7.3 Toma de conciencia** que la Entidad requiere que sean cumplidos por parte de los usuarios finales.

Cualquier incumplimiento la PA-TI-PL01 Política de Seguridad de la Información versión oficial y la PA-TI-G02 Guía de Normas y Buenas Prácticas de la Seguridad de la Información versión oficial, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Entidad.

Teniendo en cuenta lo anterior, el plan de sensibilización y comunicación incluye actividades enfocadas a identificar, mejorar, fortalecer habilidades y destrezas en las mejores prácticas de Seguridad de la Información para aplicar en procesos y actividades diarias en el Instituto.

Para lograr resultados de impacto en los servidores públicos, judicantes, pasantes y practicantes del INPEC el plan se desarrollara por fases:

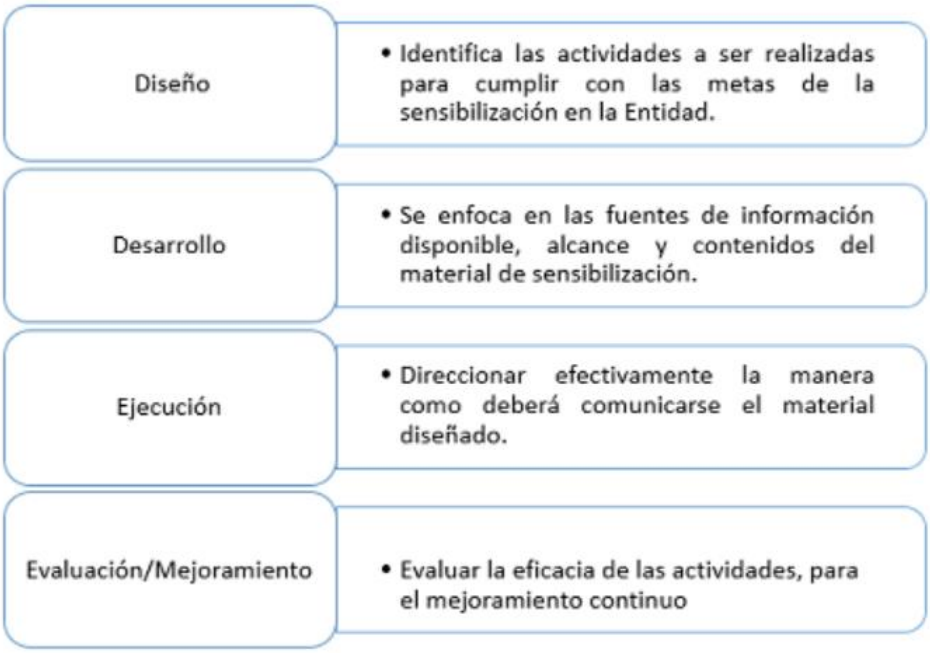

Figura 1. Fases plan de sensibilización, y comunicación de Seguridad de la Información.

3.1. Fase de diseño

El plan se diseñada teniendo en cuenta uno de los requisitos de la PA-TI-PL01 Política de Seguridad de la Información versión oficial: "Crear una cultura de Seguridad de la Información que permita tomar conciencia sobre la importancia de la seguridad de la información en los funcionarios, contratistas, practicantes y judicantes de la entidad". El modelo a desarrollar para la sensibilización será centralizado desde la Sede Central y luego distribuido de igual manera a todas las Direcciones Regionales, Dirección Escuela de Formación y ERON para que sea aplicada de manera homogénea en cada una.

Los elementos a utilizar para que el plan de sensibilización sea factible, serán orientados diseñados y aprobados por:

- El responsable de seguridad de la información en la Entidad.
- Oficina de Sistemas de Información
- Oficina Asesora de Comunicaciones

Y a su vez las alternativas serán:

- Fondos de pantalla
- Vídeos
- Boletines digitales
- Personaje y eslogan

- Folletos digitales
- Sopas de letras digitales
- Afiches digitales
- Entre otros.

3.2. Fase de desarrollo

El desarrollo/adquisición/recopilación de los materiales se basarán en roles y cada rol tendrá diferentes objetivos de sensibilización tales como:

La sensibilización es una responsabilidad compartida ya que todos formamos parte de ella. Para esta fase los responsables de su desarrollo serán orientados y aprobados por:

- El responsable de seguridad de la información en la Entidad.
- Oficina de Sistemas de Información.
- Dirección Escuela de Formación
- Subdirección de Talento Humano

Dependiendo del tema a sensibilizar.

Entre los temas más importantes de sensibilización se encuentran los siguientes, aunque de acuerdo a las necesidades y a los cambios constantes de vulnerabilidades, amenazas y vectores de ataques pueden variar:

- Gestión de contraseñas seguras.
- Malware y sus diferentes tipos.
- Buen uso de correo electrónico e identificación de correos maliciosos.
- Uso apropiado de Internet
- Escritorio limpio y pantalla despejada
- Ingeniería social
- ¿Cómo y porque es importante encriptar la información del Instituto?
- Roles y responsabilidades de seguridad de la información en la entidad
- Gestión de Incidentes (Como reportar, que se puede y debe reportar)
- Temas de control de acceso a los sistemas (privilegios de usuarios, separación de roles)
- Políticas organizacionales relacionadas con seguridad de la información
- Inducción al personal durante la vinculación al Instituto sobre deberes y responsabilidades en seguridad de la información.
- ¿Cómo protegerse de los ataques de phishing?
- Temas de ciberseguridad

Se puede disponer de material diverso para sensibilización desde varias fuentes como:

- Organizaciones profesionales y proveedores de seguridad de la información.
- Material de Internet.
- Convenios interinstitucionales
- Cursos de entrenamiento inhouse (desarrollados internamente), con el apoyo de la Dirección Escuela de Formación.
- Seminarios, talleres virtuales o presenciales de inducción y reinducción para el personal administrativo y Cuerpo de Custodia y Vigilancia del INPEC en relación a la Seguridad de la Información, con el apoyo de la Subdirección de Talento Humano y Dirección Escuela de Formación.

- Metodologías como la NIST 800-16, que define varios roles de TI y permiten dar un enfoque de enseñanza a cada rol.

Esta información o material de sensibilización puede ser presentado por temas separados o en sesiones únicas.

3.3. Fase de ejecución

Existen múltiples técnicas para la difusión de mensajes de sensibilización, la selección de cada método debe ser acorde a los recursos y tecnología a disposición dentro de los cuales pueden ser:

- Videos institucionales a través de pantallas.
- Correo Institucional
- Eventos relacionados con seguridad, capacitaciones.
- Carteles con mensajes sobre que debe y que no debe hacerse en materia de seguridad de la información.
- Boletines vía email.
- Protectores de pantalla con mensajes de sensibilización.
- Infografía
- Píldoras de seguridad

Los temas de sensibilización son breves y concretos, simples, lo que facilita en gran medida la recepción del mensaje que se está transmitiendo.

3.4. Fase de evaluación y mejora continua

El plan de sensibilización y comunicación no podrá mejorarse, sin antes saber cómo se está desempeñando al interior de la Institución, para ello, se utilizarán métricas que identifiquen la efectividad de la sensibilización de acuerdo a las necesidades y a los cambios constantes de vulnerabilidades, amenazas y vectores de ataques en el tiempo, por lo cual se puede elegir entre los siguientes tipos de métricas:

- Porcentaje de usuarios sensibilizados (a través de encuestas o evaluaciones) apropiadamente, porcentaje de ataques de ingeniería social exitosos. Con el apoyo del Grupo de Proyección, Seguridad e Implementación Tecnológica y el Responsable de Seguridad de la Información.
- Porcentaje de antivirus instalado y actualizado, porcentaje de antivirus sin instalar y desactualizados, con el apoyo del Grupo de las Tecnologías de la Información y de las áreas de sistemas de las Direcciones Regionales y ERON.
- Porcentaje de acuerdos de confidencialidad firmados, porcentaje por firmar. Con el apoyo de la Subdirección de Talento Humano y jefes de dependencias.
- Entrevistas selectivas o entrevistas grupales con el fin de identificar buenas prácticas de seguridad de la información con el apoyo del Grupo Proyección, Seguridad e Implementación Tecnológica y el Responsable de seguridad de la Información.

Cuando los usuarios reciban las sesiones de sensibilización se llevarán registros de calidad y controles sobre la participación a través de los formatos PA-DO-G01-F07 Asistencia a evento versión oficial. o PA-DO-G01-F01 Acta versión oficial, fotografías y vídeos en caso de ser presencial con el propósito de que los servidores públicos, judicantes y practicantes asuman sus respectivos compromisos con la preservación de la seguridad de la información en la Entidad. Esta evidencia puede servir para justificar algún tipo de sanción a comportamientos inadecuados o incumplimiento a las políticas de seguridad.

Bibliografía

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia MINITC, Guía No. 14 - Guía Plan de Capacitación, Sensibilización Y Comunicación de Seguridad de la Información. Versión 1.0 fecha: 17/03/2016.

Anexos

- PA-DO-G01-F07 Asistencia a evento versión oficial.
- PA-DO-G01-F01 Acta versión oficial
- PA-TI-G02 Guía de Normas y Buenas Prácticas de la Seguridad de la Información versión oficial
- PA-DO-PL01 Política de eficiencia Administrativa y Cero Papel versión oficial.
- PA-TI-PL01.V2 Política de Seguridad de la Información versión oficial

Lista de Versiones			
Versión	**Fecha de Emisión**	**Motivo de la Modificación**	**Modificaciones**
1	02/Dic/2019	creación del documento	N/A

Elaboró	Revisó	Aprobó
Nombre: María Cristina Reyes Castillo	**Nombre:** Eduardo Iván Guzmán Guzmán	**Nombre:** Adriana Cetina Hernández
Cargo: Técnico Operativo	**Cargo:** Distinguido	**Cargo:** Jefe Oficina Sistemas de Información
Fecha: 20/Dic/2019	**Fecha:** 16/Ene/2020	**Fecha:** 16/Ene/2020
	Nombre: Juan Manuel Riaño Vargas	
	Cargo: Jefe Oficina Asesora de Planeación	
	Fecha: 16/Ene/2020	