FUNCIÓN PÚBLICA

Estrategia de sensibilización de Seguridad de la información 2022

Oficina Asesora de Planeación

VERSIÓN 01
FEBRERO 2022

Versión	Fecha de versión (aaaa-mm-dd)	Descripción del cambio
01	2022-02-20	Creación del documento para la estrategia de sensibilización de seguridad de la información en la entidad, vigencia 2022

Contenido

Introducción

El Departamento Administrativo de la Función Pública DAFP, desde el Modelo Integrado de Planeación y Gestión, tiene implementado el Modelo de seguridad y privacidad de la información definido por MINTIC que se alinea con norma ISO 27001:2013, la cual enfatiza la importancia que es para las entidades salvaguardar la información sobre los principios de confidencialidad, disponibilidad e integridad de la información**.** Así mismo, se recalca la importancia de implementación de medidas de seguridad en las entidades desde el marco de la Política de Gobierno Digital en su habilitador de seguridad y la Política de Seguridad Digital, emitidas por la Ley 1341 de 2009, artículo segundo, numeral 8 y la Resolución 500 de 2021, *"por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital" r*espectivamente. En este orden, el DAFP tiene actualmente implementadas políticas y controles de seguridad que le permitan de manera efectiva proteger la información que entra a través de la recogida de información de los ciudadanos y de diferentes fuentes de información, la cual se procesa y/o transforma para posteriormente ser entrega como un trámite o servicio a nuestras partes interesadas acorde a los objetivos misionales de la entidad.

Entre las medidas y/o controles de seguridad de la información necesarios a implementar en la entidad y de manera continua son las estrategias de sensibilización y capacitación a todo el personal de la entidad de punta a punta, teniendo en cuenta que la información clasificada como privada y semiprivada en la entidad y que es manejada por funcionarios, contratistas y colaboradores desde sus diferentes roles, funciones y/o responsabilidades debe ser protegida, por lo tanto, es necesario que se propicien los mecanismos pertinentes para generar la cultura de seguridad de la información a todo el personal de la entidad.

Acorde a lo anterior, en este documento se describe la estrategia de sensibilización de seguridad de la información orientada a funcionarios, contratistas y colaboradores de Función Pública.

1. Objetivo General

Sensibilizar a todos los colaboradores de la Entidad sobre la necesidad de crear el hábito de salvaguardar la información y así lograr una cultura institucional de seguridad y privacidad de la información

1.1 Objetivos específicos

- ✓ Establecer estrategias que permita al personal de la entidad apropiarse de los conceptos que fundamentan la seguridad y privacidad de la información para su contextualización con el entorno laboral de la entidad.
- ✓ Motivar al personal de la entidad a utilizar continuamente buenas prácticas de seguridad de la información desde sus responsabilidades laborales para cerrar brechas de seguridad.
- ✓ Generar en el personal de la entidad el sentido de pertenencia y de responsabilidad que tienen cada uno sobre la información que administra y trata de la entidad para evitar atraques de ingeniería social
- ✓ Brindar al personal el conocimiento de las políticas y procedimientos existentes en la entidad para ayudar a reducir los riesgos de seguridad de la información identificados en la entidad.

2. Alcance

La estrategia de sensibilización de seguridad y privacidad de la información está dirigía a funcionarios, contratistas y colaboradores del Departamento Administrativo de la Función Pública y abarca todos los procesos y dependencias.

3. Definición de la estrategia

La estrategia se sensibilización en seguridad de la información, se planea implementar a todas las áreas de la entidad a través de diferentes técnicas de comunicación verbal y no verbal en momentos individuales y colectivos. Las temáticas orientadas a la sensibilización del personal de la entidad, se presentarán a través de un lenguaje común y fácil de entender. En los momentos en donde se presentará algún tipo de sensibilización que tenga componentes técnicos se realizaran para grupos focalizados como personal de la OTIC y en algunos casos personal de apoyo funcional de los sistemas de información de la entidad de carácter misional y corporativo tenga conocimientos técnicos previos.

En relación al tiempo de sensibilización, está programada para desarrollarse durante la vigencia 2022, en jornadas mensuales de conferencias (comunicación verbal) y envío y publicación de piezas comunicativas de seguridad de la información (comunicación no verbal) a través de diferentes medios de comunicación masiva dispuesta por la entidad. (correo electrónico, TV y portal institucional y/o intranet). En este orden de ideas, se presenta a continuación en la siguiente tabla las temáticas planteadas en la sensibilización, el medio y forma de comunicación de la temática, las áreas que deben asistir y las áreas que deben apropiarse de la información verbal y no verbal publicada.

4. Contenido para sensibilizar

Mes	Temáticas para sensibilizar	Medio y forma de comunicación	Procesos/Áreas a sensibilizar
Marzo	Conceptos básicos y principios de seguridad., socialización de Políticas	Conferencia presencial /virtual (comunicación verbal)	Todas las áreas de los procesos
Abril	Temas2: Protección de datos personales- ley 1581,manual de protección de datos de la entidad (link)	Taller virtual (comunicación verbal)	Líderes funcionales de todas las áreas
Mayo	Mapa de Riesgos - Riesgos de Seguridad. Procedimiento de Gestión de incidentes	Conferencia presencial /virtual (comunicación verbal)	Líderes funcionales de todas las áreas
Junio	Vectores de ataques de seguridad de la información y ciberseguridad. Ingeniería Social	Conferencia presencial /virtual (comunicación verbal)	Todas las áreas de los procesos
Julio	Continuidad del negocio después de un incidente de seguridad de la información o ciberseguridad	Conferencia presencial /virtual (comunicación verbal)	Todas las áreas de los procesos
Agosto	Desarrollo Seguro	Conferencia virtual (comunicación verbal)	OTIC
Septiembre	Socialización de procedimientos para la seguridad de la información	Conferencia virtual (comunicación verbal)	OTIC
Octubre	Buenas prácticas de seguridad de la información	Piezas comunicativas (comunicación no verbal)	Todas las áreas de los procesos

Noviembre	Buenas prácticas de seguridad de la información	Piezas comunicativas (comunicación no verbal)	Todas las áreas de los procesos
Diciembre	Tendencias de seguridad de la información en Colombia	Piezas comunicativas (comunicación no verbal)	Todas las áreas de los procesos
Marzo-diciembre	Socialización de procedimientos para la seguridad de la información	Charla magistral-presencial o virtual según planificación de GGH	Todas las áreas en el marco de inducción y reinducción
Abril – octubre	Conceptos básicos y principios de seguridad., socialización de Políticas	Dialogo con el Comité Directivo	Comité Directivo

5. Medios de comunicación

Los medios de comunicación utilizados para facilitar el aprendizaje de los participantes serán a través de las diferentes herramientas con las que cuenta actualmente la entidad: i) Microsoft Teams para las conferencias de las temáticas a sensibilizar programadas, ii) Piezas comunicativas se enviarán masivamente al personal de todas las dependencia a través de correo electrónico, iii) publicaciones en el portal web o intranet y iv) publicaciones en pantallas distribuidas en diferentes espacios de la entidad.

6. Fuentes bibliográficas

1. **Castro Perez. Las Claves de la Cuarta Revolución Industrial. Libros de cabecera. 2019**
2. **Petrenko Sergei. La Administración de la Ciberseguridad: Industria 4. 0. Servicio de Publicaciones de la universidad de Oviedo. 2019.**
3. **Kevin Mitnick. The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data.2017**
4. **Christopher Hadnagy. Social Engineering: The Science of Human Hacking.2018**
5. **Joseph Menn. Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World. 2019.**
6. **Pavan Duggal. Cyber resilience & Cyberlaw.2020**
7. **Mansour George. Unhackable. 2020**
8. **Tim Rains. Cybersecurity Threats, Malware Trends, and Strategies.2020**
9. **Adviera. Checklist of cyber threats & safeguards when working from home.2020.**
10. **Eset. Cibersecurity. Trends 2021. 2021. Recuperado de https://www.welivesecurity.com/wp-content/uploads/2020/11/ESET_Cybersecurity_Trends_2021.pdf**
11. **Resolución 00500 de marzo 10 de 2021. Mintic. Recuperado de https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf**
12. **Anexo 3. Resolución 1519 de 2020. Mintic. Recuperado de https://gobiernodigital.mintic.gov.co/692/articles-160770_Condiciones_minimas.pdf**
13. **Anexo 1. Modelo de seguridad y privacidad. 2021. Mintic. Recuperado de https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf**

Estrategia de sensibilización

VERSIÓN 031
Oficina Asesora de Planeación
Febrero 2022

Departamento Administrativo de la Función Pública
Carrera 6 n.º 12-62, Bogotá, D.C., Colombia
Conmutador: 7395656 Fax: 7395657
Web: www.funcionpublica.gov.co
eva@funcionpublica.gov.co
Línea gratuita de atención al usuario: 018000 917770
Bogotá, D.C., Colombia.