PLAN DE SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código SG/MIPG	127-PPPGI-10
Vigencia desde	17/06/2023
Versión	3

Proceso

Gestión de la tecnología y la información

ALCALDÍA MAYOR DE BOGOTÁ D.C.

DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO

BOGOTÁ

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El continuo crecimiento y evolución de las tecnologías de la información y comunicaciones han permitido mejorar de manera significativa el desarrollo de las funciones y procesos de las organizaciones tanto públicas como privadas, así como de las personas que, mediante el uso provechoso de los recursos tecnológicos, han logrado traer consigo beneficios en los diferentes aspectos que hacen parte de la sociedad. Sin Embargo, al mismo tiempo en que se logran avances en las tecnologías de la información y recursos tecnológicos, también han aumentado considerablemente los riesgos y amenazas viéndose afectados o vulnerable los datos e información de las organizaciones y las personas en general.

Por su parte, cuando se habla de seguridad y privacidad de la información, es necesario que exista un trabajo articulado entre procesos, recursos tecnológicos y personas con el propósito de proteger la disponibilidad, confidencialidad e integridad de la información reduciendo así la materialización potencial de riesgos y amenazas a los que están expuestos los datos e información.

No obstante, dentro de la gran cadena de factores que hacen parte de la seguridad de la información el talento humano resulta ser el eslabón más frágil puesto que se ven continuamente enfrentados a engaños, suplantación, ataques malintencionados, errores por desconocimiento e incluso en ocasiones por alguna inconformidad de tipo laboral o personal pueden llegar a convertirse en el factor encargado de ocasionar alguna afectación con repercusiones hacia las personas y entidades.

En este documento se hace referencia al fortalecimiento y toma de conciencia del personal de planta y contratistas del Departamento Administrativo de la Defensoría del Espacio Público DADEP para que tengan conocimiento de la política de seguridad de la entidad y puedan enfrentar amenazas, eventos e incidentes que atentan contra la seguridad y privacidad de la información del ámbito organizacional y personal.

2 OBJETIVO

Definir lineamientos para el desarrollo de las actividades del Plan de Sensibilización, Capacitación y Comunicación de Seguridad y Privacidad de la Información, de manera que su ejecución contribuya a la prevención, control y gestión de amenazas, eventos, incidentes y emergencias relacionadas con la seguridad digital de la Entidad. Para esto, el Plan pretende generar compromiso, cultura de seguridad y concientización acerca de la importancia de la protección de los Activos de Información del DADEP.

2.1 Objetivos específicos

- Divulgar dentro de la comunidad de usuarios de la Entidad la importancia de aplicar las buenas prácticas de seguridad informática en el uso cotidiano de los recursos tecnológicos puestos a su disposición.
- Dar a conocer las principales amenazas cibernéticas como medida preventiva para evitar la materialización de riesgos cibernéticos.
- Fortalecer el conocimiento y capacidades sobre prevención de riesgos, detección y respuesta a eventos e incidente que afectan o puedan afectar la seguridad de la información.
- Generar una cultura organizacional sobre el tratamiento de los activos de información del DADEP.
- Fomentar compromiso en los colaboradores frente a la implementación del Sistema de Gestión de Seguridad de la Información - SGSI.
- Divulgar y transferir el conocimiento sobre el ámbito legal y regulatorio relacionado con seguridad y privacidad de la información interno y externo.

3 ALCANCE

El Plan de Sensibilización y Comunicación de Seguridad de la información va dirigido a todos los colaboradores del DADEP y cubre la divulgación y socialización de las actividades de implementación del Sistema de Seguridad de la Información y principalmente, las medidas preventivas y correctivas que todos los usuarios de Tecnología de la Entidad deben tomar para el uso seguro de las herramientas tecnológicas y protección de los Activos de Información de la Entidad.

4 DEFINICIONES Y SIGLAS

Como parte del plan de sensibilización y comunicación de seguridad y privacidad de la información, hacen parte los siguientes términos:

- Activo [Según ISO 27000]
  En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- Activo de Información
  Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

- Acuerdo de Licencia
  Es una cesión de derechos entre un titular de derechos de propiedad intelectual (licenciante) y otra persona que recibe la autorización de utilizar dichos derechos (licenciatario) a cambio de un pago convenido de antemano (tasa o regalía) o de unas condiciones determinadas.

- Adware
  Software de tipo publicitario que se instala en los equipos de cómputo u otro dispositivo móvil y que haciendo uso del navegador web o ventanas muestra información no deseada.

- Amenaza [Según ISO 27000]
  Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- Antivirus
  Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware.

- Autenticación
  Procedimiento para comprobar que alguien es quién dice ser cuando accede a un computador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

- BIA
  Abreviatura de «Business Impact Analysis». Se trata de un informe que nos muestra el costeocasionado por la interrupción de los procesos críticos de negocio. Este informe nos permitirá asignar una criticidad a los procesos de negocio, definir los objetivos de recuperación y determinar un tiempo de recuperación a cada uno de ellos.

- Biometría
  La biometría es un método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.) o de comportamiento (firma, forma de andar, tecleo, etc.). Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar, etc.

- **Cloud Computing** (Computación en la nube)
  El término cloud computing o computación en la nube se refiere a un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet. Esta tendencia permite a los usuarios almacenar información, archivos y datos en servidores de terceros, de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red, resultando de esta manera innecesaria la instalación de software adicional (al que facilita el acceso a la red) en el equipo local del usuario.

- **Confidencialidad**
  Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder dicha información.

- **Cookie**
  Una cookie es un pequeño archivo que almacena información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario. Sus usos más frecuentes son: recordar datos de nombres de usuario y contraseñas, recopilar hábitos de navegación, entre otros.

- **Dirección IP**
  Número único e irrepetible con él se identifica de manera unívoca cualquier dispositivo o sistema que se conecta a una red.

- **Disponibilidad**
  Capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran. Junto con la integridad y la confidencialidad son las tres dimensiones de la seguridad de la información.

- **DRP**
  Un Plan de Recuperación ante Desastres (Disaster Recovery Plan o DRP), es un documento estructurado con los pasos y acciones que una organización debe tomar para recuperar su operación después de un incidente mayor. El tipo de

incidentes que pueden provocar que se utilice un DRP pueden ser desastres naturales, eventos mayores de disrupción de vías de comunicación, eventos sociales o políticos, ataques informáticos o físicos a las instalaciones, entre otros.

- Fuga de Datos
  La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros

- Gestión de incidentes de seguridad de la información [Según ISO 27000]
  Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

- Incidente de Seguridad
  Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

- Ingeniería Social:
  Son diferentes técnicas que emplea un delincuente cibernético para obtener información clasificada o reservada.

- Integridad
  La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que, de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.

- Malware
  Es un tipo de código malicioso o software desarrollado con el propósito de sacar provecho sobre alguna vulnerabilidad presente en un equipo de cómputo, red de comunicaciones, teléfono celular o algún otro dispositivo electrónico.

- Parche de Seguridad
  Un parche de seguridad es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden instalarse de forma automática o manual por parte del usuario.

- Phishing
  Son técnicas y métodos que utilizan los delincuentes cibernéticos para obtener información laboral o personal de carácter clasificado o reservado.

- Plan de Contingencia
  Un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía.

- Plan de Continuidad
  Un Plan de Continuidad de Negocio es un conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía.

- Políticas de Seguridad
  Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. Este término también

se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.

- Puerta Trasera
  Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema. Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores, pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos. Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el computador de la víctima, dan el control de éste de forma remota al computador del atacante.

- Ransomware
  Es un código malicioso o software que se encarga de secuestrar información de un equipo de cómputo u otro dispositivo móvil y que tiene como objetivo cobrar por el rescate de la información.

- Red Privada Virtual (VPN)
  Una red privada virtual, también conocida por sus siglas VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet. Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Se trata realmente de una conexión virtual punto a punto entre dos redes LAN usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura gracias al cifrado de la comunicación.

- Router
  Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un router está conectado al menos a dos redes, generalmente LAN (red local) o WAN (red de amplia cobertura) y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es). En términos domésticos, un router es el dispositivo que proporciona el proveedor de servicios de internet (o ISP) y que permite conectar nuestra LAN doméstica con la red del Proveedor de Servicios de Internet.

- Riesgo [Según ISO 27000]
  Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- SaaS
  Son las siglas de Software as a Service, es decir la utilización de Software como un servicio. Es un modelo de distribución de software donde tanto el software como los datos que maneja se alojan en servidores de un tercero (generalmente el fabricante del software) y el cliente accede a los mismos vía Internet. Se trata de una de las modalidades de servicio que prestan los proveedores de computación en la nube.

- Seguridad de la información [Según ISO 27000]
  Preservación de la confidencialidad, integridad, y disponibilidad de la información.

- Servidor
  Puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios, como el computador físico en el cual funciona ese software, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él.

- SGSI
  Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

- Spoofing

Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de malware. Los ataques de seguridad en las redes usando técnicas de spoofing ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

- Spyware
  Es un tipo de software que actúa como espía para recopilar información de todo tipo además de reducir el rendimiento de un equipo de cómputo o dispositivo móvil.

- Suplantación de Identidad
  Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbulling). Un ejemplo es, en las redes sociales, crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella.

- Troyano
  Se trata de un tipo de malware o software malicioso que se caracteriza por carecer de capacidad de autorreplicación. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación.

- Virtualización
  La virtualización es un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, o una red, en una máquina física, generalmente con el apoyo de un software que implementa una capa de abstracción para que la maquina física y la virtual puedan comunicarse y compartir recursos.

- Virus
  Programa diseñado para que, al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos. A diferencia de otro tipo de malware, como los gusanos, se necesita acción humana para que un virus se propague entre máquinas y sistemas. Los efectos que pueden provocar varían dependiendo de cada tipo de virus: mostrar un mensaje, sobrescribir archivos,

borrar archivos, enviar información confidencial mediante correos electrónicos a terceros, etc. Los más comunes son los que infectan a archivos ejecutables

- Vulnerabilidad [Según ISO 27000]:
  Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5 PLAN DE SENSIBILIZACIÓN, CAPACITACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Departamento Administrativo de la Defensoría del Espacio Público - **DADEP,** con el propósito de lograr la implementación y el fortalecimiento del Sistema de Gestión de Seguridad de la Información - SGSI, contribuye al fortalecimiento del uso adecuado de los recursos tecnológicos, los procesos y mejora de las capacidades en el talento humano para la prevención, detección y respuesta a eventos e incidentes que afectan la disponibilidad, integridad y confidencialidad de los datos e información.

5.1.1 Roles implicados

El logro efectivo del plan requiere el fomento y adopción de controles, lineamientos y buenas prácticas de seguridad de la información que involucra a todos los contratistas y colaboradores que hacen parte de los distintos niveles organizacionales de la entidad de la siguiente forma:

Rol	Actividades
Directivos	• Promover la participación de las sesiones de sensibilización propuestas. • Liderar la adopción y cumplimiento de medidas establecidas para la protección de los activos de información. • Apoyar con recursos e incentivos para el desarrollo e implantación del plan.
Líder o Responsable de Proceso	• Coordinar y ser partícipes de las actividades que hacen parte del plan. • Propender por el cumplimiento, adopción e implementación de las actividades de

	seguridad de la información comunicadas en el plan. • Identificar falencias o debilidades de seguridad de la información que requieran capacitación o sensibilización.
Responsable de seguridad de la información	• Ejecutar y cumplir el plan de sensibilización, capacitación y comunicación de seguridad de la información. • Establecer y consolidar métricas e indicadores de evaluación y gestión sobre la implementación del plan. • Identificar debilidades para hacerlas parte dentro del plan.
Colaboradores	• Participar en las sesiones pactadas que hacen parte del plan. • Poner en práctica las recomendaciones, buenas prácticas y controles de seguridad de la información que hacen parte del plan. • Identificar debilidades para hacerlas parte dentro del plan.

5.1.2 Audiencia

El plan de sensibilización, capacitación y comunicación de seguridad de la información está dirigido a los colaboradores del DADEP.

5.1.3 Temas de sensibilización programadas

Los temas, el material, tiempo de implementación que se consideran pertinente para su socialización y capacitación se establecen en el en el Cronograma del plan de divulgación SGSI.

- Sistema de Gestión de Seguridad de la Información - SGSI
- Políticas de Seguridad y Privacidad de la información
- Uso de las herramientas institucionales
- Procedimiento de incidentes de seguridad de la información
- Planes de Contingencia y Continuidad del Negocio
- Tratamiento de Datos personales

- Gestión de contraseñas seguras
- Software legal
- Respaldo de información
- Navegación segura
- Ataques cibernéticos
- Día internacional de la seguridad
- Temas relacionados con la seguridad
- Documentación relacionada
- Activos de información
- Riesgos digitales
- Marco regulatorio y legal
- Roles y responsabilidades

La socialización de los anteriores temas relacionados, se llevará a cabo a través de divulgación de información, charlas y diseño de piezas audiovisuales enviados a los correos institucionales, intranet y demás canales establecidos para tal fin y previamente concertados con las demás áreas de la Entidad relacionada con la creación y divulgación de los mismos.

5.1.4 Cronograma

Para lograr el objetivo de plan, se presenta el siguiente cronograma de actividades, donde se estructuran los temas, los canales de comunicación, el responsable de ejecutar la actividad, la audiencia, las herramientas o medios para llevar a cabo la comunicación, las fechas y finalmente la periodicidad.

Cabe resaltar, que el cronograma está susceptible a cambios imprevistos en el entorno externo o interno que amerite un cambio sustancial en la ejecución del mismo.

MSPI_PLAN DE COMUNICACIÓN Y SENSIBILIZACIÓN

PROCESO: GESTIÓN DE LA TECNOLOGÍA Y LA INFORMACIÓN

INSTRUMENTO: PLAN DE COMUNICACIÓN Y SENSIBILIZACIÓN

VIGENCIA: 2023

N°	ACTIVIDAD	TEMA	CANAL DE COMUNICACIÓN	RESPONSABLE	AUDIENCIA	HERRAMIENTA	Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre				FRECUENCIA
							1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
1	Reunión Equipo de Comunicaiones	Definir Metodología de trabajo, actividadesy divulgación de información	Teams,presencial	SGSI – Comunicaciones	SGSI - Comunicaciones	Reuniones	X												X								X												X				Trimestral
2	Día de la Seguridad	Sistema de Gestión de Seguridad de la Información - SGSI	Correo electrónico, Teams	SGSI - Comunicaciones	Todos los colaboradores	Piezas gráficas				X																																Mensual
		Procedimiento de incidentes de seguridad de la información				Piezas gráficas								X																													Mensual
		Navegación segura				Piezas gráficas												X																										Mensual
		Ingeniería social				Piezas gráficas																																	X					Mensual
		Ataques cibernéticos				Piezas gráficas																		X																				Mensual
		Día internacional de la seguridad				Piezas gráficas																								X														Mensual
		Rasomware				Piezas gráficas																X																						Mensual
3	Semana de la seguridad de la información	Temas relacionados con la seguridad	Correo electrónico	SGSI - Comunicaciones	Todos los colaboradores	Piezas gráficas																																				x	Anual
4	Charlas	Inducción y reinducción	Teams	SGSI	Todos los colaboradores	Inducción y reinducción													X																								Anual
		Política de seguridad y privacidad de la información				Presentaciones																										X												Semestral

Revisó y Aprobó: Syrus Asdrúbal Pacheco – jefe OTIC.

Proyectó: Carlos Alberto de la Ossa Hurtado – Contratista profesional OTIC.
Código de archivo: 140

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
3	28/04/2023	Cambio del nombre de la oficina de TIC y actualización del cronograma.

Fuentes:

[1] Symantec Glosario de seguridad. https://www.symantec.com/es/es/security_response/glossary/
[2] Panda. Glosario. http://www.pandasecurity.com/spain/homeusers/security-info/glossary/
[3] Viruslist. Glosario. https://securelist.com/encyclopedia/
[4] Safemode. Glosario. http://safemode-cl.blogspot.com.es/2006/07/glosario-de-ter
[5] CERT UY. http://www.cert.uy/inicio/sobre_seguridad/glosario/
[6] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf