Oficina Asesora de Informática

OFICINA ASESORA DE
INFORMÁTICA

Salvemos Juntos
a Cartagena

MANUAL PARA EL PLAN DE **CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN.**

Tabla de Contenido

Índice de Figuras

Índice de Tablas

Índice de Ilustración

1. INTRODUCCIÓN

En la última década, las tecnologías de información y comunicaciones se han convertido en la herramienta por excelencia para la optimización de los procesos y el funcionamiento eficaz de una empresa. Con el uso de la tecnología, surgen a su vez amenazas y vulnerabilidades asociadas, que pueden llegar a afectar la disponibilidad, privacidad e integridad de la información que se encuentra disponible en las diferentes plataformas, afectando el desempeño de los procesos y servicios de la entidad. (Ministerio de Tecnologias de la Información y Comunicaciones, 2016)

Teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Sistema de Gestión de Seguridad de la Información (SGSI) estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la Entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información. (Ministerio de Tecnologias de la Información y Comunicaciones, 2016)

Para esto, la Alcaldía de Cartagena de Indias a través de la Oficina Asesora de Informática, diseñó la Política de Seguridad Digital, la cual brinda los lineamientos para las mejores prácticas dentro de la Entidad. Teniendo en cuenta que el Recurso Humano es el pilar fundamental dado a que es el eslabón más débil, es necesario hacer el proceso de sensibilización, capacitación y comunicación para así, preservar la disponibilidad, integridad y la confidencialidad de la información; mitigando las amenazas existentes en el entorno.

2. ALCANCE

Este documento está dirigido y difundido a todo el personal de funcionarios, contratistas y terceros que realizan actividades en la Alcaldía de Cartagena de Indias.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar e implementar el plan de capacitación, sensibilización y comunicación de la Política de Seguridad Digital con el fin de que los Enlaces TI de la Alcaldía de Cartagena de Indias conozcan los lineamientos y se apropien del aseguramiento de la información, replicando las buenas prácticas en sus respectivas Dependencias.

3.2 OBJETIVOS ESPECÍFICOS

- Definir la estrategia de sensibilización por medio de divulgación con casos ejemplos de la violación de las Políticas definidas para la Seguridad Digital, con el fin de fortalecer la cultura de seguridad de la información y evitar sanciones por el incumplimiento de estas.
- Definir el plan de capacitación para establecer los lineamientos en el uso de los activos de información, con el fin de interiorizar y mitigar los riesgos asociados a estos.

4. GLOSARIO

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (Ministerio de las Tecnologías de Información y Comunicaciones, 2016)

- **Brecha:** Se denomina al espacio o ruta a recorrer entre un estado actual y un estado deseado. (Ministerio de Tecnologias de la Información y Comunicaciones, 2016)

- **Confidencialidad**: propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados, asegurando el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización (Alcaldia de Cartagena de Indias, 2023)

- **Contraseña:** Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña. (Ministerio de las Tecnologías de Información y Comunicaciones, 2016)

- **Disponibilidad**: característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones

- **Entrenamiento:** Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo. (Ministerio de Tecnologias de la Información y Comunicaciones, 2016)

- **Información**: conjunto organizado de datos generados, obtenidos, adquiridos, transformados o controlados que constituyen un mensaje sin importar el medio que lo contenga (digital y no digital) (Alcaldia de Cartagena de Indias, 2023)

- **Ingeniería Social:** "Tipo de ataque de seguridad en la cual un individuo manipula al otro con el fin de obtener información que puede ser utilizada para acceder a un sistema no autorizado, sustraer dinero o incluso suplantarla identidad de la víctima. (Ministerio de Tecnologias de la Información y Comunicaciones, 2016)

- **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas. Grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados. (Alcaldia de Cartagena de Indias, 2023)

- **Malware:** El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas. (Ministerio de las Tecnologías de Información y Comunicaciones, 2016)

- **Política:** Declaraciones de alto nivel que expresan los objetivos a cumplir de la Entidad respecto a algún tema en particular. (Ministerio de Tecnologias de la Información y Comunicaciones, 2016)

- **Rol:** Papel, función que alguien o algo desempeña. (Alcaldia de Cartagena de Indias, 2023)

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sensibilización:** Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular. (Ministerio de Tecnologias de la Información y Comunicaciones, 2016)

- **Sistema de Gestión de Seguridad de la Información (SGSI):** 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)

- **Spam:** También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina

para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing (Ministerio de las Tecnologías de Información y Comunicaciones, 2016)

- **TIC:** Tecnologías de la Información y Comunicaciones. (Alcaldia de Cartagena de Indias, 2023)

- **Virus:** Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:
  Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.
  Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.
  Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales. (Ministerio de las Tecnologías de Información y Comunicaciones, 2016)

- **Vulnerabilidad:** Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:
  - Permitir que un atacante ejecute comandos como otro usuario
  - Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
  - Permitir a un atacante hacerse pasar por otra entidad
  - Permitir a un atacante realizar una negación de servicio

5. ROLES Y RESPONSABILIDADES

A continuación, se presenta los roles y responsabilidades más comunes en capacitación en la Alcaldía de Cartagena de Indias.

Rol	Descripción	Responsable
Líder de la Política Seguridad Digital	Emitir las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de la política de Gobierno Digital, en las entidades públicas del orden nacional y territorial. De igual manera, a través de la Dirección de Gobierno Digital se desarrollan diferentes iniciativas y proyectos que buscan apalancar la implementación de la política en las entidades públicas	Ministerio de Tecnologías de la Información y Comunicación a través de la Dirección de Gobierno Digital
Responsable Institucional de la Política de Seguridad Digital	Responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Seguridad Digital. Debe garantizar el desarrollo integral de la política al interior de sus entidades, entendiendo que esta es un eje transversal y apalancado de su gestión interna, que apoya el desarrollo de las políticas de gestión y desempeño institucional.	Representante Legal - Alcalde Mayor
Responsable de orientar la implementación de la Política de Gobierno Digital	Orientar la implementación y operación de todas las políticas del Modelo Integrado de Planeación y Gestión -MIPG (entre las que se encuentra seguridad Digital); Debe articular todos los esfuerzos institucionales, recursos, metodologías y estrategias para el desarrollo de las políticas del MIPG y en esta medida, lograr que la seguridad Digital se desarrolle articuladamente con las demás políticas en el marco del sistema de gestión de la entidad.	Comité Institucional de Gestión y Desempeño

Rol	Descripción	Responsable
	Aprobar y verificar del cumplimiento de las políticas y procedimientos de seguridad y privacidad de la información. Hacer que los miembros del Gabinete sean conscientes de la criticidad de los activos de información para el desarrollo de los procesos de la Alcaldía Distrital de Cartagena de Indias. Divulgar las responsabilidades de seguridad y privacidad de la información de la Alcaldía Distrital de Cartagena de Indias con base en los lineamientos del MSPI.	
Responsable de liderar la implementación la Política de Seguridad Digital	Hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad. Las demás áreas serán corresponsables de la implementación de la Política de Seguridad Digital en los temas de su competencia. Además de: Liderar y apoyar la mejora continua para la aplicación del MSPI al interior de la Alcaldía, Asignar dentro de su equipo de trabajo quien servirá como oficial de seguridad y privacidad de la información, Apoyar las actividades relacionadas con el MSPI. En este sentido, áreas o dependencias afines a los siguientes temas también son responsables en la implementación de la política de Seguridad Digital, dada su transversalidad en la gestión de la entidad: planeación, secretaría general, servicio al ciudadano, participación ciudadana,	Jefe de Oficina Asesora de Informática en articulación con las dependencias del Distrito

Rol	Descripción	Responsable
	comunicaciones o prensa, desarrollo organizacional, talento humano, archivo y gestión documental.	
Otros roles e instancias importantes	Estas instancias deben actuar en coordinación con el comité institucional de gestión y desempeño para la toma de decisiones. Liderar y apoyar de mejora continua para la aplicación del MSPI al interior de la dependencia a cargo. Alineación de los objetivos de la dependencia para que su cumplimiento este apoyado por el MSPI. Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad y privacidad de la información para los roles definidos en la dependencia a cargo. Proveer los recursos necesarios para la implementación del MSPI al interior de la dependencia a cargo. Apoyar la capacitación y entrenamiento requerido para que los funcionarios y contratistas de la dependencia a cargo que cumplan con el MSPI. Aplicar el proceso disciplinario ante los incidentes de seguridad y privacidad de la información originada por un funcionario o contratista de la dependencia a cargo.	Nivel directivo: secretarios, asesores, directores y jefes de oficina.

Tabla 1. Roles y responsabilidades de la Política de Seguridad Digital

6. FASES DEL PLAN

A continuación, se presenta las 4 fases que compone el plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información de la Alcaldía de Cartagena de Indias.

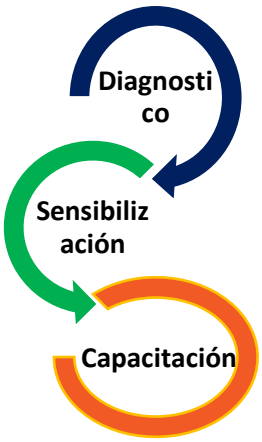

Ilustración 1. Fases del Plan de Capacitación, Sensibilización y Comunicación de la Política de Seguridad de la Información

6.1 FASES DE DIAGNOSTICO

En esta fase para poder identificar como están las dependencias del distrito con respecto a la Seguridad Digital, se hizo un proceso de Ingeniería Social enviando un correo malicioso de prueba en la cual tenía un enlace sospechoso, obteniendo los siguientes resultados:

CORREO MALICIOSO DE PRUEBA ACCEDIERON AL ENLACE SOSPECHOSO	
N° de correos enviados	307
Personas que reportaron el correo como sospechoso	10
Personas que enviaron la información requerida	19
Personas que no reportaron	278

Tabla 2. Prueba de correo malicioso

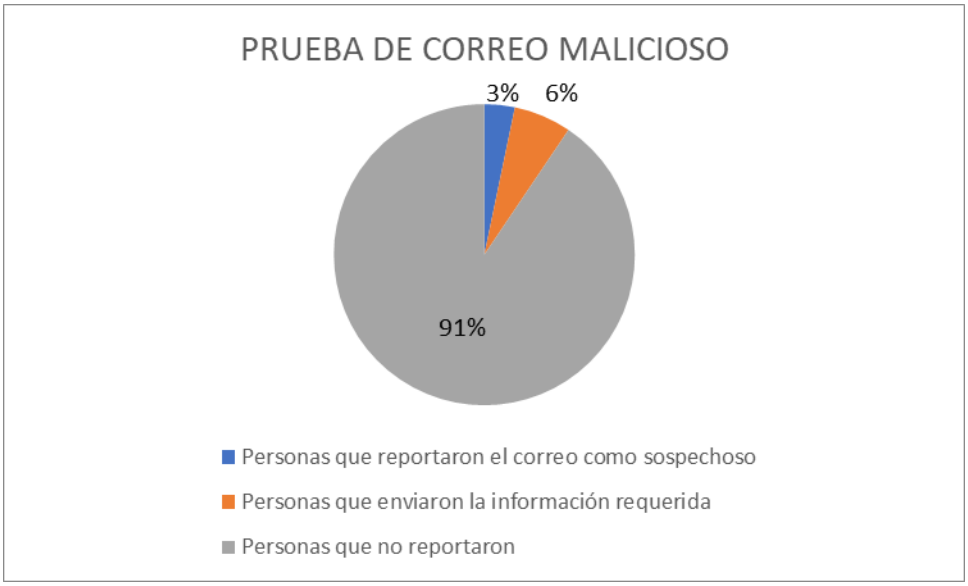

Figura 1. Porcentaje de los resultados de la prueba del correo malicioso

De las 19 dependencias que ingresaron al enlace sospechoso a continuación se muestra que Apoyo Logístico fue el que tuvo mayor ingreso al enlace, seguido de Bomberos y Secretaría de hacienda.

Dependencias	Cantidad de Incidencias
Andian-Calidad	1
Apoyo Logístico	4
Bomberos	2
Cárcel Distrital	1
Control Disciplinario	1
DADIS	1
Fiscalización	1
Fondo Territorial de Pensiones	1

Dependencias	Cantidad de Incidencias
Impuestos	1
Secretaría General	1
Secretaría de Hacienda	2
Secretaría de Planeación	1
Transparencia y Anticorrupción	1
UMATA	1
TOTAL	**19**

Tabla 3. Dependencias vs cantidad de incidencias del primer ejercicio

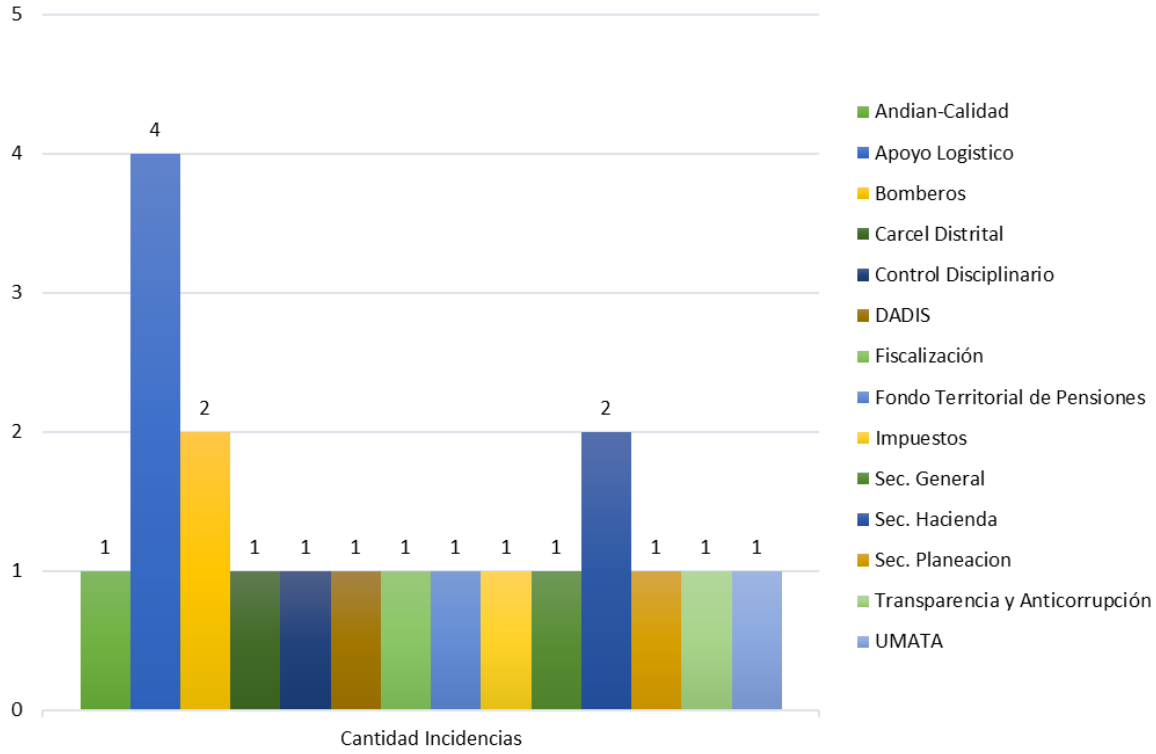

Figura 2. Dependencias vs cantidad de incidencias del primer ejercicio

Se realizó un segundo ejercicio de Ingeniería Social con las dependencias pertenecientes a la Alcaldía de Cartagena de Indias, a continuación, se presenta las diez dependencias con mayor incidencia.

Dependencias	Cantidad de Incidencias
Bomberos Limbo	158
Familias en Acción	130
Servicio Público	99
Impuesto	67

Dependencias	Cantidad de Incidencias
Secretaría del Interior y Convivencia Ciudadana	66
Contabilidad	62
Edificio T14	52
Palacio de Aduana	51
Apoyo Logístico	45
Secretaría de Hacienda	45
TOTAL	**775**

Tabla 4. Dependencias vs cantidad de incidencias segundo ejercicio

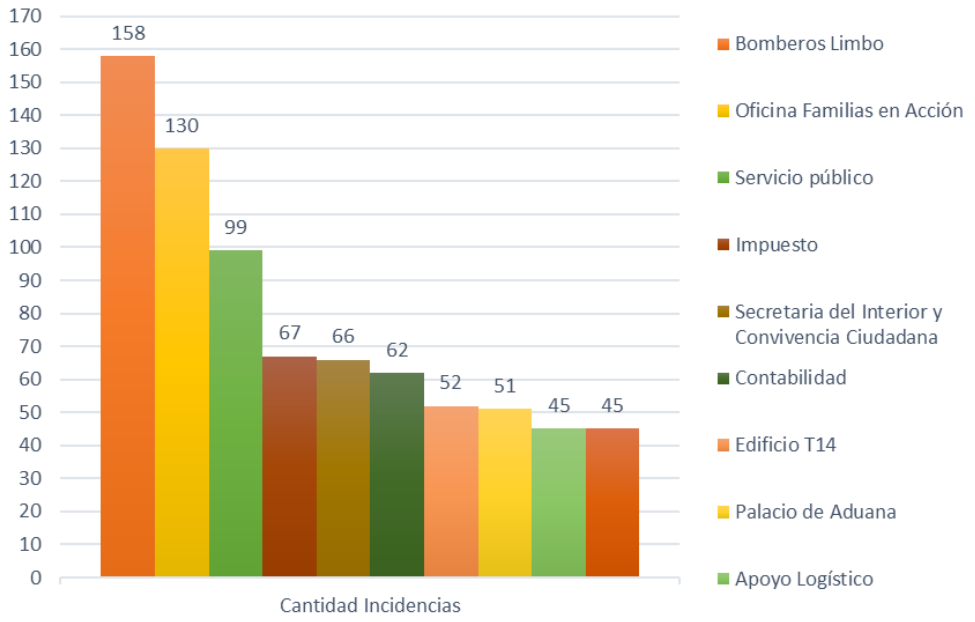

Figura 3. Dependencias vs cantidad de incidencias segundo ejercicio

Dado a que se evidenció que las dependencias del distrito ingresaban a los enlaces maliciosos que se hizo con la Ingeniería Social, se da inicio al plan de sensibilización y

capacitación a los funcionarios y contratistas del distrito para apropiar la Política de Seguridad Digital.

6.2 FASE DE SENSIBILIZACIÓN

Se definieron las actividades que facilitan la apropiación de los funcionarios y contratistas de la Alcaldía de Cartagena de Indias, la interiorización de los beneficios de estos y crear entre los involucrados un interés participativo por la implementación.

Así mismo, deberá contener:

1. La campaña de comunicación interna dirigida a la Alcaldía Distrital.
2. La campaña de comunicación externa, dirigida a los grupos de valor y la ciudadanía en general.

Los objetivos de estas serán: (i) Sensibilizar, (ii) Generar interés y, (iii) Generar involucramiento en las acciones efectuadas por la Alcaldía Distrital en el marco de la Política de Seguridad Digital y, en sí, todos los procesos que tienen que ver con tecnología

DESCRIPCIÓN	MENSAJE	PÚBLICO OBJETIVO
Administración de contraseñas	"Luis usó como contraseña para el computador su nombre seguido de los números 1,2,3. Alguien adivinó y ahora su información sensible está expuesta y está en riesgo de fraude informático"	Ventanilla hacia afuera y adentro

DESCRIPCIÓN	MENSAJE	PÚBLICO OBJETIVO
Malware y sus diferentes tipos	“Pablo abrió un archivo de riesgo, omitió todas las señales que le mostraban que era peligroso. Bastó un clic para que el malware* instalara un virus* en su computador y ahora hay un programa espía* y cinco troyanos* que comprometieron la integridad de la red corporativa*”. No seas como Pablo, ¡contamos conTIgo para protegernos de los riesgos digitales!	Ventanilla hacia afuera y adentro
Uso de correo electrónico e identificación de correos sospechosos	"Juanita dejó abierta la sesión del correo institucional en un computador de un café internet. Alguien entró y le robó todos los datos sensibles que tenía ahí. Ahora la información privada de los colaboradores y las colaboradoras está en riesgo"	Ventanilla hacia afuera y adentro
Uso apropiado de internet	“Lucia ingreso a un sitio web que no era seguro y fueron robados sus datos financieros” Evita ser como Lucia e ingresa a un sitio web seguro	Ventanilla hacia afuera y adentro
Política de escritorio limpio	"María salió apurada apagó el computador y no hizo la copia de seguridad. Ahora perdió la información por no subirla a la nube"	Ventanilla hacia afuera y adentro

DESCRIPCIÓN	MENSAJE	PÚBLICO OBJETIVO
Sanciones por incumplimiento de las políticas	"Paola instaló un software sin licencia haciendo que a la empresa le llegue una denuncia por violar los derechos de propiedad intelectual" Evita ser como Paola y usa software licenciado	Ventanilla hacia afuera y adentro
Uso y manejo de inventario	"Dora no hizo el inventario de los activos de información en su oficina y se publicó una información reservada afectando la seguridad pública de la ciudad donde reside" Evita ser como Dora y realiza el inventario de activos de información	Enlaces TI
Software permitido/prohibido en la entidad	"Samuel instaló un software pirata, y en el instante ingresó un virus afectando la continuidad segura de las operaciones de la Entidad" Evita ser como Samuel y adquiere el software de manera legal y segura	Ventanilla hacia afuera y adentro
Uso de dispositivos de la entidad fuera de las instalaciones	"Daniel no inventarió los dispositivos móviles de la entidad provocando que se perdiera y no se encontrara al responsable" ¿Qué harías tu?.	Ventanilla hacia afuera y adentro
Temas de control de acceso a los sistemas (privilegios, separación de roles)	"Jaime prestó a su compañero el usuario y contraseña del sistema ocasionando robo de información sensible de la entidad" recuerda que la contraseña es de uso personal e	Ventanilla hacia afuera y adentro

DESCRIPCIÓN	MENSAJE	PÚBLICO OBJETIVO
	intransferible y es responsabilidad del usuario el uso de las credenciales asignada	
Ingeniería social	"Ana abrió un correo sospechoso. No era una notificación de la organización, sino un código malicioso. Ella fue víctima de phishing ahora han robado la información alojada en su computador"	Ventanilla hacia afuera y adentro
Backups y recuperación	“Carmen no realizo el Backup de los equipos de la oficina y un virus eliminó la información” ¿Qué le dirías a Carmén?	Ventanilla hacia afuera y adentro
Amenazas y vulnerabilidades comunes	“Miguel descargó archivos sin revisar si eran seguros o no. Él le abrió la puerta a atacantes, que aprovecharon su descuido, y ahora aumentó la vulnerabilidad a los ataques*”. No seas como Miguel, ¡contamos conTIgo para protegernos de los riesgos digitales!	Ventanilla hacia afuera y adentro

Tabla 5. Sensibilización de la Política de Seguridad Digital

6.3 FASE DE CAPACITACIÓN

En la presente fase lo que se busca es que el personal TI, en el proceso de Seguridad Digital, tengan conocimiento y habilidades para el uso correcto de las funciones específicas a su cargo, siendo un implementador de las medidas de seguridad en cada dependencia y velar por el control y verificación de esta.

Los temas que fueron identificados para el desarrollo de las habilidades en temas de Seguridad Digital son:

1. Capacitación en riesgos de seguridad digital
2. Lineamientos de seguridad OAI
3. Carpeta ciudadana digital
4. Ciberseguridad responsabilidad de todos
5. Organización de la Seguridad de la Información
6. Gestión de activos
7. Control de acceso a aplicaciones
8. Perímetros de seguridad
9. Control de acceso a redes e internet
10. Gestión de acceso a usuarios
11. Revisión de los derechos de acceso de los usuarios
12. Seguridad física y del entorno
13. Escritorio y pantalla despejada
14. Protección y privacidad de datos personales
15. Integridad
16. Disponibilidad del servicio e información
17. Gestión de incidentes de seguridad de la información
18. Desarrollo seguro
19. Cumplimiento ley de transparencia
20. Servicios de computación en la nube
21. El Manejo de copias de seguridad

22. Gestión de seguridad de las redes
23. Protección contra código malicioso

Para la ejecución de estas capacitaciones, podrá contarse con plataformas tecnológicas propias como:

- Mis Talentos: creada para el desarrollo de cursos para fortalecer competencias digitales en funcionarios.
- Escuela de Gobierno virtual: dirigida a la ciudadanía y contiene cursos que se soporta sobre módulos.
- Plataforma de reuniones en línea (Teams): Videoconferencia en tiempo real para capacitaciones dictadas en un horario asignado para la persona, área y/o dependencia.

Las capacitaciones se podrán realizar de forma presencial de acuerdo con los requerimientos de cada dependencia y la disponibilidad de los recursos.

Las evidencias requeridas para las capacitaciones ejecutadas son:

- Asistencia
- Diapositivas
- Fotos
- Evaluación (en caso de que sea requerida)
- Certificado de asistencia (en caso de que sea requerida)

7. MONITOREO Y SEGUIMIENTO

Con respecto al monitoreo del Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información, Algunas establecidas en el presente documento se encuentran en el “Plan de Seguridad de la Información”

7.1 CAPACITACIÓN

- Indicador 1
  PCF= (NCR/NCP)*100

  PCF: Porcentaje de Cumplimiento de las actividades de capacitación en temas de TI
  NCR: Número de capacitaciones realizadas
  NCP: Número de capacitaciones programadas

- Indicador 2
  AC= NPC/NPPC
  AC: Asistencia a capacitaciones
  NPC: Número de personas capacitadas
  NPPC: Número de personas programadas a capacitar

7.2 SENSIBILIZACIÓN

- Indicador 3
  PPC= (PCE/PCP) *100
  PPC: Porcentaje de ejecución del Plan de Comunicación
  PCE= Plan de comunicación ejecutada
  PCP= Plan de comunicación planeada

8. DOCUMENTOS DE REFRENCIA

Alcaldia de Cartagena de Indias. (2023). *Instructivo para la Definición Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información.* Cartagena de Indias: Alcaldía de Cartagena de Indias.

Alcaldia de Cartagena de Indias. (2023). *Modelos de Seguridad y Privacidad de la Información.* Cartagena de Indias: Oficina Asesora de Informática.

Alcaldia de Cartagena de Indias. (2023). *Plan de Seguridad de la Información.* Cartagena de Indias: Oficina Asesora de Informática.

Ministerio de las Tecnologías de Información y Comunicaciones. (2016). *Guía para la Implementación de Seguridad de la Información en una MIPYME.* Bogotá: MinTic.

Ministerio de Tecnologias de la Información y Comunicaciones. (2016). *Elaboración de la Política General de Seguridad y Privacidad de la Información.* Bogotá: MinTic.

Ministerio de Tecnologias de la Información y Comunicaciones. (2016). *Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información.* Bogotá: MinTic.

9. CONTROL DE CAMBIOS

FECHA	DESCRICPCION DE CAMBIOS	VERSION
	Elaboración del documento	1.0

10. VALIDACION DEL DOCUMENTO

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre: Luisa Pabón – Marlín Silva **Cargo:** Asesores externos **Fecha:** 04/09/23	**Nombre:** Jasmín Herrera – Diana Manrique **Cargo:** Fecha: Gestor calidad – Asesor externo **Fecha:** **04/09/23**	**Nombre**: Ingrid Paola Solano **Cargo:** Jefe Oficina Asesora de Informática **Fecha:** **04/09/23**