Tabla de Contenido

INTRODUCCIÓN 2

OBJETIVO GENERAL 3

OBJETIVOS ESPECIFICOS 3

ALCANCE 4

GLOSARIO 5

DESCRIPCIÓN GENERAL DEL PLAN DE SENSIBILIZACIÓN, CAPACITACIÓN Y COMUNICACIÓN 7

IDENTIFICACION DE NECESIDADES DE CAPACITACION 7

DESARROLLO DE MATERIALES PARA LAS CAPACITACIONES 9

DESARROLLO DE MATERIAL PARA ENTRENAMIENTO 10

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.

A saber, que el MinTIC motiva a las entidades públicas a utilizar los medios tecnológicos como base principal para el desarrollo de sus actividades cotidianas, y que en consecuencia de lo anterior con el uso y los avances tecnológicos surgen a su vez amenazas y vulnerabilidades asociadas, las cuales pueden llegar a afectar la confidencialidad, la disponibilidad y la privacidad e integridad de la información que manejan las entidades públicas, afectando de manera drástica el desempeño normal de la entidad.

Por lo anterior la Alcaldía de Armenia, a través de la Secretaría TIC, diseño las políticas de seguridad informática de la entidad, como parte del modelo de seguridad y privacidad de la información MSPI. El cual busca que en las entidades se tengan las mejores prácticas de seguridad en el manejo y administración de los activos tecnológicos de las entidades públicas. Sin embargo, un programa o un plan con las mejores prácticas de seguridad y privacidad de la información no se basa únicamente en el aseguramiento de plataformas y procesos, sino que también debe involucrar los factores humanos, que, en muchos casos, son la principal causa de los incidentes de seguridad dentro de un sistema determinado, debido a que no conocen sobre seguridad de la información y su rol dentro de una Entidad.

OBJETIVO GENERAL

Diseñar un plan de capacitación, sensibilización y comunicación del modelo de seguridad y privacidad de la información propuesto por la Secretaría TIC y que aplica a toda la entidad.

OBJETIVOS ESPECIFICOS

- Definir los temas de capacitación en seguridad de la información, de acuerdo con las debilidades y fortalezas de cada secretaria de la Alcaldía de Armenia.

- Evidenciar las debilidades informáticas que presenta la entidad.

- Socializar las políticas de seguridad de la información diseñadas por la Secretaría TIC.

- Lograr que cada funcionario conozca sus roles y responsabilidades de seguridad y privacidad de la información dentro de la entidad

- Evaluar, medir y cuantificar, si las políticas y el plan de sensibilización de seguridad de la información implementados generaron impacto en el desarrollo de las actividades de la Entidad.

- Mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática.

ALCANCE

De acuerdo a la implementación del modelo de seguridad y privacidad de la información MSPI este plan de sensibilización, capacitación y comunicación deberá estar dirigido a los funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general.

El plan de sensibilización, de seguridad de la información, es un programa efectivo
que busca que todos los funcionarios de la entidad cumplan y se capaciten de acuerdo a las mejores prácticas de seguridad de la información mediante actividades, capacitaciones, talleres y socializaciones.

GLOSARIO

Seguridad de la información (SGSI): preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad (Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2006).

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: Condición que garantiza que la información consignada en un documento ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación (Ministerio de Tecnologías de la información y comunicaciones, 2017).

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

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.

Entrenamiento: Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.

Política: Declaraciones de alto nivel que expresan los objetivos a cumplir de la Entidad respecto a algún tema en particular.

Brecha: Se denomina al espacio o ruta a recorrer entre un estado actual y un estado deseado.

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 suplantar la identidad de la víctima.

Amenaza: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Antivirus: Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento de los sistemas de información.

Backups: Es una copia de seguridad de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida o robo.

Servidores: Computador que responde peticiones o comandos de un computador cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

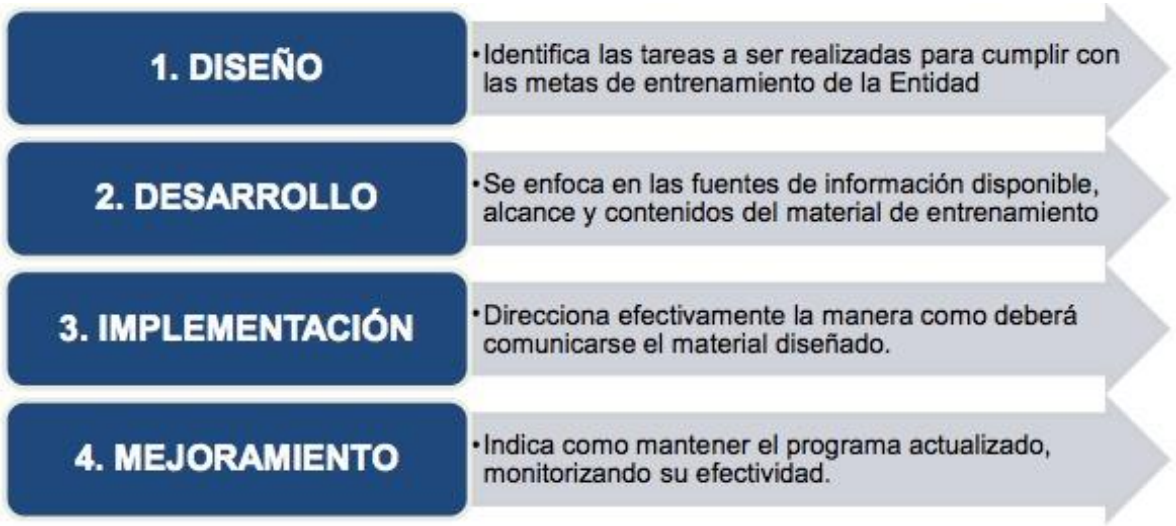
Software: Programas y documentación de respaldo que permite y facilita el uso del pc. El software controla la operación del hardware.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

DESCRIPCIÓN GENERAL DEL PLAN DE SENSIBILIZACIÓN, CAPACITACIÓN Y COMUNICACIÓN

El plan de sensibilización, capacitación y comunicación en seguridad de la información explica de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la Entidad, requiere que sean cumplidos por parte de todos los usuarios del sistema. Cualquier incumplimiento a las políticas, 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, un plan de capacitación, sensibilización y comunicación adecuado, debe llevarse a cabo con base a las siguientes 4 fases:



IDENTIFICACION DE NECESIDADES DE CAPACITACION

La mayoría de las vulnerabilidades provienen desde el interior de las propias empresas (empleados descontentos, fraude interno, accesos no autorizados, poca motivación, carencia de entrenamiento organizacional y desconocimientos de las políticas de seguridad), es por eso que desde la secretaría TIC de la alcaldía de Armenia, se propone realizar una identificación de los problemas más comunes que supone la seguridad de la información en la entidad; Con esto se pretende plantear en la siguiente etapa de este plan, capacitaciones orientadas a las necesidades más importantes que tienen los funcionarios de la Alcaldía de Armenia.

Problemas más comunes en las organizaciones son los siguientes:

- Uso inadecuado de las contraseñas de los equipos, correos electrónicos y demás aplicativos que se emplean en la entidad.

- Mal uso del internet, no existe conciencia sobre mejores prácticas a la hora de navegar en la web.

- Mal uso del correo electrónico empresarial, el cual es utilizado muchas veces para actividades personales e inscripción en páginas web de dudosa procedencia.

- Falta control de acceso a sitios restringidos para las personas, se evidencia muchas veces fácil acceso a computadores de funcionarios públicos.

- Uso inadecuado de dispositivos USB, como discos duros, memorias, etc.

- Copias de seguridad de los equipos de cómputo de los funcionarios, que respalden la información contra perdida o daños.

- Falta de capacitación y sensibilización de la política de escritorio limpio y pantalla limpia en los equipos de los funcionarios.

A estas malas prácticas y/o problemas más comunes se deberán agregar las identificadas en el diagnóstico que deberá realizar la secretaría TIC a la alcaldía de Armenia.

Roles y necesidades en capacitación más comunes

SECRETARIOS DE DESPACHO Y SUBSECRETARIOS, DIRECTORES, ENTRE OTROS DE LA ALCALDÍA DE ARMENIA	Deben conocer y entender las leyes y directivas que forman la base del programa de seguridad, también deben comprender el liderazgo que su rol tiene y que son el ejemplo a seguir de todas las demás unidades.
SECRETARIA TIC Y PERSONAL ENCARGADO DE LA SEGURIDAD DE LA INFORMACION	Son los asesores expertos en seguridad, deben estar bien preparados en políticas de seguridad y buenas prácticas
FUNCIONARIOS QUE TRABAJAN CON EQUIPOS DE LA ENTIDAD	Deben entender bien las políticas de seguridad, así como también conocer sobre los controles de seguridad y la relación que tienen con los sistemas que manejan.

ADMINISTRADORES DE SISTEMAS Y PERSONAL DE SOPORTE	Estos funcionarios deben tener un buen nivel de preparación a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del Entidad de manera apropiada.
USUARIOS FINALES	Requieren de un alto grado de sensibilización sobre la seguridad y las reglas de comportamiento adecuadas con los sistemas que tienen a disposición.

DESARROLLO DE MATERIALES PARA LAS CAPACITACIONES

El desarrollo/adquisición/recopilación de los materiales debe basarse en 2 premisas:

1. ¿Qué comportamiento se desea reforzar? (Sensibilización).
2. ¿Qué habilidades es necesario que sean aprendidas y aplicadas por los usuarios? (Entrenamiento).

Cabe aclarar que la sensibilización es algo que aplicará para toda la Entidad por igual. Todos los empleados deben ver la información entregada de sensibilización como una responsabilidad compartida en seguridad de la información y que todos son importantes en esa labor.

Entre los temas más importantes de sensibilización se encuentran los siguientes, aunque de acuerdo a las necesidades identificadas puede variar la cantidad:

1. Manejo responsable del internet, riesgos asociados.
2. Seguridad en redes wifi privadas y públicas.
3. Uso adecuado del correo electrónico empresarial, redes sociales y aplicativos misionales de la entidad.
4. Manejo adecuado de contraseñas.
5. Copias de seguridad y su importancia para dar continuidad a las actividades a causa de pérdida o daño del equipo de cómputo.
6. Software permitido y no permitido en la entidad
7. Ingeniería social.
8. Protección contra los virus.
9. Sanciones por incumplimiento de las políticas.
10. Gestión de incidentes (que reportar, donde puedo reportar).
11. Spam.
12. Seguridad En El Puesto De Trabajo.
13. Politicas de seguridad y privacidad de la información de la entidad.

DESARROLLO DE MATERIAL PARA ENTRENAMIENTO

Para desarrollar el material de entrenamiento pueden emplearse los siguientes métodos (debe considerarse una relación de costo-beneficio con cada uno):

Letreros y Afiches

Ten CUIDADO con los MENSAJES de ***TEXTO*** que recibes en tu celular

Podrían ser una **ESTAFA**

SECRETARÍA TIC | ESPA TODOS Alcaldía de Armenia

Fondos de Pantalla de equipos

ESPA TODOS Alcaldía de Armenia

Recuerda que los equipos de la Administración Municipal se bloquean cada cinco (5) minutos de tiempo de inactividad, lo anterior con el fin de evitar accesos no autorizados de personas ajenas a la entidad en el equipo de cómputo.

SECRETARIA TIC | ESPA TODOS Alcaldía de Armenia — Campaña de la Secretaría TIC, como parte de las políticas de seguridad y privacidad de la información de la Alcaldía de Armenia

Folletos

POLÍTICAS DE SEGURIDAD INFORMATICA

Las políticas de seguridad informática de la Alcaldía de Armenia, son un conjunto de buenas practicas que aseguran la integridad y confidencialidad de la información que se maneja en la entidad

A QUIEN VA DIRIGIDAS?

Funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general

Las políticas de seguridad informática y controles serán de obligatorio cumplimiento para todos los servidores públicos de planta, contratistas y terceros que hagan uso de los activos de la Administración Municipal..

Las excepciones al cumplimiento de las políticas de seguridad informática serán autorizadas única y exclusivamente por la Secretaría TIC .

QUE PRETENDEN?

- 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.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Alcaldía de Armenia.
- Garantizar la continuidad del negocio frente a incidentes.

A QUIEN CONTACTAR SI OCURRE UN INCIDENTE

•Secretaría TIC

•Teléfono: (036) 741 7100 ext: 224

•A través de la mesa de ayuda

SECRETARIA TIC | ESPACIO TODOS Alcaldía de Armenia

Seguridad Informática

POLÍTICAS DE SEGURIDAD INFORMATICA

Las políticas de seguridad informática de la Alcaldía de Armenia, son un conjunto de buenas practicas que aseguran la integridad y confidencialidad de la información que se maneja en la entidad

A QUIEN VA DIRIGIDAS?

Funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general

Las políticas de seguridad informática y controles serán de obligatorio cumplimiento para todos los servidores públicos de planta, contratistas y terceros que hagan uso de los activos de la Administración Municipal..

Las excepciones al cumplimiento de las políticas de seguridad informática serán autorizadas única y exclusivamente por la Secretaria TIC .

QUE PRETENDEN?

- 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.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Alcaldía de Armenia.
- Garantizar la continuidad del negocio frente a incidentes.

A QUIEN CONTACTAR SI OCURRE UN INCIDENTE

•Secretaria TIC

•Teléfono: (036) 741 7100 ext: 224

•A través de la mesa de ayuda

SECRETARIA TIC | ESPACIO TODOS Alcaldía de Armenia

Elaborado por:	Revisado por:	Aprobado por:
COMITÉ OPERATIVO	**Gonzalo Garzón Diaz** Enlace	**Giovanny Zambrano Londoño** Líder del Proceso