Conceptos de políticas de seguridad informática

Contenido

Lista de figuras

Introducción

En este material, se abarcarán las Políticas de Seguridad Informática (PSI) o también conocidas como Plan de Acción de Seguridad Informática, tema de gran importancia para el abordaje del programa, porque es donde se aplicará el conocimiento adquirido en el desarrollo del mismo, elaborando un plan de acción, el cual protegerá la información de la empresa.

Mapa conceptual

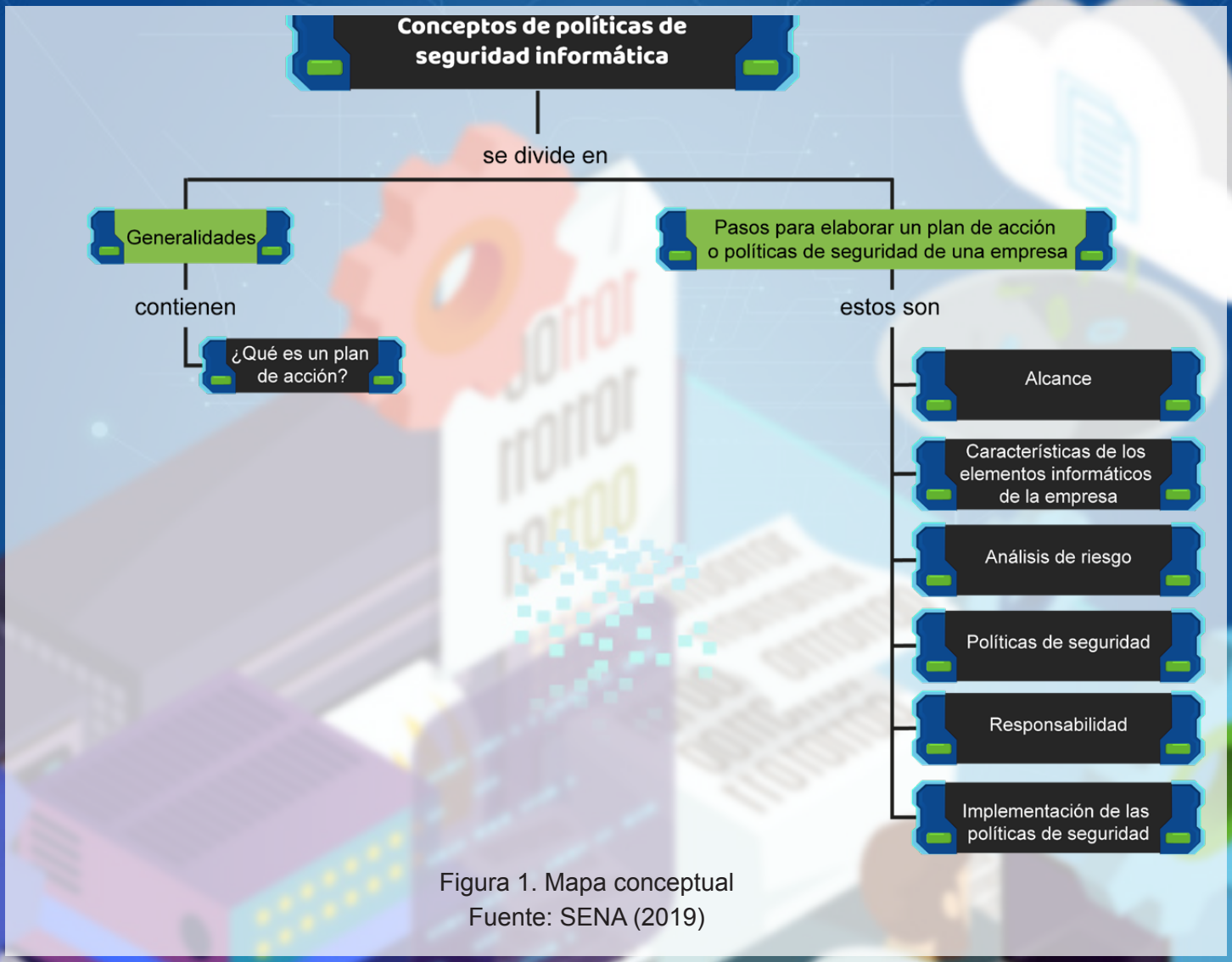


Figura 1. Mapa conceptual
Fuente: SENA (2019)

1. Generalidades

1.1 ¿Qué es un plan de acción?

Los nuevos advenimientos han generado, en los profesionales de las tecnologías informáticas, una gran preocupación por disminuir las amenazas frente a los ataques y proteger la información de las organizaciones. Es verdad que la tecnología de punta ha acelerado los sistemas de manera ágil y eficaz, pero así mismo, los ha vuelto vulnerables frente a los riesgos de los posibles ataques, los cuales pueden dañar las bases de datos de información de las redes de tecnología de la empresa. Por lo tanto, es importante establecer los controles adecuados para brindar protección a la privacidad de los archivos de información que se transmiten. Los planes de acción también se denominan Plan de Seguridad Informática o Políticas de Seguridad Informática (PSI) y estas se definen como los controles que se implementan en una empresa para garantizar el buen flujo de datos de información. Su objetivo es garantizar que la información de la empresa esté protegida tanto en la parte de *hardware* (equipos de cómputo y redes), de *software* (sistemas operativos y aplicativos de uso exclusivo de la empresa y ofimáticos) y de los usuarios que se encuentran implicados en el uso diario de estos.

2. Pasos para elaborar un plan de acción o políticas de seguridad de una empresa

Las Políticas de Seguridad Informática (PSI) se elaboran teniendo en cuenta los siguientes pasos:

2.1 Alcance

Figura 2. Alcance
Fuente: SENA (2019)

En esta primera etapa, se determina exactamente cuál será la organización a la que se le aplicarán dichas políticas de seguridad, teniendo en cuenta que cada empresa maneja su propia base de datos de información y es sobre esta que se establecen los posibles riesgos informáticos. En esta etapa también se deben considerar a todos los usuarios que manejan la base de información de la empresa.

Ejemplo de un alcance

Este Plan de Seguridad Informática (PSI) está elaborado exclusivamente para la empresa (se plantea el nombre de la empresa, la ciudad donde funciona y su dirección). Las políticas establecidas en este documento deben ser de carácter obligatorio para todas las dependencias de la empresa, al momento de acceder a la información.

2.2 Características de los elementos informáticos de la empresa

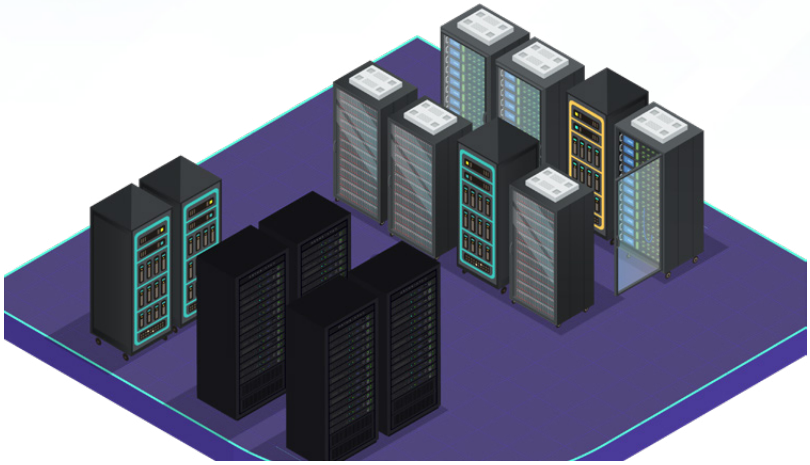


Figura 3. Equipos de computo
Fuente: SENA (2019)

Se recomienda realizar una revisión detallada de todos los elementos informáticos que se encuentran instalados e identificar en qué oficina se hallan, esto con el fin de precisar cuál es la función y la información que se maneja. Así, se podrán priorizar los niveles de seguridad que cada usuario y equipo debe tener al momento de elaborar un PSI.

Ejemplo

La red instalada en la empresa (nombre de la empresa) es de tipo (nombre del tipo de red) y está compuesta por (número de equipos con sus características, la dependencia en que están instalados y la información que manejan); los funcionarios y las dependencias de la empresa son (nombres de los funcionarios y de las dependencias) y cada uno de ellos maneja información de tipo (descripción de la base de información que se maneja).

2.3 Análisis de riesgo

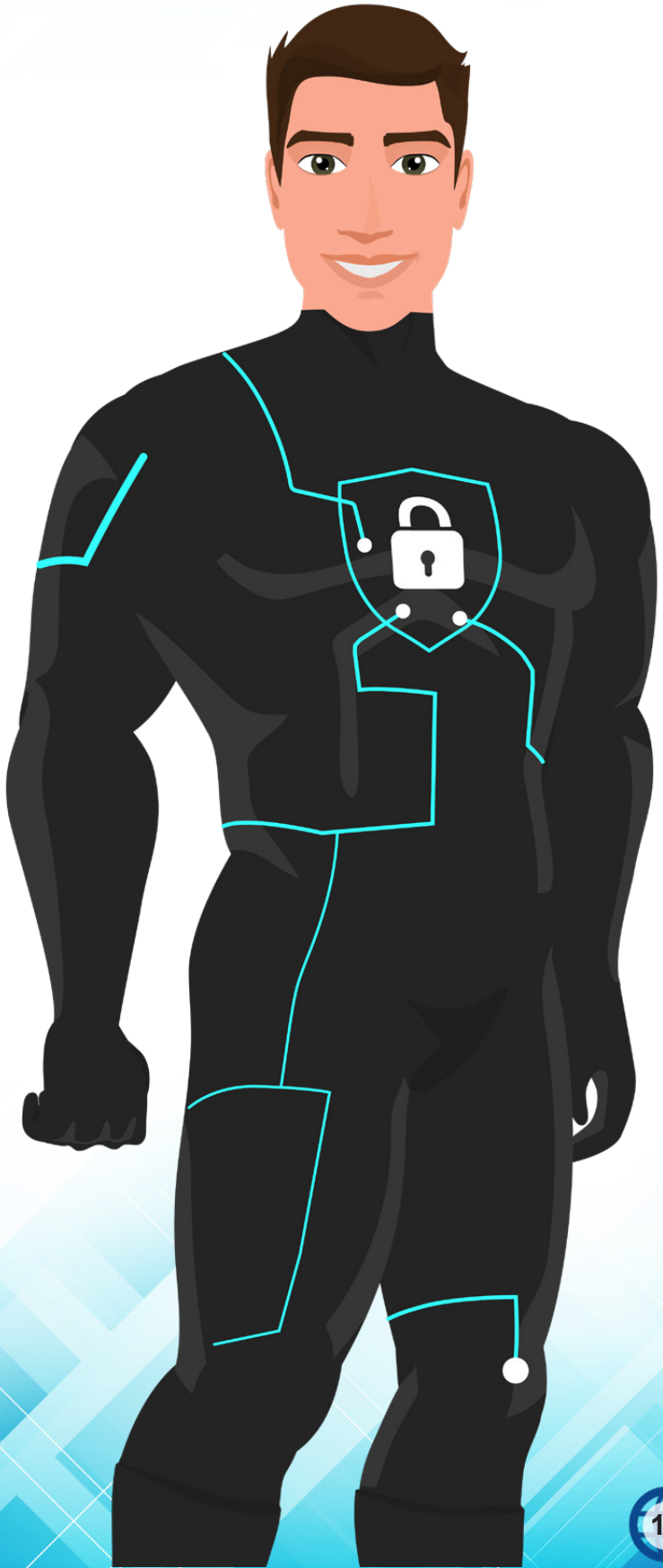
Figura 4. Riesgos
Fuente: SENA (2019)

Con el análisis obtenido de los temas estudiados anteriormente, se podrán definir las dependencias de la empresa a las cuales se debe proteger la información de manera prioritaria. De igual forma, se debe analizar cuál es la dependencia que maneja la información más importante, cuál sería la amenaza más impactante para dicha información, cuál sería el daño ocasionado al momento de un ataque informático y cuáles serían las dependencias afectadas.

Ejemplo

- La red de información es una de las partes principales que se debe proteger al momento de establecer las políticas de seguridad.
- Los servidores donde se hacen los *backup* de seguridad también deben tener un capítulo especial en un Plan de Seguridad Informática.

2.4 Políticas de Seguridad Informática



En este paso se deben establecer los controles y procedimientos que se van a tener en cuenta para proteger la información, e indicar las condiciones que cada usuario de la empresa como administrador de la información de acuerdo con su dependencia, debe determinar para no poner en riesgo la base de información.

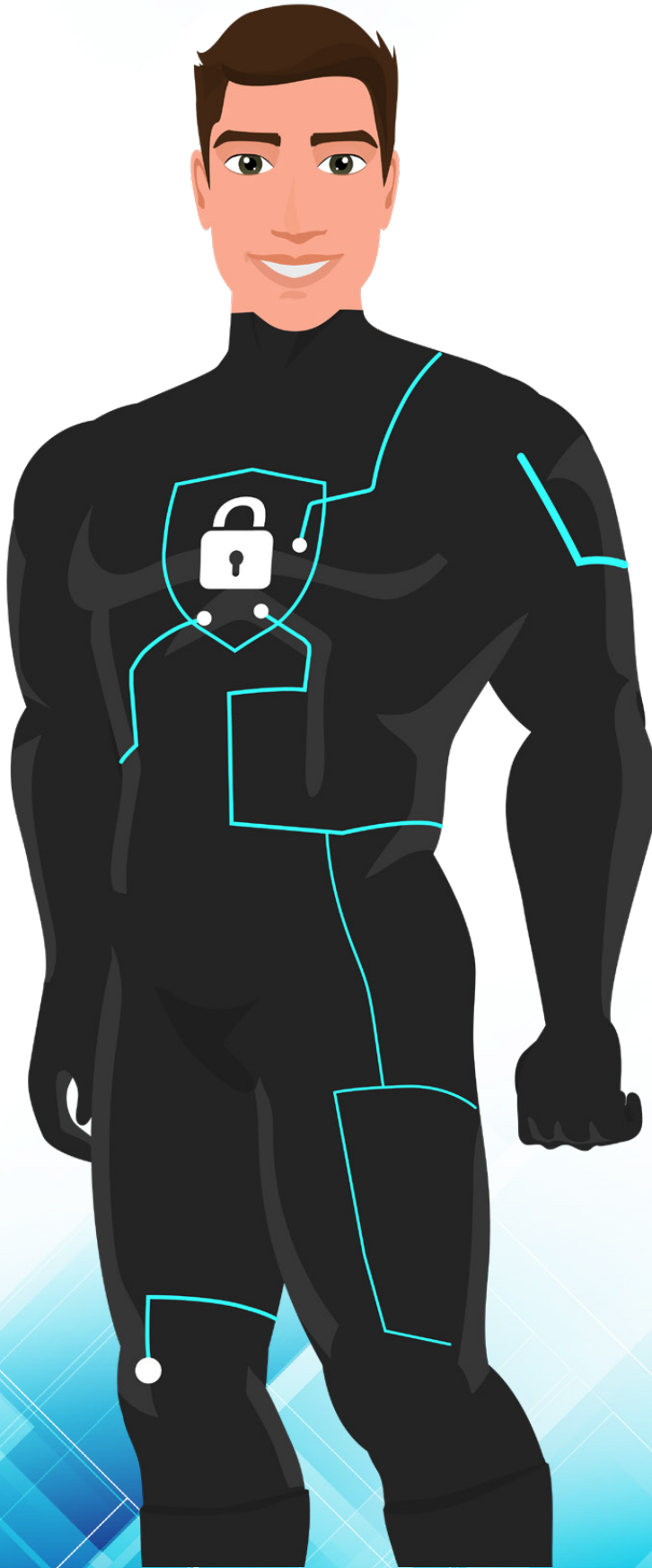
Las PSI se deben cumplir de forma general en la empresa, ya que son obligatorias en todas las dependencias en las que se tenga acceso a los datos.

Ejemplo

El plan de acción que se puede implementar sobre los equipos de cómputo de la empresa es: establecer cronogramas de mantenimientos preventivos, limpieza interna y externa, revisión de instalaciones eléctricas reguladas y de instalaciones de corrientes hidráulicas; para evitar afectaciones en la información.

2.5 Responsabilidad

Es la asignación de atributos y permisos que se le generan a cada usuario para administrar la base de datos de la información. De esta manera, el administrador de la red tecnológica debe tener conocimiento de las funciones que tiene cada usuario en la dependencia, con el fin de establecer las PSI más adecuadas para la misma.



Ejemplo

El administrador de la red tecnológica de la información llevará el control y el seguimiento, para garantizar el estricto cumplimiento de las políticas establecidas, como por ejemplo, el registro de ingreso y cierre de sesiones de los usuarios.

2.6 Implementación de las Políticas de Seguridad Informática

Al momento de implementar las PSI se debe tener en cuenta puntos claves donde se identifique que la información es más vulnerable, para generar controles en esos aspectos.

Algunos de los elementos a considerar para la implementación de las PSI son los siguientes:

Protección del disco duro

El disco duro es la parte del computador donde reposa toda la información, en este sentido es una de las partes que hay que proteger. Su vulnerabilidad frente a los riesgos es alta, por lo tanto se deben establecer políticas de seguridad, como por ejemplo: realizar copias de seguridad periódicamente, controles sobre el debido manejo de encendido y apagado del mismo, establecer contraseñas para el acceso a la información, entre otros.

Figura 5. Disco duro
Fuente: SENA (2019)

Memorias USB y discos externos

Al momento de usar herramientas como USB y discos extraíbles se debe, en lo posible, generar controles para el acceso a estos elementos dentro de la CPU, bloqueando los puertos, para que el usuario tenga que solicitar autorización para su uso. El administrador de la información será el encargado de autorizar la conexión de estos, haciendo un saneo de las unidades USB y habilitando los puertos para su instalación a la CPU. Este sería un control efectivo frente al uso de estos recursos.

Figura 6. Memoria USB
Fuente: SENA (2019)

Figura 7. Antivirus
Fuente: SENA (2019)

Antivirus

Aplicativos lógicos que se ejecutan al momento de detectar un virus que puede atacar la información. Se debe establecer un plan de acción para que este antivirus se encuentre licenciado y garantice su actualización diaria.

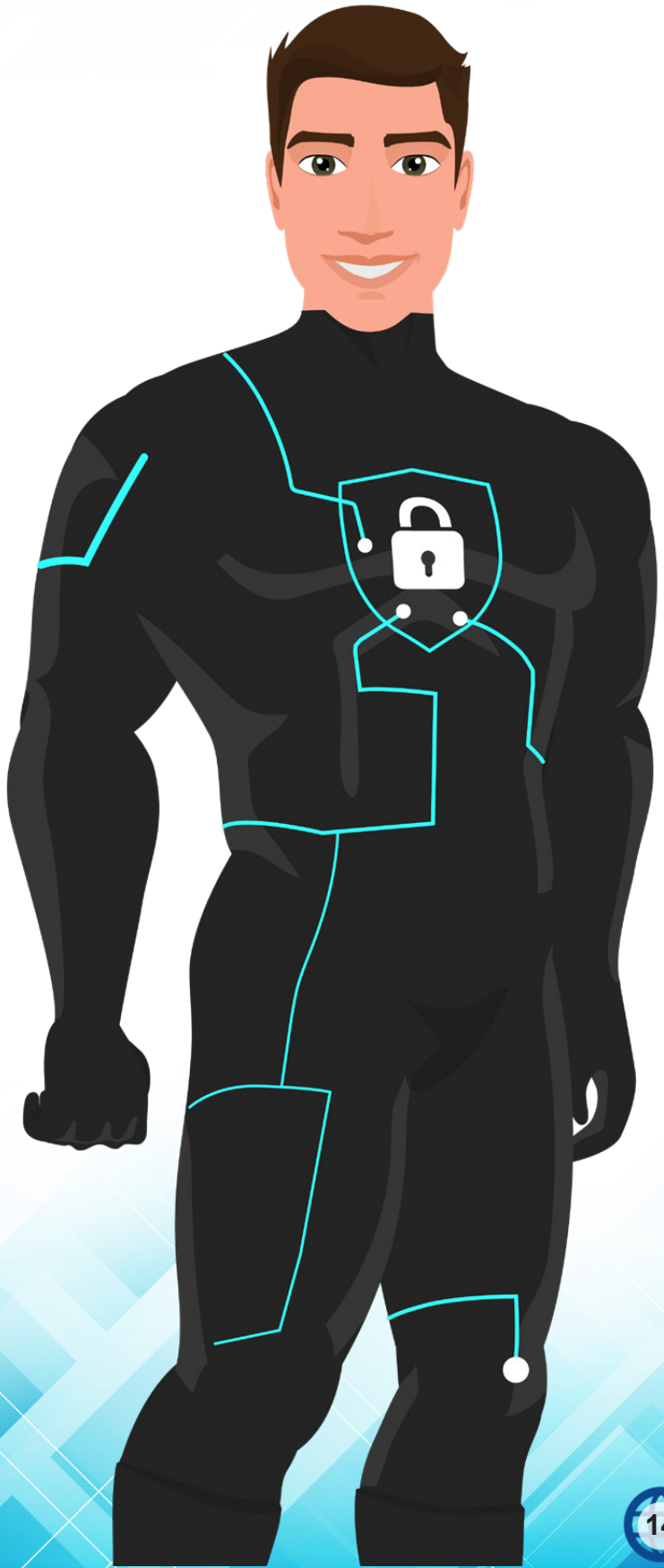


Figura 8. Contraseña
Fuente: SENA (2019)

Contraseñas seguras

Es importante proteger el acceso a la base de datos de información. Desde el mismo momento que se enciende el computador se requiere tener control de contraseñas o claves de usuario. Estas deben poseer políticas especiales, como por ejemplo: usar mínimo ocho caracteres; usar al menos una mayúscula, una minúscula y algún carácter especial (* - _ .); y se recomienda ser cambiada periódicamente. Estos controles de políticas de seguridad ayudan a evitar los ataques informáticos.

Referentes bibliográficos

Ministerio de ambiente y desarrollo sostenible. (s.f.). *Política de seguridad informática*. Recuperado de http://www.minambiente.gov.co/index.php/tecnologias-de-la-informacion-y-la-comunicacion/gestion-ti/politica-de-seguridad-informatica

Secretaría de TIC, Ciencia, Tecnología e Innovación. (2013). *Políticas de seguridad informática de la gobernación del Meta*. Recuperado de https://www.meta.gov.co/web/sites/default/files/adjuntos/M-TIC-01%20POLITICA%20SEGURIDAD%20V3.pdf

Tuyú Technology. (2017). *¿Por qué es tan importante la seguridad informática?* Recuperado de www.tuyu.es/importancia-seguridad-informatica/

Créditos

Gestor del proceso de recursos digitales

Juan Bautista Londoño Pineda

Responsable de producción y creación

Jhoana Andrea Vásquez Gómez

Evaluador de calidad instruccional

Erika Alejandra Beltrán Cuesta

Desarrollador de contenidos

Olga Elena Meneses Camino

E-pedagogo instruccional

Juan Carlos Ramírez Molina

Evaluador de contenidos

Lina Marcela Cardona Orozco

Creativo de recursos didácticos

Cristian Andrés Osorio Caiza

Carlos Andrés Díaz Botero

Carolina Ramírez Martínez

Melissa Ochoa Alvarado

Desarrollador Full-Stack

Daniel Enciso Arias

Francisco José Lizcano Reyes

Luis Felipe Zapata Castaño

Luis Gabriel Urueta Álvarez

Germán Alberto Rodríguez Lievano

Leyson Fabián Castaño Pérez

Centro Agroindustrial - Regional Quindío

Centro Agropecuario - Regional Risaralda

2019