Lectura 3

Recomendaciones para proteger tu información

Mantenga su software actualizado. Cualquiera que sea el sistema operativo, navegador u otro software que use, manténgalo actualizado. Configúrelos para que se actualicen automáticamente de modo de no dejar ningún hueco abierto que los piratas informáticos pudieran aprovechar.

Haga copias de seguridad de sus archivos. No hay ningún sistema completamente seguro. Cree copias de seguridad (*back up*) fuera de línea de los archivos importantes. De ese modo, podrá seguir accediendo a sus archivos si su computadora sufre un ataque.

Use contraseñas sólidas. Cuanto más extensas mejor – al menos 12 caracteres. La complejidad también ayuda a fortalecer una contraseña. Combine números, símbolos y letras mayúsculas en el medio de la contraseña, no al principio o al final. No use un mismo patrón para prolongar una contraseña. Nunca use la misma contraseña para más de una cuenta o para cuentas personales y comerciales. Si las anota, guárdelas en un lugar seguro. Considere la posibilidad de usar un administrador de contraseñas, una aplicación de fácil acceso que le permite almacenar todas sus contraseñas en un solo lugar. Asegúrese de proteger su administrador de contraseñas con una contraseña maestra sólida, y solo use un administrador de contraseñas de una compañía de buena reputación. No comparta las contraseñas por teléfono, mensajes de texto ni por email.

Active un sistema de doble autentificación. Para iniciar la sesión en una cuenta habilitada para el sistema de doble autentificación hay que ingresar la contraseña y otro dato adicional. El segundo dato podría ser un código enviado a su teléfono o un número generado por una aplicación o por un dispositivo o token de seguridad. Esto protege su cuenta aunque se haya comprometido su contraseña.

No deje su computadora portátil, teléfono u otros aparatos sin vigilar en lugares públicos, ni siquiera en un carro cerrado. Estos aparatos pueden contener información delicada – y también resulta costoso reemplazarlos. Si desaparecen, la información almacenada puede caer en manos de ladrones de identidad. También puede activar la codificación del aparato para cifrar todos los datos de cada aparato. Esto reduce el riesgo para la información delicada en caso de que le roben o pierda su aparato.

Proteja todos sus aparatos con contraseñas. Si accede a la red de su negocio desde una aplicación instalada en su teléfono o tablet, use también una contraseña sólida para esa aplicación.

PIENSE ANTES DE COMPARTIR SU INFORMACIÓN

Proteja la información de las cuentas. *Cada vez* que alguien le pida información de su negocio – ya se por email, mensaje de texto, llamada telefónica o formulario electrónico – piense si realmente puede confiar en ese pedido. Los estafadores dirán o harán cualquier cosa – o se harán pasar por cualquiera – para conseguir números de cuentas y de tarjetas de crédito, números de Seguro Social u otras credenciales. Los estafadores lo apurarán, presionarán o amenazarán para conseguir que les dé información de su compañía.

Transmita información delicada únicamente a través de sitios web codificados. Si en su compañía hacen trámites bancarios o compras en internet, limítese a usar sitios que usen codificación para proteger la información que viaja desde su computadora al servidor del sitio. Busque las letras **https** al principio del domicilio web en la barra de su navegador. Fíjese que las letras https aparezcan en todas las páginas del sitio que visite, no solamente cuando inicia la sesión.

DEFINICIÓN DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA

¿Que son las normas de seguridad? • Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red institucional.

¿Que son las políticas de seguridad?

Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

BENEFICIOS

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC´s) en la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge – CVS.

Referencia bibliográfica

Lectura 3

Comisión Federal de comercio. (2017, 2 mayo). Conceptos básicos sobre seguridad informática para pequeños negocios. Recuperado 27 octubre, 2018, de https://www.ftc.gov/es/consejos/para-empresarios/conceptos-basicos-sobre-seguridad-informatica-para-pequenos-negocios