**Objetivo:** Informar a organizaciones sobre medidas que pueden tomar para aumentar la seguridad de sus sistemas de información, computadoras y de red



El avance de la tecnología de la información ha hecho que administrar una pequeña empresa sea más fácil que nunca, pero su organización, así también como sus clientes y su información pueden estar en riesgo a menos que ponga las medidas de seguridad cibernética apropiadas.

**Las mejoras prácticas de seguridad cibernética**

* **Realice una auditoría inicial** para determinar las exposiciones potenciales de su organización así también como para establecer un plan de acción para identificar e implementar los controles apropiados.
* **Establezca políticas escritas** que detallen las protecciones de seguridad cibernética de su compañía, incluyendo temas como protocolos de contraseñas, lineamientos para el uso de internet, control de la información del cliente y penalidades por violación de esta política.
* **Mantenga el hardware y el software actualizado** para disminuir el riesgo de los últimos malwares y otras amenazas a la seguridad.
* **Asegure su conexión a internet,** mediante medidas que incluyan la implementación de un cortafuegos y asegurándose que las señales de Wi-Fi estén aseguradas y cifradas.
* **Administre el acceso de los empleados** al internet o a la información de los clientes mediante la creación de identificaciones protegidas por contraseñas para todos los empleados y solo permitirles el acceso necesario a los sistemas para que cumplas con su trabajo.
* **Mantenga separados los sistemas para pagos** de otros sistemas potencialmente menos seguros.
* **Trabaje con bancos** para asegurarse de que los sistemas y servicios de pago que tiene sean seguros y confiables.
* **Haga regularmente copias de seguridad de la información vital**, incluyendo documentos internos e información de los clientes.
* **Almacene las copias de seguridad en otro lugar,** ya sea en una locación remota o en la nube.
* **Implemente medidas de seguridad físicas,** como mantener el equipamiento de red, los servidores y otro hardware cerrado bajo llave o en áreas de acceso restringido.
* **Asegure los dispositivos móviles** obligando a que lleven contraseña e instalando sistemas confiables de seguridad y anti fraude.
* **Obligue a los empleados a cambiar sus contraseñas** en intervalos regulares, y considere implementar sistemas de autenticación multifactoriales.

Este formulario documenta que la capacitación anterior fue presentada a los participantes enumerados. Al firmar a continuación, cada participante reconoce haber recibido esta capacitación.

Organización: Fecha:

Capacitador: Firma del capacitador:

**Participantes de la clase:**

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma:

Nombre: Firma: