



Preguntas Frecuentes de Seguridad



¿Qué es la seguridad informática?

Es una disciplina científica encargada de identificar riesgos e implantar las medidas de seguridad requeridas para mitigar los efectos de posibles ataques sobre bienes informáticos.

¿Porqué la seguridad informática afecta de alguna manera a todos?

En el mundo actual y globalizado , prácticamente todos tenemos información personal almacenada de manera electrónica en algún lugar: por ejemplo, un numero de identidad (RFC), información confidencial como datos del padrón electoral, cuentas bancarias, etc. Esta información electrónica es un activo que debe ser protegido.

¿Porqué es importante el tema de la seguridad para las organizaciones?

Las empresas y organizaciones deben atender su negocio, siendo conscientes del nivel de riesgo de sus activos y administrándolo. Además, deben proteger la información de sus clientes, por ética, por salud de su negocio o por disposiciones legales y normativas.

¿Es la seguridad un tema solo de tecnología?

No. Es de cultura, tecnología y buenas prácticas de usuarios. El eslabón más débil en la cadena de seguridad de un sistema es el usuario.

¿Es insegura Internet?

Si, mucho. Pero es también el medio mas poderoso para efectuar negocios. Así que hay que aprender a tomar sus beneficios, disminuyendo el riesgo de manera inteligente.

¿Son inseguras las redes empresariales?

El universo de atacantes es diferente. Las redes empresariales tienen atacantes internos, a veces de manera inconsciente. La diferencia es que los activos más valiosos de una organización viven en la red interna, así que deben ser protegidos de manera diferente, de manera integral y no mediante piezas aisladas de tecnología.

¿Tiene solución el tema de la seguridad?

El tema de seguridad es un tema de administración del riesgo. Las organizaciones, como las personas, deben aprender a administrar el riesgo. Nunca se elimina del todo, hay que vivir con un nivel que sea tolerable. Por tal razón, no existe el concepto de un sistema completamente seguro.

¿Cómo administro el riesgo en seguridad?

Mediante la cultura de los usuarios, la adopción de buenas prácticas informáticas y la implantación de tecnología, todo en procesos vivos que hay que administrar. El tema de seguridad no se resuelve de una vez y para siempre. Un activo debe protegerse de manera que la inversión ejercida en él sea equiparable al beneficio obtenido en relación al valor de la información que éste posee.

¿Qué son los hackers informáticos?

La palabra hacker, en un principio, se refería al experto en programación cuya meta era compartir sus conocimientos y experiencias con otros hackers. Actualmente, aplicamos este distintivo a todos aquellos que realizan piratería informática y delitos en Internet, cuando en realidad deberíamos decir crackers. La finalidad de estos últimos, es causar el mayor daño posible y robar información para uso propio en computadoras personales o redes empresariales.

¿Hay hackers en México, o de dónde son?

Si. Existen hackers éticos y no éticos. Los primeros son profesionales de la seguridad y los segundos son piratas informáticos.

¿Cuáles son las formas de ataque informático más comunes?

Los más conocidos son:

- a) Robos de identidad para fraudes bancarios mediante ataques de phishing.
- b) Alterar el contenido de las paginas de sitios web de organizaciones (recordemos los recientes casos de la pagina de López Obrador o ataques a instituciones de gobierno).
- c) Propagación de código maligno al interior de las redes de las organizaciones: virus, gusanos, troyanos, etc.

Últimamente los ataques se han sofisticado, buscando obtener un claro beneficio económico por parte del atacante, mediante extorsiones, transacciones

fraudulentas, etc. Los ataques en muchos casos pueden ser conducidos por organizaciones criminales.

¿Porqué se ha incrementado el poder de los ataques en los años recientes?

Hay varios factores:

1. Cada vez es más fácil conseguir herramientas en Internet de uso sencillo y con un poder mayor de daño.
2. Las redes y sistemas de las organizaciones cada día son mas complejas. La complejidad implica mayor inseguridad.
3. Beneficio económico para el atacante. Por ejemplo, Internet se utiliza mucho para conducir transacciones bancarias en línea y es un terreno fértil para el fraude.
4. El anonimato y los alcances de Internet. El atacante puede estar en China o al otro lado del mundo utilizando algún servidor comprometido de alguien mas en Australia o en Brasil.

¿Cuáles son las implicaciones legales de los ataques informáticos en México?

Aunque la legislación en México esta retrasada en este sector, algunas de las formas en que puedes incurrir en faltas legales son:

1. Existen las leyes de propiedad intelectual y delitos informáticos que pueden ser violadas.
2. Delitos que persigue la unidad de policía informática de la PFP, como pornografía infantil, venta de drogas y armas, piratería, etc.
3. Falta de cumplimiento a normativa. Ejemplo, Nueva Ley de Mercado de Valores, disposiciones de CNBV, Sarbanes-Oxley para las empresas publicas estadounidenses, etc. Esto puede significar robo de información confidencial, robo de números de tarjetas de crédito, y por consiguiente multas por incumplimiento de dicha normativa.
4. Tus computadoras pueden ser usadas para atacar algún otro sitio , lo que significa responsabilidad legal para tu organización o tu persona, etc.

De hecho, ya existe la figura del abogado cibernético encargado de atender estos temas

¿De qué manera una organización puede abordar el tema de la Seguridad ?

1. Medir el nivel de Riesgo.
2. Plantear una estrategia de administración del riesgo.
3. Definir políticas de seguridad e Implantarlas en la organización.
4. Cultura al usuario.

5. Administrar de manera continua los procesos de seguridad.

¿Existe una solución única a la seguridad informática?

No, cada quien debe resolverla a la medida de sus necesidades.

¿Quiénes son o deberían ser responsables de la seguridad en una organización? La seguridad empieza con los directivos. Ellos tienen que fomentar la cultura de seguridad a toda la organización, aunque la seguridad compete a todos. De hecho, en la normativa estadounidense para empresas públicas, la alta dirección es responsable de la seguridad en la organización y la falla en su cumplimiento puede significarle responsabilidades civiles y hasta criminales.

¿Son seguras las denominadas redes inalámbricas o wireless?

Recordemos que no existe la seguridad total en ningún sistema. Pero si es posible hacer una red inalámbrica tan segura como una red cableada.

¿Cómo puedo asegurarme yo de que mi banco tiene medidas de seguridad implantadas que me protejan?

Cada banco es responsable de administrar el nivel de riesgo de sus clientes y hay metodologías para conducir este proceso. Los usuarios a su vez deben de cumplir su parte de mejores prácticas, cultura de seguridad y tecnología en sus computadoras.

¿Es seguro comprar en Internet?

Es difícil de generalizar. Yo preguntaría...Es seguro pagar con tarjeta de crédito en un restaurante? La respuesta es que depende del restaurante. Hoy por hoy, es tan peligroso que un mesero se lleve tu tarjeta en un restaurante no confiable como comprar en un sitio de dudosa reputación. Una buena idea es documentarse acerca de la tienda virtual en Internet mismo.

¿Cómo me puedo proteger?

Obedeciendo tres principios básicos:

- Cultura informática.
- Tecnología (antivirus, firewalls, anti spyware, etc).
- Procesos de administración (parches de seguridad periódicos, actualización de antivirus, etc).

¿Qué es un fraude informático?

Un ejemplo es la realización de una transacción bancaria efectuada en mi nombre sin mi consentimiento, afectando mi patrimonio.

¿Esos ataques pasan en México o solamente en otros países?

Pasan todos los días en México y en todo el mundo.

¿Cuál es el valor que NextiraOne aporta a sus clientes en materia de Seguridad?

NextiraOne proporciona tranquilidad a sus clientes, adecuando el nivel de riesgo a sus necesidades y permitiéndoles atender su negocio, no temas de tecnología. Con nuestra experiencia en redes, diseñamos e implantamos redes seguras, mitigando las amenazas desde la red misma, concibiendo la seguridad como una arquitectura y agregando servicios cuyo fin es de administrar la seguridad como un proceso.