

Charla BarCamp 2009:

Información Segura Para Todos

Versión: 1.0

Fecha: 31/10/2009

Autor: Matias Katz



mkit | Soluciones
Informáticas
www.mkit.com.ar | info@mkit.com.ar

En las próximas páginas mostraremos una serie de medidas simples y efectivas para preservar al máximo la seguridad de nuestra información.

Se discutirán 4 temas principales:

- Passwords
- Encriptación
- Limpieza y Orden
- Redes Sociales

Los passwords son la medida de seguridad mas económica y simple que existe, por ende representan la medida menos efectiva.

El mejor remedio para combatir esta ineffectividad es la implementación de un control que otorgue el mayor provecho de la tecnología.

Simple metodologías de uso y mantenimiento de los passwords personales de cada uno nos brindarán un incremento significativo de la seguridad de la información que tengamos protegida a través de su uso.

- Passwords Largos: La cantidad mínima recomendable es de 7 caracteres, pero cuantos mas largo sea, mas seguro será.
- Caracteres Complejos: Combinar letras, mayúsculas, números y símbolos dentro de nuestra cadena de passwords incrementan su seguridad en un 1000%
- Passphrases: Una alternativa al uso de passwords complejos y largos es la implementación de frases completas como contraseña.

- Passwords sin relación: No utilizar dentro del password cadenas de texto que contengan datos personales ni información que sea posible de adivinar o averiguar.
- Passwords únicos: Cada perfil y recurso debería estar protegido por un password único, independiente, y sin relación con otros usados.
- Cambio de Password: El password debería ser cambiado mensual o bimestralmente, sin repetir los últimos 5 usados.

La encriptación es el proceso de securización de diferentes tipos de recursos gracias a la codificación constante de sus contenidos.

Esta técnica se puede aplicar a conexiones Web, computadoras y laptops, discos rígidos, pendrives, e-mails, y muchos destinos mas.

La encriptación brinda seguridad a través de la confidencialidad, proveyendo al usuario de la posibilidad de publicar su información libremente de una manera segura.

- Protección Física: Toda laptop hoy en día le provee al usuario la función de encriptación por Hardware de su disco rígido.
- Protección Lógica: Existen diferentes aplicaciones para todo sistema operativo que permiten la encriptación on-the-fly de discos rígidos externos, pendrives, memorias flash, etc.
- Protección de E-mails: Existen varias herramientas que permiten la encriptación de los E-mails entrantes y salientes, y la protección de la base de datos de correo.

- Protección de E-mails 2: Muchos proveedores de correo electrónico actuales permiten el uso de sus servicios a través de canales seguros.
- Navegación Segura: A la hora de efectuar un trámite de alta importancia en la web, es imprescindible antes asegurarse de estar navegando en un área segura.
- Firma Digital: Provee un nivel de seguridad significativamente alto. Lentamente está ganando cobertura y relevancia a nivel nacional.

Ninguna medida de seguridad es válida si no se la respeta y cumple con las mayores medidas de precaución.

Muchas veces el eslabón mas débil no es la persona, sino el medio por el cual se transmite la información que se desea asegurar.

En dichas circunstancias, la persona no tiene poder de control sobre la situación, ni conocimiento del problema.

- PC Segura: El uso de una PC de la cual no se confíe su origen, o su nivel de mantenimiento, debilita la seguridad de la información perteneciente al usuario.
- Rastros Inevitables: El uso normal de una PC deja rastros inevitables. Al finalizar su uso, dichos rastros deben ser eliminados.
- Información: La PC es un medio de comunicación y operación. Durante su uso, cierta información personal puede ser utilizada. Es importante no dejar esa información disponible luego de usarla.

Las redes sociales representan el 50% de la navegación web diaria.

Sus portales contienen infinidad de información personal valiosa de cada uno de sus miembros.

Dicha información personal puede ser fácilmente utilizada en nuestra contra por una persona malintencionada.

- No Mucha Información: La información revelada en las redes sociales debe ser mínima y trivial, y sin relación directa con nuestra vida privada.
- Configurar el Portal: Las opciones por defecto de las redes sociales permiten una confianza transitiva entre personas y el acceso completo al perfil del usuario por parte de cualquier cercano.
- Verificar: Siempre que se lea o se escuche cierta información dentro de una red social, verificar personalmente sobre la veracidad del contenido publicado.

- Redes Sociales, no Públicas: El pertenecer a una red social no significa que uno deba conseguir la mayor cantidad de amigos. Las redes sociales fueron creadas para mantener las conexiones entre amigos digitalmente. Los amigos de uno deben ser... amigos.
- Buscarse: Buscarse a uno mismo regularmente permite identificar que nivel de información sobre uno está disponible públicamente en la Web, y de esa forma saber si uno está expuesto.

Matias Katz
IT Consultant
Security Specialist

matias@matiaskatz.com

www.matiaskatz.com

Preguntas?