

Principio 5: “No hables con extraños”

Abundan en la actualidad cientos de redes sociales, con diversos objetivos: conocer gente, entablar amistades, compartir fotos, contactos laborales, y otros. Pero poco conoce el usuario sobre cuál es el destino y uso de la información que es subida y compartida con el mundo.

Las redes sociales han ingresado en las vidas de los usuarios. Aquellos que diariamente chequean sus correos, sean estos personales o laborales; habrán recibido, en algún momento, invitaciones en su bandeja de entrada para conectarse con un amigo o un desconocido. Muchos también, porque no, las habrán enviado.

Christian D. Doyle, profesor de Tecnologías de la Información de la Universidad Austral en Argentina, explica que *“el objetivo principal de las redes sociales virtuales es agrupar individuos que tienen necesidades similares. Éstas pueden ser laborales, sentimentales, sociales, lúdicas, etc., todo depende de la red social vinculante. De esta manera, de forma gratuita o muy económica, ayudan a las personas miembro a conseguir lo que buscan o quieren”*¹.

A pesar de los beneficios de las redes sociales, es importante tomar conciencia de los riesgos que estas acarrearán. En primer término, las barreras para relacionarse con desconocidos no son tan claras como en la vida real, donde es muy simple determinar si un contacto es o no conocido. En el mundo digital, el usuario tiende a relacionarse con contactos de los cuales desconoce el grado de confianza existente. Esto puede generar una pérdida de privacidad (ver *Principio 1: “Cuida tu privacidad”*) y en el caso de los menores puede causar problemas cada vez más frecuentes, como el Ciberacoso. Además, las redes sociales son utilizadas para la propagación de malware y, nuevamente en el caso de los menores, para cometer delitos más graves, como la generación de redes de pedofilia.

Cualquiera sea el caso, el usuario debe ocuparse, tomar conciencia y cuidarse. Si bien es cierto que los sitios Web de redes sociales pueden ampliar el círculo de amigos de un individuo; la exposición puede incrementar los peligros. No es recomendable brindar todo tipo de datos privados por la Web, y menos aún si el usuario es menor de edad. En estos casos, como ya se explicó, los peligros son aún mayores.

Precauciones

Para utilizar con seguridad las redes sociales, es recomendable tener en cuenta los siguientes consejos:

- **Evitar exponer información sensible.** No entregar datos privados, como por ejemplo un domicilio o números telefónicos, salvo que sea estrictamente necesario. En el primer caso, además de preservar la integridad física, el usuario protege a su familia.
- **No divulgar el correo electrónico.** No solo para el resguardo de la privacidad, sino a efectos de evitar ser víctimas del spam, el usuario debe preocuparse por no

¹ <http://www.universia.net.co/secciones-home/destacado/el-vertiginoso-crecimiento-de-las-redes-sociales-en-latinoamerica.html>

exponer su correo electrónico en espacios que puedan ser consultados públicamente.

- **No informar las vacaciones.** Evitar informar los momentos en que posiblemente el usuario deje su domicilio inhabitado.
- **Acompañar a los menores.** El usuario debe auxiliar a los menores en el uso de estas tecnologías, asesorarlos respecto a qué información se está revelando, y compartir con ellos dudas e inquietudes. Además, es necesario concientizar al menor de los riesgos existentes en este tipo de herramientas.
- **No contactar desconocidos.** De la misma forma que en la vida real el usuario no se relaciona con desconocidos, mantener las redes de contactos limpias de individuos a los que el usuario desconozca. De recibir invitaciones de contactos de desconocidos, el usuario debe rechazarlas o consultar a la persona que realizó la invitación.
- **Configurar las redes sociales.** En la mayoría de los casos, por defecto, las configuraciones de privacidad en las redes sociales son muy laxas. No es lo mismo que los datos del usuario lo puedan ver solo sus contactos a que sean públicos. Por lo tanto, el usuario debe dedicar tiempo a personalizar las configuraciones y ajustar el nivel de exposición de la información.

Autor: Nelson Fernandez - Openware

El presente artículo es uno de los principios publicados por **Openware**, en el marco de la **Semana Internacional de la Seguridad Informática**. Para visualizar el resto de los textos de concientización, consulte el siguiente sitio Web:
http://www.openware.biz/es/noticias/semana_internacional_de_la_seguridad_informatica_principios_de_seguridad_%E2%80%9Cdale_valor_tu_inf

Licencia

El presente artículo es liberado bajo [licencia Creative Commons](#).

Usted es libre de:

- copiar, distribuir, exhibir, y ejecutar la obra.
- hacer obras derivadas de ella.

Bajo las siguientes condiciones:

- Usted debe atribuir la obra en la forma especificada por el autor o el licenciante.
- Usted no puede usar esta obra con fines comerciales.
- Si usted altera, transforma, o crea sobre esta obra, sólo podrá distribuir la obra derivada resultante bajo una licencia idéntica a ésta.

<http://creativecommons.org/licenses/by-nc-sa/2.5/ar/>