

## Principio 2: “No brindes información indebida”

La **Ingeniería Social** es la técnica que consiste en manipular al usuario para lograr que este brinde información voluntariamente. Esta también puede ser utilizada para lograr que un usuario ejecute una acción deseada por el atacante.

Un ejemplo muy sencillo es realizar un llamado telefónico a un empleado de la organización, presentarse como el departamento de sistemas e indicar que están existiendo problemas en la red. Posteriormente, se solicita al usuario que cierre la sesión y que indique su contraseña para hacer unas pruebas.

Así de sencillo un atacante puede conseguir credenciales válidas para loguearse en la red. Aunque parezca extremadamente simple, este tipo de técnicas es de las más utilizadas para conseguir información. En palabras sencillas, la Ingeniería Social es el arte de conseguir información de otra persona por medio de habilidades sociales.

También es frecuentemente utilizada en combinación con otros ataques. Por ejemplo, para propagar troyanos. Un troyano es un archivo malicioso que simula ser un archivo inofensivo para lograr que el usuario lo instale por sí mismo en el equipo. En estos casos, la Ingeniería Social es utilizada, por ejemplo, para enviar correos con imágenes tentadoras para el usuario o textos indicando grandes beneficios. Una Web que invite a descargar una aplicación paga, de forma gratuita (con un mensaje de “GRATIS” llamativo en tamaños y colores) está utilizando la Ingeniería Social para lograr sus objetivos.

Si uno observa detenidamente esta técnica, no existe un robo de información claro ni un acto delictivo explícito por parte del “atacante” en estos hechos. Incluso es la misma víctima quien termina siendo el principal cómplice del delito.

Uno de los ingenieros sociales más conocidos, llamado [Kevin Mitnick](#), postula que la Ingeniería Social se basa en cuatro principios:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir “No”.
- A todos nos gusta que nos alaben.

Estos son útiles para comprender los motivos por los cuales esta técnica funciona.

## Precauciones

Para evitar ser víctima de técnicas de Ingeniería Social, el usuario debe:

- **Chequear la identidad:** cuando se entrega información sensible es importante asegurar que la persona que la está recibiendo es quien dice ser.
- **No brindar información personal:** cuando se solicita al usuario brindar información que se ha brindado anteriormente, negar la entrega de esta información y remitir al hecho de que el solicitante debería conocer esa información
- **Verificar:** ante la duda, chequear por otro medio la veracidad de la solicitud de información. Por ejemplo, en el caso de un llamado telefónico el usuario puede indicar que “ahora está ocupado” pero que “se comunicará en breve para brindar la información”.
- **Analizar el medio:** las personas y organizaciones serias no solicitan información



personal por medios inseguros (por ejemplo una contraseña por correo electrónico). El usuario debe evaluar cuando se le solicita información, si la misma está siendo solicitada correctamente.

La Ingeniería Social es una técnica antigua que se perfecciona día a día; y no hay tecnología capaz de proteger al usuario. No existe usuario que esté protegido contra esta técnica, y todos los consejos valiosos remiten a la concientización y al uso del sentido común y criterio para pensar, antes de brindar información indebida.

**Autor:** Sebastián Bortnik - 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](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 licenciente.
- 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/>