CDMX
CIUDAD DE MÉXICO
Junta de Asistencia Privada del Distrito Federal

No. 67
Martes 23 de enero de 2018

Tecnológico

MARTES DE TIPS
EN FORTALECIMIENTO INSTITUCIONAL
Guía para Internet más seguro Parte 2

Comunicación | Administrativo | Legal | Asistencial | Análisis y Supervisión | Financiero | Desarrollo Institucional

En esta ocasión, continuamos con los consejos para un Internet más seguro, en aspectos de nuestra vida digital más allá del espacio laboral; **fuera de la oficina, cuando se usan las redes sociales y la nube**.

FUERA DE LA OFICINA

1. Dispositivos móviles

En las computadoras portátiles, tabletas y teléfonos inteligentes, además de nuestros datos personales, es común el resguardo de información sensible de la oficina (ej. correo electrónico). Estos dispositivos pueden ser robados o extraviados, por lo que debemos tomar en cuenta:

- **Nunca** debe ser el **único lugar** donde guarde **información importante**
- Cuente con un **NIP o contraseña**
- Aunque sean dispositivos personales, **piense dos veces antes de instalar cualquier aplicación** y hágalo únicamente desde tiendas de aplicaciones reconocidas, así evitará infecciones por malware y su consecuente pérdida de información
- **No ocupe las características de GPS y localización** de su teléfono o tableta, a menos que sea necesario. Estos datos pueden ser utilizado para un ataque mediante la Ingeniería Social[1].
- Si la información es sumamente importante y requiere un dispositivo portátil para trabajar con ésta, considere alternativas para **encriptar** los discos duros de los equipos

1 Martes de Tips No. 66 – Guía para Internet más seguro Parte 1 (5 diciembre 2017).

Además:

- No **descuide** la computadora, tableta o teléfono inteligente, siempre téngalo a la vista
- Tenga **cuidado** con las personas que hay alrededor suyo en los **espacios públicos**

2. Computadora pública

- **No** haga **operaciones financieras** o consultas de **información sensible**, como el correo electrónico
- Si accede a su correo electrónico o a redes sociales, use el **"modo privado" del navegador**, para evitar que se guarde información en el equipo
- **Nunca** utilice discos duros externos y USB con información importante (ej. FIEL), para evitar robo de información o la infección del dispositivo con un malware.

3. Conexiones Wi-Fi públicas

- Sólo usarlas para la **navegación no esencial** en Internet
- **No** las use para **operaciones financieras** o consultas de **información sensible**
- Visite páginas con **seguridad instalada** (símbolo de "candado" o barra de navegación color verde)
- Hay **redes apócrifas** en los lugares públicos. Si no está seguro a qué red conectarse, pregunte al administrador
- Instale una **VPN (red privada virtual)**, como *PsiphonInc* y *thetunnelbear*, cuando requiera hacer un uso continuo de redes públicas

Es importante entender que **cualquier información** o **archivo electrónico** publicado en Internet es permanente y transmisible. Por esto, debemos cuidar las configuraciones de seguridad de nuestras redes sociales, sitios web, carpetas de archivos en la nube, etc.

REDES SOCIALES

1. Las redes sociales son públicas no privadas

Se le recomienda:

- Defina qué tan **públicos** serán su perfil e información
- Evalúe las redes a utilizar, en especial visite sus **políticas de privacidad**
- Establezca **límites** adecuados para lo compartido en línea
  - Publique aquello con lo que se sentiría cómodo de escuchar o ver en público
  - No publique imágenes, videos o comentarios inapropiados
- Sea **selectivo** con las personas que acepta como "amigos"
- Tenga cuidado cuando **conozca en persona a alguien que lo contactó en línea**. Hágalo en un lugar público y dígale a otros dónde estará
- En un correo electrónico o por teléfono, **nunca se le pedirán datos personales o contraseñas**

2. En el trabajo

Se sugiere que:

- Las **publicaciones o respuestas** deben corresponder con los valores de la institución
- Instaure **políticas de redes sociales**
- Si varios usuarios utilizan una c**uenta compartida**, establezca quién la utiliza y en qué momento
- Si "**etiqueta**" o menciona a sus colaboradores, aliados o beneficiarios en una publicación, estará **revelando involuntariamente más información** sobre ellos de la que cree, utilice esta función con cuidado
- Cuente con un **permiso explícito** para emplear imágenes de personas; si no, difumine sus rostros en fotos y videos
- Algunos servicios ofrecen roles diferentes para niveles distintos de privilegios. Asigne **roles a su personal según corresponda**
- Informe a voluntarios y nuevos colaboradores sobre las **políticas y uso de las redes sociales institucionales**

LA NUBE

Si utiliza servicios corporativos de la nube, **cualquier persona con usuario y contraseña** para iniciar sesión, puede acceder. Para este caso se sugiere:

- Cada miembro o voluntario debe tener **datos únicos** de inicio de sesión
- **Restrinja el acceso** de los colaboradores en base a funciones o perfiles de puesto
- **Verifique los permisos y correos** de los destinatarios de los archivos en la nube que desea compartir
- Realice copias de seguridad de la información realmente importante, fuera de línea (discos duros externos)

CONCLUSIÓN

Estas recomendaciones son para hacer **más segura** nuestra vida digital, dentro y fuera de la oficina, con dispositivos personales o de trabajo, fijo o móviles; debemos aplicar las que sean más pertinente de acuerdo a los roles que desempeñemos en nuestra instituciones y vida privada.

Referencias:

Techsoup. (19 de diciembre de 2016) *Guía para Internet más Seguro*. Techsoup. Consultado electrónicamente el 17 de abril de 2017, 17:20 horas en http://bit.ly/2gOBkwM

Este documento fue elaborado por el maestro **Arturo Valdés Mendoza**,
Coordinador de la Dirección de Tecnología de Información y Comunicación
Tel. 5279 7270 ext. 7287 avaldes@jap.org.mx

Contacto Martes de Tips
Katya Butrón Yáñez
Tel. 5658 5897 ext. 8014 kbutron@jap.org.mx.