CDMX CIUDAD DE MÉXICO
Junta de Asistencia Privada del Distrito Federal

Nueva Etapa • No. 66
Martes 5 de diciembre de 2017

Tecnológico

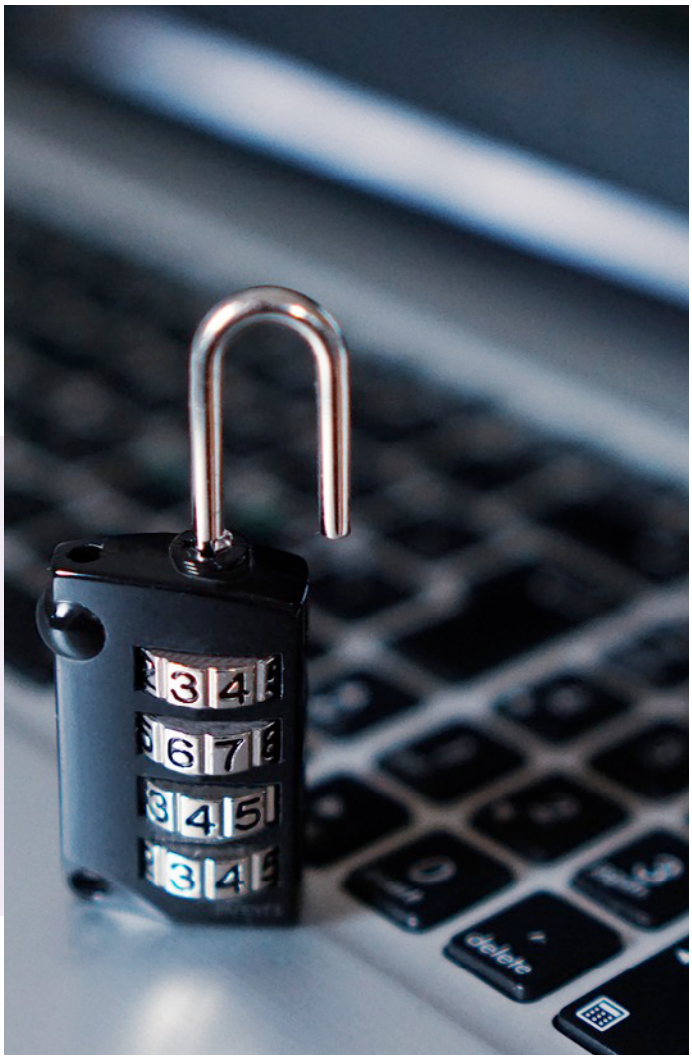
MARTES DE TIPS
EN FORTALECIMIENTO INSTITUCIONAL

Guía para Internet más seguro Parte 1

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

El uso de la Internet nos ha permitido ser más efectivos en el desempeño de nuestras actividades cotidianas. Nos permite comunicarnos a través de las redes sociales con otras personas sin importar el lugar en el que se encuentren. Además con éste hacemos mejor nuestro trabajo al **acercarnos** todo tipo de información y facilitarnos herramientas en línea para enriquecerlo.

Con la Internet también expandimos nuestro espacio de trabajo con el uso de la nube, la cual nos permite tener disponible nuestros archivos en cualquier sitio a cualquier hora y guardar una copia de respaldo en caso de pérdida accidental o por algún otro tipo de problema. El uso de dispositivos conectados a Internet hace que sea **transparente el lugar y el equipo que utilicemos para consultar la información** propia o de trabajo, lo que nos hace ser más eficientes en estos ámbitos.



Sin embargo, esta disponibilidad tan amplia de nuestra información (en todo momento, en cualquier lugar y con cualquier dispositivo) también conlleva el tener un manejo adecuado de la misma. Hay muchas amenazas en Internet que pueden poner en riesgo la información, uno de los activos más importantes de personas y organizaciones. Por esta razón, a continuación listaremos recomendaciones que pueden ser de utilidad para un manejo seguro y más adecuado de nuestra información. Estos consejos estarán organizados en cuatro áreas: en la oficina, fuera de ésta, cuando se usen redes sociales o la nube.

EN LA OFICINA

1. Establezca políticas en el uso de sus contraseñas

Las **contraseñas** deben ser consideradas con la misma importancia que la seguridad física de las instalaciones de su organización. Esto le ayudará a protegerse de aquellas personas (externas, pero también internas) que busquen acceder a su equipo o a su información, adivinando la contraseña usando frases o números, programas o virus informáticos instalados en los aparatos.

- Las contraseñas seguras **deben incluir** mayúsculas y minúsculas, número y símbolos.
- Deben ser diferentes para los distintos sitios web que utilice. Puede utilizar algún programa de administración de contraseñas para conservarlas y recordarlas.
- **No mezcle** contraseñas de uso personal con las contraseñas de la organización.
- Para recuperar contraseñas de servicios en línea utilice **preguntas y respuestas** poco frecuentes, relacionadas pero que no hagan sentido a terceros. Ejemplo: en lugar de usar su información puede utlizar la de uno de sus hijos: color de su mascota o modelo del auto del vecino.
- Hay que cambiar con frecuencia las contraseñas, al menos una vez al semestre. Si es posible c**onfigurar los sitios web** o sistemas para que solicite el cambio automático de las mismas.

2. Actualice su software

Un software desactualizado tiene mayor probabilidad de ser vulnerado y facilitan el trabajo de los delincuentes para robar la información valiosa de las personas u organizaciones.

- Mantener actualizados todo el **software o apps** de los equipos. Si es posible configurar las actualizaciones para que éstas sean automáticas.
- **Instalar antivirus**, firewall locales o software anti-spyware. Muchos de éstos los incluyen los equipos o existen versiones gratuitas.
- **Mantener los sistemas operativos** actualizados de todos sus equipos y dispositivos (Pc, laptops, tabletas y teléfonos).

3. Evite la ingeniería social

A través del correo electrónico se tienden trampas para engañar ofreciendo donativos inexistentes, ofertas irreales o trabajos con sueldos sobredimensionados con el **objetivo de defraudar económicamente,** obtener información para acceder a cuentas de banco o para descargar virus o algún otro tipo de malware. Por ello es recomendable:

- No abrir correos electrónicos de remitentes desconocidos, menos si son sobre temas que nos estén relacionados con la labor de la organización o si están en idiomas ajenos al nuestro.

- Se debe tener un software anti-spam para bloquear aquellos correos electrónicos apócrifos, disminuyendo los ataques de virus y engaños con la técnica de "ingeniería social".
- Descartar los correos con redacciones incongruentes, faltas de ortografía o que al leerlos suenen "artificiales". También identifique correos con vínculos a sitios web extraños o no relacionados con la labor de la organización.
- Ofertas, trabajos, donativos desproporcionados o que soliciten dinero para recuperarlos son fraudes y no hay que hacerles casos.
- En un correo electrónico o por teléfono nunca se le pedirá que proporcione datos de usuarios y contraseñas de servicios bancarios o tarjetas de crédito, ni información personal. Así que no proporcione esta información aunque el remitente parezca legítimo.

4. Evite programas que "secuestren" su información

El ransomware es un tipo de malware que **encripta la información** del disco duro de los equipos de cómputo y pide un rescate a cambio de quitar esta restricción.
- No instale software ilegal.
- Mantenga actualizado el sistema operativo, software y apps de todos sus dispositivos.
- Tenga instalado un antivirus en todos los dispositivos.
- Realice respaldos de la información más importante de la organización.

5. Navegue seguro

- Evite descargar software, archivos o cualquier tipo de contenido de sitios web no oficiales o de dudosa procedencia, aunque estos vínculos estén sugeridos por correos de entidades "oficiales".
- Verifique que las **URL** de los sitios web que soliciten datos importantes comiencen con **HTTPS://**. Además, estos sitios tiene el icono de un candadito y/o utilizan un fondo un color verde en la barra de navegación.
- Utilice un sólo equipo para las operaciones bancarias (nómina o donativos) o para el llenado de formularios con información sensible (relacionada con la población que asiste). Igualmente, designe a uno o dos personas exclusivamente para el uso de dicha máquina.

6. Defina políticas de inducción de seguridad en su organización

El personal de nuevo ingreso o reasignado a un nuevo puesto deberá recibir una breve plática de consejos se seguridad asociados al manejo de información que conlleva sus nuevas funciones.
- Establezca nuevas contraseñas para evitar que el personal que ya no esté en la organización pueda acceder a los sistemas o sitios web.
- Explique las políticas de contraseñas (mantenerlas ocultas y no compartirlas) de uso de la información, del respaldo de la misma, de uso del equipo de cómputo, así como de los permisos para trabajar fuera de los horarios de trabajo normales.
- Explique qué hacer en caso de pérdida de información (por robo o extravío), virus o algún otro incidente de seguridad que surja.

7. Establezca accesos restringidos en redes inalámbricas

para visitantes (si existe) o evite compartir a externos el acceso a su red de Internet, en especial si se trata de teléfonos inteligentes.

8. Asegúrese que estas políticas y consideraciones las conozca y entienda

todo el personal de su organización.

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 **Arturo Valdés Mendoza,** Coordinador de la Dirección de Tecnología de Información y Comunicación.
5279-7270 ext. 7287
avaldes@jap.org.mx

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