Revelador Institucional. Boletín No. 23 de la Oficina de Control Interno

Diego Orlando Bustos Forero

mar 02/07/2013 4:08 p.m.

Bandeja de entrada

Para:ANI <ANI@ani.gov.co>;

BOLETÍN No. 23

¿ESTAMOS COMPLETAMENTE SEGUROS?

TIPS PARA LA SEGURIDAD DE LA INFORMACION

Este boletín tiene el propósito de proveer información básica sobre la seguridad informática para usuarios de computadoras e internet. Ningún sistema es invulnerable pero creemos que siguiendo los consejos que ofrecemos aquí puedes dar un gran paso para proteger la seguridad de tus datos públicos, tus datos privados y tu identidad en internet. De la misma manera, contribuir significativamente a la protección de la información de la entidad.

ñLas organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadoresò
ï Kevin Mitnick

ñSi piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnologíaò
ï Bruce Schneier

Tema Central

La seguridad informática abarca proteger la información previniendo, detectando y respondiendo a los ataques, garantizando que la información que tenemos cumpla con la triada CID de seguridad:

- Confiabilidad
- Integridad
- Disponibilidad

¿Cuáles son los riesgos?

Hay muchos riesgos, algunos más serios que otros. Por mencionar los más comunes:

- Virus
- Robos de información (Phishing, Adware, Snooping, Sniffing)
- Suplantación de Identidad en redes sociales o en intranet (Spoofing, Pharming,)
- Daños parciales o totales de los sistemas de almacenamiento, o del hardware o en general, por agentes externos, internos o naturales
- Mal funcionamiento del software (Malware)
- Robo de claves con fines delictivos (Hacker, Cracker)

Lamentablemente, no hay una garantía 100% de que algunos de estos episodios no le ocurrirán, aún con las mejores precauciones, pero hay pasos que se pueden tomar para minimizar las probabilidades.

Consejos Básicos

1. **Copias de seguridad – Respaldo de la información (Backup)**

Disponer de un buen respaldo es esencial. Las pérdidas de datos pueden darse o por robo, fallas en el sistema o simplemente por un error.

El consejo más importante que podemos ofrecer a cualquier organización, colectivo o individuo es siempre mantener respaldo de la información digital importante o que cambie frecuentemente.

Todo tipo de almacenamiento digital es propenso a fallas. Los discos duros, cd's, dvd's, y memorias de usb pueden fallar en cualquier momento. Es difícil predecir las condiciones bajo las cuales eso puede pasar. La única solución viable para prevenir la pérdida de datos es mantener múltiples respaldos de tu información incluso opciones como almacenamiento remoto cifrado (la nube)

Utilizar una combinación de los medios mencionados puede ser ideal. Sin importar el método que escojas es altamente recomendable hacer un plan de respaldos de tu información y hacerlo de forma periódica y sistemática.

2. Contraseñas

Disponer de contraseñas con un alto grado de seguridad y realizar una actualización de las mismas, es muy recomendable. Parece algo obvio, sin embargo, muchas empresas no lo tienen en cuenta.

Son muchas las ocasiones en las que estamos encargados de proteger el acceso y control de un sin fin de información sobre nuestro trabajo, dinero, identidad, vida personal y la de otros con una serie de números y/o letras que no debemos olvidar. Esta situación se complica por el hecho de que tenemos que recordar varias contraseñas a la vez.

- Contraseñas seguras y fuertes

  - No utilice una cuenta sin contraseña ni deje una contraseña vacía, esto sin duda es la práctica más insegura que existe.
  - Nunca utilice la contraseña que el sistema le da por omisión, siempre debe cambiarla por una contraseña nueva.
  - Nunca utilice una contraseña derivada de sus datos personales como: nombre, fechas especiales, numero de cedula, teléfono, dirección o nombres o apodos de familiares o mascotas.

- Nunca elija como contraseña una palabra o una frase basada en palabras que aparecen en el diccionario o del lenguaje común. Estas contraseñas serán adivinadas fácilmente.

- La contraseña debe utilizar 8 caracteres o más.
- La contraseña debe ser una mezcla de letras, números y símbolos.
- Evita que algún carácter se repita
- La mezcla de caracteres que componen tu contraseña deben parecer completamente azarosas. Ejemplo: **%UoAg&e0a6**

- No olvidar la contraseña
- No repetir contraseñas
- No compartir las contraseñas
- No escribir la contraseña en papeles
- Cambiar contraseñas cada seis meses

3. Protección

- ***Antivirus:*** Instale un Antivirus y actualícelo con frecuencia. Analice con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.
- ***Firewall:*** Impide a usuarios ajenos o no autorizados, entrar a la red.
- ***Antispam y filtro Web:*** Evita la recepción de correos no deseados.
- ***Anti-spyware:*** Evita que se introduzcan en su equipo programas espías destinados a recopilar información confidencial sobre el usuario.
- ***Anti-malware:*** Impide la instalación de software mal intencionado.

4. Correo

- ***Cuidado con los datos adjuntos:*** Si no lo conoce, no lo abra… los correos electrónicos de direcciones extrañas o que tienen archivos adjuntos como .pps, .zip, .exe, etc.
- No abra mensajes de correo de remitentes desconocidos.
- Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.
- No propague aquellos mensajes de correo con contenido dudoso y que le piden ser reenviados a todos sus contactos. Este tipo de mensajes, conocidos Estas cadenas de e-mails se suelen crear con el objetivo de captar las direcciones de correo de usuarios a los que posteriormente se les enviarán mensajes con virus, phishing o todo tipo de spam.
- Utilice algún tipo de software Anti-Spam para proteger su cuenta de correo de mensajes no

deseados.

5. Internet

Navegue por páginas web seguras y de confianza. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de internet. En estos casos reconocerá como páginas seguras aquellas que cumplan dos requisitos:

1. Deben empezar por https:// en lugar de http.
2. En la barra del navegador debe aparecer el icono del candado cerrado. A través de este icono se puede acceder a un certificado digital que confirma la autenticidad de la página.

6. Otros Aspectos a tener en cuenta:

- Actualizar el sistema operativo y las aplicaciones con regularidad.
- Evitar compartir el computador con desconocidos
- Evitar utilizar los cybercafe o café internet
- No compartir discos duros externos o memorias usb con desconocidos
- Utilizar responsablemente las redes sociales
- Utilizar buscadores alternativos
- Acostumbrar cerrar las sesiones al terminar
- Evitar efectuar operaciones privadas en redes abiertas y públicas
- Guardar cautela en la utilización de programas de acceso remoto (Log me in, Teamviewer)
- En lo posible, desconectar Internet cuando no se necesite
- Educar a quienes comparte información

En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su equipo informático, para tratar de evitarlas o de aplicar la solución más efectiva posible.

Cuidar nuestros sistemas es una obligación que los usuarios tenemos que asumir cuando los creadores del software o del sistema operativo han cometido errores, por lo que en última instancia la seguridad depende de nosotros.

Con un muy cordial saludo,

Diego Orlando Bustos Forero
Jefe de Oficina - 6
Oficina de control Interno
Presidencia
PBX: 571 - 3791720 Ext: 1422
Calle 26 Nro. 59 - 51 Edificio T4, Piso 2
Bogotá D.C. – Colombia - www.ani.gov.co

Por favor piense en el medio ambiente antes de Imprimir este correo