Pontificia Universidad JAVERIANA Bogotá

Recomendaciones de Seguridad Informática

Febrero de 2011

DTI Dirección de Tecnologías de Información

Pontificia Universidad JAVERIANA Bogotá

Legislación

Ley 1273 de 2009

- Hurto por medios informáticos
- Acceso abusivo a sistema informático
- Violación de datos personales
- Transferencia no consentida de activos
- Suplantación de sitios web para capturar datos personales
- Daño informático
- Interceptación de datos informáticos
- Obstaculización ilegítima de sistemas informáticos o red de telecomunicaciones.

- Según la Policía Nacional, en el 2010 se presentaron 979 denuncias de delitos por medios informáticos, lo que representó un aumento de 66 por ciento con relación al 2009,
- 'transferencia no consentida de activos' para sumar en conjunto 2.953 millones de pesos

Pontificia Universidad JAVERIANA Bogotá

Lineamientos institucionales

MANUAL DE NORMAS Y LINEAMIENTOS GENERALES
PARA EL USO ADECUADO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

3.3.1. Normas sobre el uso de las redes informáticas institucionales
3.3.2. Normas sobre el uso de cuentas de Servicios Informáticos Institucionales
3.3.3. Normas sobre el uso de contraseñas
3.3.4. Normas sobre el uso de los recursos tecnológicos
3.3.5. Normas para el uso de la infraestructura física de telecomunicaciones

«La aplicación de las normas y lineamientos contenidos en el presente manual son de obligatorio cumplimiento para los usuarios de las Tecnologías de Información y Comunicaciones de la Pontificia Universidad Javeriana. El usuario deberá leer y observar estas normas; el desconocimiento de las mismas no le exime de las responsabilidades y sanciones internas, así como de tipo legal a las que haya lugar, las cuales recaerán exclusivamente en el infractor.

La violación de cualquiera de estas normas podrá causar al usuario la suspensión y/o cancelación de la cuenta de Servicios Informáticos Institucionales, la suspensión indefinida de todos los servicios tecnológicos y demás sanciones contempladas en los reglamentos de la Universidad o en contratos firmados entre las partes, así como las de tipo legal a las que haya lugar.

Es responsabilidad de todos los usuarios informar a la Dirección de Tecnologías de Información cualquier sospecha de incumplimiento de esta norma»

Pontificia Universidad JAVERIANA Bogotá

Cuentas de servicios informáticos institucionales o cuentas de usuario

Definición(1) : Registro electrónico individual para un usuario de los servicios informáticos institucionales que tienen asociados, entre otros datos:

- Un nombre (ID usuario, user ID, login name, user name)
- Una contraseña (password)
- Información que identifica al titular
- Tipo de vinculación con la comunidad universitaria
- Sus privilegios de acceso a uno o varios servicios informáticos y/o su perfil en un sistema de información

(1) Según: Normas y Lineamientos Generales para el Uso adecuado de la Tecnologías de Información y Comunicación . Pontificia Universidad Javeriana. Diciembre 2009

Pontificia Universidad JAVERIANA Bogotá

Cuentas de servicios informáticos institucionales o cuentas de usuario

Algunos de los servicios y sistemas asociados son los siguientes:

- Módulos Financieros y de Recursos Humanos
- Correo electrónico Exchange
- Correo tradicional *correo web*
- Módulos de SAE, SIAP, si lo tiene
- Bases de datos digitales de la Biblioteca
- Red inalámbrica
- Computador de escritorio asignado dentro del dominio UJaveriana, si lo tiene.

Pontificia Universidad JAVERIANA Bogotá

Cuentas de servicios informáticos institucionales o cuentas de usuario

Módulos Financieros y de Recursos Humanos

- Los usuarios con permisos deberán seguir los procedimientos establecidos tanto para su aprovisionamiento como para el des – aprovisionamiento de permisos.
- Para el aprovisionamiento es necesario la aprobación del jefe inmediato y la revisión por parte del líder funcional dueño del Módulo.
- El des - aprovisionamiento se debe solicitar para los cambios de cargo, licencias, retiros o despidos, entre otros.
- Próximamente se contará con procedimiento oficial a través de la mesa de servicios de la DTI que cubra los módulos financieros, de gestión humana y el sistema de administración de estudiantes

Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Contraseñas o *passwords*

Las siguientes normas y requisitos que deben cumplir las contraseñas cada vez que se asigne o se realice el cambio [2]:

- Su longitud debe ser mínimo de ocho (8) caracteres
- Estar compuestas por caracteres alfanuméricos (números y letras). Se recomienda una letra mayúscula, un número. Las contraseñas que utilizan letras y números son más difíciles de adivinar.
- No podrán reusarse ninguna de las ultimas 3 contraseñas utilizadas
- Las contraseñas deberán cambiarse de forma obligatoria cada 60 días.

(2) Según: Circular DTI 001/2010 DIRECTRICES PARA EL CAMBIO DE CONTRASEÑAS, dirigida al personal administrativo. Pontificia Universidad Javeriana. Junio de 2010

Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Contraseñas o *passwords*

Las siguientes normas y requisitos que deben cumplir las contraseñas cada vez que se asigne o se realice el cambio [2]:

- La contraseña no deben contener el nombre de cuenta del usuario o de su nombre completo, ya sea de forma parcial o completa.
- No escriba las contraseñas en ningún medio, ni las revele por vía telefónica, correo electrónico ni por ningún otro medio.
- No comparta su contraseña. Las contraseñas son de uso personal y por ningún motivo "las preste" a otros usuarios. En ningún caso los administradores de las cuentas de servicios informáticos le pedirán su contraseña.
- No digite sus claves secretas en computadores de otras persona, de sitios públicos y/o no confiables.

(2) Según: Circular DTI 001/2010 DIRECTRICES PARA EL CAMBIO DE CONTRASEÑAS, dirigida al personal administrativo. Pontificia Universidad Javeriana. Junio de 2010

Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Correo electrónico

Tenga en cuenta que el correo electrónico a través de las redes informáticas e Internet no es seguro. Sea precavido con los mensajes de correo electrónico que envía, recibe y conserva:

- No abra archivos adjuntos al correo electrónico de personas desconocidas, sospechosas, de una fuente de poca confianza o si el asunto del mensaje es dudoso, pueden contener "virus", los cuales podrían dañar su PC.
- Borre "cadenas" de correo electrónico y correos con propaganda (*spam*) de su buzón, pueden ser fastidios u ofensivos y pueden generar riegos de seguridad y privacidad.
- Estar alerta es la mejor defensa contra los engaños "*phishing*".
- Si llegara a recibir un correo electrónico anunciando que su cuenta de ahorro ha sido cerrada, o que es necesario que usted confirme un pedido, o que es necesario que envíe su contraseña, no responda el correo ni "de *click*" en ninguno de los enlaces resaltados en el correo. Si usted quiere confirmar si el correo electrónico es legítimo, contacte telefónicamente o por escrito a la organización o a la persona directamente.

Recuerde que la Dirección de Tecnologías de Información, administradora del servicio de correo electrónico de la Universidad, no hace solicitudes de información personal por este medio.

Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Internet

- Cuando use un programa de mensajería instantánea (por ejemplo: MS Messenger), no lea mensajes ni "de *click*" en enlaces que le envíen usuarios. La mensajería instantánea puede ser un medio para transmitir virus y otros programas maliciosos, y es otra manera para iniciar engaños "*phishing*".

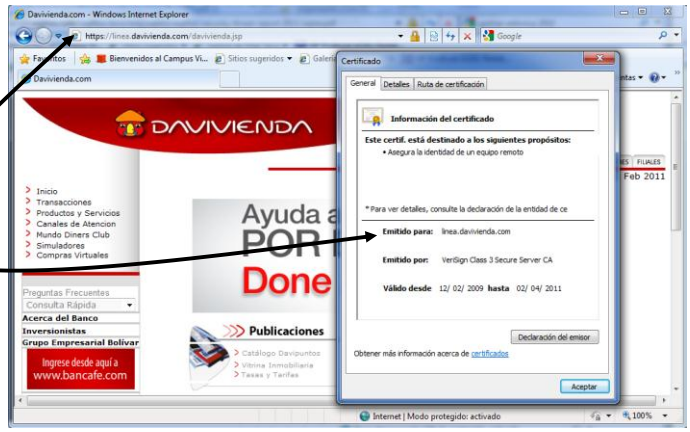
- Proceda con cautela cuando descargue archivos desde Internet. Revise que el sitio Web al que se conecta es legítimo y acreditado. Si tiene dudas es recomendable que no descargue el archivo. Si usted descarga programas (software) de Internet, sea especialmente cuidadoso con los programas que no tienen costo, los cuales frecuentemente ocultan programas no deseados…

Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Internet

- Por eso tenga siempre cuidado con su cuenta de usuario y contraseña. No la revele a nadie por ningún motivo, ni a través de ningún medio y siempre que las use hágalo en computadores conocidos



Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Internet

- Realice siempre sus transacciones desde un computador seguro.
- No acuda a los café Internet para hacer operaciones bancarias.
- No olvide revisar sus extractos de cuenta y de tarjetas de crédito regularmente. Los robos de identidad permiten usar su información personal para abrir cuentas, hacer compras, y enredarle la vida.
- Por eso verifique con frecuencia el estado de sus cuentas y tarjetas.
- Si usted descubre que su información personal ha sido comprometida, alerte a las bancos de inmediato para que le bloqueen sus cuentas y tarjetas.

Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Información y el computador

- Recuerde siempre cerrar la aplicación cuando haya terminado. Es rápido, fácil y evita que otra persona tenga acceso a la aplicación a su nombre.
- Bloquee su computador en el momento en que se retire del puesto de trabajo. Lo podrá desbloquear con su contraseña del usuario.
- En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, tenga cuidado de dejar la información confidencial protegida bajo llave. Esto incluye: CDs, DVDs, dispositivos de almacenamiento USB, entre otros.
- Realice sus actividades en lo posible solo desde el computador de oficina asignado.

En algunos sitios públicos delincuentes están instalando programas para obtener sus claves y realizar posteriormente transacciones fraudulentas a su cuenta.

Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Información y el computador

- Asegúrese de que su PC tenga un buen antivirus. Revise que el software de antivirus en el computador se mantenga instalado y actualizado.
- Verifique que el sistema operativo de su computador y todos sus aplicativos (software) se encuentre actualizado en las ultimas versiones a las que tenga derecho.
- Genere copias de sus archivos (back up) frecuentemente. Si un virus infecta sus archivos, al menos podrá reemplazarlos con una copia. Una recomendación es que almacene sus copias (guardadas en CDs o memorias "USB") en un sitio físico seguro diferente al de su computador

Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Información y el computador

- El uso de medios de almacenamiento removibles (USBs, CDs, DVDs, disquetes, reproductores de mp3, entre otros) y equipos personales portátiles debe realizarse con precaución. Es importante verificar que estos dispositivos se encuentren libres de virus y código malicioso, antes de utilizarlos en su computador.
- Un virus o programa malicioso pude dañar su información o pretender robarle datos personales, contraseñas o información valiosa almacenada, transmitida o tecleada en su computador.

Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Evite ser burlado con técnicas de ingenieria social

1. Recuerde que si algo suena demasiado bueno para ser verdad, muy probablemente lo sea.
2. Pregúntese usted mismo: porque debería YO tener un tratamiento especial sobre millones de otros usuarios de internet. Si usted no encuentra una buena razón, esto probablemente es una estafa.
3. No crea en todo lo que lee. Solo porque un email o un sitio web parece atractivo no significa que le este diciendo la verdad.
4. Se paciente y cuidadoso. Muchos usuarios han sido victimas de internet debido a que no se detuvieron a pensar, y en su lugar actuaron impulsivamente y dieron *click* en un «sexy» enlace o en un adjunto que parecía interesante sin pensar en la posibles consecuencias.
5. A menos que usted este seguro de la identidad de una persona o de una autoridad que le requiera información, nunca provea su información personal o información acerca de su organización.

Pontificia Universidad JAVERIANA Bogotá

Normas, recomendaciones y buenas prácticas

Evite ser burlado con técnicas de ingenieria social

6. No revele información personal o financiera por email. Desconfíe de los emails que le indica que siga un enlace para ingresar la información.
7. Si usted cree que un email no es legitimo, intente verificarlo contactando a la compañía directamente. Pero no use la información de contacto indicada en el email, esta puede ser falsa; busque la información de contacto usted mismo.
8. Verifique dos veces las URLs de los sitios web que visita. Algunos sitios web de phishing lucen idénticos a los reales, pero la URL podría ser substancialmente diferente.
9. Sea cauteloso al enviar información sensitiva a través de internet si usted no confía en la seguridad del sitio web.
10. Sospeche de llamadas y correos no solicitados que preguntan por información acerca de empleados de la organización y otro tipo de información. Esta puede ser una llamada de un estafador.

Pontificia Universidad JAVERIANA Bogotá

Referencias

1. 'Ciberatracos' en todo el país crecieron un 96 por ciento. http://www.eltiempo.com/economia/negocios/ARTICULO-WEB-NEW_NOTA_INTERIOR-8829280.html
2. http://www.sophos.com/security/topic/security-threat-report-2011.html
3. https://www-935.ibm.com/services/us/iss/xforce/trendreports/
4. http://www.symantec.com/business/theme.jsp?themeid=threatreport
5. http://www.websense.com/content/threat-report-2010-introduction.aspx
6. http://dvlabs.tippingpoint.com/toprisks2010

Pontificia Universidad JAVERIANA Bogotá

GRACIAS

Nelson Gómez
Asistente de Seguridad Informática
email: ngomez@javeriana.edu.co
Febrero 2011

DTI Dirección de Tecnologías de Información