COSTA RICA
GOBIERNO DEL BICENTENARIO
2018 - 2022

MINISTERIO
DE CIENCIA, TECNOLOGÍA
Y TELECOMUNICACIONES

Ministerio de Ciencia, Tecnología y Telecomunicaciones
2020

MICITT - DGD - CSIRT-CR
csirt@micitt.go.cr

Ministerio
de Educación Pública

Curso de Buenas Prácticas de Higiene Digital para Profesores MEP-CSIRT-CR

COSTA RICA
GOBIERNO DEL BICENTENARIO
2018 - 2022

micitt

mep
Ministerio de Educación Pública

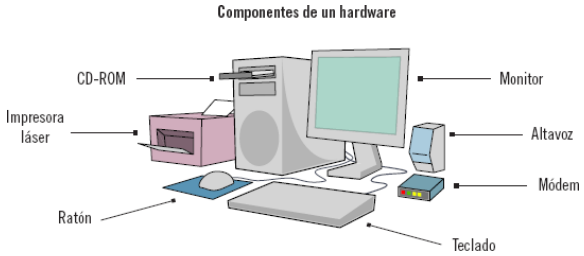
Temas	
1. Introducción a la seguridad en sistemas de información.	**1.1. Conceptos de seguridad en los sistemas.** **1.2. Clasificación de las medidas de seguridad.**
2. Ciberseguridad.	**2.1. Concepto de ciberseguridad.** **2.2. Amenazas más frecuentes a los sistemas de información.** **2.3. Tecnologías de seguridad más habituales.** **2.4. Gestión de la seguridad informática.**
3. Software malicioso	**3.1. Conceptos sobre software malicioso** **3.2. Clasificación del programa malicioso.** **3.3. Ingeniería social y redes sociales.**
4. Seguridad en redes inalámbricas del hogar	
5. Herramientas de seguridad.	**5.1. Medidas de protección.** **5.2. Control de acceso de los usuarios al sistema operativo.** **5.3.Gestión segura de comunicaciones, carpetas y otros recursos compartidos.** **5.4. Protección frente a código malicioso.** **5.5. Medidas de seguridad en configuración de aplicaciones**

Introducción a la seguridad en sistemas de información

Conceptos de seguridad en los sistemas.

Clasificación de las medidas de seguridad.

Seguridad de Hardware



Seguridad de Software

Seguridad de Red

¿Cuáles son las amenazas a la red?

Los más comunes incluyen:

- Virus
- Gusanos
- Spyware
- Ataques de hackers
- Ataques de denegación de servicio
- Intercepción o robo de datos
- Robo de identidad

Los componentes de seguridad de red incluyen:

- Antivirus
- Antispyware
- Cortafuegos (Firewall)
- Redes privadas virtuales (VPN)

Ciberseguridad

La ciberseguridad es la práctica de defender las computadoras , los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información.

La ciberseguridad trata de trabajar en robustos sistemas que sean capaces de actuar antes, durante y después.

Amenazas más frecuentes a los sistemas de información

- Malware
- Virus
- Spyware
- Ransomware
- Phishing
- Vishing
- Suplantación de identidad

EVITE SER VÍCTIMA DE ESTAFA

¿Qué es el Vishing?

Práctica delictiva que consiste en **engañarle** para robarle **información confidencial por medio del teléfono,** haciéndose pasar por una persona o empresa de confianza.

1. La víctima recibe una llamada telefónica de un supuesto empleado bancario

2. Le hacen ingresar a una página original de alguna entidad de Gobierno para realizar un trámite, con el fin de que la víctima no piense que es una estafa.

3. Le indican que debe de realizar dicho trámite y usar su Firma Digital

4. Una vez que indique que no tiene Firma Digital, le hacen ingresar a otra página web, la cuál es falsa y es donde le hacen caer, y extraen sus datos personales.

¿CÓMO EVITARLO?

- No proporcione sus datos personales vía telefónica.
- Las empresas y los bancos NUNCA van a solicitar datos financieros, por ejemplo sus números de tarjetas de crédito o débito, ni por teléfono o Internet, cuando no haya sido usted quien inició el trámite.
- Si desconfía de la llamada, mejor sea usted quién llame directamente a la empresa o al banco.

NO SE DEJE ENGAÑAR

COSTA RICA
GOBIERNO DEL BICENTENARIO
2018 - 2022

MICITT
MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

MEP
Ministerio de Educación Pública

Tecnologías de seguridad más habituales

- Actualizadores de programas
- Herramientas en línea
- Antivirus
- Control parental

Gestión de la seguridad informática

- **Gestión y control de sistemas antivirus**
  Debemos verificar que todos los equipos se encuentren en el sistema de gestión del antivirus.

- **Gestión de Actualizaciones Automáticas**
  Debemos revisar que las actualizaciones se han realizado correctamente.

- **Gestión de Copias de Seguridad**
  Plantear una buena estrategia de copias de seguridad es básico hoy en día.

Ingeniería social y redes sociales

"Arte o ciencia de manipular a las personas para que realicen acciones que pueden ser o no del interés del objetivo"

"Acto de manipular personas y desarrollar acciones o divulgar información"

Se puede hablar de la ingeniería social como una especie de hacking humano. Así como en el hacking se deben realizar tareas de obtención de información de un posible objetivo, de igual forma la obtención de información es la base de los ataques de ingeniería social, con la diferencia que normalmente el objetivo del ataque será una persona.

Consejos para aplicar y protegernos de posibles ataques de ingeniería social

- Establecer los controles de privacidad a través de redes sociales, esto es permitir el acceso a información sólo a sus amigos y/o familiares.
- No publicar información personal como dirección de sus casas, teléfonos, lugares de trabajo, ya que si ocultamos esta información ya no sería utilizada por los atacantes para establecer contacto y así realizar ataques o engaños contra usted y familiares o amigos cercanos.
- Evitar realizar publicaciones de lugares a los que frecuenta o asiste.
- Hay que evitar publicar los estados de ánimo o problemas con los que contamos, porque este tipo de información la pueden usar para establecer contacto ofreciendo ayuda o consejos y así ganar la confianza de la víctima.
- Dentro de las redes sociales evitar dar clic a cualquier enlace, porque estos pueden enviarlos a sitios o a descargar aplicaciones con código malicioso que pueden obtener información acerca de ustedes o quien utilice la computadora.
- Evitar cualquier riesgo al salir siempre apropiadamente de sus cuentas, asegurarse de que todo lo cerró bien y que nadie va a poder obtener su información.

Seguridad en redes inalámbricas del hogar

Si protegemos nuestra wifi evitamos el riesgo de que alguien se conecte a ella sin nuestro permiso, y que la utilice para descargar, o enviar spam.

Es importante proteger nuestra wifi, para esto debemos de :

- Cambiar el usuario por defecto para la administración del router
- Utilizar contraseñas robustas
- Elegir cifrado WPA2
- Configurar para controlar quién se puede conectar

Herramientas de seguridad

Medidas de Protección

- No abrir nunca emails sospechosos, Ante la duda, lo más seguro es eliminarlo.
- Una medida relacionada con el correo es agregar aquellas direcciones de correo seguras o/y conocidas a la lista blancas, esto para recibir correos solamente de ellos; y aquellas que son sospechosas agregarlas a la lista negra o también llamada spam.
- Instalar un buen software antivirus es un primer paso recomendable para conseguir un equipo seguro, de esta forma se podrían detectar posibles amenazas, errores o incidentes que pudieran afectar la seguridad. Por ejemplo, existen numerosas opciones, tanto gratuitas como de pago para proteger tu equipo.
- Mantener actualizados los sistemas operativos, aplicaciones y todo el software (lo que incluye también el antivirus, importante mantener el antivirus actualizado)
- Realizar backups de la información.
- Evitar la descarga e instalación de programas desde sitios web que no ofrezcan las debidas garantías de seguridad.
- No hacer clic en las ventanas emergentes de publicidad.
- Concientizar y formar para que hagan un uso correcto de sus equipos y dispositivos.

Control de acceso de los usuarios al sistema operativo

El control de acceso implica quién tiene acceso a sistemas informáticos específicos y recursos en un momento dado.

- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan por ejemplo instalaciones de trabajo remoto.

Tipos de control de accesos

- Gestión de accesos de usuario
- Control de accesos al sistema operativo
- Control de acceso a la información y aplicaciones
- Control de accesos en red

Métodos de control de accesos

- Contraseñas
- Certificados
- Limitación del tiempo de conexión
- Control de acceso a las aplicaciones
- Restricciones por IP
- Dispositivos Biométricos

Gestión segura de comunicaciones, carpetas y otros recursos compartidos

Para evitar estar expuesto a estos ciberataques, hay que tener en cuenta lo siguiente:

- Si no conoce la procedencia de un correo electrónico y le llegan varios correos electrónicos al día, llévelos a la carpeta de SPAM.
- Deshabilite la carga de imágenes automática.
- ¡Cuidado con los archivos adjuntos! Si desconoce la procedencia del remitente procure no abrirlos.
- Borre el historial del navegador periódicamente.
- Evite marcar la opción de guardar contraseñas.

- Utilice diferentes contraseñas para las cuentas de correo electrónico a las que tienes acceso.
- Modifique las contraseñas con cierta frecuencia (4-6 meses).
- No abra correos con ofertas, regalos o falsas promociones.
- Asegúrese de cerrar la sesión de correo cada vez que termine de trabajar.
- Cuidado con las redes wifi públicas (normalmente sin contraseña).
- Utilice la copia oculta CCO cuando envíe correos a varias personas, de esta manera se ocultará sus correos a los demás.
- No publique su correo electrónico en sitios web, foros, redes sociales o espacios donde se comparte contenido.
- Si va a compartir carpetas, tener claro el nombre de
- usuario y darle los permisos correspondientes.

Protección frente a código malicioso.

Un método para proteger a los usuarios contra el malware es a través de la educación. Es vital informar a las personas de la necesidad de apegarse a estrictas reglas de conducta mientras realizamos actividades en Internet.

Por esto se recomienda contar con una protección Antivirus.

Medidas de seguridad en configuración de aplicaciones

- Utilice las funciones de sala de espera
- Asegúrese de que la protección con contraseña esté activada.
- No comparta enlaces a teleconferencias a través de mensajes de medios sociales.
- No permita que los participantes compartan la pantalla por defecto.
- No utilice el vídeo en una llamada si no es necesario.
- Bloquee una reunión una vez que todos los participantes se hayan unido a la llamada.
- No grabe las reuniones a menos que lo necesite.

Videos relacionados

- https://www.youtube.com/watch?v=2E4oGJdPHv0
- https://www.youtube.com/watch?v=iC2tmUPKqJ0
- https://www.youtube.com/watch?v=tmfk9Fplhx4

Gracias

MINISTERIO
DE CIENCIA, TECNOLOGÍA
Y TELECOMUNICACIONES

COSTA RICA
GOBIERNO DEL BICENTENARIO
2018 · 2022

Ministerio
de Educación Pública