UNA UNIVERSIDAD NACIONAL COSTA RICA
DTIC Dirección de Tecnologías de Información y Comunicación

BOLETÍN DTIC

1 de setiembre de 2022
Boletín 11
dtic@una.cr

Noticias, comentarios y anuncios tecnológicos

En esta edición:

Seguridad informática – CSIRT

En materia de ciberseguridad, el Ministerio de Ciencias, Innovación, Tecnología y Telecomunicaciones (MICITT) crea al Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR), como la instancia que coordina las acciones para prevenir y responder ante los incidentes y amenazas en seguridad informática que puedan afectar a las instituciones del Estado en general.

El CSIRT-CR remite por medio del correo electrónico y de forma regular, boletines y comunicados relacionados con incidentes informáticos, y actualizaciones de software requeridas para minimizar el riesgo asociado al uso de tecnologías de información y comunicación.

En la UNA, estos boletines son remitidos de forma expedita al personal informático universitario, con el fin de que se tomen las acciones necesarias en esta materia en el accionar académico y administrativo a nivel de facultades, centros y sedes de la universidad.

Si usted desea ser incluido en esta lista de envíos electrónicos, puede solicitarlo al correo electrónico: cgt@una.cr

Infografías de ciberseguridad

El CSIRT-CR en conjunto con otras organizaciones ha preparado una serie de infografías de ciberseguridad de consulta rápida, las cuales pueden ser consultadas en el siguiente sitio web:

https://www.micitt.go.cr/ciberseguridad/

Las temáticas de estas infografías son:

- Phishing
- Ciberseguridad en el uso de dispositivos móviles en el entorno laboral
- Cómo utilizar contraseñas seguras
- Qué es un malware
- Protección de datos personales
- Protección de datos biométricos
- Seguridad en el uso de internet en los hogares
- Ciberseguridad en el uso de dispositivos móviles
- Ciberseguridad para no tecnólogos
- Peligros en las redes sociales

Infografía de Phishing. Fuente: CSIRT-MICITT

Ciberseguridad para el teletrabajador

El enlace web indicado, suministra de forma adicional una serie de infografías dirigidas al teletrabajador, en los siguientes temas:

- Ciberseguridad
- Combata la desinformación
- Salud digital
- Ciberseguridad para la organización: controle quién entra a su casa
- Higiene digital
- Confidencialidad
- Mejore la seguridad

¿Según las alertas del CSIRT-CR, ¿qué tipo de software debe ser actualizado?

La actualización del sistema operativo y las aplicaciones de software en general entregan mejoras del producto, corrigen defectos o vulnerabilidades de los programas de cómputo, o ambas.

Esta es una labor ordinaria que debe llevarse a cabo de forma cotidiana, con toda la seriedad del caso.

Además de la actualización de software especializado de plataformas empresariales o similares tales como Vmware, Oracle, Cisco, Moodle y otras; se reciben recomendaciones dirigidas a la actualización de una serie de software de usuario final tales como: Google Chrome, Zoom, Firefox, productos de Adobe, y las mejoras o "updates" permanentes para ambientes de Microsoft Windows, y ocasionalmente para dispositivos de Apple.

Lo anterior no significa que los productos son malos. Más bien, estos constituyen una base importante de forma directa o indirecta de nuestro trabajo cotidiano. Sin embargo, son objeto permanente del análisis por parte de terceros, que particularmente buscan "huecos de seguridad" que permitan utilizar eventualmente estas soluciones como herramientas de ataque, o el ingreso no autorizado a los computadores que utilizamos de forma regular.