UNIVERSIDAD DE COSTA RICA

CI Centro de Informática

31 de mayo de 2022

El Centro de Informática avisa:

Medidas de seguridad ante nuevos ciberataques a instituciones públicas

El Centro de Informática le recuerda, tanto al personal gestor de TI como a la comunidad universitaria en general, mantener y reforzar las medidas de ciberseguridad dado el reciente ciberataque sufrido por la Caja Costarricense de Seguro Social (C.C.S.S.) la madrugada de este martes.

El Ransomware es un ataque dañino que restringe el acceso al sistema operativo infectado, secuestrando los datos de las personas usuarias y de las instituciones vulneradas, para posteriormente solicitar un pago de rescate, que no siempre asegura la recuperación de la información

Desde este Centro hemos concretado una serie de acciones para prevenir un ataque cibernético dentro de la Institución; sin embargo, es de vital importancia que las personas usuarias se mantengan alerta ante mensajes maliciosos, ya sea por correo electrónico, mensaje de texto o llamada telefónica, ya que usualmente son los principales focos de ataque.

Por lo anterior, recomendamos tomar las siguientes medidas preventivas:

- Utilice contraseñas robustas y que sean difíciles de descifrar, cambiarlas periódicamente y si es posible active el MFA o factor múltiple de autenticación. En caso de requerir ayuda, puede contactar al personal de TI de su unidad.
- Respalde la información de manera periódica; en este sentido le instamos a que utilice la solución de **OneDrive** 1 TB para respaldos en la nube provista por la Universidad como parte del licenciamiento de MS Office 365; el OneDrive le advertirá sobre detección de ransomware y le guiará en la recuperación de versiones anteriores que no estén infectadas.
- Instale una solución de seguridad confiable en sus equipos, que cumpla con las funciones de antispam, webfilter y antivirus. En los equipos de la Universidad, el

antivirus utilizado es el Eset y si requiere ayuda, contacte el personal de TI de su Unidad. Ahora bien, para equipos personales opcionalmente se cuenta con una solución de seguridad disponible la cual pueden solicitar a través del gestor de TI de su unidad o en su defecto contactando de manera directa al CI.

- Mantenga sus equipos actualizados, tanto el sistema operativo como las aplicaciones que se utilicen.
- Evite abrir archivos adjuntos o enlaces de correos en los que se desconoce al remitente.
- Evite hacer clic en enlaces de descarga de redes sociales o sistemas de mensajería instantánea como facebook, twitter, whatsapp, telegram, entre otros.
- Mostrar en el sistema operativo las extensiones de los archivos que por defecto vienen ocultas, para evitar abrir archivos maliciosos.
- Deshabilitar las conexiones de Escritorio Remoto (Protocolo RDP) cuando no sea necesario.
- En caso de extorsión, evite el pago de la recompensa solicitada, ya que esta no asegura la recuperación de la información y podría fomentar que se continúe con el proceso de extorsión.

Recordemos que la seguridad de la información es responsabilidad de todas las personas que conformamos la comunidad universitaria y por consiguiente, les instamos a seguir las recomendaciones expuestas y publicadas en el micrositio de ciberseguridad del CI: https://ci.ucr.ac.cr/ciberseguridad.

Finalmente, en caso de dudas o consultas, puede comunicarse con el Centro de Informática al teléfono 2511-5000 o al correo electrónico ci5000@ucr.ac.cr