UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
INFORMACIÓN IMPORTANTE DE CIBERSEGURIDAD

En atención a la solicitud del personal de ciberseguridad del Centro de Informática, desde la Unidad de Tecnologías de Información y Comunicación (UTIC), les comunicamos que:

1. En los próximas semanas se estarán comunicando las medidas que entrarán a regir en la institución, tendientes a incrementar la seguridad de la información y la red universitaria. Entre ellos:

- Obligatoriedad de contar con el antivirus institucional en los equipos propiedad de la UCR.
  - Las personas que utilizan equipos personales para el teletrabajo, deberán tener instalado en la computadora una licencia personal válida de antivirus, tener activo el cortafuego o firewall y mantener el sistema operativo con las últimas actualizaciones disponibles. Todo esto correrá por su propia cuenta según lo establecido en el apartado L27 Instrumentalización de los *Lineamientos Generales del Programa de Teletrabajo de la UCR*.

- El Centro de Informática será el responsable de elaborar la lista del software autorizado para realizar la conexión mediante VPN. Por tanto, en cuanto nos la comuniquen, procederemos a divulgarla. Esta lista resultará de gran interés particularmente para las personas que utilizan sus equipos personales para teletrabajar, ya que aquellos propiedad de la institución, serán atendidos desde la UTIC.

- Es urgente que nos comuniquen cuáles personas están utilizando su equipo personal para teletrabajar, ya que debemos reportarlas al Centro de Informática para que ellos puedan coordinar directamente con esas personas la instalación del nuevo software para la conexión al servicio de VPN institucional. Es importante señalar que este software comprobará el cumplimiento de requisitos de seguridad indicados en el anterior punto y, en caso de incumplimiento, no permitirá la conexión a la red hasta que se satisfagan todos los aspectos de seguridad.

- En el caso de los equipos instalados en las oficinas, el sistema de ciberseguridad ejecutará una comprobación del cumplimiento de requisitos de seguridad y, en caso de incumplimiento aislará el equipo comprometido o dudoso, hasta que se satisfagan todos los requerimientos de seguridad. Si se diera esta situación, desde la UTIC realizaremos los ajustes necesarios para el cumplimiento y poder solicitar la reconexión del equipo a la red institucional.

- Sin distinción de la ubicación del equipo utilizado para cumplir las labores diarias (en la oficina o en el hogar), el sistema de seguridad ejecutará, sin intervención del usuario y sin la posibilidad de cancelar, la exploración de todos los dispositivos móviles que se conecten a los equipos para evitar la contaminación con software malicioso. Es necesario tener presente esta acción, ya que el dispositivo no estará disponible para su uso hasta que haya finalizado la exploración y sea seguro abrirlo en el equipo para acceder a su contenido.

2. En cumplimiento de la instrucción girada por la Unidad de Riesgo y Seguridad del Centro de Informática, se estará coordinando con cada persona que tiene a préstamo equipos de la institución, para que lo traiga a la UTIC con la intención de efectuar la actualización e instalación del software institucional.

3. En el caso de las personas que utilizan sus propios equipos, estamos en la mayor disposición de guiarlos para que cumplan en todos sus extremos, las medidas de seguridad que establecerá la institución, ya que su incumplimiento significará la imposibilidad de conectarse a la red de la UCR, por lo que se invalida el convenio de teletrabajo al no satisfacerse lo dispuesto en el inciso d), numeral 8 de ese documento.

4. En el comunicado distribuido por el Centro de Informática el día 10 de mayo, se avisa de la exclusión temporal de acceso a la herramienta Dropbox dentro de la red institucional. En el mismo comunicado, se sugiere a los usuarios trasladar los archivos localizados en Dropbox hacia OneDrive, ya que esta última ofrece 1TB de espacio, así como la verificacion de los archivos en caso de qu ese encuentren infectados por algún Ransomware o virus informático. De esta forma se, podrán consultar sus archivos de forma segura dentro de la red de la UCR.

Asimismo, les recordamos la importancia de mantener una actitud proactiva en cuanto a la ciberseguridad, considerando:

1. Dudar de cualquier correo electrónico que no se haya solicitado, y de manera especial, aquellos que nos solicitan dar clic sobre un enlace o digitar nuestras credenciales. Este comportamiento se debe mantener aún cuando recibamos correos de personas conocidas.

2. Cambiar las claves de acceso a cuentas de correo, bancos y otros, al menos cada 90 días. Es de suma importancia que no sean claves utilizadas recientemente. Según la tabla de tiempo promedio para conocer una contraseña (ver final de este documento), de la compañía de ciberseguridad

Hive Systems, lo recomendable para la contraseña, es establecer un patrón de fortaleza alto con una longitud mínima de 12 dígitos que incluya:
- Al menos una letras mayúscula.
- Al menos una letra minúscula.
- Al menos un número.
- Al menos un carácter especial (+, *, #, $, @, &, ?, !) cuando el sistema lo permita.

3. Nuestra institución a realizado una gran inversión en equipos de protección que repelen una inmensa cantidad de ataques, pero es necesaria nuestra colaboración para no abrir portillos que le permita a los atacantes burlar esos sistemas.

4. Les recordamos que al recibir correos sospechosos, los reenvíen a ABUSE@ucr.ac.cr para que sean colocados en la lista negra y se minimice el riesgo de infiltración.

Finalmente, es necesario mencionar que nuestro trabajo se realiza con las solicitudes de asistencia que, por medio del sistema de tiquetes, ustedes nos hacen. Por tanto los instamos a utilizarlo con mayor frecuencia, ya que esto nos permite priorizar la atención y rendir el informe correspondiente.

Muchas gracias,

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

Instantly = Instantáneamente
secs = segundos
mins = minutos
hours = horas

days = días
weeks = semanas
months = meses
years = años

(x)k years = (x)miles de años
(x)m years = (x)millones de años
(x)bn years = (x)miles de millones de años
(x)tn years = (x)billones de años

https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=header

Tabla tiempo estimado para conocer la contraseña.