8 DE ENERO DE 2024

CIRCULAR
UNA-CGT-CIRC-004-2024

PARA: COMUNIDAD UNIVERSITARIA
DE: CENTRO DE GESTIÓN TECNOLÓGICA (CGT)

ASUNTO: ELEMENTOS BÁSICOS DE CIBERSEGURIDAD A CONSIDERAR

Estimada comunidad universitaria:

Como elementos de ciberseguridad relacionados con el uso de las tecnologías de información y comunicación, y teniendo en cuenta el aumento de las estafas y el cibercrimen que se ha suscitado a nivel nacional, se transcriben para su valoración y atención una serie de consideraciones básicas que fueron publicadas en el pasado mes de setiembre del 2020 por este medio.

Asimismo, se recuerda la circular UNA-DTIC-CIRC-012-2023 - "PROTECCIÓN DE COMPUTADORES CON SOFTWARE DE SEGURIDAD" del pasado 5 de octubre de 2023, que indica el procedimiento a utilizar para habilitar el servicio de protección de dispositivos con sistema operativo Windows, utilizando la solución de "Microsoft Defender". Esta circular puede ser consultada en el siguiente enlace:

https://agd.una.ac.cr/share/s/-Dz6x9H5TaePe0rInF03sA

Adicionalmente, se recuerda que se ha habilitado un apartado de Ciberseguridad, en donde se han colocado los materiales remitidos por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), abordando las siguientes temáticas: navegación web segura, ciberseguridad personal, compras en línea seguras, wifi público y seguridad, consejos de seguridad para navegar en la web, consejos de seguridad para uso del correo electrónico, ciberseguridad para dispositivos portátiles y consejos para contraseñas seguras. El enlace web es el siguiente:

https://documentos.una.ac.cr/handle/unadocs/15679

1. Utilice contraseñas complejas, sin significado que pueda ser asociado a su persona. Que sean extensas, con números, letras mayúsculas y minúsculas, así como con caracteres especiales.

2. Cambie de forma periódica su contraseña, de la misma forma en que algunos bancos lo obligan cada cierto tiempo.

3. Utilice contraseñas diferentes, particularmente para sistemas o aplicaciones críticas o estratégicas.

4. Las contraseñas son personales, no las comparta. Ciertos procesos asociados implican una responsabilidad que puede trascender al ámbito administrativo o penal.

5. Para cambio de contraseñas, utilice los medios y métodos formales de la organización o institución que corresponda. Evite utilizar enlaces web recibidos para este objetivo.

6. Establezca en la medida de lo posible un segundo factor de autenticación. Esto es, una segunda contraseña como las que piden los bancos al momento de ingresar a una plataforma de internet banking.

7. Mantenga los correos electrónicos alternativos y números de teléfono actualizados en todas las aplicaciones o servicios públicos que requieran de estos datos.

8. No conteste correos electrónicos sospechosos, que pida información reservada o restringida, o al menos que lo lleve a dudar.

9. Evite ingresar a enlaces web en donde no se tenga la de cuál sitio web se trata, o si un enlace web le pide cambiar una contraseña.

10. Desconfíe de los mensajes de texto o de mensajería de WhatsApp desconocidos o que no pueda verificar de forma absoluta, en donde le pidan información personal o confidencial, o lo redirijan a un sitio web externo desconocido.

11. Utilice los enlaces web oficiales que la organización o institución suministre, particularmente en aquellos en donde se van a llevar a cabo transacciones financieras o similares. De igual forma, refiérase a comunicados oficiales, de canales oficiales tal como el correo electrónico institucional

12. No ingrese a enlaces o sitios web desconocidos, ni descargue archivos de los que no está seguro. Eventualmente podría contaminar o poner en riesgo su computador.

13. Mantenga actualizada una solución de protección informática para el computador, tipo "internet security". Generalmente este es un producto comercial. Un antivirus por sí solo o gratuito, era suficiente en el pasado, mas no en el presente.

14. Evite utilizar redes inalámbricas públicas para llevar a cabo transacciones comerciales. De igual forma, es preferible que aprenda cómo se configura e ingresa a una red inalámbrica, ya que eventualmente la utilizará fuera de la institución - o fuera del país - y tendrá que hacerlo por sí mismo.

15. Evite mantener charlas amistosas con supuestos funcionarios de instituciones públicas o privadas que de forma amable e insistente tratan de obtener información confidencial mediante la vía telefónica. Es mejor recibir un insulto al cortar la llamada que a perder eventualmente sus ahorros.

16. Para información importante, valore mantener un respaldo de estos datos en un sitio alterno, actualizado en el tiempo. Esta información puede dañarse o perderse en cualquier momento debido a la impericia o a un fallo en el equipo o hardware respectivo, o en el peor de los casos, puede ser víctima de secuestro (ramsonware).

17. Mantengamos el sistema operativo de nuestro computador o dispositivo, así como sus aplicaciones actualizadas. Estas actualizaciones son mejoras de producto, y también cubren problemas de seguridad.

18. Procedamos a bloquear nuestro computador o dispositivo cuando nos alejamos de él. Esto es hasta cierto punto extremo, pero en condiciones presenciales en muchas instituciones es mandatorio.

19. Cuando compartamos el computador con terceros, apliquemos en la medida de lo posible las anteriores observaciones: actualización de software, bloqueo de computador, respaldos de información, etc.

20. En caso de manejo de información sensible, aprendamos a encriptar esta información. Nuestro computador puede ser objeto de hurto, robo, o pueda requerir ser atendido en un taller de reparación.

21. Evitemos ingresar a sitios web que nos piden contraseñas que no utilicen el protocolo "https", el cual aparece al inicio del enlace del sitio web. Este tema es mucho más amplio y deben considerarse otros aspectos, sin embargo, es el primer elemento para tomar en cuenta.

22. La mayoría de los sistemas universitarios - sino todos - permiten hoy en día utilizar la web para llevar a cabo los procesos a nuestro cargo. Su conceptualización fue diseñada de esa forma, y por ende se utiliza el protocolo "https" indicado anteriormente.

23. No utilice software ilegal o "pirata". Este tipo de soluciones puede contener software malicioso (malware) que puede estropear su sistema operativo, y por ende la continuidad de su labor diaria.

Atentamente,

CENTRO DE GESTIÓN TECNOLÓGICA

MAYKOL PHILLIPS SEAS (FIRMA)
PERSONA FISICA, CPF-09-0085-0108.
Fecha declarada: 08/01/2024 02:13:47 PM
Esta es una representación gráfica únicamente,
verifique la validez de la firma.

Maykol Phillips Seas
Director Asesor en Desarrollo Tecnológico