UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Dirección de Tecnologías de Información y Comunicación

Elementos de interés asociados a la ciberseguridad

Maykol Phillips Seas

5 de Mayo de 2022

Preámbulo

En nuestro entorno, toda actividad humana está asociada de manera directa o indirecta a las tecnologías de información y comunicación: educación, salud, finanzas, seguridad, cultura; independientemente de la profesión que ejerzamos …

Todo se encuentra – en mayor o menor medida – tecnificado.

En resumen, las necesidades actuales en materia de ciberseguridad son:

Adquisición y renovación de plataformas e infraestructura; y adquisición de servicios especializados (que tienen un costo importante, de forma permanente).

Recurso humano exclusivo para esta actividad, y no dedicado a múltiples tareas ordinarias desintegradas.

Plan de formación permanente de adquisición y fortalecimiento de capacidades y competencias tecnológicas, dirigido a la comunidad universitaria.

La mejor forma de comunicar aspectos asociados a la ciberseguridad es mediante la vía del correo electrónico, sin embargo, sabía usted que la comunidad universitaria recibió de las listas de distribución de correo interno la siguiente cantidad de mensajes electrónicos:

2018: 4961
2019: 5550
2020: 7193
2021: 6598
2022: 1902 (321 de tipo oficial)

Por lo tanto, es muy difícil comunicar de forma efectiva elementos de ciberseguridad para su respectivo cumplimiento.

El Departamento de respuesta a Incidentes de Seguridad Informática (CSIRT) del MICITT solicita:

- Cambio de contraseña de todos los sistemas de información y afines, por parte de todos los usuarios (esto se puede “forzar”, con una consecuencia operativa grave)

- Aplicación del segundo factor de autenticación o 2FA, equivalente al token bancario. En correo electrónico, solo se han aplicado 195 de aproximadamente 6000 correos electrónicos activos.

- Instalación de software de protección en todos los computadores institucionales.

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Acciones llevadas a cabo:

- “Hardening” o aseguramiento de servidores de cómputo de forma continua
- Configuraciones avanzadas de los servicios de comunicación brindados (DNS y web particularmente)
- Aplicación de restricciones a tráfico inusual de internet, el cual es 24 x 7
- Capa de protección adicional contra ataques volumétricos desde la internet (provisto por el ICE)
- Varias circulares indicando, los pasos a seguir por parte del usuario final
- Otras de índole técnico

En materia de infraestructura de plataforma tecnológica:

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

- Los ataques informáticos SIEMPRE han existido. Esto no es un tema reciente, simplemente, aumentó en cantidad y complejidad.

- Se necesita experticia técnica especializada para asegurar los recursos informáticos existentes. Nuestro personal es, escaso. Ver circular **UNA-DTIC-CIRC-007-2022.**

- Las tareas técnicas de aseguramiento de estos recursos son numerosas, variadas, complejas y de carácter permanente.

- Han habido intrusiones exitosas a servidores de cómputo por parte de terceros. La pregunta es: ¿por qué ?

- La DTIC, no pude seguir entregando plataformas tecnológicas a personal universitario que carece de las competencias técnicas para administrar estos recursos.

- La DTIC ha estado planteando el tema de recursos para ciberseguridad, por un período de 10 años.

En materia de usuario final:

- Plan de comunicación continuo
- Aprendizaje constante de elementos de ciberseguridad
- No puede haber una dependencia continua del recurso informático universitario (ya que este no estará presente los fines de semana, vacaciones, recesos institucionales ...)
- Obligatoriedad en la aplicación de las instrucciones remitidas para este efecto
- Debemos concentrarnos en la gobernanza de T.I para poder enfocarnos en proyectos y esfuerzos estratégicos (incluyendo ciberseguridad), y dejar de atender de forma permanente solicitudes no planificadas

Acciones básicas a tomar (1)

- Actualizar constantemente el software de los dispositivos tecnológicos: computadores, tabletas, dispositivos móviles, dispositivos del hogar en general.
- No compartir credenciales o contraseñas de correo electrónico, sistemas de información, bancos o cualquier aplicación en general.
- Utilizar contraseñas diferentes y complejas para cada facilidad tecnológica a usar, resguardarlas correctamente y cambiarlas periódicamente

Acciones básicas a tomar (2)

- Evitar utilizar software desconocido, de origen incierto o no autorizado.
- Instalar y mantener actualizado un software del tipo Internet Security, al menos en el computador, del tipo comercial (de pago)
- Habilitar el doble factor de autenticación (2FA) en sistemas críticos, por ejemplo bancos, sitios de compras en línea y afines.
- No conectarse a redes WiFi públicas, o del todo desconocidas, particularmente para llevar a cabo transacciones en línea.
- Utilizar sitios web transaccionales seguros, y verificarlos (no solamente es https)

Acciones básicas a tomar (3)

- No abrir correos electrónicos sospechosos y abrir sus archivos adjuntos
- No abrir enlaces web desconocidos, que probablemente son falsos y nos llevarán a una página web muy parecida, a la original (suplantación de identidad)
- Escribir de forma directa la dirección de sitios web generalmente asociados a comercio electrónico o la banca.
- Utilizar correos electrónicos privados para trámites personales.
- Generar correos electrónicos alternativos para otro tipo de transacciones en línea.

Acciones básicas a tomar (4)

- Detener de forma inmediata los intentos forzados para brindar información personal, particularmente por la vía telefónica
- Acordar institucionalmente, las formas oficiales de comunicación entre jefaturas y grupos de trabajo, que evite la suplantación de identidad
- Seguir los procedimientos institucionales para encargar la ejecución de labores formales
- Definitivamente, no “dar click” a cualquier mensaje de software. Es decir, debe existir absoluta certeza de lo que se hace y lo que no se hace.

Acciones básicas a tomar (5)

- Desactivar o eliminar accesos de sistemas no utilizados, o de sitios donde la persona no labore más
- Llevar a cabo respaldos periódicos de información, como contingencia
- Definir el uso de firma digital para procedimientos oficiales
- Generar un perfil de invitados WiFi con contraseña fuerte en el hogar
- Valorar lo que se publica en redes sociales y lo que no debe publicarse