Preguntas y Respuestas CSIRT-CR

1. **¿Cómo me doy cuenta cuando tengo virus en la computadora?**

   Algunos de los comportamientos que normalmente tienen las computadoras infectadas son:

   - Se pone muy lenta
   - Las aplicaciones no inician o no responden
   - Los programas dejan de funcionar
   - Internet no conecta o se pone muy lento
   - Cuando estamos en una página en Internet se abren ventanas o páginas no solicitadas.
   - Pérdida total o parcial de archivos y carpetas que tenemos en la computadora
   - Se desactiva el antivirus que tenemos instalado
   - Se cambia el idioma que tenemos configurado
   - Aparece en la pantalla información extraña e imágenes desconocidas
   - Se ejecutan solos algunos programas
   - Se envían correos a nuestros contactos
   - El sistema operativo no arranca

   Se recomienda que se utilice un antivirus y antimalware para revisar el equipo si sospecha de tener algún virus.

2. **¿Es necesario el acompañamiento de los padres de familia cuanto estamos en contacto directo con los estudiantes, ya sea Teams o cualquier medio digital? Para nuestra protección como docente.**

   Se recomienda que los padres acompañen a los menores de edad en su proceso de aprendizaje en medios digitales, ya que no es aconsejable que los menores usen el dispositivo tecnológico sin supervisión, y ante cualquier duda de los procedimientos que deben seguir deben de preguntar al MEP para que les indiquen cómo proceder

3. **¿Qué tan peligroso es conectarse en los Wi-Fi libres de locales?**

   El Wi-Fi nos ha permitido aprovechar el servicio de internet en lugares públicos. Sin embargo, debemos de pensar en que tan seguras son estas conexiones, porque:

- Podemos ser víctimas de ataques “Man in the Middle”, se traduce a “hombre en el medio”, se relaciona con la presencia de un intermediario entre la víctima y el sitio que ésta visita.
- Nos pueden robar datos personales e información confidencial
- Pueden existir redes WiFi falsas que se presentan sin clave
- El router puede estar vulnerado.

Por lo cual **NO** es recomendable acceder a redes públicas, ya que podemos ser víctimas de los ciberdelincuentes.

4. Si yo hago mi respaldo en la nube, ¿tiene la misma seguridad que si lo hago en un dispositivo físico, o está en peligro mi información?

Ambos respaldos tienen sus ventajas y desventajas.

Las copias de seguridad locales deben de guardarse en dispositivos externos, puede ocurrir cualquier eventualidad, ya que estos dispositivos pueden sufrir daños físicos que lleven a la pérdida total de la información, esta vulnerabilidad no ocurre en la Nube.

Las Copias de Seguridad en la nube son vulnerables a malas sincronizaciones y accesos no autorizados que de igual manera llevan a la pérdida total de la información. Puesto que un borrado accidental, inmediatamente se sincroniza eliminándolo de todos los dispositivos, lo mismo ocurre si modificamos algún archivo de forma equivocada, automáticamente se sincroniza y se modifica erróneamente en todos los dispositivos.

Por esto se recomienda que sean simultáneos, que se realicen tanto Copias de Seguridad en la nube para mantener la información actualizada y disponible en cualquier sitio de trabajo, pero sin dejar de tener las Copias de Seguridad Local, en dispositivos de almacenamiento, que se encuentra de manera externa y se conserve un histórico de archivos almacenados.

5. **¿Cómo verificar que un correo electrónico que me llega sea auténtico por ejemplo del banco?**

   Es importante considerar los siguientes aspectos:

   - El dominio de la dirección de email no coincide con el del banco.
   - Faltas de ortografía o de concordancia
   - El correo solicita información personal
   - El asunto del correo es de máxima alerta
   - Generalmente se incluyen archivos adjuntos no confiables.

   Y el aspecto más importante es recordar que el banco nunca le pedirá sus datos personales ni por correo ni por teléfono

6. **¿Qué es el control parental? ¿Es un software?**

   Control parental son herramientas que van a permitir a los padres y madres a poder controlar y a limitar los contenidos que sus hijos e hijas acceden en Internet desde sus dispositivos (computadoras, celulares, tablets). Dónde se puede monitorear la navegación, restringir contenidos no aptos para menores, así como bloquear páginas o usuarios que pueden ser una amenaza para los niños y niñas., así como establecer límites de tiempo de uso del dispositivo

   Son aplicaciones que se instalan es su dispositivo y se configuran para su uso.

7. **¿Cuáles son los pasos a seguir para denunciar legalmente alguna estafa informática?**
   En casos de denuncias por delitos informáticos, debe proceder a interponerla en el Organismo de Investigación Judicial, en el siguiente enlace podrá encontrar la información pertinente https://sitiooij.poder-judicial.go.cr/index.php/ayuda/video-respuestas/item/10715-que-se-debe-hacer-para-presentar-una-denuncia

8. **En nuestra institución nos piden evidencias del trabajo hecho por los estudiantes (fotos de mensajes, conversaciones o correos que los estudiantes nos envían). ¿Eso no es violación también?**

   De igual forma que en físico reciben las tareas de sus estudiantes para los fines de evaluar, ahora deben recibir las tareas y trabajos de manera digital y deben ser registrados y utilizados para el fin de evaluar el aprendizaje, ante dudas de cómo

proceder debe comunicarse con el MEP para que le indique los procesos a seguir para las tareas o trabajos en formato digital.

9. ¿Por qué En los delitos cibernéticos y/o telefónicos no permiten las grabaciones como prueba si es la más viable?

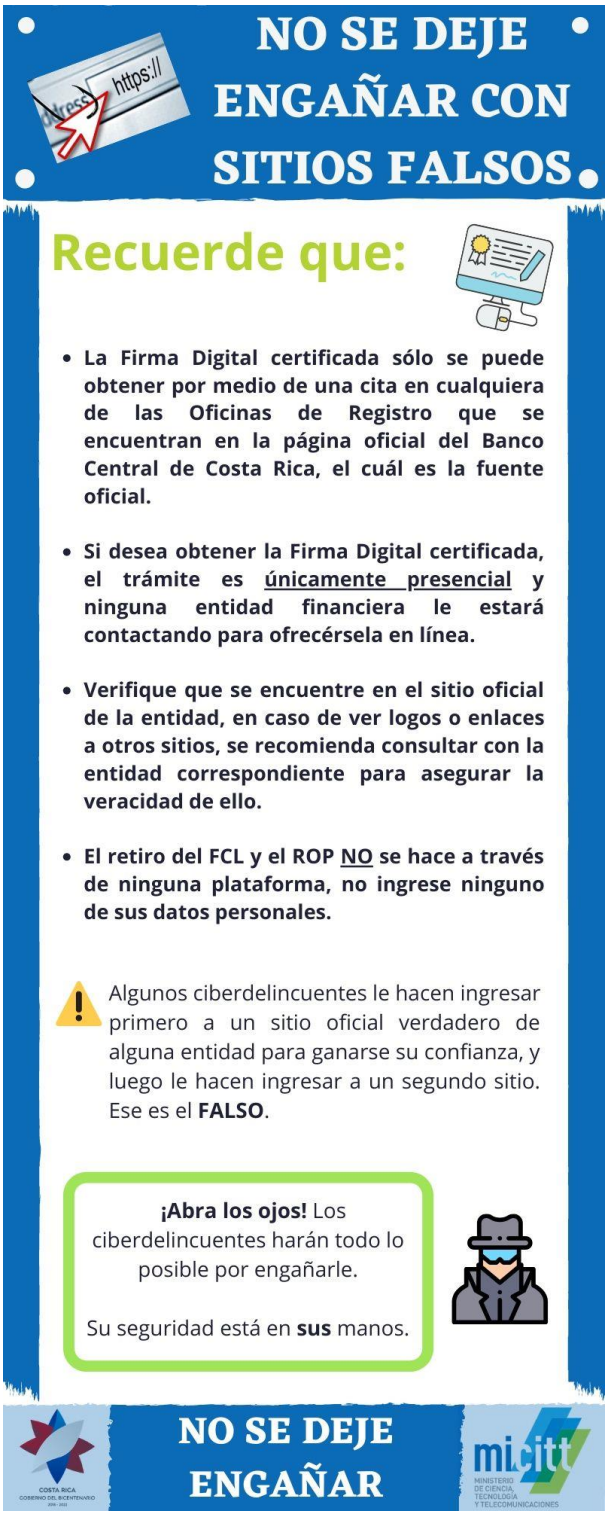
Cada caso implica un análisis distinto, por lo que no se podría generalizar que no se permitan, lo que debe existir es un debido proceso de la prueba digital aportada, en caso de tener que presentar este tipo de prueba recomendamos se asesore con abogados en la materia de delitos informáticos que estudie el caso y le indique el mejor proceso a seguir.

10. ¿La firma digital se presta para estafas?

No, la firma digital es un dispositivo tecnológico robusto y seguro, ya que, para utilizar firma digital certificada, se usan dos factores, algo que la persona tiene (la tarjeta) y algo que la persona sabe (PIN). Algunos casos que se han conocido de estafas, lo que hacen los cibercriminales es utilizar el tema de firma digital para atraer la atención de la persona (como gancho para ejecutar la estafa) por medio de Ingeniería Social para que la persona ingrese a otros sitios, los cuales son falsos, y brinde información sensible, como sus datos bancarios, con la cual se realiza la estafa, es por esta razón que no debe brindar nunca sus datos personales.

Se adjuntan infografías para guía sobre este tema:


NO SE DEJE ENGAÑAR CON SITIOS FALSOS
NO SEA UNA VÍCTIMA DE ESTAFA
Tome en cuenta las siguientes recomendaciones:
1 El certificado de la página web debe de ser mayor a 3 meses.
2 La mayoría de los sitios web oficiales terminan en:
- Gobierno .go.cr
- Financiero .fi.cr
- Salud .sa.cr
- Organización .or.cr
Si en una llamada telelefónica indican que ingrese a una página "oficial de gobierno" que finalice con .com
DESCONFÍE.
TENGA EN CUENTA!!
https://www.NombredeDominioCR.com
Verifique que la dirección web a la que va a ingresar sea https
Dar clic al candado que se encuentra a la izquierda, para asegurarse que el certificado tenga una validez de 1 año o más.
Si el dominio tiene CR antes del punto de la extensión, no se confíe, no significa que sea un sitio oficial.
.go.cr
.fi.cr
.sa.cr
.or.cr
.com
.net
SITIOS .COM QUE SI SON OFICIALES
- bancobcr.com
- baccredomatic.com
- bancobct.com
- bancocathay.com
- bnfondos.com
- grupoimprosa.com
- lafise.com
- becasmicitt.com
- ins-cr.com
- grupoice.com
- scotiabankcr.com
- coopeande1.com
- credilat.com
- prival.com
- crpreviene.com
- coopelecheros.com
- munigoicoechea.com
- procomer.com
- aldesa.com
NO SE DEJE ENGAÑAR


NO SE DEJE ENGAÑAR CON SITIOS FALSOS
Recuerde que:
• La Firma Digital certificada sólo se puede obtener por medio de una cita en cualquiera de las Oficinas de Registro que se encuentran en la página oficial del Banco Central de Costa Rica, el cuál es la fuente oficial.
• Si desea obtener la Firma Digital certificada, el trámite es únicamente presencial y ninguna entidad financiera le estará contactando para ofrecérsela en línea.
• Verifique que se encuentre en el sitio oficial de la entidad, en caso de ver logos o enlaces a otros sitios, se recomienda consultar con la entidad correspondiente para asegurar la veracidad de ello.
• El retiro del FCL y el ROP NO se hace a través de ninguna plataforma, no ingrese ninguno de sus datos personales.
Algunos ciberdelincuentes le hacen ingresar primero a un sitio oficial verdadero de alguna entidad para ganarse su confianza, y luego le hacen ingresar a un segundo sitio. Ese es el FALSO.
¡Abra los ojos! Los ciberdelincuentes harán todo lo posible por engañarle.
Su seguridad está en sus manos.
NO SE DEJE ENGAÑAR