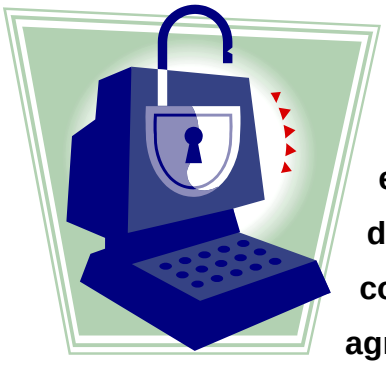
MANUAL DE BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN



Al igual que las amenazas informáticas en general, los códigos maliciosos fueron evolucionando al mismo tiempo de las tecnologías de información y comunicación, aumentando considerablemente el nivel de complejidad y agresión. Es por eso que la visión y la filosofía de CFP VERGE DE CORTES consideran la protección de manera proactivo, no sólo a través de sus soluciones de seguridad sino también a través de la educación.

Es necesario que los usuarios incorporen buenas prácticas para proteger el ámbito de información, y prevenir más la posibilidad de formar parte del conjunto que engloba a las potenciales y eventuales víctimas de cualquiera de las amenazas, que constantemente buscan tirar provecho de las debilidades humanas. Pero para eso inevitablemente se deben conocer los peligros latentes, y como detenerlos a través de mecanismos de prevención.

El presente documento expone medidas de seguridad tendentes a minimizar el volumen de "potenciales víctimas", brinda herramientas preventivas para cada una de las tecnologías y servicios más populares y más
utilizados por los usuarios y aborda en cada punto los mecanismos de prevención que permiten detectar, de manera tempranera y sin acciones complejas, las acciones maliciosas más comunes.

El presente código de buenas prácticas en seguridad informática está orientado a todo el personal que trabaja para lo en nombre de CFP VERGE DE CORTES.

2. MANTENER ACTUALIZADO El SISTEMA OPERATIVO Y Las APLICACIONES

Malware (del inglés malicious software), también llamado badware, software malicioso o software malintencionado es un tipo de software que tiene como objetivo infiltrarse o dañar un ordenador sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático es utilizado en muchas ocasiones para referirse a todos los tipos de malware, incluyendo los verdaderos virus.

La historia del malware los brindan la respuesta de por qué es importante mantener actualizados los sistemas operativos (SO) y las aplicaciones con sus correspondientes parches de seguridad.

En cuanto a este aspecto de la seguridad, las medidas prácticas de prevención se enfocan en:

- **No descargar actualizaciones desde sitios de dudosa reputación y hacerlo sólo desde sitios de confianza. Descargar las actualizaciones desde sitios no oficiales implica un potencial riesgo de infección.**
- **Descargar las actualizaciones a través de los mecanismos ofrecidos por el fabricante.**
- **Para las plataformas Microsoft se pode:**
    - **Acceder al sitio web de Windows Update para obtener los últimos parches de seguridad.**
    - **Configurar en el Centro de Seguridad de Windows la automatización, o no, de descarga de actualizaciones.**
    - **Implementar (en ámbitos corporativos) los WSUS (Windows Server Update Services) de Microsoft.**

3. ASEGURAMENTO DEL SISTEMA OPERATIVO

Otro de los aspectos importantes en materia de prevención, radica en configurar el sistema operativo para hacerlo más seguro. Entre las buenas prácticas que se pueden tener en cuenta se encuentran:

- **Utilizar contraseñas fuertes. El empleo de contraseñas donadas de recordar es otra de las debilidades que los códigos maliciosos suelen aprovechar para propagarse por los recursos de información.**
- **Crear un perfil de usuario con privilegios restringidos. Por defecto, usuario que crean las plataformas Windows al punto de su implementación posee privilegios administrativos. Esto es un factor que aumenta la probabilidad de infección.**
- **Deshabilitar la ejecución automática de dispositivos USB. Los dispositivos de almacenamiento que se conectan al puerto USB constituyen un vector de ataque muy empleado por el malware para la propagación, sobre todo, de vermes.**

- **Configurar la visualización de archivos ocultos ya que la mayoría de los códigos maliciosos se esconden en el sistema con este tipo de atributos.**

- **Configurar la visualización de las extensiones de archivos para poder identificar las extensiones de los archivos descargados y no ser víctimas de técnicas como la doble extensión.**

4. PROTECCIÓN EN El CORREO ELECTRÓNICO

El correo electrónico constituye una de los canales de propagación/infección de malware más utilizados por atacantes; por lo tanto es importante que los usuarios incorporen como hábito determinadas prácticas que permitan prevenir los ataques realizados a través de que códigos maliciosos.

En consecuencia, a continuación se presenta una serie de medidas preventivas orientadas a aumentar la seguridad durante lo uso del correo electrónico.

4.1 Spam

Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican, de alguna o varias maneras al receptor.

Constituye uno de los principales medios de propagación de una importante cantidad de códigos maliciosos y por lo tanto se recomienda:

- **No confiar en correos spam con archivos adjuntos y explorar el archivo antes de ejecutarlo. Esto asegura que no se ejecutará un malware.**
- **Cuando se reciben adjuntos, prestar especial atención a las extensiones de estos, ya que suelen utilizar técnicas de engaño como la doble extensión o espacios entre el nombre del archivo y la extensión de este.**

- **Evitar publicar las direcciones de correo en sitios web de dudosa reputación como foros, chats, entre otros.**
- **Utilizar filtros anti-spam que permitan el filtrado del correo no deseado.**
- **No responder jamás el correo spam. ES preferible ignorarlos y/o borrarlos, ya que se responde se confirma que la dirección de correo se encuentra activa.**
- **Dentro de lo posible, evitar el re-envío de mensajes en cadena, ya que**

suelen ser utilizados para recoger direcciones de correo activas.

- **Si de todas formas se desea enviar mensajes en cadena, es recomendable hacerlo siempre con copia oculta para que quien lo recibe léela sólo la dirección del emisor.**
- **Utilizar claves seguras y cambiar la contraseña con periodicidad.**

- **Configurar la pregunta secreta, además, de una forma que no sea adivinable para fortalecer aún más la seguridad de la cuenta.**
- **Como medida de seguridad extra, bloquear las imágenes de los correos y descargarlas cuando se asegure de que el correo no es dañino.**
- **También es preferible que se evite ingresar el nombre de usuario y su respectiva contraseña en sitios de los cuales no se tenga referencia.**

4.2 Phishing

El phishing es una modalidad delictiva encuadrada en la figura de estafa realizada a través de Internet, y constituye otra de las amenazas de seguridad más propagadas a través del correo electrónico caracterizado por intentar adquirir información confidencial de forma fraudulenta (cómo puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

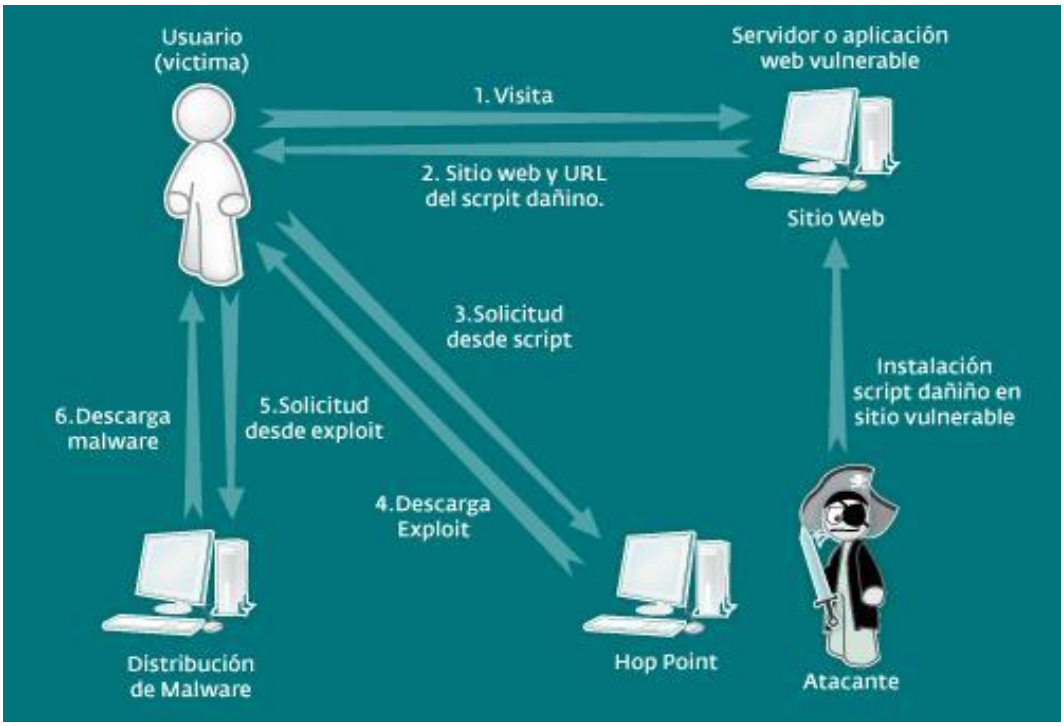
Entre las buenas prácticas de seguridad que se recomiendan a los usuarios, para que estos eviten ser víctimas del phishing, están las siguientes:

- **Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio.**
- **Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles.**
- **No hacer clic sobre enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden re-direccionar hacia sitios web clonados o hacia la descarga de malware.**
- **Asegurarse de que la dirección del sitio web al cual se accede comience con el protocolo https. La "s" final, significa que la página web es segura y que toda la información depositada en esta viajará de manera cifrada.**
- **Verificar la existencia de un certificado digital en el sitio web. El certificado digital se despliega en pantalla al hacer clic sobre la imagen del candado.**
- **Revisar que el certificado digital no caducara, ya que este podría haber sido manipulado intencionalmente con fines maliciosos.**

- **Comunicarse telefónicamente con la compañía para descartar la posibilidad de ser víctimas de un engaño, si se tiene dudas sobre la legitimidad de un correo.**
- **Jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través del correo electrónico, ya que la comunicación podría ser interceptada y robada.**
- **Habituarse a examinar periódicamente la cuenta bancaria, con el fin de detectar a tiempo alguna actividad extraña relacionada con la manipulación de la cuenta o transacciones no autorizadas.**

5. SEGURIDAD EN La NAVEGACIÓN

Nos últimos años, Internet se transformó en una plataforma de ataque donde acciones delictivas se llevan a cabo a través de diferentes técnicas como por ejemplo el Drive-by-Download que permite infectar masivamente los usuarios simplemente ingresando a un sitio web determinado. Mediante esta técnica, los creadores y diseminadores de malware propagan sus creaciones aprovechando las vulnerabilidades existentes en diferentes sitios web e inyectando código dañino entre su código original.



En consecuencia, es fundamental navegar con cautela y tener presentes las recomendaciones más importantes. Entre ellas:

- **Impedir la ejecución de archivos desde sitios web sin verificar previamente que es lo que dice ser. ES importante no hacer clic sobre el botón ejecutar ya que esto provoca que el archivo se ejecute**

  automáticamente después de descargado, dejando a la margen a posibilidad de verificar su integridad.

- **Descargar programas de seguridad solamente desde lo sitio oficial de este, para evitar la descarga de archivos que pudiesen previamente ser manipulados con fines delictivos.**
- **A ser posible, leer atentamente las políticas de privacidad de las aplicaciones descargadas desde sitios web no oficiales o de dudosa reputación, antes de instalarlas.**
- **No realizar la instalación de complementos extras como barras de tareas o protectores de pantallas sin verificar previamente su autenticidad.**
- **Configurar el navegador web para minimizar el riesgo de ataques a través de este.**

6. SEGURIDAD EN REDES SOCIALES

En la actualidad, las redes sociales son muy populares y los usuarios las utilizan masivamente; estas características las transforman en importantes focos de propagación de malware. Por tal motivo, se torna necesario tener en cuenta y aplicar las siguientes medidas preventivas:

- **Intentar no publicar información sensible y confidencial, debido la que personas extrañas pueden aprovechar esta información con fines maliciosos.**
- **También es recomendable evitar la publicación de fotografías propias y de familiares.**
- **Mantener la privacidad del perfil; es decir, configurar el perfil para que no sea público.**
- **No responder a las solicitudes de desconocidos, ya que pueden contener códigos maliciosos o pueden formar parte de actividades delictivas.**
- **No abrir contenidos con spam a través de este medio. De este modo se evita formar parte del ciclo de vida del spam.**
- **Cambiar periódicamente la contraseña para evitar que esta sea descubierta fácilmente.**
- **Antes de aceptar contactos espontáneos, es recomendable verificar su existencia y que realmente provienen de quien dice ser.**

7. SEGURIDAD EN MENSAJERÍA INSTANTÁNEA

Otro medio de comunicación popular, y que se emplea masivamente, es la mensajería instantánea, que, en consecuencia, constituyen uno de los vehículos más explotados por diferentes amenazas, dentro de las cuales una de las más activas es el malware.

Para prevenir ser víctimas de acciones maliciosas llevadas a cabo a través de esta tecnología, se recomienda aplicar alguna de las medidas de seguridad que a continuación se describen:

- **Evitar aceptar cómo contacto cuentas desconocidas sin verificar a quien pertenece, ya que en la mayoría de los casos se trata de intentos de engaños con fines maliciosos.**
- **No descargar archivos sospechosos, sobre todo cuando vienen acompañados de mensajes genéricos o en otro idioma. Esto constituye una de las características principales de los códigos maliciosos que se propagan a través de este canal de comunicación.**
- **En caso de descargar archivos, explorarlos con una solución antivirus.**
- **Configurar en la mensajería a exploración automática de archivos en el momento de su recepción. La mayoría disteis clientes consideran la posibilidad de configurarlos con un antivirus.**
- **ES recomendable, al igual que con el correo electrónico, no hacer clic sobre los enlaces incrustados en el cuerpo del mensaje, ya que pueden direccionar las páginas con contenido malicioso o hacia la descarga de malware.**
- **En el compartir información confidencial a través de este medio ya que esta puede ser interceptada y robada con fines delictivos.**
- **Cuando se reciben mensajes conteniendo uno enlace no esperado, es recomendable preguntar si la otra persona realmente lo envió; de este modo se pode verificar la autenticidad de este.**

8. SEGURIDAD EN DISPOSITIVOS DE ALMACENAMIENTO

Los dispositivos de almacenamiento que se conectan a través del puerto USB (memorias, cámaras digitales, teléfonos móviles, etc.), constituyen otro de los mayores focos de propagación/infección de códigos maliciosos.

Por lo tanto, es necesario tener presente alguna de las siguientes medidas que ayudan a mantener el ámbito de información con un nivel acomodado de seguridad, ya sea en ámbitos corporativos como en ámbitos caseros:

- **Establecer políticas que definan el uso correcto de dispositivos de almacenamiento. Esto ayuda a tener claro las implicancias de seguridad que lleva consigo el uso de estos dispositivos.**
- **Brindar acceso limitado y controlado de los usuarios que utilizan estos dispositivos, para controlar la propagación de potenciales amenazas y el robo de información.**
- **De ser necesario, registrar el uso de estos y/o habilitar/deshabilitar puertos del tipo USB.**
- **Si se transporta información confidencial en estos dispositivos, es recomendable cifrarla. De esta manera, en caso de robo o extravío, la información no podrá ser vista por terceros.**
- **ES recomendable explorar con el antivirus cualquier dispositivo que se conecte el ordenador para controlar a tiempo una posible infección.**
- **Deshabilitar la ejecución automática de dispositivos en los sistemas operativos Microsoft Windows, ya que muchos códigos maliciosos aprovechan la funcionalidad de ejecución automática de dispositivo**

s de las plataformas Microsoft para propagarse a través de un archivoAutorun.inf.