ÓRGANO JUDICIAL

DIRECCIÓN DE INFORMÁTICA

Circular D.I. 006

PARA: **TODOS LOS DESPACHOS JUDICIALES Y ADMINISTRATIVOS**

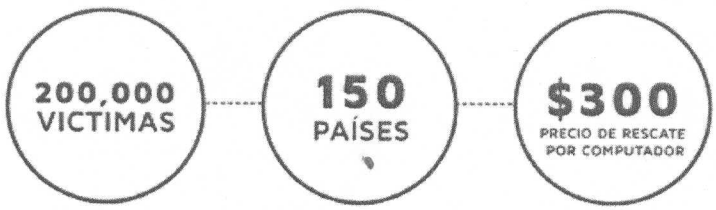
DE: **Ing. Indira Gómez, Directora.**

ASUNTO: **ADVERTENCIA DE SEGURIDAD**

FECHA: **22 de mayo de 2017**

Por este medio hacemos de su conocimiento la siguiente información:

ADVERTENCIA DE SEGURIDAD



Hoy en día las empresas públicas y privadas están siendo atacadas por Ransomware. Un ransomware (del inglés ransom, 'rescate', y ware, por software) es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate. Este programa esta teniendo un alcance masivo con mecanismos de auto-propagación que afecta potencialmente a los sistemas operativos Windows. Este tipo de ataque afecta a muchas empresas alrededor del mundo y hay varios reportes de empresas en Latinoamérica.

Métodos de propagación.

Normalmente un ransomware se transmite tanto como un troyano o como un gusano, infectando el sistema operativo, por ejemplo: con un archivo descargado o explotando una vulnerabilidad de software. En este punto, el ransomware se iniciará y cifrará los archivos del usuario con una determinada clave, que sólo el creador del ransomware conoce y proveerá al usuario que la reclame a cambio de un pago.

Cómo actúa

Este tipo de virus se camufla dentro de otro archivo o programa apetecible para el usuario que invite a hacer click. Algunos ejemplos de estos camuflajes serían:

- Archivos adjuntos en correos electrónicos.
- Vídeos de páginas de dudoso origen.
- Actualizaciones de sistemas.
- Programas, en principio, fiables como Windows o Adobe Flash.

Luego, una vez que ha penetrado en el ordenador, el ransomware se activa y provoca el bloqueo de todo el sistema operativo, lanza el mensaje de advertencia con la amenaza y el importe del rescate que se ha de pagar para recuperar toda la información. Además, en ocasiones incluyen en la amenaza la dirección IP, la compañía proveedora de Internet y hasta una fotografía captada desde la webcam.

Aunque nuestra infraestructura de seguridad informática esta protegida contra este tipo de ataques, bien es cierto que hay un factor que no podemos controlar: el factor humano por lo que recomendamos lo siguiente:

- Uso de USB sólo dentro de la red del Órgano Judicial: Ya se han dado casos que computadoras son infectadas constantemente debido al mal uso de USB, debido a que la información es transportada fuera de las computadoras del Órgano Judicial y conectadas a computadoras externas lo que conlleva una alta probabilidad de contagio de virus y agentes maliciosos.
- Sólo abrir correos electrónicos de fuentes confiables: Muchos usuarios abren cualquier correo y dan click a los links que aparecen en los mismos lo que puede provocar la descarga de códigos maliciosos; sino se conoce el lugar de dónde proviene puede reenviar el mismo a seginfo@organojudicial.gob.pa para el análisis del mismo y proceder a eliminar el correo.
- Acceso a páginas de internet que pueden contener código malicioso: Muchas páginas de internet de descarga de archivos y programas, juegos, sitios de redes sociales, entretenimiento, almacenamiento en la web, etc pueden tener infecciones que se propagan en la computadora sólo con visitar al sitio, por lo que se tiene bloqueado el acceso."

Por todo lo expuesto, y siguiendo recomendaciones de los fabricantes de equipos y programas de seguridad informática, se ha procedido a aplicar políticas de seguridad que implican la restricción de sitios maliciosos y bloqueo de acceso a dispositivos usb.

Por estas razones los equipos de seguridad con los que cuenta el Órgano Judicial restringen los sitios web de acuerdo a su nivel de riesgo, y se han bloqueado el acceso a usb en determinados momentos, ya hemos sido infectados con ransomware en algún momento, pero se ha podido controlar el brote; este tipo de ataque puede hacer que se pierda toda la información de la computadora infectada sin que se pueda recuperar, a menos que tenga copias de seguridad externamente.

Por todo lo manifestado, solicitamos se apliquen las medidas recomendadas para minimizar en lo posible cualquier tipo de contagio.