

## Recomendaciones para evitar el ingreso del *ransomware*



Todos hemos escuchado la palabra **ransomware** por lo menos una vez en estos últimos días. Y es que nos es para menos. Bancos, empresas, instituciones médicas de todo el mundo, todos bajo alarma por este ciberataque "sin precedentes".

Según la Oficina de la policía europea Europol, el ciberataque dejó más de 200.000 víctimas, principalmente empresas, en al menos 150 países.

Aquí algunas recomendaciones para evitar el ingreso del ransomware:

- ✓ Tener actualizaciones y **antivirus** instalados.
- ✓ En particular existe un "**parche**" en la actualización de Windows que impide que el virus se propague por la red, lo cual fue informado oportunamente a los responsables de seguridad de la información de las distintas instituciones de nuestra comunidad.
- ✓ **Actualizar** todos los dispositivos Windows a las últimas versiones y configurar las actualizaciones automáticas.
- ✓ Crear un respaldo externo de los archivos de computadoras y servidores, en particular, **en servidores de archivos y en la nube**.
- ✓ A las empresas que cuenten con redes WiFi a la que se conecten computadoras portátiles se les sugiere **extremar las precauciones** en cuanto al control de los equipos que se conecten.
- ✓ Como detalle técnico, es posible mitigar la propagación a nivel de red, bloqueando el tráfico en los puertos: 137/UDP y 138/UDP, 139/TCP 445/TCP.
- ✓ Se recomienda no tener las computadoras expuestas directamente a internet sin un **Firewall**.
- ✓ Tener cuidado al recibir correos electrónicos con adjuntos. Solo abrir los que se conocen.
- ✓ Observar detenidamente el texto de un correo que trae adjunto: por lo general los que traen software malicioso o virus tienen una redacción distinta a la que usaría cualquier persona.

- ✓ Si se recibe un adjunto con la **extensión .exe, no abrirlo nunca.**
- ✓ **En caso de detectarse una infección,** se debe aislar de la red el equipo afectado, apagarlo y, posteriormente, contactar a un especialista de seguridad informática.

Por mayor seguridad, lo invitamos a consultar sobre nuestros servicios de **Gestión de Infraestructura, Cloud Computing y Respaldos de datos.** Todos soportados por un equipo de técnicos e ingenieros especializados.

➤ Gestión de  
infraestructura

➤ Gestión de  
Software

➤ Consultoría /  
Gestión de Proyectos

➤ Gestión de Recursos Humanos / Outsourcing de personal

➤ Monitoreo y soporte 24hs los 365 días del año. / Tercerización de Personal Técnico