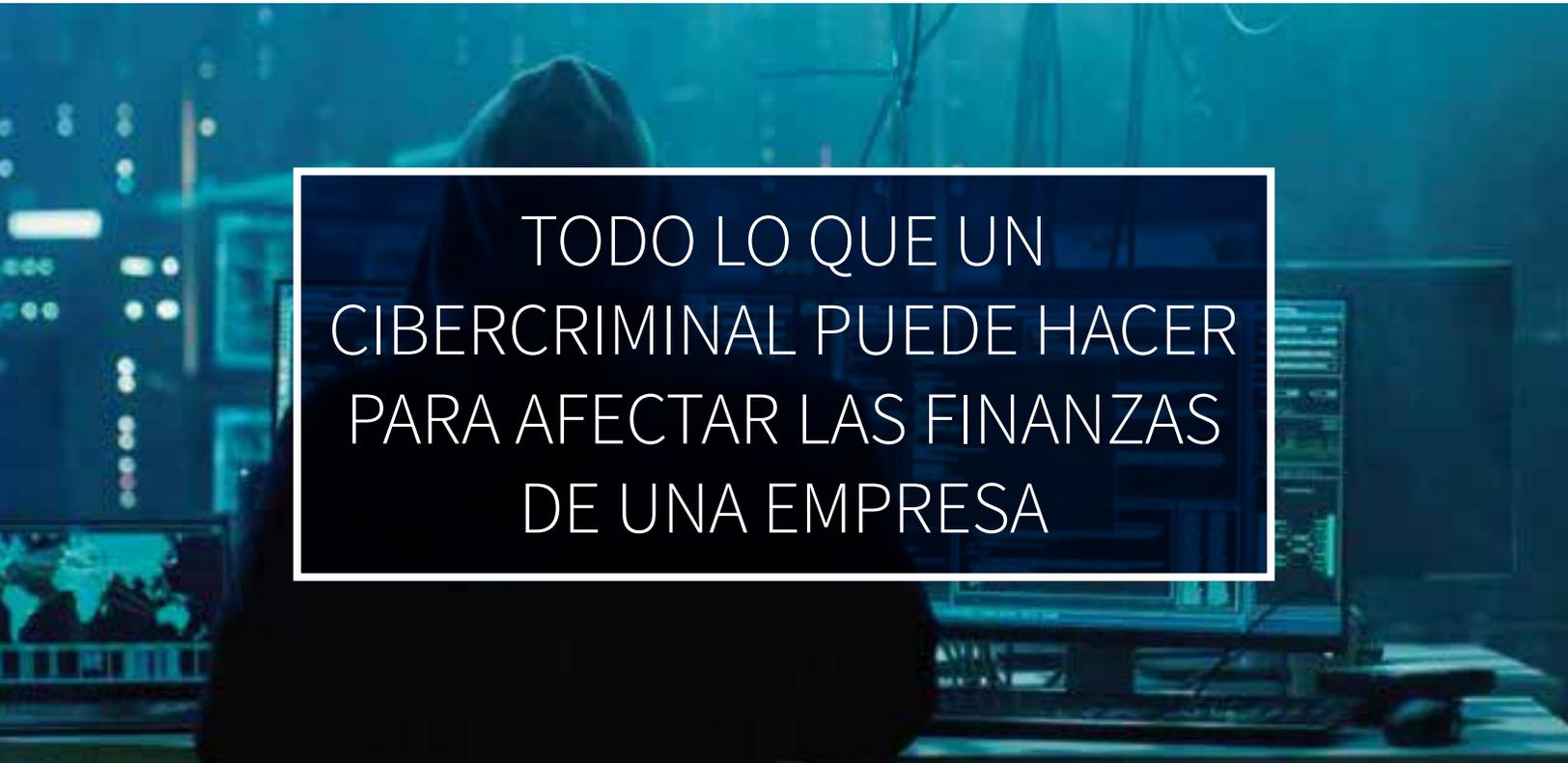




Managed secure IT | no matter what



TODO LO QUE UN  
CIBERCRIMINAL PUEDE HACER  
PARA AFECTAR LAS FINANZAS  
DE UNA EMPRESA

Un número cada vez mayor de cibercriminales desarrollan herramientas diseñadas para vulnerar la seguridad de tu empresa y afectarla en donde más duele: sus finanzas.

Entre las armas más comunes de este tipo de hackers destacan malware, bots, ransomware y protocolos fraudulentos que van drenando los recursos de una compañía sin que nadie se de cuenta hasta que ya es demasiado tarde.

# Security

Tal vez el ataque no sea directamente a los números de una empresa, pero sí a la estructura que usa para contabilizar inversiones, ingresos y egresos.

Un ataque cibernético no solo se traduce en el robo de recursos, sino también en el secuestro de información vital por el que un gran número de compañías de clase mundial acaban pagando una sustancial suma de dinero por su liberación.

Este tipo de ataques representan pérdidas por millones de dólares, no solo en robos, sino también en la interrupción del flujo de ingresos y la pérdida de confianza de los clientes y proveedores.



Este fenómeno es incluso más común en México, donde aún no hay protocolos establecidos para proteger a las empresas de los cibercriminales que busquen vulnerarlas.

Por esta y más razones, la proliferación del ciberdelito se ha acelerado más durante los últimos años y, según los informes más recientes sobre seguridad digital para empresas, el cibercrimen no se detendrá a menos que las empresas comiencen a invertir más en su seguridad cibernética.



Iniciativas como el Plan Nacional de Ciberseguridad diseñado por la oficina de la Estrategia Digital Nacional (EDN) son excelentes pasos para regular el crimen que afecta a las empresas, pero mientras este no se comience a ejecutar y se consolide a gran escala, los criminales continuarán operando sin obstáculo alguno.



De acuerdo a un estudio reciente de la firma de seguridad Norton, el costo del cibercrimen ascendió a más de 94 mil millones de dólares, tan solo durante el año pasado y más de la mitad de la población de Europa se ha visto afectada por las actividades ilícitas de unos cuantos.

De este porcentaje, uno muy importante afecta directamente a las empresas que no han invertido en una arquitectura integral de seguridad digital basada en la Nube que permita a los empleados de una compañía operar bajo estrictos estándares de protección contra el cibercrimen.



# Security

La integración de nuevos canales de comunicación y fuentes de ingresos como las redes sociales, el Internet of Things y el Cloud Computing se convierten en canales ideales para convertirse en víctima de un fraude o un robo cibernético, pero junto a estas nuevas tecnologías también se desarrollan formas innovadoras y económicamente asequibles de protección contra las amenazas.



En México hay especialistas en seguridad digital enfocada en empresas que podrían ayudar a cualquier CFO a proteger su área de expertise, que son, además de costeables, una gran inversión para asegurar el futuro financiero de cualquier negocio, sin importar su escala o giro.

La protección financiera contra criminales cibernéticos nunca debe ser tomada a la ligera pues cuando una brecha de seguridad se abra y las finanzas comiencen a sufrir golpe tras golpe, cualquier Jefe de Finanzas deseará haber tenido un experto en seguridad digital cerca.

## Síguenos en nuestras redes sociales:



MexisMX



Servicios  
Administrados  
Mexis, S.A. de C.V.



Mexis TI



Servicios  
Administrados  
Mexis, S.A. de C.V.