Canon

Empresas bajo ataque:
Ciberamenazas y Soluciones efectivas.

Ver más >>

Canon

Contenido

Introducción

El entorno de ciberseguridad en México ha experimentado un incremento alarmante en la frecuencia y sofisticación de ciberataques. Durante el primer semestre de 2024, se registraron más de 31 mil millones de intentos de ciberataques en el país, colocando a México como la nación más afectada de América Latina[1].

Las principales industrias afectadas incluyen manufactura, salud, transporte, logística y el sector financiero. La falta de preparación y la alta conectividad de las organizaciones mexicanas han convertido al país en un objetivo atractivo para actores maliciosos que buscan robar información, interrumpir operaciones y realizar extorsiones a gran escala.

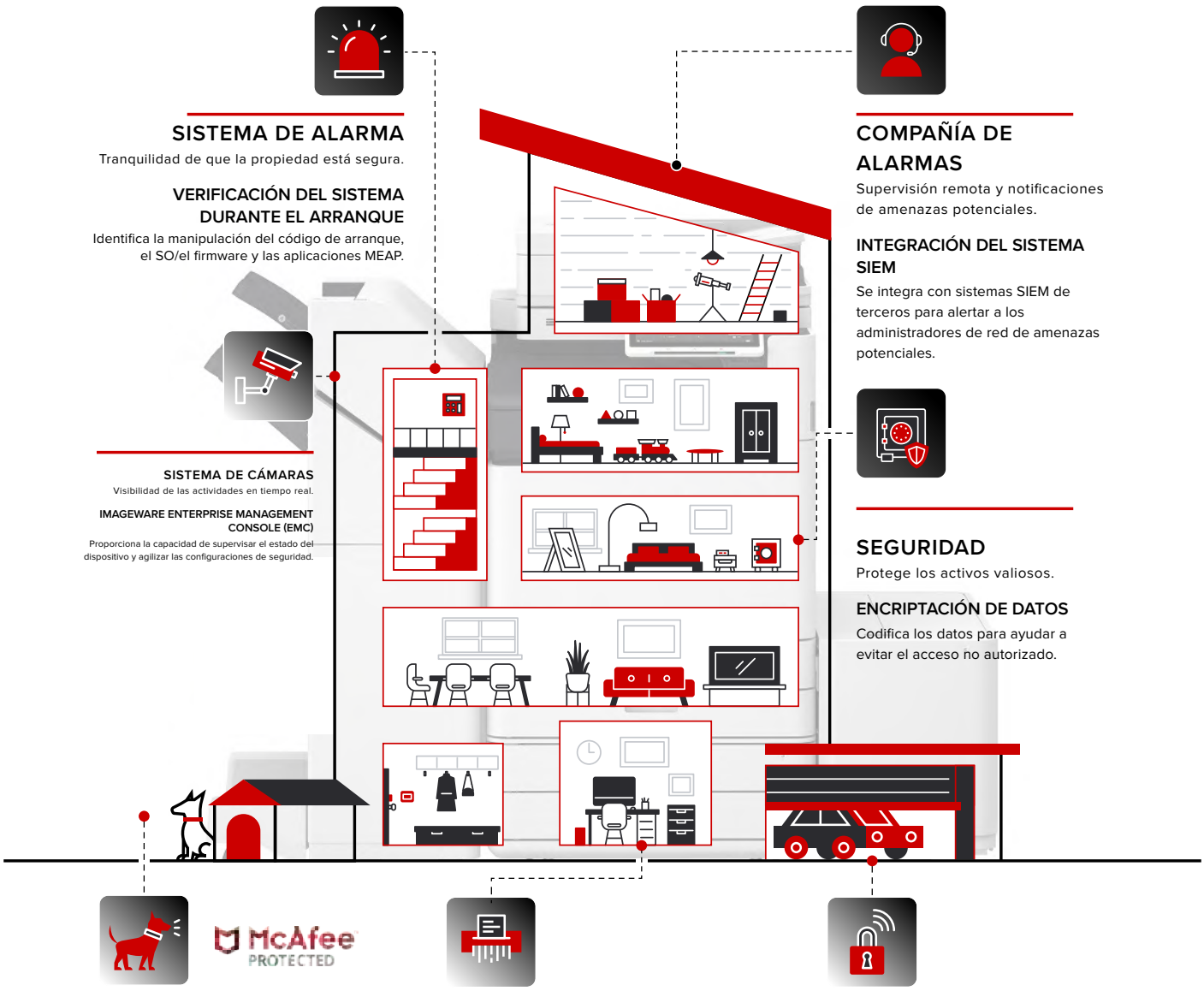
Además, un 65% de las empresas mexicanas confirmaron haber sido víctimas de violaciones de ciberseguridad en 2023, y se espera que esta tendencia continúe en 2024 debido a la adopción acelerada de tecnologías digitales sin las medidas de seguridad adecuadas[2].

Estos incidentes resaltan la necesidad urgente de implementar soluciones avanzadas y prácticas de ciberseguridad para proteger los activos de las empresas.

Este documento explora seis tipos de ciberamenazas que representan un riesgo significativo para las organizaciones y analiza cómo Canon, como proveedor de soluciones de tecnología y seguridad documental, puede contribuir a la prevención y mitigación de estos riesgos.

CÓMO PROTEGER LOS DATOS DE SU EMPRESA DE LA MISMA MANERA QUE PROTEGE SU HOGAR

Protegemos nuestros hogares con funciones de seguridad para controlar el acceso y proteger los objetos de valor, y sus impresoras multifuncionales deberían ayudarle a hacer lo mismo. La línea más reciente de imageRUNNER ADVANCE de Canon cuenta con una amplia variedad de características de seguridad para mantener sus datos seguros.



SISTEMA DE ALARMA

Tranquilidad de que la propiedad está segura.

VERIFICACIÓN DEL SISTEMA DURANTE EL ARRANQUE

Identifica la manipulación del código de arranque, el SO/el firmware y las aplicaciones MEAP.

SISTEMA DE CÁMARAS

Visibilidad de las actividades en tiempo real.

IMAGEWARE ENTERPRISE MANAGEMENT CONSOLE (EMC)

Proporciona la capacidad de supervisar el estado del dispositivo y agilizar las configuraciones de seguridad.

COMPAÑÍA DE ALARMAS

Supervisión remota y notificaciones de amenazas potenciales.

INTEGRACIÓN DEL SISTEMA SIEM

Se integra con sistemas SIEM de terceros para alertar a los administradores de red de amenazas potenciales.

SEGURIDAD

Protege los activos valiosos.

ENCRIPTACIÓN DE DATOS

Codifica los datos para ayudar a evitar el acceso no autorizado.

PERRO GUARDIÁN

Protege contra amenazas inesperadas.

CONTROL INTEGRADO DE MCAFEE

Utiliza listas blancas para ayudar a prevenir la ejecución de programas malignos (malware), así como la manipulación de firmware y aplicaciones.

TRITURADORA DE PAPEL

Protege la información confidencial para que no caiga en las manos equivocadas.

BORRADO DE LOS DATOS DE LA HDD

Elimina los datos del trabajo después de cada tarea mediante un proceso de sobrescritura.

BLOQUEO INTELIGENTE

Otorga acceso solo a través de una clave o código de acceso.

AUTENTICACIÓN DEL DISPOSITIVO

Requiere que los usuarios verifiquen su identidad para obtener acceso al dispositivo.

Principales ciberamenazas y prevención con las soluciones de Canon.

1. Campañas de espionaje.

Descripción de la amenaza:

Las campañas de espionaje se llevan a cabo a través de técnicas avanzadas como spear-phishing y el uso de software espía. Grupos organizados se enfocan en objetivos gubernamentales y militares para recopilar información estratégica. En 2022, se hizo público el lanzamiento de la operación Desert Falcons, donde se utilizó malware móvil para robar información confidencial de funcionarios en el Medio Oriente[3].

En México, el uso de técnicas de espionaje ha crecido, particularmente en sectores estratégicos como manufactura y logística. La falta de controles de acceso y segmentación de red facilita que los atacantes se infiltren en las comunicaciones empresariales.

¿Qué gana el hacker?

El acceso a información confidencial y de inteligencia, que luego es vendida en el mercado negro o utilizada para obtener ventaja competitiva y manipular decisiones políticas y empresariales.

¿Qué hace el hacker después del ataque?

Los hackers monitorean las comunicaciones de la víctima a largo plazo, roban datos sensibles y los transfieren a sus servidores para su análisis o venta.

¿Cómo puede ayudar Canon?

Canon ofrece soluciones como **uniFLOW**, que aseguran la gestión de documentos confidenciales con políticas de acceso basadas en roles y cifrado de información. Estas herramientas permiten monitorear el flujo de documentos y restringir el acceso a información sensible mediante autenticación multifactorial.

uniFLOW

Acciones preventivas:

- ☑ Implementar autenticación avanzada en todos los dispositivos Canon.
- ☑ Cifrado de documentos para asegurar que los datos robados sean inutilizables sin las claves correctas.
- ☑ Auditoría de seguridad para detectar comportamientos sospechosos en tiempo real.
- ☑ Simulaciones de spear-phishing ayudan a preparar a los empleados y detectar deficiencias en los controles de acceso.

Síntomas de un ataque:

Actividad de red inusual, conexiones a servidores externos desconocidos y aplicaciones que se ejecutan sin autorización.

Reacción inmediata:

Desconectar los sistemas afectados, realizar un análisis forense y cambiar las credenciales para evitar nuevas filtraciones.

2. Robo de datos.

Descripción de la amenaza:

El robo de datos se produce cuando un atacante obtiene acceso a bases de datos confidenciales de una empresa.

Durante 2023, más del 60% de las empresas mexicanas fueron víctimas de ataques que resultaron en la pérdida de información crítica[2].

¿Qué gana el hacker?

Información como datos financieros, registros de clientes y propiedad intelectual que se puede vender en la dark web o usar para chantajear a la organización.

¿Qué hace el hacker después del ataque?

Los datos se utilizan para extorsionar a la empresa, cometer fraudes o desarrollar ataques de spear-phishing dirigidos.

¿Cómo puede ayudar Canon?

Canon proporciona herramientas como el **Secure Audit Manager** que permiten monitorear y registrar todas las actividades en dispositivos multifuncionales, detectando intentos de acceso no autorizados y movimientos de datos sospechosos.

Acciones preventivas:

- ☑ Configurar cifrado avanzado en archivos y documentos almacenados en dispositivos Canon.
- ☑ Autenticación basada en tarjetas de identificación para asegurar que solo personal autorizado tenga acceso a funciones de escaneo y copiado.
- ☑ Pentestings especializados que permiten identificar los riesgos y las debilidades en las bases de datos antes de que los atacantes puedan explotarlas.

Síntomas de un ataque:

Archivos cifrados sin autorización, transferencias masivas de datos y cambios inesperados en la configuración del sistema.

Reacción inmediata:

Desconectar el sistema afectado de la red, contactar a las autoridades y especialistas en recuperación de datos.

3. Vulnerabilidades críticas en sistemas.

Descripción de la amenaza:

Las vulnerabilidades en sistemas operativos, como GNU/Linux, son puertas de entrada comunes para atacantes que buscan comprometer la infraestructura y obtener control del entorno.

En México, las empresas suelen descuidar la aplicación de parches de seguridad, lo que las hace vulnerables a este tipo de ataque[1].

¿Qué gana el hacker?

Control total del sistema, lo que le permite instalar malware, robar información y permanecer dentro del entorno sin ser detectado.

¿Qué hace el hacker después del ataque?

Los atacantes instalan puertas traseras, minan criptomonedas o lanzan ataques a otras empresas desde el sistema comprometido.

¿Cómo puede ayudar Canon?

Canon proporciona actualizaciones regulares de firmware y software para sus dispositivos, lo que mitiga las vulnerabilidades en sus sistemas multifuncionales.

Acciones preventivas:

- ☑ Implementar un sistema de gestión automatizado para mantener todos los dispositivos actualizados.
- ☑ Controlar las políticas de seguridad para evitar la ejecución de scripts no autorizados en dispositivos Canon.
- ☑ Pruebas automatizadas verifican que los parches de seguridad se implementen correctamente en dispositivos esenciales.

Síntomas de un ataque:

Rendimiento lento, comandos desconocidos y archivos modificados sin motivo.

Reacción inmediata:

Reinstalar el software comprometido y modificar todas las claves de acceso.

4. Inyección de SQL.

Descripción de la amenaza:

La inyección de SQL es una técnica de ataque donde se manipulan formularios web para acceder a bases de datos. Este tipo de ataque puede resultar en el robo o modificación de información sensible.

En México, sectores como el retail y financiero son los más afectados por SQL debido a malas configuraciones en las bases de datos[2].

¿Qué gana el hacker?

Acceso directo a bases de datos que contienen información crítica como registros financieros y contraseñas.

¿Qué hace el hacker después del ataque?

Los atacantes venden el acceso a estas bases de datos o modifican la información para cometer fraudes.

¿Cómo puede ayudar Canon?

Canon no protege directamente las bases de datos, pero su software de captura y digitalización asegura que los documentos ingresados en sistemas críticos no contengan código malicioso.

Acciones preventivas:

- ☑ Validar entradas en los flujos de trabajo y configurar políticas para rechazar documentos sospechosos con dispositivos de impresión Canon.
- ☑ Mediante **ingeniería social**, un atacante podría obtener acceso inicial que facilite este tipo de ataques; las pruebas de penetración ayudan a validar la robustez de las aplicaciones web.
- ☑ Detener el acceso a la base de datos y aplicar parches de seguridad.

Síntomas de un ataque:

Cambios no autorizados en la base de datos y errores de ejecución.

5. Riesgos en dispositivos IoT.

Descripción de la amenaza:

Los dispositivos del Internet de las Cosas (IoT) como cámaras de seguridad, sensores industriales y routers son objetivos atractivos para los ciberdelincuentes debido a sus configuraciones de seguridad básicas y la ausencia de monitoreo constante. En México, los sectores de manufactura y logística son particularmente vulnerables a estos riesgos, ya que dependen de la infraestructura IoT para sus operaciones diarias[1].

Un estudio[4] reveló que los dispositivos IoT sin asegurar exponen a las empresas a ser utilizados en ataques DDoS, botnets o incluso espionaje industrial. Las organizaciones que no aplican parches y mejoras de seguridad regularmente se convierten en objetivos fáciles para los ciberdelincuentes. Además, se advierte que los dispositivos más vulnerables incluyen routers, cámaras IP y dispositivos médicos, los cuales representan el 75% de las infecciones de IoT registradas.

¿Qué gana el hacker?

El acceso a estos dispositivos permite a los atacantes usarlos como puntos de entrada a la red empresarial, lanzar ataques de denegación de servicio distribuido (DDoS) o utilizarlos para monitorear la infraestructura de manera encubierta.

¿Qué hace el hacker después del ataque?

Los dispositivos IoT comprometidos se agregan a botnets controladas por el atacante, se usan para espiar las operaciones de la empresa o se emplean para atacar a terceros. Los atacantes pueden alquilar estas redes de dispositivos a otros grupos para realizar operaciones más amplias.

¿Cómo puede ayudar Canon?

Canon ofrece dispositivos de impresión y escaneo conectados con capacidades de gestión avanzada y seguridad integrada, que permiten controlar de manera centralizada el acceso y uso de cada dispositivo IoT en la red. Canon también trabaja con soluciones como **uniFLOW**, que puede monitorear y gestionar los dispositivos en tiempo real, restringiendo el acceso a funciones críticas.

Acciones preventivas:

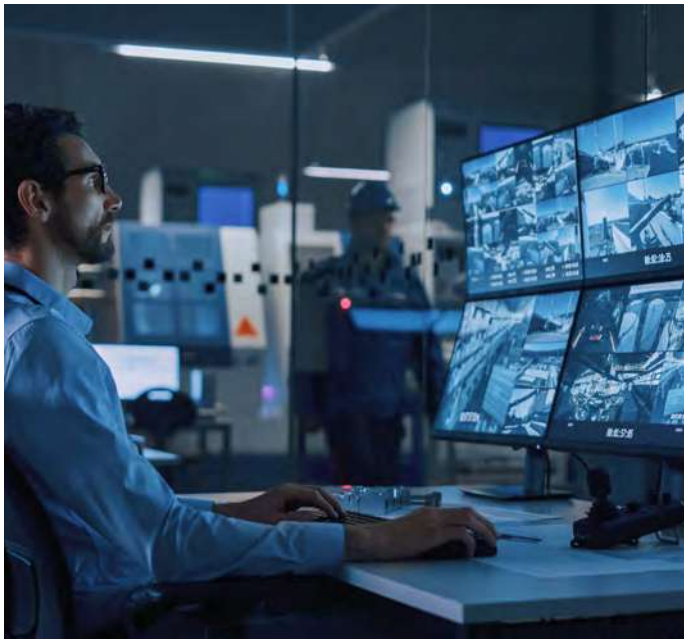
- ☑ Implementar segmentación de red para aislar dispositivos IoT y limitar el acceso solo a usuarios y servicios específicos.
- ☑ Configurar autenticación avanzada y cifrado para todos los dispositivos Canon que se conectan a la red.
- ☑ Monitoreo en tiempo real para detectar actividades anómalas y recibir alertas automáticas de posibles intrusiones.
- ☑ Los **pentest dirigidos** permiten evaluar la exposición de dispositivos IoT y recomendar mejoras en la segmentación de redes.

Síntomas de un ataque:

Comportamiento anormal en los dispositivos, caídas inesperadas de la red o reducción del rendimiento. También se pueden observar intentos de conexión a servidores externos no autorizados.

Reacción inmediata:

Desconectar los dispositivos sospechosos de la red, restablecer las configuraciones a valores seguros y realizar una auditoría exhaustiva del tráfico para identificar posibles brechas.



6. Botnets controladas por actores externos.

Descripción de la amenaza:

Una botnet es una red de dispositivos comprometidos que están bajo el control de un atacante. Los dispositivos infectados se utilizan para lanzar ataques a gran escala, como la denegación de servicio (DDoS) o el envío masivo de correos electrónicos maliciosos.

En México, se ha registrado un aumento de este tipo de ataques debido a la falta de segmentación de red y seguridad en dispositivos conectados[1].

¿Qué gana el hacker?

El control de cientos o miles de dispositivos permite a los atacantes realizar ataques coordinados, interrumpir servicios de empresas y gobiernos, o alquilar la botnet a otros criminales.

¿Qué hace el hacker después del ataque?

Los dispositivos infectados se utilizan para lanzar ataques DDoS que pueden derribar sitios web, interrumpir operaciones de TI o servir como herramientas para ejecutar campañas de spam y fraude digital.

¿Cómo puede ayudar Canon?

Canon proporciona soluciones para monitorear de manera centralizada todos los dispositivos de impresión conectados, detectando cambios en el comportamiento de estos y actividad inusual que podría indicar la existencia de una botnet. Además, los sistemas de administración de Canon pueden segmentar los dispositivos críticos y aislar rápidamente aquellos que presentan comportamientos sospechosos.

Acciones preventivas:

- ☑ Implementar políticas de acceso específicas para limitar la comunicación de dispositivos Canon con otros equipos de la red.
- ☑ Establecer configuraciones avanzadas de firewzall en dispositivos Canon para bloquear comunicaciones no autorizadas.
- ☑ Actualizar el firmware de los dispositivos para prevenir que se exploten vulnerabilidades conocidas. Simulaciones de ataques distribuidos permiten preparar la infraestructura de la organización para resistir ataques DDoS y evitar que sus dispositivos sean secuestrados.

Síntomas de un ataque:

Aumento repentino en el uso del ancho de banda, dispositivos que muestran actividad anormal o conexiones a servidores remotos sin autorización.

Reacción inmediata:

Desconectar la red afectada, reiniciar los dispositivos en modo seguro y aplicar parches de seguridad. Monitorear el tráfico para identificar el punto de entrada del ataque.

Conclusión

La ciberseguridad ya no es opcional, necesitas protegerte.

Hoy en día, las empresas que no toman medidas para protegerse están simplemente entregando las llaves de su negocio a los ciberdelincuentes. Con amenazas cada vez más sofisticadas como el espionaje digital, el robo de datos y las botnets, la seguridad ya no es opcional.

Las organizaciones deben entender que reforzar su infraestructura es una inversión, no un gasto. Las compañías que no implementen controles de seguridad, monitoreo continuo y buenas prácticas de gestión estarán facilitando la tarea a los atacantes, poniendo en riesgo su reputación y su viabilidad operativa. En pocas palabras, tomar acción evitará ser un blanco fácil para los ciberdelincuentes.

Fuentes de consulta:

1. Empresas mexicanas sufrieron 31 mil ciberataques en primer semestre de 2024 Grupo Milenio.
2. Aumentan los ciberataques: más del 60% de las empresas mexicanas aseguraron haber sufrido vulneraciones en 2023 ManageEngine.
3. Threat Actor Profile: AridViper SOCRadar® Cyber Intelligence Inc.
4. IoT Device Security in 2024: The High Cost of Doing Nothing Asimily.

Proteja a las personas, la propiedad y los datos con las Soluciones de Seguridad Canon

Canon ofrece soluciones para proteger y gestionar información empresarial confidencial y espacios físicos seguros.

Seguridad de Impresión

Dado que los datos confidenciales se mueven regularmente entre el escritorio, el dispositivo móvil y las impresoras multifunción de un usuario, es importante tomar medidas para ayudar a proteger su entorno de impresión. Las plataformas **imageRUNNER ADVANCE DX e imagePRESS Lite** ofrecen una variedad de capacidades de seguridad para ayudar a facilitar la confidencialidad, accesibilidad y disponibilidad de su información.

Su socio confiable en ciberseguridad para impresión

Proteja sus Documentos y Datos con las Soluciones de Impresión Segura de Canon.

uniFLOW

Seguridad en todos sus datos y documentos

En Canon entendemos que la seguridad de sus documentos y datos es una prioridad critica en el mundo empresarial actual, nuestras Soluciones de Impresión con Ciberseguridad están diseñadas para ofrecerle tranquilidad y confianza, asegurando que sus impresiones y documentos estén protegidos contra las amenazas cibernéticas en constante evolución.

Nuestros Beneficios

CONTROL DE ACCESO

Las impresoras multifunción de oficina se pueden compartir entre varios empleados, departamentos e invitados externos. Canon tiene una variedad de soluciones para ayudar a controlar el acceso y el uso de los dispositivos.

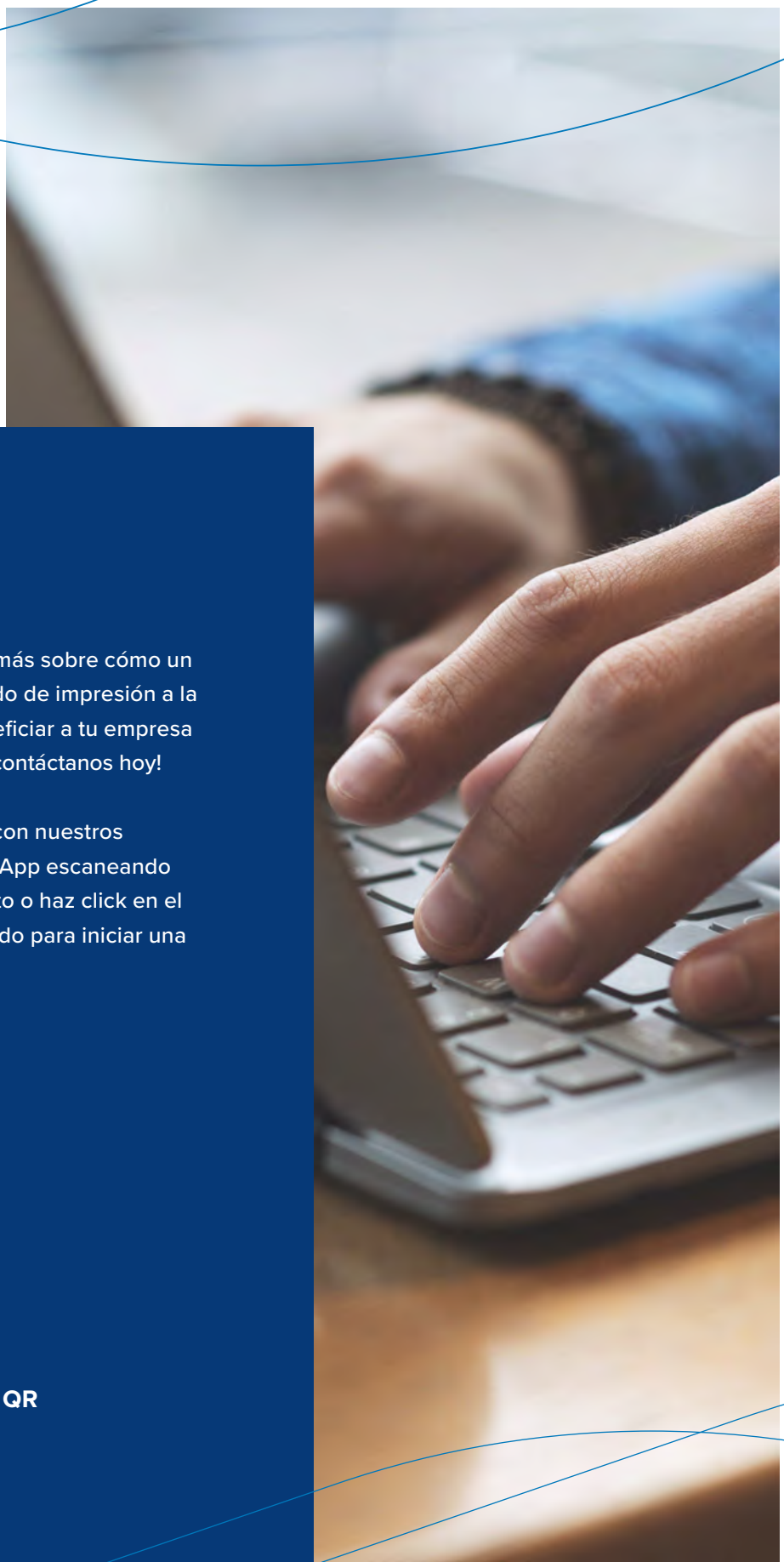
PROTEGER LOS DATOS TRANSMITIDOS O ALMACENADOS

Las impresoras multifunción han evolucionado hasta convertirse en dispositivos sofisticados y conectados que pueden trasmitir y recibir información. Canon tiene soluciones para ayudar a proteger los datos del acceso no autorizado.

Trellix

PROTÉJASE CONTRA LAS AMENAZAS CIBERNÉTICAS

Las impresoras multifunción pueden convertirse en un objetivo para los piratas informáticos. Canon tiene soluciones para ayudar a garantizar que los dispositivos estén protegidos contra posibles alteraciones de su firmware y aplicaciones.



Canon

Si deseas explorar más sobre cómo un servicio administrado de impresión a la medida puede beneficiar a tu empresa ¡No esperes más y contáctanos hoy!

Ponte en contacto con nuestros expertos por WhatsApp escaneando el código QR adjunto o haz click en el enlace proporcionado para iniciar una conversación.

Escaneé el código QR

ó haga clic aquí

No espere más para llevar su empresa al siguiente nivel.

¡Contáctenos hoy!

www.canon.com.mx

Síguenos en nuestras redes sociales:

Blvd. Manuel Ávila Camacho No.138, piso 17, Col. Lomas de Chapultepec, C.P. 11000, Ciudad de México.