GUÍA ICC SOBRE CIBERSEGURIDAD PARA LAS MIPyMES
Pasos para las MIPyMES para proteger sus negocios de amenazas de ciber seguridad durante la crisis de Covid-19.

La nueva pandemia del Coronavirus (**COVID-19**), es una crisis económica y de salud sin precedentes, que afecta las vidas y el sustento de los trabajadores, así como las operaciones continuas de las empresas a nivel global.

Micro, pequeñas y medianas empresas (**MIPyMES**) y sus trabajadores, así como los empresarios y los emprendedores o trabajadores independientes, se encuentran entre los más afectados. Es imperativo que todas las partes tomen decisiones y acciones urgentes para combatir las repercusiones económicas del COVID-19 y salvaguardar el funcionamiento actual y futuro de la economía global.

La International Chamber of Commerce (**ICC**), como la Organización Mundial de las Empresas y representante de más de 45 millones de compañías en más de 100 países ha lanzado la campaña para salvar a nuestras Pymes: "Save Our SMEs", para i) destacar el impacto devastador del COVID-19, en las pequeñas empresas y sus empleados; ii) asegurar políticas efectivas y respuestas fiscales a nivel internacional y nacional; y iii) proporcionar recursos y herramientas a las pequeñas empresas para ayudarlas a enfrentar el choque económico sin precedentes que se desarrolla ante nosotros.

Las disrupciones del COVID-19 aumentan el riesgo de ciber-ataques en las MIPyMES

Para garantizar la continuidad de las empresas, proteger a los trabajadores y continuar atendiendo a los clientes durante la pandemia, muchas organizaciones están volviendo en línea, partes sustanciales de su operación

A raíz de la crisis, ha habido un aumento en el uso de herramientas digitales y en línea, primordialmente para soportar la comunicación. Esto crea nuevas oportunidades para que actores maliciosos aprovechen los efectos disruptivos de las crisis y apunten a las MIPyMES para ciber-ataques.

Incluso, antes de la crisis actual las MIPyMES eran cada vez más el blanco de los ciber-ataques debido a la falta de recursos para implementar soluciones integrales de ciber-seguridad. Un informe reciente sugiere que las pequeñas empresas son el objetivo de más del 40% de los ciberataques con una perdida promedio por ataque de más de 188,000 USDs[1].

Los cibercriminales han capitalizado las herramientas parciales utilizadas por MIPyMES para proteger sus operaciones[2] y usan a las MIPyMES como el "eslabón más débil" para explotar sus conexiones a empresas más grandes en la cadena de suministro.

En 2019, se estimó que uno de cada cinco pymes habían sido víctimas de ataques de ransomeware[3]. Los ataques de *phishing*, también han alcanzado su nivel más alto en tres años, donde las pequeñas organizaciones han recibido correos electrónicos maliciosos en una tasa mayor. [4]

La adopción a gran escala de soluciones tecnológicas de trabajo desde el hogar, mayor actividad en la atención al cliente y un mayor uso de servicios en línea por parte de las MIPyMES en respuesta a las medidas de restricción del COVID 19 han exacerbado estos riesgos, ejerciendo una gran presión sobre los controles de seguridad cibernética que los cibercriminales han sido ágiles para explotar.

Ahora con mayores riesgos de seguridad, es vital que las empresas puedan identificar las amenazas a la seguridad cibernética y gestionar eficazmente sus sistemas de información durante la crisis actual, como parte de sus planes de continuidad de negocio.

Riesgos clave de ciber-seguridad para MIPyMES en el contexto de la crisis de Covid-19

[1] Verizon, *Data Breach Investigations Report* (2019).

[2] Symantec, *Internet Security Threat Report* (Vol 24, February 2019).

[3] Datto, *Datto's Global State of the Channel Ransomware Report* (2019).

[4] APWG, *Phishing Activity Trends Report* (Q3, 2019).

La siguiente sección, proporciona una tipología de los riesgos actuales de ciber-seguridad y establece pasos concretos que pueden tomar las MIPyMES para mejorar la seguridad de sus operaciones:

Ataques de Phishing y vulneración del correo electrónico de negocio utilizando COVID-19 como anzuelo

Los esquemas de phishing y vulneración del correo electrónico de negocios a menudo proliferan después de las crisis, para explotar el miedo y la confusión. A raíz de la crisis del COVID 19, se ha dado una oleada de correos electrónicos maliciosos, que utilizan técnicas básicas de ingeniería social para atraer a los usuarios a proporcionar información valiosa bajo falsas pretensiones. Los cibercriminales a menudo se hacen pasar por una agencia legítima o una fuente confiable como la Organización Mundial de la Salud y autoridades locales para convencer a las personas a compartir datos sensibles.

Distribución de software malicioso (malware), utilizando COVID-19 como anzuelo

Del mismo modo, los actores maliciosos están utilizando COVID-19 como un señuelo para distribuir *malware* e interferir con redes empresariales. Las empresas de seguridad cibernética han identificado múltiples familias de malware, incluyendo software para secuestrar el equipo y programas para espiar al usuario usando temas relacionados con COVID-19 para infectar un dispositivo y obtener acceso no autorizado a la red. Esto puede comprometer datos sensibles y causar gran daño a los sistemas de TI de una MIPyME.

Trabajo remoto y amenazas a la cadena de suministro

Asegurar la infraestructura para el trabajo remoto sigue siendo un desafío para muchas MIPyME.

El uso de las aplicaciones para el trabajo remoto abundaba sin controles antes de la crisis de COVID-19, pero a medida que los trabajadores utilizan cada vez más los dispositivos personales para garantizar la continuidad del negocio, muchas comunicaciones tienen lugar fuera de los firewalls de la empresa. Esto puede aumentar significativamente los riesgos de ciber seguridad para las MIPyMES dado que las aplicaciones para trabajo remoto a menudo son el objetivo de actores maliciosos. La dependencia de las MIPyMES en las herramientas tercerizadas y servicios basados en la web, pueden aumentar el riesgo en general**.**

Mayor vulnerabilidad debido a la falta de conciencia

Las amenazas a la ciber seguridad a menudo permanecen fuera del radar y, por mucho, el mayor riesgo para las MIPyMES es la falta de conocimiento o la subestimación de las amenazas de ciber seguridad. En el entorno actual, donde las MiPymes se centran directamente en abordar las tensiones operativas, abordando problemas de liquidez y asegurando la salud y los medios de vida de su fuerza laboral, las amenazas a la ciber seguridad pueden ser subestimadas.

A continuación, sugerimos varios pasos fáciles que pueden ayudar rápidamente a aumentar la resiliencia de ciberseguridad de las MIPyMES.

Pasos fáciles para las MIPyMES para proteger sus negocios ante amenazas de ciber seguridad durante la crisis de Covid19

- **Crear conciencia dentro de la organización: los empleados son la primera línea de defensa contra los ciberataques**

En 2018, más del 50% de los incidentes de seguridad fueron el resultado de un error humano en lugar de un ataque deliberado[5]. Además, muchos incidentes de seguridad que resultan de un ataque deliberado pueden ser evitados si las personas tomasen las medidas adecuadas. Los empleados deben comprender sus responsabilidades diarias en el manejo, protección, y soporte de datos y redes de la empresa. Esta incluye pasos simples como seleccionar contraseñas seguras y garantizar el uso de un correo electrónico responsable. Es importante destacar que los empleados deben ser conscientes de posibles estafas y malware para reconocerlo y abstenerse de compartir e informar sobre material maliciosos de manera oportuna.

La MIPyMES también deben implementar políticas a nivel de toda la empresa que creen una cultura de seguridad de la información que prohíba el uso de software sin licencia, actualizando todo el software regularmente para ayudar a incluir parches de seguridad y establecer una política de navegación segura, estableciendo reglas para redes sociales.

ICC se ha asociado con el Cyber Readiness Institute para ofrecer asesoría y capacitación para MIPyMES, desde consejos y guías rápidas, hasta un programa integral de capacitación en resiliencia cibernética, disponible de forma gratuita en siete idiomas (árabe, chino, inglés, francés, japonés, portugués y español).

- **Fortalecer la política y los procedimientos de gestión de acceso remoto**

Las MIPyMES deben lidiar con un entorno de acceso remoto cada vez más complejo, a la luz del rápido aumento del teletrabajo y la proliferación de dispositivos (teléfonos, computadoras portátiles, tabletas, ya sean propiedad de la empresa, personales, compartidos, públicos o una combinación de ellos),

5 Kaspersky, *The State of Industrial Cyber Security* (2019).

así como las diferentes formas de conectarse a Internet (wifi doméstico o público, punto de acceso proporcionado por la compañía) y acceder a los datos de la compañía (Red Privada Virtual, tecnología basada en la nube u otra). Por lo tanto, es importante que las MIPyMES establezcan pautas claras para sus empleados con respecto al uso adecuado del acceso remoto.

Como regla general, los dispositivos proporcionados por las compañías, deben preferirse a los dispositivos personales o públicos.

Del mismo modo, las redes privadas y los puntos de acceso a redes (hotspots) proporcionados por la empresa deberían preferirse a las redes públicas, salvo el uso de una Red Privada Virtual (VPN).

Los sistemas basados en la nube, los sistemas centralizados de intercambio de archivos o un sitio dedicado para compartir archivos con supervisión de la empresa deben usarse para acceder y compartir documentos.

La International Chamber of Commerce y el Cyber Readiness Institute, también se han asociado para ofrecer un seminario web de capacitación en línea para gerentes y empleados de PYME para alinear mejor el trabajo remoto, con los requisitos de seguridad cibernética. El webinar de capacitación en línea se basa en una serie de guías rápidas de CRI sobre cómo asegurar la fuerza de trabajo remota.

- **Asegure los portales de proveedores y otros sistemas externos**

Es crucial que las MIPyMES identifiquen, evalúen y administren todos los puntos de entrada con el objetivo subyacente de hacer que los sistemas de información sean impermeables a la manipulación externa. Los pasos prácticos rápidos incluyen la actualización y el parcheo de software, la actualización de contraseñas y el fomento de la autenticación de múltiples factores.

Esto también implica una mayor comunicación con los socios comerciales para asegurar las redes en toda la cadena de suministro. Mostrar liderazgo en ciberseguridad puede aumentar la resistencia general en toda la cadena de

suministro y reforzar las credenciales de las MIPyMES con socios comerciales existentes o potenciales.

- **Actualice los planes de respuesta a incidentes en un entorno más distribuido**

Debido a la naturaleza evolutiva de las amenazas cibernéticas, incluso las empresas bien protegidas pueden experimentar violaciones de seguridad. Las empresas operan en un entorno donde el riesgo puede minimizarse, pero no eliminarse por completo. Una respuesta rápida es crítica para mitigar y, cuando sea posible, evitar los efectos perjudiciales de un ataque.

La gestión exitosa de incidentes incluye una estrategia de comunicación clara con las partes interesadas internas y externas, así como el apoyo de terceros especializados para ayudar a contener y remediar el incidente. Las MIPYMES también deben involucrarse de manera proactiva con las fuerzas del orden y las agencias de supervisión especializadas para ayudar a abordar las ciber amenazas cada vez más sofisticadas.

Con respecto al riesgo de ataque cibernético en la crisis actual, también aconsejamos a las MIPyMES que sigan las pautas y recomendaciones gubernamentales emitidas por los equipos nacionales de respuesta a emergencias informáticas (CERTs), e instar a los administradores públicos a proporcionar información actualizada y completa sobre las amenazas de ciber seguridad específicas a nivel local que enfrentan las empresas.

La Guía de seguridad cibernética para empresas de la International Chamber of Commerce, ofrece un enfoque integral para señalar acciones efectivas y ayuda a guiar las discusiones para los equipos de administración y tecnología de la información. El documento presenta un cuestionario de autoevaluación de seguridad y un conjunto de cinco principios para reducir el riesgo asociado con incidentes de seguridad cibernética. Los principios están respaldados por una lista de verificación de seis pasos esenciales que toda empresa debe tomar para establecer guías en seguridad de la información.

Es importante destacar que esta guía puede ayudar a las empresas a relacionarse con socios comerciales y redes más amplias para evaluar y asegurar mejor todos los puntos de entrada. (versión en español disponible)

Finalmente, alentamos a las MIPyMES a participar activamente con las numerosas iniciativas en materia de seguridad cibernética de la International Chamber Of Commerce (ICC). La Comisión de Economía Digital del ICC reúne a empresas de todos los tamaños para evaluar las amenazas cibernéticas y ofrecer recomendaciones personalizadas para abordar este problema multifacético con énfasis en soluciones adaptables y flexibles.

*Traducción al español, realizada por ICC México
con el apoyo de Manuel Haces Aviña. Manager of Public Policy &
Government Affairs de Google México