



OTROS  
DOCUMENTOS

---

2020



# Impacto de la COVID-19 en la ciberseguridad en Canadá

Oficina Económica y Comercial  
de la Embajada de España en Ottawa

Este documento tiene carácter exclusivamente informativo y su contenido no podrá ser invocado en apoyo de ninguna reclamación o recurso.

ICEX España Exportación e Inversiones no asume la responsabilidad de la información, opinión o acción basada en dicho contenido, con independencia de que haya realizado todos los esfuerzos posibles para asegurar la exactitud de la información que contienen sus páginas.

icex



OTROS  
DOCUMENTOS

7 de mayo de 2020  
Ottawa

Este estudio ha sido realizado por  
Luisa Yajaira López Jaspe

Bajo la supervisión de la Oficina Económica y Comercial  
de la Embajada de España en Ottawa

<http://Canada.oficinascomerciales.es>

Editado por ICEX España Exportación e Inversiones, E.P.E., M.P.

NIPO: 114-20-021-0



# Índice

1. Impacto de la COVID-19 en la ciberseguridad	4
2. Tendencias en ciberseguridad	6





# 1. Impacto de la COVID-19 en la ciberseguridad

En la actualidad, la pandemia de la COVID-19 no sólo ha alterado los sistemas mundiales de salud, económicos, políticos y sociales, sino que también plantea una amenaza invisible en el espacio digital debido al riesgo de ataques cibernéticos, que se aprovechan de la mayor dependencia de las herramientas digitales y de la incertidumbre acerca de la crisis.

En este contexto, el aumento del trabajo remoto y del comercio electrónico, así como el retraso acumulado en el mantenimiento y la actualización de los programas informáticos favorecen un incremento de los ataques cibernéticos que sacan partido de la situación, como ha se ha apreciado en las últimas semanas desde la irrupción del coronavirus.

Durante la emergencia sanitaria por la COVID-19, velar por las cadenas de suministro del sistema de salud, el sistema financiero y el cumplimiento de la ley resulta particularmente crítico. De ahí, la creciente importancia de las medidas de ciberseguridad en el seno de las organizaciones, tanto públicas como privadas.

En esta línea, el Centro Antifraude Canadiense (CAFC, por sus siglas en inglés) ha emitido un boletín de alertas relacionadas con la COVID-19 acerca de estafas, fraudes, *phishing* y virus, entre otros<sup>1</sup>. Asimismo, el Centro Canadiense de Ciberseguridad (Cyber Centre, en inglés, Canadian Centre for Cyber Security) ha creado una alerta especial para organizaciones de la salud<sup>2</sup>, más otras consideraciones de interés que han de tomar en cuenta los ciudadanos para prevenir y evitar los ataques cibernéticos.

Por otro lado, según la firma especializada en ciberseguridad Sophos<sup>3</sup>, el número de dominios registrados que incluyen la palabra “covid” o “corona” ha aumentado vertiginosamente en las últimas semanas y, a la vez, de manera correlativa, el número de dominios relacionados con spam e intentos de *phishing*. Estos ataques se relacionan con enlaces que suelen contener *malware* o *ransomware* a través de correos electrónicos y páginas web que simulan ser de instituciones oficiales.

<sup>1</sup> <https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm>

<sup>2</sup> <https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations>

<sup>3</sup> [https://www.airdberlis.com/insights/blogs/thespotlight/post/ts-item/cyberattacks-and-cybersecurity-measures-amid-the-covid-19-pandemic?utm\\_source=Mondaq&utm\\_medium=syndication&utm\\_campaign=LinkedIn-integration](https://www.airdberlis.com/insights/blogs/thespotlight/post/ts-item/cyberattacks-and-cybersecurity-measures-amid-the-covid-19-pandemic?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration)



Por último, hay que destacar que, como medida de prevención, la contratación de ciberseguros está aumentando con objeto de cubrir el riesgo empresarial de paralización de la actividad por causa de un ciberataque.

ICEX

## 2. Tendencias en ciberseguridad

El instituto de investigación The Conference Board of Canada<sup>4</sup>, a través de su Consejo de Ciberseguridad (Cyber Security Council), recalca la importancia de crear un sistema de protección contra los ciberataques.

En primer lugar, propone la creación de un nuevo marco legal en Canadá para proteger la cadena de suministro<sup>5</sup>, consistente en la identificación de los diferentes niveles de gestión, operaciones o técnicos que acompañan la transformación digital en este sector. Por ejemplo, si una empresa desarrolla una actividad que forma parte de una cadena de suministro considerada crítica, podría acceder a una guía para desarrollar sus capacidades internas y cumplir con un complejo sistema de desarrollo en el proceso de digitalización, tanto interno como externo.

Para fortalecer estas cadenas de suministro críticas, las empresas y organizaciones deberían contar con un plan de actuaciones que contemplase los diferentes escenarios posibles ante la aparición de determinadas amenazas. Por otro lado, sería necesario adoptar una serie de reglas comunes de aplicación a todas las empresas que integran una cadena de suministro, incluyendo la seguridad digital exigible y normas de auditoría para evitar fallos en los proveedores intermedios. Asimismo, estas empresas deberían adherirse a un conjunto estándar de definiciones para protocolos de seguridad.

En segundo lugar, menciona la necesidad de evolucionar continuamente en las prácticas, políticas y controles de informes de violación de privacidad digital. Además, subraya la importancia de intercambiar información sobre incidentes cibernéticos, algo que facilitaría la notificación temprana de las incidencias y permitiría proteger al ecosistema de mayores daños.

Por último, otra de las tendencias que se observarán<sup>6</sup> es el aumento de cursos de formación para empleados en materia de ciberseguridad, como respuesta al incremento de las amenazas digitales.

En conclusión, esta coyuntura supone un cambio de paradigma en la implementación de estrategias relacionadas con la ciberseguridad tendente a reducir las vulnerabilidades digitales de las empresas y organizaciones públicas.

---

<sup>4</sup> <https://www.conferenceboard.ca/networks/csc/default.aspx>

<sup>5</sup> <https://www.conferenceboard.ca/insights/blogs/supply-chain-cybersecurity-is-critical-especially-during-covid-19>

<sup>6</sup> [https://obj.ca/article/sponsored-otus-oax-how-associations-are-rethinking-risk?utm\\_source=newsletter&utm\\_medium=objtoday&utm\\_campaign=otus\\_group\\_oax\\_2020&utm\\_term=march\\_30\\_2020](https://obj.ca/article/sponsored-otus-oax-how-associations-are-rethinking-risk?utm_source=newsletter&utm_medium=objtoday&utm_campaign=otus_group_oax_2020&utm_term=march_30_2020)

# ICEX

Si desea conocer todos los servicios que ofrece ICEX España Exportación e Inversiones para impulsar la internacionalización de su empresa contacte con:

**Ventana Global**

913 497 100 (L-J 9 a 17 h; V 9 a 15 h)

[informacion@icex.es](mailto:informacion@icex.es)

Para buscar más información sobre mercados exteriores [siga el enlace](#)

[www.icex.es](http://www.icex.es)

