# Las cinco medidas de ciberseguridad que toda organización debería implementar en la era post-COVID

Las organizaciones, tras afrontar los retos, amenazas y, en algunos casos, ataques que la época de crisis por el Coronavirus nos ha traído en lo que se refiere a ciberseguridad, se encuentran en el camino hacia la llamada *nueva normalidad*.

El escenario de trabajo en remoto y el levantamiento de infraestructuras no habituales que muchas compañías se han visto obligadas a implementar para dar respuesta a esta circunstancia, han producido, en muchos casos, una sensación de indefensión y, en otros, ha mostrado la vulnerabilidad de sus sistemas ante los ciberdesafíos de la pandemia.

Desde el inicio de esta crisis, SIA, una compañía de Indra, líder en el mercado de la seguridad de la información en España y Portugal por volumen de negocio en servicios de valor añadido, ha analizado cerca de 10.000 elementos que corresponden a una amenaza real de COVID-19 en todo el mundo. El vector de ataque principal elegido por los cibercriminales para llevar a cabo sus campañas maliciosas ha sido el correo electrónico, mediante el cual, han tratado de infectar o han infectado los sistemas de sus víctimas, a través de ataques de ingeniería social, ya sea mediante phishing, malware o las conocidas fake news.

Ante esta situación excepcional, las compañías, ahora más que nunca, se enfrentan al reto de **proteger la información y activos** que soportan sus procesos de negocio, y **gestionar adecuadamente los riesgos** de ciberseguridad a los que se exponen. Los especialistas en ciberseguridad han tenido que reaccionar con agilidad y dedicar mayores esfuerzos a, no sólo mantener, sino reforzar esa protección.

En este sentido, para muchas organizaciones **la ciberseguridad se ha convertido en una prioridad que ha venido para quedarse, como una cuestión de negocio** y no sólo tecnológica.

Para Luis Álvarez, CEO de SIA, “lo fundamental en este camino hacia una mayor seguridad en las organizaciones, es comenzar por identificar los riesgos, poner en marcha acciones para protegerlos, determinar una estrategia para detectar posibles ataques, contar con especialistas para poder reaccionar eficazmente y, por último, disponer de las capacidades para recuperarse de los mismos”.

En todo este proceso, es fundamental ir de la mano de un experto. “**La ciberseguridad** ya no es una cuestión de tecnología o informática en general, sino que **requiere del conocimiento de especialistas**, para que realmente aseguren la protección de los datos importantes”, añade Álvarez. Un error frecuente es pensar que uno solo se puede proteger adecuadamente. La velocidad a la que cambian las condiciones de la ciberseguridad exige la colaboración de empresas especializadas.

La demanda de estos servicios ha experimentado un incremento significativo como consecuencia del aumento de la actividad online producido por el teletrabajo. Fundamentalmente, en el trabajo desde casa, las condiciones del entorno no son las más adecuadas habitualmente; se utilizan, por ejemplo, computadoras de uso personal para trabajar, lo que abre nuevos agujeros de seguridad, y nos ha hecho más vulnerables, fruto del

María Emilia Fumagalli
mefumagalli@llorenteycuenca.com
15. 6154.8988

María Mercedes Paz
mpaz@llorenteycuenca.com
15. 6980.484

miedo o la angustia por la pandemia, a las nuevas formas de atacar de los ciberdelincuentes. Así **las compañías están más abiertas y expuestas a un mayor riesgo de ataques**.

Las **amenazas que el entorno de trabajo remoto ha traído** consigo exigen a las empresas una protección y detección diferente a la de la etapa pre-COVID. El blanco principal de estas son las aplicaciones y datos centrales de la organización, las comunicaciones o la forma de acceder a ellos, los equipos que se utilizan y las personas que actúan.

La respuesta adecuada no es otra que aplicar un entorno renovado de ciberseguridad. Respuesta que, como apunta el CEO de SIA, "nos ha exigido como especialistas, en primer lugar, acompañar a las organizaciones a **auditar su entorno tecnológico de seguridad** para detectar dónde podían estar expuestas y, tras este paso, proponerles y **establecer un plan de trabajo con medidas adicionales de protección**".

Para poner en marcha esas medidas, las empresas han revisado principalmente tres ámbitos: cobertura del riesgo, producido inadvertidamente por personas (empleados, colaboradores o clientes), formalización de transacciones (firma digital de contratos y operaciones) y detección de ataques.

Como resultado de ese análisis y en la era post-COVID, las organizaciones, para ser más **seguras, ágiles y eficientes,** deberían llevar a cabo las siguientes acciones:

1. **Auditar** las infraestructuras y soluciones de seguridad implantadas.
2. Reforzar o implantar medidas adicionales de **protección** del teletrabajo.
3. Una mejor **identificación de los usuarios**, encriptación de la información y un adecuado control de accesos, mediante proyectos de gestión de la identidad.
4. Adoptar soluciones de **firma digital para securizar los procesos empresariales**.
5. Revisar con frecuencia el nivel de **concientización** de los profesionales de la organización, la **efectividad** de las medidas y realizar **simulaciones de ataques** tratando de comprobar cómo se reacciona ante ellos.

Fruto de esta crisis y de la nueva coyuntura global, muchas compañías han decidido centrar sus esfuerzos e inversiones en acciones contundentes que puedan marcar la diferencia entre una empresa altamente segura y otra que no lo es, garantizando así la continuidad de su actividad. Afortunadamente, hoy en día, existe una oferta cada vez más amplia y especializada en **soluciones que posibilitan a las entidades públicas y privadas avanzar en el objetivo de un ciberespacio seguro para sus negocios**.

**Indra en Argentina**

En Argentina, Indra tiene presencia desde 1993, con una destacada trayectoria en la provisión de soluciones y servicios tecnológicos. Cuenta con dos Centros de Producción de Software, que aplican los modelos de productividad más vanguardistas y desarrollan una importante actividad de I+D, en la Ciudad Autónoma de Buenos Aires y en la provincia de Córdoba. Además, la compañía cuenta con un Laboratorio y Centro de Producción y Distribución para Transporte y Tráfico, en la provincia de Buenos Aires. Indra forma parte, tanto en el sector público como privado, de algunos de los proyectos innovadores claves para el desarrollo económico y tecnológico de Argentina en los mercados de Transporte & Defensa, y Tecnologías de la Información (TI) a través de su filial Minsait.

**Acerca de Indra**

María Emilia Fumagalli
mefumagalli@llorenteycuenca.com
15. 6154.8988

María Mercedes Paz
mpaz@llorenteycuenca.com
15. 6980.484

Indra (http://www.indracompany.com) es una de las principales compañías globales de tecnología y consultoría y el socio tecnológico para las operaciones clave de los negocios de sus clientes en todo el mundo. Es un proveedor líder mundial de soluciones propias en segmentos específicos de los mercados de Transporte y Defensa, y una empresa líder en consultoría de transformación digital y Tecnologías de la Información en España y Latinoamérica a través de su filial Minsait. Su modelo de negocio está basado en una oferta integral de productos propios, con un enfoque end-to-end, de alto valor y con un elevado componente de innovación. A cierre del ejercicio 2019, Indra tuvo unos ingresos de 3.204 millones de euros, más de 49.000 empleados, presencia local en 46 países y operaciones comerciales en más de 140 países.

María Emilia Fumagalli
mefumagalli@llorenteycuenca.com
15. 6154.8988

María Mercedes Paz
mpaz@llorenteycuenca.com
15. 6980.484