



**En esta nueva sesión de los talleres digitales de R el auditorio conoció las claves para mantener protegida a la empresa en proceso de digitalización**

## ***Ciberseguridad en las pymes: riesgos y recursos en un entorno digital***

- ***En el encuentro virtual de esta mañana los portavoces analizaron con detalle las principales carencias de las empresas en el campo de la Ciberseguridad y propusieron caminos para trabajar protegidas a día de hoy en el entorno digital.***
- ***El experto en marketing de R y del Grupo Euskaltel, Íñigo González, subrayó la gran importancia de la Ciberseguridad, en línea con la apuesta clara de R por la digitalización de las empresas, y por responder de manera sencilla a sus necesidades actuales.***
- ***Álvaro Briceño, experto en Ciberseguridad de la consultora Fractalia, coincidió con González al destacar que es esencial el compromiso y la concienciación de toda la compañía con la seguridad digital.***
- ***Como en anteriores talleres digitales de R, la jornada de hoy, práctica e interactiva para el auditorio, se desarrolló en el edificio virtual de R y del Grupo Euskaltel “The Tech Experience”, lugar de encuentro y reflexión sobre tendencias tecnológicas y oportunidades para los negocios.***
- ***R continúa acompañando a las empresas gallegas en sus procesos de digitalización para que sigan siendo competitivas a todos los niveles y en cualquier escenario del mundo.***

**Viernes, 4 de junio de 2021.-** Tras dos sesiones de encuentros digitales dedicadas al gobierno y la explotación del dato en la empresa respectivamente, el taller de esta mañana desgranó lo esencial de otro de los temas que más preocupan y más atención están reclamando en el segmento empresarial en la actualidad: la **Ciberseguridad**.

Y, en concreto, la ciberseguridad en organizaciones que compiten a un nivel menos ambicioso que las grandes cuentas pero que no por ello -o tal vez por ello- corren y correrán serios riesgos en el universo digital si no toman precauciones inmediatas para protegerse de ciberataques o intrusiones de cualquier tipo.

“*Ciberseguridad en las pymes*” es el título del encuentro interactivo que congregó digitalmente esta mañana a responsables de empresas en el auditorio del edificio virtual [The Tech Experience](#), lugar de encuentro de **R** y del Grupo para la reflexión sobre tendencias tecnológicas y oportunidades para los negocios de la mano de expertos.

Así, tras el citado análisis del dato como objeto de gobernanza y explotación en las organizaciones, en el taller de hoy se analizaron los **riesgos** a los que esa información puede permanecer expuesta y los **recursos imprescindibles** para protegerla todo lo posible. En suma, las vulnerabilidades, recomendaciones de seguridad y soluciones disponibles para proteger a la pequeña y mediana empresa en el ámbito de la Ciberseguridad.

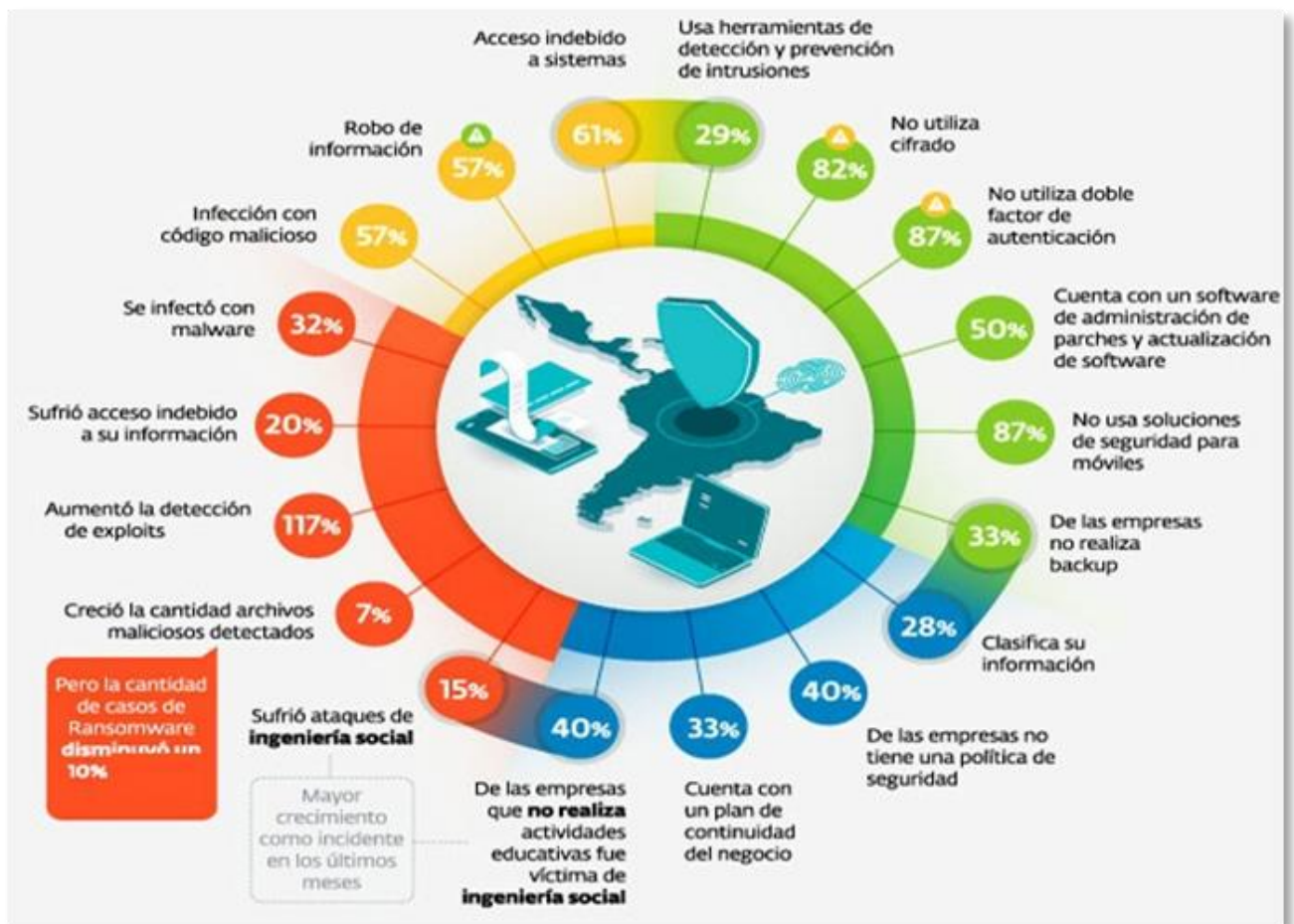
En este sentido, Íñigo González, responsable de *Go to Market* de **R** y del Grupo, aseguró que *“la nueva realidad digital exige a las empresas, más que nunca, disponer de sistemas de seguridad que garanticen que su actividad diaria y sus planes de negocio pueden llevarse a cabo sin riesgo. Lo más importante es la concienciación plena (“mindset digital”) de los responsables de las empresas de que la información es el activo más importante que posee su negocio, y de ahí que haya que protegerlo en todo momento de los riesgos inherentes al universo digital. Pero esto no implica que sea imprescindible invertir en herramientas y recursos que supongan grandes desembolsos para proteger los negocios (...)”*

## **Un gran reto, un camino por recorrer**

Según un estudio reciente de Google sobre el panorama actual de la ciberseguridad en pymes en España, un **87%** de las pequeñas y medianas empresas todavía **no disponen de soluciones de seguridad** para los móviles; un **33%** de ellas **no realiza back up** de su información (sistemas de respaldo, copias de seguridad), y tan solo un **33% cuenta con un plan de continuidad** de negocio.

Íñigo González incidió también en la premisa de que **la información es el activo más importante** que posee un negocio y, como tal, *“debemos protegerla ante las vulnerabilidades a las que está expuesta. (...) Los métodos de protección que en el pasado funcionaban, como el antivirus, ya no son suficientes actualmente porque tanto los sistemas informáticos como sus dispositivos evolucionan a una velocidad vertiginosa y es necesario dotarse de herramientas y medidas complementarias, mantenerlas y tenerlas continuamente actualizadas”*.

Y como ejemplo, el portavoz de **R** se refirió al teletrabajo: “Permitir en estos tiempos el trabajo a distancia sin seguir unas pautas de seguridad puede resultar muy arriesgado para las organizaciones. Ahí está el peligro de que los ‘ciberdelincuentes’ puedan acceder a la red de la empresa y la información que se gestiona, o que potencialmente los empleados utilicen herramientas no permitidas y pongan en situación de riesgo a la compañía. La figura de un experto digital es clave, en este sentido, para acompañar a las empresas”.



\* Fuente: Estudio de panorama actual de la ciberseguridad en pymes en España. Google

## Recursos para un entorno ‘ciberseguro’ en las pymes

Por su parte, Álvaro Briceño, Director de servicios de Ciberseguridad y soporte IT de la consultora *Fractalía*, especializada en seguridad digital, expuso una serie de recomendaciones y soluciones posibles ante este cambio del concepto de seguridad en negocios y comercios.

*“Lo primero y más importante -aseguró Briceño- es el necesario compromiso empresarial con la seguridad digital: el punto de partida es una permanente concienciación de toda la compañía sobre la realidad de las amenazas digitales”.*

(...) “Pero además -continuó- hay otros recursos para reforzar un entorno ‘ciberseguro’, como el uso de **herramientas de seguridad** (antivirus, firewall, etc..) solventes y reconocidas en el mercado; el acceso fácil y rápido a un **soporte de seguridad** ante posibles incidentes, el fomento de entornos seguros de **red** al que se conectan los/as empleados/as o clientes/as; el mantenimiento de los **dispositivos siempre actualizados**; las **copias de seguridad** continuas, sobre todo de los datos más críticos; el uso de **contraseñas potentes** en la organización; sin olvidar que también es necesario asegurar los **dispositivos móviles**”.

Ahí está el reto, sin duda: ese camino que cada vez más organizaciones deciden recorrer para garantizar el verdadero éxito de sus procesos de digitalización. La Ciberseguridad ya no es un plus optativo para grandes corporaciones sino una necesidad esencial para que cualquier empresa o negocio, sea del tamaño que sea, pueda desarrollarse con seguridad y competir en su mercado.

## **sumarios**

**Íñigo González**

***“Apostar por la digitalización de las empresas conlleva necesariamente apostar por la ciberseguridad”***

***“La información es el activo más importante del negocio, y hay que protegerlo en todo momento de los riesgos inherentes al universo digital”***

**Álvaro Briceño**

***“El punto de partida es una permanente concienciación de toda la compañía sobre la realidad de las amenazas digitales”***

***“Un entorno ‘ciberseguro’ exige herramientas y soporte de seguridad, entornos de red robustos, dispositivos siempre actualizados, contraseñas seguras y copias de respaldo, entre otras cosas”***

