

Retos de la ciberseguridad en entornos empresariales



Las autoridades conminan a los empresarios a denunciar los casos de hackeo de los que son víctimas y evitar el pago por liberación de datos para que las redes dedicadas a este tipo de delito no reinclidan en los ataques con fines extorsivos. FOTO GETTY

[EMPRESAS](#) [CIBERATAQUE](#) [FOROS EL COLOMBIANO](#)

POR JUAN CAMILO QUICENO RAMÍREZ | PUBLICADO HACE 26 MINUTOS

[-](#) [a+](#) [a-](#)

Expertos que participaron en foro de EL COLOMBIANO advirtieron que, incluso, deberían promoverse pólizas para minimizar riesgos. Detalles.

Antes de la pandemia del covid-19, el perímetro para defender los datos en propiedad de las compañías estaba delimitado en sus propias infraestructuras.

Una vez que la crisis sanitaria obligó a implementar el trabajo en casa, el área de riesgo se trasladó hasta los hogares de todos los colaboradores y es necesario invertir en el blindaje de sus unidades para disminuir los posibles ataques y el robo de información.

Esta fue una de las principales conclusiones lanzadas por los expertos en el foro "Empresa: cómo proteger su información en el mundo digital".

Edgardo Alfonso Arrieta, gerente de Ciberseguridad y Ciberdefensa en **Ecopetrol**, comentó que, en la nueva normalidad, las compañías pasaron de tener 30 oficinas a tener entre 9.000 y 10.000 de ellas, entendiéndose que cada computador instalado en el domicilio de los trabajadores es una sede empresarial.

A su modo de ver, el principal reto con el boom del trabajo en casa consiste en identificar los riesgos que podrían generarse en ese entorno doméstico.

"Hoy día tenemos un ecosistema tan amplio que es muy difícil pensar que desde una sola aplicación podremos blindarlo todo", comentó.

En este sentido, tal como lo expuso, hace falta enseñar a los colaboradores cómo hacer un uso adecuado de la información, administrarla y clasificarla de manera correcta.

Identificar los riesgos

Con base en la experiencia adquirida a partir de la adopción emergente del trabajo remoto, Eddy Neyib Llanos, director de Ciberseguridad de Grupo Réditos, apuntó que "cuando tu llegas a tener que trabajar desde casa, en el computador corporativo que tengas, te vas a conectar a una red wifi donde también están conectados otros dispositivos sobre los que la compañía no tiene gestión ni control".

"La idea –añadió– es comenzar a identificar, con un enfoque basado en riesgos, las amenazas que se producen en ese entorno de hogar y como subsanarlas o mitigarlas".

Con esto en mente, resaltó que es "importante" observar las soluciones en ciberseguridad disponibles en el mercado y comenzar a usarlas con miras a lograr conexiones más seguras en las redes corporativas desde las casas de los empleados.

El primer escudo

Para Olga Lucía López, vicepresidente ejecutiva de Tecnología de ISA, los empleados son la primera línea de defensa cuando se trata de ciberseguridad.

"Hay que insistir, persistir y no desistir en ello para que cada uno tenga conciencia de ese tema", subrayó.

En esta línea, agregó que los riesgos deben gestionarse y aquellos por fuera del alcance de la empresa deberían pasar a una póliza.

Aunque afirmó que "gracias a la consciencia de los empleados" en ISA no se ha presentado ningún evento de esta clase, señaló que es importante compartir las experiencias entre las mismas organizaciones y "capitalizar esos aprendizajes".

En el caso de su firma, según sus palabras, la seguridad digital es un tema primordial, toda vez que se encargan de operar infraestructura crítica, como el sistema de interconexión eléctrica, que de llegarse a paralizar, generaría un efecto transversal al resto de sectores y hogares.

Por su parte, Alexander Parra, fe de Servicios de Seguridad de Información y Tecnología del Grupo Éxito, expuso que la ciberseguridad ya no es un asunto exclusivo de las grandes compañías.

"Las empresas pequeñas y con competitividad en el mundo de lo digital deben empezar a prepararse igual que cualquier empresa grande", complementó.

Allí, desde su óptica, es clave contar con un plan de acción y tener claro por qué se maneja información y los canales digitales que podrían estar expuestos.

"Seguramente –dijo– encontrarán muchos elementos de valor si analizan con metodologías de riesgo cuáles son las amenazas que pueden tener".

Todos pueden ser objetivo

El campo de acción para la ciberdelincuencia ha crecido, según lo afirmó Carlos Arias, jefe de ventas de Fortinet Colombia, quien agregó que los ataques informáticos iniciaron con las grandes compañías, pero han ido desescalando hacia organizaciones de menor tamaño.

Por ello, argumentó que las pequeñas y medianas empresas también migrarán a terrenos digitales y deberán establecer cuál será el modelo tecnológico que mejor se adapte a ellas. En este orden de ideas, recomendó optar por arquitecturas integradas, puesto que mezclar diversas marcas en seguridad puede terminar afectando la interoperabilidad de los sistemas y, así mismo, incrementa los costos al tratar de enlazarlas a todas.

"Otro consejo importante es tener plataformas integrales de inteligencia artificial detrás de todo esto y plataformas de monitoreo integrales", puntualizó el experto.

No debe ocultarlo

El Teniente Coronel Julián Ricardo Buitrago, jefe del Centro Cibernético de la Policía Nacional, confirmó que hay un aumento en las denuncias por delitos cibernéticos y conminó a las compañías a denunciar estos eventos y no ocultarlos por factores de reputación, dado que si pagan por liberar datos, los hackers seguirán repitiendo esta conducta incontables veces

2,5

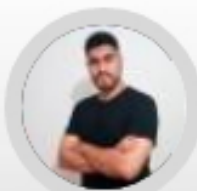
Millones es el déficit de profesionales en la industria 4.0 según la firma IBS.

CONTEXTO DE LA NOTICIA

PARÉNTESIS

SIGUE EL DÉFICIT DE PROFESIONALES

De acuerdo con Iván Castaño, director de Ruta N, los perfiles asociados con la cuarta revolución industrial, entre ellos los de ciberseguridad, siguen siendo deficitarios. Tal como lo indicó, se calcula que en el ámbito mundial hacen falta 2,5 millones de profesionales en esta área y, en este caso, Colombia y Medellín no son la excepción. "Desde Ruta N buscamos que, desde las mismas comunidades, se genere el interés en este tipo de tecnologías". De igual manera, anotó que con la estrategia Valle del Software, "buscamos llevar a Ruta N hasta las 16 comunas y los cinco corregimientos de Medellín".



JUAN CAMILO QUICENO RAMÍREZ

Soy afortunado por que me gano la vida haciendo lo que amo. Fanático de la salsa brava y los timbales. Amo a mi familia.

[Seguir a @juanquic4](#)

[REPORTE UN ERROR](#)

[AGREGAR INFORMACIÓN](#)

Porque entre varios ojos vemos más, queremos construir una mejor web para ustedes. Los invitamos a reportar errores de contenido, ortografía, puntuación y otras que consideren pertinentes. (*)

¿CUÁL ES EL ERROR?*

¿CÓMO LO ESCRIBIRÍA USTED?

INGRESE SUS DATOS PERSONALES *

TERMINOS Y CONDICIONES

ACEPTO TÉRMINOS Y CONDICIONES

LOS CAMPOS MARCADOS CON * SON OBLIGATORIOS

ENVIAR

LO MÁS LEIDO

LO MÁS COMPARTIDO

MÁS RECIENTES

1

Colombia tiene un leve descenso en casos covid diarios

2

Denuncia por abuso sexual en jardín de Buen Comienzo es por 14 niños: ICBF

3

Parlamento Romano pidió a la UE suspender tratados con Colombia

4

Dos motociclistas pierden la vida en accidentes en Bello y Rionegro

5

¿Quiénes son los jóvenes que se pueden vacunar?

NOTAS DE LA SECCIÓN

>

Ecopetrol refuerza presencia en Asia con dos nuevas subsidiarias

>

Retos de la ciberseguridad en entornos empresariales

>

Detalles del proyecto del Gobierno para potenciar ahorro pensional

>

Avianca inauguró ruta de Medellín a Punta Cana; mañana lanzará trayecto a Cancún

>

¿Aumentó el desempleo por el Paro Nacional? Esto dice el Dane