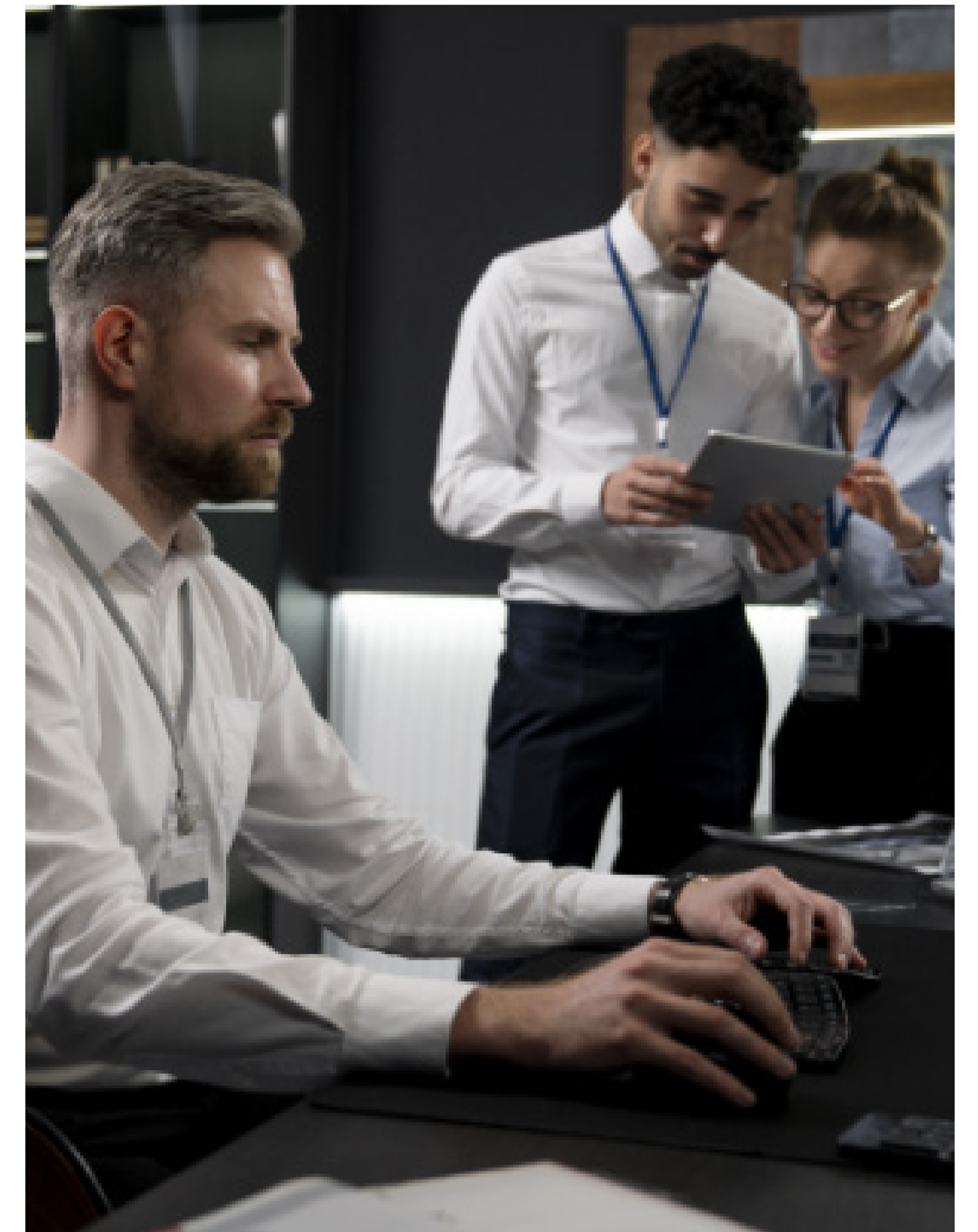


"BITDEFENDER GRAVITYZONE: NUEVAS HERRAMIENTAS PARA UNA CIBERSEGURIDAD EMPRESARIAL MÁS FUERTE Y EFICIENTE"

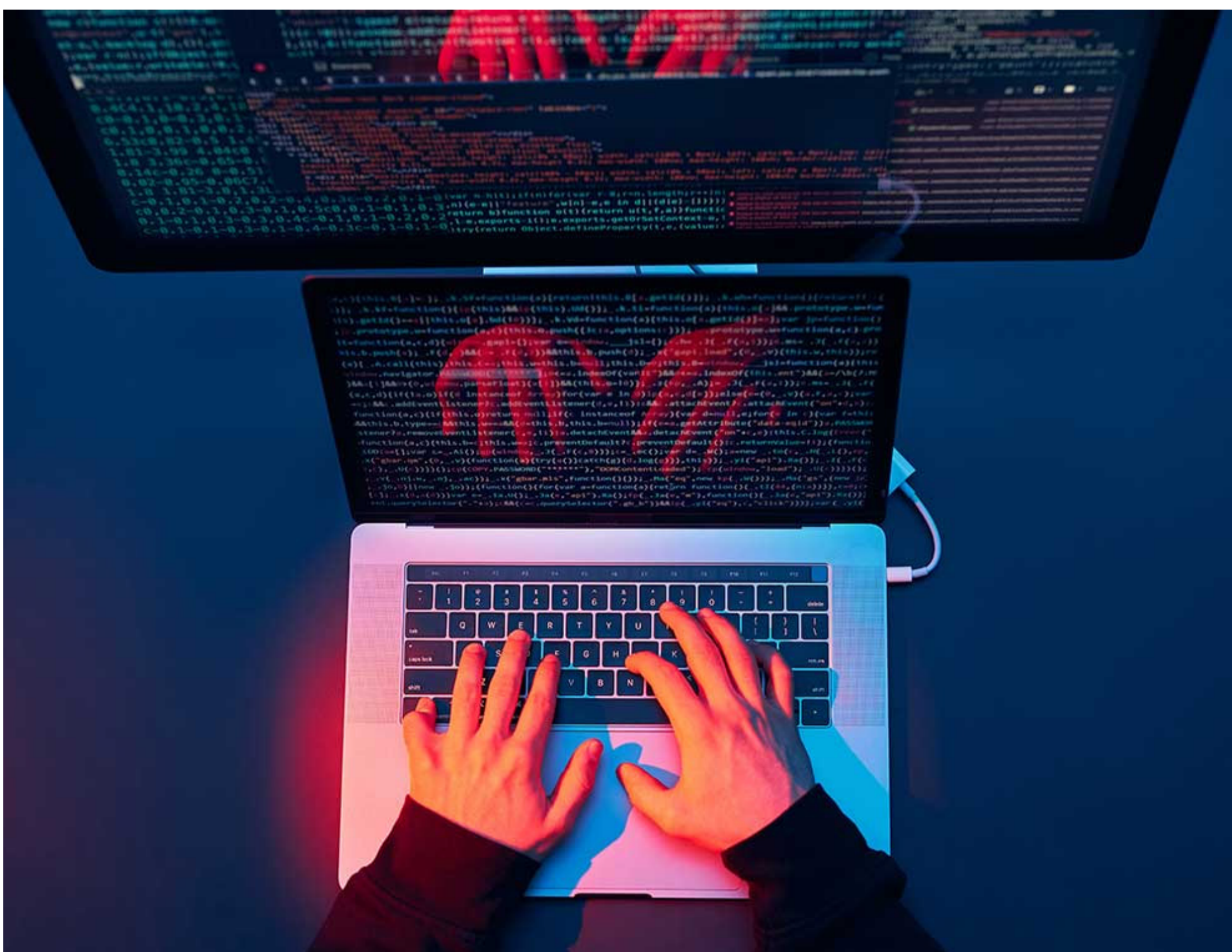
Bitdefender GravityZone se actualiza con nuevas funciones para reforzar la ciberseguridad empresarial. Ahora ofrece un informe de cumplimiento DORA, herramientas avanzadas para analistas de seguridad y mejoras en XDR, que optimizan la detección y respuesta ante amenazas en entornos de Azure AD. Estas innovaciones permiten una protección integral y eficiente en todas las capas de seguridad.

Los administradores ahora cuentan con más opciones en la sección de Red y una mejor integración con Active Directory. Además, la protección antimanipulación y la lista de bloqueo de rutas amplían la seguridad en múltiples plataformas.

[Lee el artículo completo escrito por Grzegorz Nocon](#)



FUNKSEC: EL GRUPO DE RANSOMWARE QUE USA IA PARA ATACAR EMPRESAS GLOBALES



En el último mes, el grupo de ransomware FunkSec ha ganado notoriedad por su creciente actividad y el uso de inteligencia artificial (IA) en sus ataques. Desde noviembre de 2024, FunkSec ha afectado a más de 120 organizaciones de sectores como gobierno, defensa, tecnología, finanzas y educación, especialmente en EE. UU., India, España y Mongolia. Aunque su uso de IA podría parecer sofisticado, en realidad refleja una limitada experiencia en desarrollo de códigos, lo que los lleva a depender de la IA para crear y ejecutar su malware.

La reciente versión 2.0 de su ransomware incluye mejoras en antidesdoblamiento y un panel RaaS, lo que podría aumentar su capacidad de ataque. Bitdefender Enterprise recomienda a las organizaciones reforzar su seguridad con soluciones avanzadas, como IntelliZone, para estar preparadas ante amenazas emergentes. Para más detalles sobre las tácticas de FunkSec y cómo proteger a tu empresa.

[Visita el artículo completo aquí](#)

```

1  # Funksec V1.5
2
3  # **Congratulations** # Your organization, device has been successfully infiltrated by funksec ransomware!
4
5  # **Stop**
6  - Do NOT attempt to tamper with files or systems.
7  - Do NOT contact law enforcement or seek third-party intervention.
8  - Do NOT attempt to trace funksec's activities.
9
10 # **What happened**
11 - your files encrypted by funksec ransomware, be careful to play or try decrypt the files because you just will lose
12 - We stole all your data.
13 - No anti-virus will restore it; this is an advanced ransomware.
14 - your data will be leaked if you don't pay ransom
15
16 # **Ransom Details**
17 - Decryptor exe fee: **0.1 BTC**
18 - Bitcoin wallet address: `bclqrhnt6cqsxt0qmlcaq0wcaqv6pafm82vtxfeq`
19 - Payment instructions:
20   1. Buy 0.1 bitcoin.
21   2. Install session from: https://repsession.org/
22   3. Contact us with this ID to receive the decryptor: 0538d726ae3cc264c1bd8e66c6c6fa366a3dfc589567944170001e6fdbea9e
23
24 # **How to buy bitcoin**
25 - Go to [Coinbase](https://www.coinbase.com/) or any similar website like [Blockchain](https://www.blockchain.com/),
26
27 # **Who we are**
28 - We are an advanced group selling government access, breaching databases, and destroying websites and devices.
29
30 # **Websites to visit**
31 - download tor : https://www.torproject.org/
32 - funkiyd7c6j3vvc52k2gml2u746fa51rwal2kjem6tvofj17rwid.onion
33 - funknqn44slumgagnewe60intbooukaup1k4yr1gtycew3ergraid.onion
34 - funkxxkovr7ctngbjnthdajav4ggex53k6m2x3esjwlxrb3qiztid.onion
35
36 # Funksec V1.5
37

```

Bitdefender®

¡REGRESO A CLASES SEGURO! BITDEFENDER PERÚ LANZAMOS CAMPAÑA CON DESCUENTO



En febrero iniciamos la campaña "Este regreso a Clases es Cool con Bitdefender Perú", realizando activaciones en distintos puntos de venta. Nuestro objetivo es informar e incentivar a padres, estudiantes y docentes sobre la importancia de proteger sus dispositivos con una sólida defensa digital en esta temporada escolar.

En marzo continuaremos compartiendo contenido valioso sobre las soluciones de Bitdefender, destacando sus beneficios y promoviendo nuestra oferta del 50% de descuento. Invitamos a todos a visitar nuestra web www.bitdefenderperu.com y aprovechar esta oportunidad para reforzar su seguridad digital.

DEFENSA DIGITAL PARA ESTE "REGRESO A CLASES"



Con el regreso a clases 2025, la tecnología se ha convertido en una herramienta clave para el aprendizaje, pero también expone a estudiantes, padres y docentes a riesgos digitales. Por ello te recomendamos cinco acciones para una Defensa Digital efectiva: usa contraseñas seguras, descarga apps solo de tiendas oficiales, configura la privacidad en redes sociales, emplea herramientas de control parental y educate sobre fraudes digitales y ciberacoso.

Claudia Torres, jefe comercial de Intecnia Corp, destaca la importancia de dialogar con las escuelas sobre las medidas de ciberseguridad y promover un entorno educativo más seguro.

[Para leer la nota completa, visita nuestro blog.](#)



Síguenos en nuestras redes sociales para mayor información:

