

Q&A

Ciberinteligencia Aplicada:

Lo que todo responsable de ciberseguridad debe saber

Protección contra Riesgos Digitales (DRP)

1. ¿QUÉ ES UN SERVICIO DE DIGITAL RISK PROTECTION (DRP) Y CÓMO CONTRIBUYE A LA ESTRATEGIA DE CIBERSEGURIDAD DE UNA EMPRESA?

Un servicio de DRP identifica y mitiga riesgos digitales externos como robo de datos, fraude y suplantación de identidad.

- **Protege activos expuestos** fuera del perímetro (dominios, IPs, marcas, logos, VIPs).
- **Monitoriza** web abierta, *deep* y *dark web* en busca de amenazas.
- Aporta **prevención proactiva**, detectando fases tempranas de amenazas que pueden escalar.
- **Complementa otras soluciones** dentro de la estrategia de seguridad.

2. ¿POR QUÉ LAS EMPRESAS DEBERÍAN ADOPTAR UNA SOLUCIÓN DE DRP?

DRP permite detectar y neutralizar riesgos digitales externos antes de que afecten al negocio, ofreciendo una capa adicional de visibilidad y protección fuera del perímetro tradicional.

- **Ofrece visibilidad** sobre lo que ocurre con la información de una empresa fuera del perímetro.
- Responde a preguntas clave: ¿hay filtraciones?, ¿robo de credenciales?, ¿dónde se expone la información y quién la usa?

- **Protege datos sensibles** y reduce la probabilidad de ataques.
- **Refuerza la protección de marca y la confianza** de clientes y socios.

3. ¿QUÉ SECTORES DE LA INDUSTRIA SE BENEFICIAN MÁS DEL USO DE UN SERVICIO DE DRP?

DRP es útil para cualquier organización, pero ciertos sectores obtienen un beneficio especialmente alto debido a su nivel de exposición y volumen de datos sensibles.

- Sectores más beneficiados: financiero, salud, telecomunicaciones y comercio electrónico.
- **Casos de uso frecuentes:**
 - Retail: detección de tiendas online falsas.
 - Empresas del IBEX: exposición de información y suplantación de VIPs.
- **Riesgos comunes:** fraude, robo de datos y ciberataques.
- **Objetivo de DRP:** proteger activos críticos y salvaguardar la reputación frente a amenazas externas.

DRP actúa desde el primer momento en que se detecta una amenaza, alertando al responsable de ciberseguridad y activando medidas para mitigar su impacto y proteger la imagen de la organización



4. ¿QUÉ ALCANCE TIENE UN SERVICIO DE DRP PARA IDENTIFICAR Y MITIGAR AMENAZAS QUE AFECTEN A MI EMPRESA?

Un servicio de DRP permite una vigilancia integral de entornos digitales externos con el objetivo de anticiparse a los riesgos antes de que impacten en el negocio, utilizando inteligencia obtenida de las mismas fuentes que usan los atacantes.

- **Ámbitos cubiertos:**
 - Web abierta: foros públicos, redes sociales, bases de datos públicas.
 - *Deep y dark web*: foros *underground*, mercados negros, dominios *.onion*, canales de Telegram.
- **Amenazas detectadas:**
 - Exposición de información.
 - Abuso de marca y suplantación de identidad.
 - Venta de credenciales, tarjetas robadas y apps móviles maliciosas.
 - Detección de actividad hacktivista y preparativos de ataques (*phishing*, *ransomware*...).

5. ¿DE QUÉ FORMA DRP DA RESPUESTA A LAS AMENAZAS Y AYUDA A PROTEGER LA REPUTACIÓN Y LA INTEGRIDAD DIGITAL FRENTE A AMENAZAS EXTERNAS Y FRAUDES?

DRP actúa desde el primer momento en que se detecta una amenaza, alertando al responsable de ciberseguridad y activando medidas para mitigar su impacto y proteger la imagen de la organización, lo que permite preservar su integridad digital y mantener la confianza pública.

- **Notificación inmediata** al responsable de

ciberseguridad ante una detección.

- **Mitigación preventiva**, como el bloqueo del acceso a contenidos maliciosos (ej. páginas de *phishing*).
- **Eliminación definitiva** de la amenaza:
 - Cierre de dominios sospechosos.
 - Solicitud de retirada de contenidos.
 - Desindexación en Google o inclusión en listas negras.

6. ¿QUÉ TAN RÁPIDO PUEDE UN SERVICIO DE DRP RESPONDER A UN INCIDENTE IDENTIFICADO?

Un servicio de DRP permite actuar desde el primer minuto, alertando en tiempo real para que los equipos de seguridad puedan responder de forma inmediata y mitigar el impacto del incidente, aunque el tiempo del *takedown* definitivo dependerá de la complejidad del caso.

- **Alerta en tiempo real** tras la detección de la amenaza.
- **Respuesta preventiva inmediata** por parte del equipo de seguridad.
- **Tiempo de *takedown* variable** según:
 - Localización del dominio (más rápido en registros locales, más lento en dominios internacionales).
 - Naturaleza del ataque (tipo de amenaza).
 - Colaboración externa necesaria (proveedores, autoridades, etc.).

7. ¿QUÉ RIESGOS Y CONSECUENCIAS PUEDE ENFRENTAR UNA EMPRESA QUE NO CUENTA CON UN SERVICIO DE DIGITAL RISK PROTECTION (DRP)?

Sin un servicio de DRP, una empresa se enfrenta a una total falta de visibilidad externa, lo que la deja expuesta a amenazas no detectadas, como fraudes, robo de identidad, filtraciones de datos, y explotación de vulnerabilidades.

- **Riesgos principales:**
 - **Falta de visibilidad** en la web abierta, *deep web* y *dark web*.
 - **Exposición a ataques no detectados** como fraude y suplantación de identidad.
 - **Falta de contención de amenazas avanzadas** que no son cubiertas por soluciones tradicionales.
 - **Riesgos financieros y daños a la reputación.**
 - **Sanciones regulatorias** en caso de filtraciones de datos sensibles.



Acerca de Telefónica Tech:

Telefónica Tech es un integrador de tecnología global, líder en transformación digital. La compañía cuenta con una amplia oferta de servicios y soluciones tecnológicas integradas de Ciberseguridad, Cloud, IoT, Big Data o Inteligencia Artificial. En todas estas verticales, contamos tanto con nuestras propias tecnologías como también con los mejores ecosistemas de partners estratégicos y así nos lo reconocen tanto los analistas de la industria como nuestros clientes. Y todo ello es posible también gracias a nuestros hubs en España, UK, Alemania, Brasil e Hispam llegamos a más de 5,5 millones de clientes en más de 175 países.

Si tienes alguna duda y quieres saber más sobre cómo podemos ayudarte, por favor:

→ [CONTÁCTANOS](#)



2025 © Telefónica Cybersecurity & Cloud Tech S.L.U. junto a Telefónica IoT & Big Data Tech S.A. Todos los derechos reservados.

La información contenida en el presente documento es propiedad de Telefónica Cybersecurity & Cloud Tech S.L.U. junto a Telefónica IoT & Big Data Tech S.A. (en adelante "Telefónica Tech") y/o de cualquier otra entidad dentro del Grupo Telefónica o sus licenciantes. Telefónica Tech y/o cualquier compañía del Grupo Telefónica o los licenciantes de Telefónica Tech se reservan todos los derechos de propiedad industrial e intelectual (incluida cualquier patente o copyright) que se deriven o recaigan sobre este documento, incluidos los derechos de diseño, producción, reproducción, uso y venta del mismo, salvo en el supuesto de que dichos derechos sean expresamente conferidos a terceros por escrito. La información contenida en el presente documento podrá ser objeto de modificación en cualquier momento sin necesidad de previo aviso.

La información contenida en el presente documento no podrá ser ni parcial ni totalmente copiada, distribuida, adaptada o reproducida en ningún soporte sin que medie el previo consentimiento por escrito por parte de Telefónica Tech. El presente documento tiene como único objetivo servir de soporte a su lector en el uso del producto, servicio o tecnología descrito en el mismo. El lector se compromete y queda obligado a usar la información contenida en el mismo para su propio uso y no para ningún otro.

Telefónica Tech no será responsable de ninguna pérdida o daño que se derive del uso de la información contenida en el presente documento o de cualquier error u omisión del documento o por el uso incorrecto del producto, servicio o tecnología. El uso del producto, servicio o tecnología descrito en el presente documento se regulará de acuerdo con lo establecido en los términos y condiciones aceptados por el usuario de este para su uso. Telefónica Tech y sus marcas (así como cualquier marca perteneciente al Grupo Telefónica) son marcas registradas. Telefónica Tech y sus filiales se reservan todos los derechos sobre las mismas.

[Ver nuestra política de privacidad aquí](#)