

SERVICIOS DE CIBERSEGURIDAD PARA EMPRESAS

FRENTE A LOS RETOS DE
LA TRANSFORMACIÓN
DIGITAL

Introducción

La transformación digital ha traído consigo grandes ventajas para las empresas: mayor productividad, competitividad y presencia en el mercado. No obstante, la digitalización también conlleva retos en el mismo ámbito, que hacen necesario que las empresas dispongan de una **estrategia de servicios de ciberseguridad robusta que gestione de la mejor manera las amenazas y riesgos.**

La ciberseguridad se ha vuelto indispensable dentro de los procesos corporativos para garantizar la continuidad de sus servicios y **minimizar cualquier tipo de impacto de forma holística con la finalidad de protegerse contra una amplia gama de amenazas digitales.** De este modo, contar con aliados a través de servicios especializados, con herramientas de vanguardia y expertos en el ámbito permite garantizar la óptima gestión de seguridad.

A continuación, abordaremos en profundidad qué debes saber sobre los principales servicios de ciberseguridad para diferentes organizaciones y sectores.

Servicios de ciberseguridad: ¿Qué son y cuál es su utilidad?

Son soluciones diseñadas para las entidades en sus 5 dimensiones: **disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad**. Al contar con soluciones específicas de ciberseguridad, podremos:

- **Maximizar la seguridad e integridad de los datos gestionados, de acuerdo con su nivel de sensibilidad o confidencialidad:** tanto propios como de clientes, especialmente necesario en empresas que gestionan grandes volúmenes de información.
- **Garantizar la protección de toda la estructura de red:** indispensable para la continuidad de todas las tareas cotidianas del negocio, permitiendo que sus servicios estén disponibles sin interrupciones.
- **Asegurar el cumplimiento de los requerimientos legales y normativos en temas de ciberseguridad y protección de datos:** exigidos en diferentes industrias y mercados.

- **Reducir impactos ante situaciones adversas y ciberincidentes:** que puedan ocasionarse, así como minimizar su ocurrencia optimizando la gestión de estos.
- **Disminuir el riesgo de pérdidas financieras y reputacionales, derivadas de un ciberincidente:** que puede repercutir en crisis organizacionales.



¿Cuáles son los servicios de ciberseguridad que tu organización necesita?

Para la prevención de cualquier incidente relacionado con la seguridad informática de tu negocio, es importante contratar a un proveedor de servicios de ciberseguridad capacitado, con experiencia demostrada que pueda **hacer un análisis real de acuerdo con tu sector y naturaleza organizacional**.

De igual manera, cualquier organización necesita una **estrategia de ciberseguridad** orientada a gestionar sus riesgos, que contemple un ciclo robusto orientado a: identificar, proteger, detectar, responder y recuperar.



Recomendaciones para escoger servicios de ciberseguridad

En general, la elección de un servicio de soluciones especializadas amerita una serie de consideraciones importantes:

Evaluar las **necesidades de la empresa**, considerando el tipo de industria y sector de mercado al cual pertenece.

Asegurar que el proveedor utiliza **herramientas efectivas** y que todas sus soluciones se integren a la infraestructura existente.

Elegir **soluciones escalables**, que puedan adaptarse a las nuevas necesidades, desafíos y amenazas que enfrentará la empresa.

Soluciones de ciberseguridad de Cipherbit-Grupo Oesía

Cipherbit-Grupo Oesía cuenta con un porfolio global de diferentes soluciones de ciberseguridad que **contemplan y garantizan una gestión de ciberseguridad holística** para todos sus clientes. Dentro de estas soluciones, podemos destacar:

- **Servicio de Monitorización 24x7 (SOC)**: Se trata de un servicio de monitorización continua del tráfico de red, tanto entrante como saliente, que es analizado en busca de potenciales patrones maliciosos. Permite una detección temprana de amenazas y, por ende, una actuación rápida para evitar un posible compromiso de la organización. Los equipos están compuestos por expertos de diferentes niveles de actuación, que posibilita llevar a cabo un ciclo de detección, contención y resolución en tiempo real.
- **Equipo de Hacking Ético**: Nuestro equipo de expertos técnicos en auditorías realiza las mismas técnicas que utilizan los ciberdelincuentes, pero con la finalidad de detectar activamente potenciales vulnerabilidades, tanto en aplicaciones como en sistemas de red, para así evitar que sean explotados por terceros actores.

- **Consultoría Normativa y de Cumplimiento:** Contamos con un equipo legal especializado en diferentes normativas de ciberseguridad nacionales e internacionales, como ISO27001, ENS, ISO22301, DORA, NIS2, RGPD (entre otras), que prestan soluciones de diferentes tipos, de acuerdo con las necesidades específicas de cada cliente: auditorías, adecuaciones, GAP análisis, etc.
- **Ciberentrenamiento, Concienciación y Formación:** La primera barrera de ciberseguridad es el ser humano. Por ello, nuestro equipo experto en formación y concienciación en materia de ciberseguridad ofrece estrategias con diferentes actividades dinámicas e interactivas, así como simulaciones de ataque de ingeniería social, para medir el nivel de cultura de seguridad de los usuarios y poder realizar concienciación orientada a minimizar los riesgos vinculados.
- **Seguridad Industrial:** Especialmente diseñados para la securización de infraestructuras y redes OT, permite asegurar la integridad y continuidad de prestación de los servicios de redes industriales, cumplimiento de controles y adecuación a normativas sectoriales, como **NIS2**.



Por

Olga Peñascal

Directora de Ciberseguridad
de Cipherbit-Grupo Oesía

A close-up photograph of a person's hand in a dark suit jacket touching a tablet. In the background, a light blue square contains a dark blue silhouette of a person wearing a suit and tie.

Crear un mundo mejor,
más eficiente, seguro y sostenible

grupooesia.com

