



Evaluación de Vulnerabilidades
Pruebas de penetración
Gestión de identidad y Acceso
Análisis y Protección de Red
Prevención de Pérdida de Datos (DLP)
Seguridad de Aplicaciones
Monitoreo de Seguridad y Respuesta a Incidentes
Educación en Ciberseguridad
Seguridad en la Nube
Análisis Forense Digital
Cumplimiento Normativo



CyberAttack
AUDITORÍA & FORMACIÓN

**Protege Tu Negocio
Protege Tu Éxito**



Quienes somos

Empresa especializada en ciberseguridad, ubicada en Roquetas de Mar - Almería. Más de 20 años en el sector de la informática.

Historia: Desde 1994, programando y dando servicios de seguridad en sistemas. En 2021, junto con otros profesionales del sector como ingenieros de sistemas, programadores y formadores en ciberseguridad, nace CBA, para dar solo y exclusivamente servicios de ciberseguridad.

Equipo: Contamos con auditores / formadores profesionales certificados en diversas disciplinas.

Que ofrecemos

Ofrecemos servicios de auditoría, consultoría y formación en ciberseguridad. Auditamos siguiendo los marcos:

- **ISO/IEC 27001.**
Este estándar establece los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI) dentro del contexto general de la gestión de riesgos empresariales.
- **NIST Cybersecurity Framework.**
Desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, este marco proporciona directrices para la mejora de la ciberseguridad organizacional, basándose en funciones clave como Identificar, Proteger, Detectar, Responder y Recuperar.

Y organizaciones como:

- **OWASP Top Ten.**
Organización que marca o propone puntos de auditoría para aplicaciones/paginas Web.
- **ENISA.**
La Agencia de la Unión Europea para la Ciberseguridad, que trabaja en colaboración con los estados miembros de la Unión Europea para mejorar la ciberseguridad en toda la región.

Servicios

Evaluación de Vulnerabilidades: Realización de auditorías de seguridad para identificar posibles brechas y debilidades en la infraestructura de TI.

Penetration Testing (Pruebas de Penetración): Simulación de ataques cibernéticos para evaluar la resistencia y capacidad de defensa de los sistemas.

Gestión de Identidad y Acceso: Implementación de soluciones para gestionar y proteger el acceso a sistemas y datos, utilizando autenticación multifactor y control de acceso.

Firewall y Protección de Red: Configuración y gestión de firewalls para filtrar el tráfico no autorizado y proteger las redes contra ataques.

Prevención de Pérdida de Datos (DLP): Implementación de medidas para evitar la fuga accidental o maliciosa de información confidencial.

Seguridad de Aplicaciones: Revisión y protección de aplicaciones contra posibles vulnerabilidades y ataques, incluyendo el desarrollo seguro de software.

Monitoreo de Seguridad y Respuesta a Incidentes: Supervisión continua de la actividad de red para detectar y responder a posibles incidentes de seguridad de manera rápida y eficiente.

Educación en Ciberseguridad: Programas de formación y concienciación para empleados, con el objetivo de mejorar las prácticas de seguridad y reducir el riesgo de amenazas internas.

Cifrado de Datos: Implementación de técnicas de cifrado para proteger la confidencialidad de los datos almacenados y transmitidos.

Seguridad en la Nube: Evaluación y mejora de la seguridad de las soluciones basadas en la nube, así como la implementación de políticas y controles adecuados.

Análisis Forense Digital: Investigación de incidentes de seguridad para determinar el origen y la extensión de un ataque, así como para recopilar evidencia legal.

Cumplimiento Normativo: Asegurarse de que las operaciones de seguridad cumplan con regulaciones y estándares específicos de la industria.

Protección contra Malware y Amenazas Persistentes Avanzadas (APTs): Implementación de soluciones para detectar, prevenir y responder a malware y ataques APT.

Actualizaciones y Parches de Seguridad: Mantenimiento constante de sistemas y aplicaciones para aplicar parches de seguridad y mitigar vulnerabilidades conocidas.

Seguridad de Dispositivos Móviles: Implementación de políticas y soluciones para proteger la información en dispositivos móviles y garantizar la seguridad de las comunicaciones.

Análisis de riesgos. Da una visión a la dirección de tu empresa, para poder abordar posibles incidencias en seguridad.

Formación

Te asesoramos sobre la mejora formación para tu crecimiento personal o empresarial. Nuestro equipo está compuesto por formadores profesionales que colaboran o han colaborado con empresas y organismos oficiales como:

Empresas.

- Arelance.
- Pue.
- SkillSoft.
- Ec-Council.
- Universidad de Barcelona.

Por medio de estas empresas, hemos formado en:

Organismos.

- Incibe.
- SEPE.
- PDI Chile.

Fundaciones.

- Fundación Once.
- Fundación Secretariado Gitano.

Deja que te orientemos en las mejores certificaciones y cursos del mercado, tanto de acceso gratuito como de pago.

