Grant Thornton

# Ciberseguridad & DFIR

La resiliencia que tu empresa necesita

# Gobierno, Riesgo y Cumplimiento (GRC)

Servicios de asesoría relacionados con una o varias normas de ciberseguridad, sean manuales de buenas prácticas o reglamentos de obligado cumplimiento por la actividad de la empresa, sus características o su sector.

La tecnología ha invadido todos los aspectos de las organizaciones, las amenazas se han multiplicado, y las exigencias también (leyes, normas, requisitos de clientes o proveedores, …). En esta situación, la gobernanza de la ciberseguridad y su alineación estratégica es esencial. Improvisar ya no es una opción.

**Análisis de aplicabilidad.** Determina el nivel de obligatoriedad de una o varias normas para una empresa específica.

**Evaluación GAP.** Determina el nivel de cumplimiento real de una empresa respecto a una norma en concreto, con recomendaciones para la evolución de dicho nivel de cumplimiento hasta alcanzar los objetivos de la organización.

**Evaluación de impacto.** Analiza los riesgos asociados a una o varias normas para una empresa específica.

**Asistencia de cumplimiento, total o parcial.** Desarrollo de tareas dirigidas a alcanzar el nivel de cumplimiento deseado en una o varias normas.

- Desarrollo de Planes Directores de Seguridad.
- Análisis y plan de gestión de riesgos.
- Desarrollo de políticas y procedimientos.
- Reingeniería de procesos.

Algunas normas:

- RGPD
- DORA
- NIS2
- ISO 27001/27002
- ENS
- ISO 22301
- PCI DSS
- NIST CSF 2.0
- ISA99/IEC 62443
- ISM/BIMCO
- COBIT

# Servicios de Red Team

Servicios de ciberseguridad ofensiva. Se utilizan las mismas tácticas y técnicas que usan los atacantes reales, para simular un ataque de forma realista y a la vez controlada.

Mediante estos servicios se pueden evaluar distintos aspectos de nuestra seguridad, ya sean vulnerabilidades técnicas, humanas u organizativas. Se trata de servicios con un alto nivel de personalización en función de la organización, sistemas, infraestructura, y los objetivos que se persigan.

**Análisis de vulnerabilidades.** Se identifican posibles vulnerabilidades de un sistema en concreto o de toda la infraestructura. En el alcance se determinarán los sistemas a analizar, la profundidad del análisis, o limitar el conjunto de vulnerabilidades a comprobar (como en el análisis OWASP Top 10).

**Test de intrusión.** Se busca valorar el posible impacto de un ataque real contra uno o varios sistemas, o toda la organización. Es el servicio más parecido a un ataque real, aunque se deben establecer previamente unas “reglas de juego”, según los objetivos buscados y la criticidad de los sistemas a atacar. También puede ser muy útil para medir la capacidad de respuesta del equipo de defensa.

**Test de ingeniería social.** Puede estar incluido en las “reglas de juego” de un test de intrusión, o realizarse de forma independiente. Se busca evaluar vulnerabilidades, pero en este caso en las personas relacionadas con la organización. Su forma más básica es una prueba de Phishing.

# Servicios de Blue Team

Servicios orientados a reducir la probabilidad de que ocurra un incidente, es decir, a prevenir. También se pueden incluir aquí los servicios de monitorización, que en función de la etapa en la que detecte la amenaza, servirán para evitarla o al menos para reducir su impacto mediante una respuesta temprana.

- **Arquitectura de seguridad.** Análisis y diseño de la infraestructura de la organización enfocada a la seguridad de la información.
- **Auditoría de código.** Revisión de aplicaciones, procedimientos de desarrollo seguro.
- **Bastionado de sistemas.** Configuración segura de los sistemas, planes de mantenimiento de la seguridad o de gestión de vulnerabilidades.
- **Operaciones de seguridad.** Configuración y explotación de los sistemas de seguridad de la organización.
- **Instrucciones Técnicas.** Desarrollo de procedimientos e Instrucciones Técnicas adecuadas a la empresa y sus mejores prácticas reales.
- **Inteligencia de amenazas y cibervigilancia.** Un informe puntual o una vigilancia continuada en el tiempo, con el objetivo de detectar amenazas inminentes o simplemente posibles para una persona u organización en particular.
- **Concienciación.** Acciones puntuales o planes de mejora continua de la concienciación de los usuarios en ciberseguridad. El objetivo es romper el mito de que el usuario es el eslabón más débil y convertirlo en nuestra medida de seguridad más importante (firewalls humanos).
- **Formación.** Formación especializada en ciberseguridad, normalmente dirigida a los departamentos técnicos o de seguridad.

# CSIRT

Servicios orientados a la gestión de incidentes, para la mejora continua de la resiliencia.

En el escenario actual de exposición y amenazas, la prevención es necesaria pero no suficiente. La preparación es fundamental para responder de la mejor forma posible cuando ocurran incidentes, es decir, con rapidez, coordinación y eficiencia. Sólo así se logra minimizar impactos y asegurar la continuidad de las operaciones.

- **Incident Readiness Assessment.** Ninguna empresa está tan preparada para enfrentarse a un incidente como cree. Evaluar el nivel de madurez, sea en los aspectos más técnicos (forensic readiness) o en todos los procesos implicados, es el primer paso para avanzar por el buen camino.
- **Planes y Procedimientos.** Plan de Continuidad (BCP), Recuperación (DRP), Respuesta a Incidentes (IRP), playbooks específicos, etc.
- **Ejercicios y simulacros.** Nadie quiere pasar por un incidente. Por tanto, para entrenar nuestra capacidad y descubrir puntos débiles, la mejor opción es un simulacro de incidente. Desde simulacros puramente técnicos, hasta ejercicios Table Top (TTX) de alto nivel diseñados para el Comité de Crisis.
- **Equipo de respuesta rápida.** Cuando llega el temido momento, nuestros especialistas pueden allanar el camino de vuelta a la normalidad. Más allá de los aspectos técnicos, es vital prestar atención a todas las áreas implicadas (legal, comunicación, financiera, operaciones, etc.).
- **DFIR.** Nuestro equipo de Forensic cuenta con amplia experiencia en todo tipo de investigaciones multidisciplinares a nivel nacional e internacional, así como en la elaboración de informes periciales y su posterior ratificación.

## Sobre nosotros

Vamos más allá con tu empresa para ofrecerte una experiencia diferencial. Somos una Firma global líder de servicios profesionales de Auditoría, Consultoría de Negocio, Tecnología e Innovación y Asesoramiento Fiscal, Legal, Financiero y Outsourcing.

En el mundo, estamos presentes en 150 mercados con más de 76.000 profesionales. En España contamos con un total de 11 oficinas repartidas por todo el territorio nacional y un equipo de más de 850 profesionales. Nuestros clientes nos avalan con un índice de Satisfacción del Cliente (CSI) de 9,12 puntos. Además, Grant Thornton España ha sido elegida Firma del Año de la red global de Grant Thornton en 2023.

## Grant Thornton, una Firma líder internacional


Grant Thornton ha sido seleccionada en el top 100 de Global Investigations Review 2024, que incluye las principales consultoras en investigaciones

## Contacto

**Cristina Muñoz-Aycuens**
Head of Cyber & DFIR
Cristina.Munoz-Aycuens@es.gt.com
T. (+34) 91 576 39 99

**GrantThornton.es**