

CSIRT

COMPUTER SECURITY INCIDENT RESPONSE TEAM

GMV estructura su oferta de Servicios Gestionados tipificados bajo el concepto CSIRT (Computer Security Incident Response Team). Se establecen distintos modelos de prestación para los mismos, que abarcan desde el modelo de externalización total (a través de nuestros Centros de Servicio) hasta diversos esquemas de co-explotación del servicio (a través de nuestras Oficinas de Seguridad).



GMV
Isaac Newton, 11 P.T.M. Tres Cantos 28760 Madrid ESPAÑA
www.gmv.es marketing.TIC@gmv.es

 www.facebook.com/infoGMV
 [@infoGMV_es](https://twitter.com/infoGMV_es)


INNOVATING SOLUTIONS

CENTROS DE SERVICIO

Nuestros Centros de Servicios disponen de los recursos hardware, software y comunicaciones requeridos para dar una solución multi-tecnología, acorde con la demanda altamente heterogénea de los clientes de GMV. Operan en un modelo de alta disponibilidad, disponiendo de mecanismos de redundancia, tanto local como geográfica según el Sistema de Gestión de Continuidad de Negocio de GMV, certificado por BSI bajo la norma BS 25999.

Los Centros de Servicio proporcionan un modelo de prestación 7x24. La gestión y operativa se fundamenta en el Sistema de Gestión de Servicios TI de GMV, certificado por AENOR bajo la norma ISO 20000.

La seguridad de los Centros de Servicios se articula en torno a un conjunto de controles físicos, técnicos y administrativos que garantizan la confidencialidad, integridad y disponibilidad de la información gestionada, tanto de GMV como de sus clientes. Estos controles de seguridad, así como la gestión de los mismos, se integran con el Sistema de Gestión de Seguridad de la Información de GMV, certificado por AENOR bajo la norma ISO 27001.

Los servicios proporcionados incluyen:

MONITORIZACIÓN

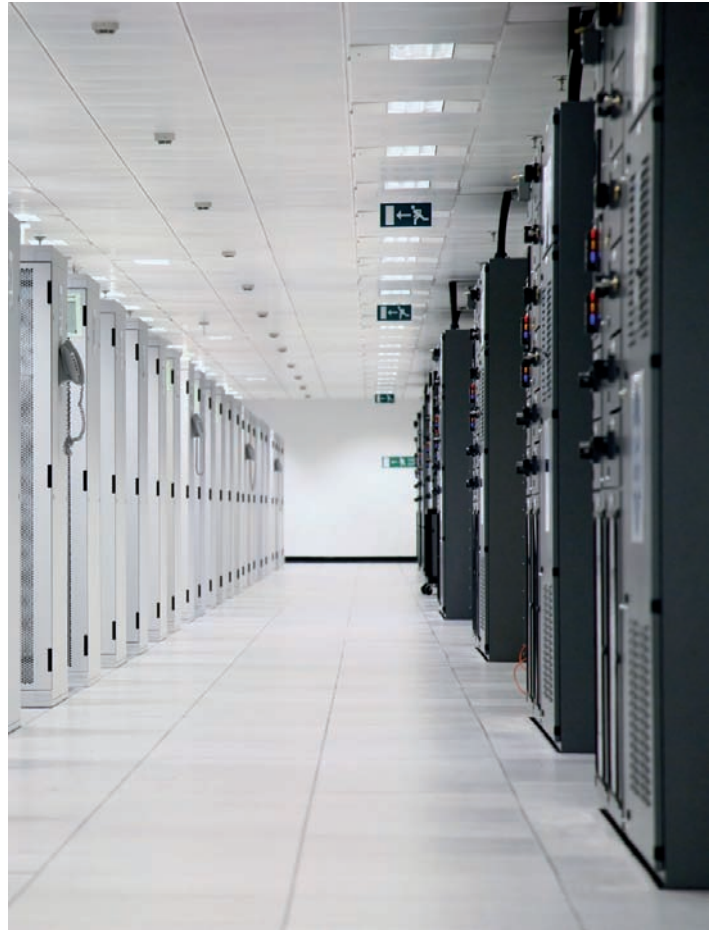
Los servicios de monitorización de plataformas, controles y servicios permiten chequear el estado de la disponibilidad y seguridad de infraestructuras y servicios, pudiendo identificar los elementos que están operando de forma inhabitual o cerca de su límite de capacidad, detectar actividad maliciosa, cuellos de botella o incidentes de seguridad potenciales. Una parte fundamental de estos servicios corresponden a los de centralización y gestión de logs/eventos de seguridad.

VIGILANCIA DIGITAL: ATALAYA

Atalaya es el Servicio de Vigilancia Digital que GMV presta a sus clientes, con el objetivo de saber qué información se publica a través de diferentes fuentes (redes sociales, blogs, buscadores, etc) o qué acciones se desarrollan que puedan suponer una amenaza o daño a la imagen corporativa. Con este servicio se facilita un control preventivo sobre el fraude, la fuga de información, hacktivismo y manifestaciones o ataques contra la organización o su personal clave.

GESTIÓN DE VULNERABILIDADES: GESTVUL

GestVul es el Servicio de Gestión de Vulnerabilidades que GMV presta a sus clientes, que permite conocer y gestionar el estado de seguridad que presentan los sistemas de información. Para ello realiza periódicamente una serie de pruebas automatizadas que permiten controlar todas las fases de una auditoría de seguridad, generar informes y analizar la evolución de las vulnerabilidades corregidas, mejoras en los índices de exposición, etc.



GESTIÓN DE INCIDENCIAS

El Servicio de Gestión de Incidencias tiene como objetivo dotar a la organización de la capacidad operativa para detectar, analizar, evaluar y dar respuesta a incidentes de seguridad. Para ello GMV cuenta con las metodologías, procedimientos e ingenieros con conocimientos suficientes en las distintas tecnologías de seguridad y con capacidad para cubrir tanto el soporte de aplicaciones como de infraestructuras en horario 7x24. Se complementa con servicios de Parcheado y Bastionado continuado, así como los servicios de Intervención Rápida para sistemas críticos.

GESTIÓN DE EVIDENCIAS

La gestión de evidencias cobra especial relevancia cuando la investigación de un incidente tiene como objetivo, no sólo identificar las causas y el impacto de lo que ha sucedido, sino también emprender acciones judiciales en caso de detectarse algún comportamiento ilegal en el ámbito del incidente. En este último caso será necesario, en algún momento del proceso, presentar las evidencias recopiladas en una causa judicial lo que obliga a tratar dichas evidencias con unas garantías que aumenten las posibilidades de que sean aceptadas por un juez. En GMV utilizamos las buenas prácticas españolas en las que trabaja el subcomité SC-27 de Aenor, cuyo seguimiento permite aumentar las posibilidades de que las evidencias recopiladas sean admitidas ante un juez.