

Análisis de correos sospechosos	Análisis de correos que puedan contener ciber amenazas, el objetivo es determinar si el correo es malicioso, en caso de ser malicioso identificar el tipo de técnicas utilizadas por los atacantes y proponer una solución.
Bastionado de Webs CMS	Aplicar parches y medidas de prevención en Webs desarrolladas con CMS como Wordpress, Drupal y Joomla. Con el fin de reducir las vulnerabilidades.
Monitorización SOC	Servicio continuo de monitorización de la ciber seguridad de los activos de una organización (sistemas, red, AD, etc): <ul style="list-style-type: none"> • Detección/bloqueo de ciber ataques. • Respuesta a incidentes. • Uso de equipo humano, profesionales de la ciberseguridad. • Personalizable para las necesidades de la organización. • Nuestro objetivo prioritario es prevenir y detectar las ciber amenazas.
Respuesta a incidente	Servicio de respuesta rápida para contener/analizar incidentes de ciber seguridad y poner soluciones a estas.
Threat intelligence	Monitorización y recopilación continua de las amenazas activas (leaks, vulnerabilidades, etc) en Internet que afectan a la organización.
Bastionado GNU/Linux	Aplicar parches y medidas de prevención en sistemas GNU/Linux. Con el fin de reducir las vulnerabilidades.
Bastionado Windows y Active Directory	Aplicar parches y medidas de prevención en sistemas Windows y Active Directory. Con el fin de reducir las vulnerabilidades.
Bastionado industrial (ICS/OT)	Aplicar parches y medidas de prevención en sistemas y redes ICS, previamente se realiza un análisis para estudiar las distintas posibilidades de bastionado.