BOLETÍN SEMANAL DEL MCCE

Del 28/08 al 03/09 de 2026



Las grandes empresas tecnológicas demandan una respuesta global frente a los ciberataques con IA

Diversas multinacionales tecnológicas han firmado un acuerdo marco para coordinar la defensa contra amenazas digitales avanzadas que emplean inteligencia artificial. Esta iniciativa promueve la transferencia de datos sobre vectores de ataque en tiempo real para proteger infraestructuras críticas globales. La cooperación prevé el desarrollo de protocolos comunes de mitigación inmediata y la creación de alianzas normativas para neutralizar operaciones encubiertas e intrusiones automatizadas.

Más información



Las redes eléctricas sufren ataques graves como medio desestabilizador

Las infraestructuras eléctricas inteligentes enfrentan ciberamenazas crecientes por el aumento de dispositivos conectados y el uso de tecnologías obsoletas. Estos ataques buscan causar impacto geopolítico o económico mediante la interrupción del suministro y el robo de información estratégica.

Más información



España fomenta la participación pública en la estrategia digital

El Gobierno impulsa un proceso participativo para actualizar la estrategia nacional hacia el año 2030. Diversos sectores sociales y económicos colaboran en la definición de las nuevas prioridades tecnológicas y de seguridad. Esta iniciativa busca establecer un marco normativo adaptado a los retos actuales de la digitalización.

Más información

BOLETÍN SEMANAL DEL MCCE

Del 28/08 al 03/09 de 2026



Los avances en inteligencia artificial aumentarán los presupuestos de seguridad

El auge de los ciberataques automatizados y las técnicas de suplantación impulsadas por sistemas inteligentes obligará a las organizaciones a destinar presupuestos millonarios a la protección digital. Las previsiones señalan que el gasto global en esta materia crecerá de forma exponencial durante el trienio.

Más información



El consumo energético o un comportamiento anómalo alertan de un software malicioso

El sobrecalentamiento inusual, el agotamiento rápido de la batería y el consumo excesivo de datos móviles indican una posible intrusión en el dispositivo. La presencia de software malicioso oculto ejecuta procesos en segundo plano para extraer información personal sin autorización.

Más información

Otras noticias

Campañas de ingeniería social atacan a los empleados de hostelería

Diversos ciberdelincuentes dirigen correos fraudulentos al personal del sector hotelero para infectar los sistemas informáticos. Los atacantes adjuntan enlaces y archivos maliciosos bajo la fachada de gestionar reservas o confirmar pagos de clientes. La intrusión en estas plataformas expone credenciales internas y permite el robo masivo de datos confidenciales.

Más información

Los ciberdelincuentes manipulan con engaños psicológicos

Las ciberestafas tienen éxito porque los delincuentes aprovechan sesgos de la conducta humana como la falsa sensación de autoridad y la urgencia. Los atacantes saturan la capacidad de juicio mediante sobrecarga de información y pequeños compromisos previos para manipular a sus víctimas. El exceso de confianza facilita la efectividad de estos engaños.

Más información