GUÍA DE FUENTES

Ciberseguridad

CENTRO DE ANÁLISIS

Y PROSPECTIVA

CONTENIDO

DATOS DE CONTACTO

INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (INCIBE)

https://www.incibe.es/

Avenida José Aguado, 41

Edificio INCIBE

24005 León

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

La actividad de INCIBE se apoya en tres pilares fundamentales: la prestación de servicios, la investigación y la coordinación.

- Servicios: INCIBE promueve servicios en el ámbito de la ciberseguridad que permiten el aprovechamiento de las TIC y elevan la confianza digital. En concreto, INCIBE trabaja en la protección de la privacidad de los usuarios, fomenta el establecimiento de mecanismos para la prevención y reacción en cuanto a incidentes de seguridad de la información, minimizando su impacto en el caso de que se produzcan, y promueve el avance de la cultura de la seguridad de la información a través de la concienciación, la sensibilización y la formación.
- Investigación: INCIBE cuenta con una importante capacidad para abordar proyectos complejos de diversa naturaleza y con un fuerte componente innovador. La dinámica de sus operaciones está orientada a la investigación, lo que permite que INCIBE cuente con capacidad para generar inteligencia en ciberseguridad como motor para abordar su aplicación en nuevas tecnologías y mecanismos que reviertan también en la mejora de los servicios.
- Coordinación: INCIBE participa en redes de colaboración que facilitan la inmediatez, globalidad y efectividad a la hora de desplegar una actuación en el ámbito de la ciberseguridad, contando siempre con una perspectiva basada en la experiencia y en el intercambio de información. Por ello, la coordinación y colaboración con otras entidades, tanto públicas como privadas, nacionales e internacionales, de todo el ámbito de la ciberseguridad es un factor imprescindible para la actividad de INCIBE.

PUBLICACIONES Y DOCUMENTACIÓN

El Instituto Nacional de Ciberseguridad (INCIBE), como entidad de referencia para el desarrollo de la ciberseguridad y de confianza digital, tiene entre sus cometidos fomentar la cultura de seguridad entre los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos. Uno de los elementos que utiliza

INCIBE para fomentar esta cultura de la seguridad es la creación de guías y estudios sobre temas relacionados con la ciberseguridad. Estas guías y estudios tienen como finalidad aportar tanto un valor práctico como teórico a fin de promover y mejorar la seguridad digital en todos los ámbitos de la sociedad y, sobre todo, para administradores de sistemas y técnicos en ciberseguridad.

Alerta temprana. Desde esta sección, INCIBE proporciona diversa información con el objetivo de facilitar a los lectores las últimas novedades relativas a vulnerabilidades, publicación de avisos y el acceso a un repositorio con los casos más relevantes relativos a la ciberseguridad. Además, si lo desea puede suscribirse a los boletines de actualidad de INCIBE para estar puntualmente informado de las últimas vulnerabilidades y avisos de seguridad en Tecnologías de la Información, a través de la sección Suscripción.

Respuesta y Soporte. INCIBE ofrece también un servicio de asistencia y soporte desde el cual se puede solicitar asistencia ante un incidente de seguridad o realizar consultas sobre legislación vigente en materia de tecnologías de la información.

Bitácora de ciberseguridad. Este servicio ofrece un repositorio con información, noticias, sucesos o cualquier evento importante en materia de ciberseguridad, con la idea de poderlo consultar a modo de histórico de “que ha pasado” en determinada fecha.

DATOS DE CONTACTO

CENTRO CRIPTOLÓGICO NACIONAL (CCN)

https://www.ccn.cni.es/

C/Argentona, 20

28023 MADRID

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

El Centro Criptológico Nacional (CCN) es el responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, además de garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

El CCN fue creado en el año 2004, a través del Real Decreto 421/2004, adscrito al Centro Nacional de Inteligencia (CNI). De hecho, en la Ley 11/2002, de 6 de mayo, reguladora del CNI, se encomienda a dicho Centro el ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información y de protección de la información clasificada, a la vez que se confiere

a su secretario de Estado director la responsabilidad de dirigir el Centro Criptológico Nacional. Por ello, el CCN comparte con el CNI medios, procedimientos, normativa y recursos.

PUBLICACIONES Y DOCUMENTACIÓN

Series CCN-STIC. Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Marco Legal. En este apartado se puede consultar la legislación española de referencia (Leyes, Real Decretos, etc.), teniendo en cuenta, dentro del contexto jurídico europeo, los siguientes ámbitos: protección de datos personales, protección de consumidores, firma electrónica y sociedad de la información.

DATOS DE CONTACTO

CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS (CNPIC)

http://www.cnpic.es/

Email: ses.cnpic-buzon@interior.es

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) es el órgano que se encarga de impulsar, coordinar y supervisar todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior, en relación con la protección de las infraestructuras críticas españolas.

Su objetivo principal es impulsar y coordinar los mecanismos necesarios para garantizar la seguridad de las infraestructuras que proporcionan los servicios esenciales a nuestra sociedad, fomentando para ello la participación de todos y cada uno de los agentes del sistema en sus correspondientes ámbitos competenciales. Mediante la integración de todos estos esfuerzos, se pretende fomentar un modelo de seguridad

basado en la confianza mutua, creando una asociación público-privada que permita minimizar las vulnerabilidades de las infraestructuras críticas ubicadas en el territorio nacional.

PUBLICACIONES Y DOCUMENTACIÓN

Guías SCADA. Dentro de las TIC en el ámbito de las infraestructuras críticas, es habitual la existencia de sistemas de control industrial, que presentan ciertas peculiaridades con respecto a los sistemas tecnológicos empleados en otros ámbitos, debido a la importancia que se presta a la operatividad en tiempo real y al grave impacto que tendría cualquier incidente sobre ellos. En este sentido el CNPIC, gracias al acuerdo de colaboración que tiene con el Centro Criptológico Nacional (CCN), presenta una serie de guías de interés para la seguridad de los sistemas de control industrial, también conocidos comúnmente como sistemas SCADA.

DATOS DE CONTACTO

CCN-CERT

https://www.ccn-cert.cni.es/

Email: info@ccn-cert.cni.es

C/Argentona, 20

28023 MADRID

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema

Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a esta normativa, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país (aquellos que son esenciales para la seguridad nacional y para el conjunto de la economía española).

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

PUBLICACIONES Y DOCUMENTACIÓN

Guías CCN-STIC de Seguridad. Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las

amenazas y vulnerabilidades detectadas por el CCN-CERT. El grueso de las Series están especialmente dirigidas al personal de las Administraciones Públicas y empresas y organizaciones de interés estratégico (parte privada del portal) y otras de difusión pública para todos los usuarios. De igual modo, algunas de las series están clasificadas como Difusión Limitada (DL) o Confidencial (C) y, por tanto, es necesaria su solicitud al CCN-CERT.

Informes de Ciberseguridad CCN-CERT. Informes elaborados por el grupo de expertos del CCN-CERT con distinta periodicidad.

Guías SCADA. Los sistemas SCADA o sistemas de Supervisión, Control y Adquisición de Datos comprenden todas aquellas soluciones de aplicación que recogen medidas y datos operativos de equipos de control locales y remotos. Los datos se procesan para determinar si los valores están dentro de los niveles de tolerancia y, de ser necesario, tomar medidas correctivas para mantener la estabilidad y el control. La seguridad de los sistemas SCADA es especialmente relevante en el ámbito de las Infraestructuras Críticas. Un fallo en una Infraestructura Crítica supone un perjuicio para toda la sociedad, en muchos casos para todo un país y su entorno. Su seguridad trasciende el ámbito de la empresa y requiere del asesoramiento y el control de organismos superiores.

Seguridad al día. Este apartado le ofrece la información más actual en materia de ciberseguridad, recopilada de fuentes propias y de terceros y centrada en las noticias diarias extraídas de enlaces externos, las alertas y vulnerabilidades de los principales fabricantes y la actividad del propio CCN-CERT.

DATOS DE CONTACTO

CENTRO NACIONAL DE EXCELENCIA EN CIBERSEGURIDAD (CNEC)

https://www.cnec.university/

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

El CNEC es un centro dependiente del ICFS de la UAM (en colaboración con la EPS) dedicado a la formación, entrenamiento, investigación y desarrollo tecnológico de excelencia en materia de ciberseguridad y ciberinteligencia para el incremento de la eficacia de la lucha contra la criminalidad.

El CNEC forma parte del proyecto puesto en marcha por la Dirección General de Home Affairs de la Comisión Europea en

2009 para dotar a los países miembros de ayudas para la creación de Centros Nacionales de Excelencia en Ciberseguridad con el objetivo de formar la red europea de centros dedicados a la formación y desarrollo tecnológico para la lucha coordinada contra el fenómeno creciente de la cibercriminalidad. Así mismo, esta red forma parte de la Estrategia Europea de Ciberseguridad de la Unión Europea, promovida por la Comisión Europea.

Fue en julio de 2011 cuando el Instituto ICFS optó a este proyecto, aunando en su solicitud al Cuerpo Nacional de Policía (Brigada de Investigación Tecnológica), la Guardia Civil (Grupo de Delitos Telemáticos), y al grupo empresarial S21sec. Hacia mediados de noviembre de 2012 la Dirección General de Home Affairs comunicó la concesión de las ayudas al proyecto "Centro Nacional de Excelencia en Ciberseguridad" e inmediatamente comenzaron a trabajar. De tal forma que hoy se puede decir que el CNEC ya es una realidad para España.

Para lograr los objetivos propuestos, el CNEC inició su andadura juntando los esfuerzos de la academia, organismos oficiales y empresas del sector, conformando un cluster cohesionado cuya vocación es la continuidad y expansión, tanto a otras empresas como organismos oficiales.

DATOS DE CONTACTO

GLOBB SECURITY

http://globbsecurity.com/

Email: info@globbtv.com

Calle Hermanos de Andrés, 2

28029 Madrid

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

Globb Security es el sitio web de referencia para los profesionales y entusiastas de la seguridad digital. En Globb Security se encuentran las últimas noticias sobre ciberseguridad, seguridad de datos y privacidad, vulnerabilidades y malware, ciberdelincuencia, así como contenidos sobre software y hardware para seguridad, entrevistas con expertos y contenido

didáctico, para ampliar y poner al día los conocimientos sobre seguridad.

PUBLICACIONES Y DOCUMENTACIÓN

Agenda: Toda la información actualizada de los próximos eventos del sector.

Entrevistas: Encuentros con los protagonistas de la actualidad de la seguridad informática, expertos, gurús y representantes de las empresas del sector.

How-To: Demostraciones de productos o tecnologías, tutoriales y guías prácticas.

Mundo Hacker: Acceso a los vídeos del programa sobre seguridad tecnológica más importante del sector.

Reviews: Análisis de los últimos productos y servicios del mundo de la seguridad, realizados tanto por el equipo de expertos de GlobbTV como por gurús y expertos profesionales del sector.

Whitepapers: Documentos de alto valor creados por expertos o empresas de seguridad: informes, estudios, información sobre últimos productos…

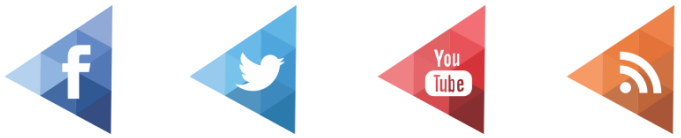
DATOS DE CONTACTO

OFICINA DE SEGURIDAD DEL INTERNAUTA (OSI)

https://www.osi.es

Email: consultas@osi.es

REDES SOCIALES



OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

En la Oficina de Seguridad del Internauta (OSI) de INCIBE proporcionan la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.

Su objetivo es reforzar la confianza en el ámbito digital a través de la formación en materia de ciberseguridad. En la OSI de INCIBE trabajamos para:

- Ayudar a los usuarios a llevar a cabo un cambio positivo de comportamiento en relación con la adopción de buenos hábitos de seguridad.

- Hacerles conscientes de su propia responsabilidad en relación con la ciberseguridad.
- Contribuir a minimizar el número y gravedad de incidencias de seguridad experimentadas por el usuario.

En este portal se encuentra información general sobre la seguridad en Internet y herramientas que ayudan a navegar más seguro. Además, a través del canal de avisos se puede estar actualizado de las últimas alertas de seguridad.

DATOS DE CONTACTO

ASOCIACIÓN NACIONAL DE CIBERSEGURIDAD Y PERICIA TECNOLÓGICA (ANCITE)

http://www.ancite.es/

Email: info@ancite.es

C/ Claudio Coello, 24 3º A3

28001 Madrid

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

La Asociación Nacional de Ciberseguridad y Pericia Tecnológica -ANCITE- abarca toda la geografía nacional. Su proyección profesional está enmarcada dentro del ámbito de la seguridad informática y las Nuevas Tecnologías de la Información y la

Comunicación, tratando todos los temas relacionados con la informática y la ciberseguridad; tales como auditorías, periciales, forenses, mediaciones, defensa jurídica tecnológica, pruebas de estrés de seguridad, etc.

Han firmado acuerdos de reciprocidad, con las Asociaciones de Ciberseguridad y Pericia Informática y/o Tecnológica existentes en las diferentes Comunidades Autónomas. Debido a estos acuerdos entre asociaciones, no solo abarcan por completo el Territorio Nacional sino que están capacitados para desarrollar cualquier pericia tecnológica –por compleja que sea–, gracias a la cantidad y calidad de los profesionales a los que pueden acceder.

ANCITE es una entidad privada sin ánimo de lucro y de carácter asociativo que acoge a profesionales de alto nivel en activo relacionados con el sector de las Nuevas Tecnologías, la Seguridad de la información, de las comunicaciones y del Derecho Tecnológico.

La asociación está constituida por profesionales contrastados en las diferentes especialidades informáticas; y ya se ha convertido en pieza básica e indispensable en pericias para empresas, particulares y Administraciones de Justicia que han necesitado de sus servicios, para conocer y recibir un dictamen profesional acerca de los diferentes tipos de delitos informáticos, conflictos, incumplimientos y desavenencias, tasaciones y valoraciones en procesos particulares, judiciales, leales, científicos y forenses.

DATOS DE CONTACTO

OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (ONTSI)

http://www.ontsi.red.es/

Email: observatorio@red.es

Edificio Bronce

Plaza Manuel Gómez Moreno, s/n

28020 Madrid

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información es un órgano adscrito a la entidad pública empresarial Red.es, cuyo principal objetivo es el

seguimiento y el análisis del sector de las Telecomunicaciones y de la Sociedad de la Información.

ONTSI elabora, recoge, sintetiza y sistematiza indicadores, elabora estudios y ofrece servicios informativos y de actualidad sobre Sociedad de la Información, siendo actualmente el Observatorio público sobre la Sociedad de la Información líder en España.

ONTSI es, además, punto de encuentro y de diálogo entre el sector de las Tecnologías de la Información y las Comunicaciones y las distintas administraciones públicas, para la definición de políticas y su posterior evaluación.

PUBLICACIONES Y DOCUMENTACIÓN

Área de Estudios. Es la encargada de la realización de estudios que analizan el desarrollo de la Sociedad de la Información en España, en el ámbito de los hogares y ciudadanos, empresas y en el sector de las Tecnologías de la Información y las Comunicaciones.

Área de Indicadores-Datos Sector TIC. Sintetizar y analizar indicadores y datos sobre Sociedad de la Información, estructurados por sectores, por fuentes de información, así como un apartado específico de indicadores eEurope. También es el área encargada de la realización de informes específicos para asesorar a los distintos organismos y poderes públicos sobre implantación de la Sociedad de la Información en España y en la UE.

Herramienta ONTSI.Data. ONTSI.data es una herramienta con la que podrá elaborar sus propios informes con los principales indicadores de la Sociedad de la Información, del sector de las Tecnologías de la Información y las Telecomunicaciones para España, países de la Unión Europea y miembros de la OCDE.

DATOS DE CONTACTO

THIBER

http://www.thiber.org/

Calle Alcalá 75, 2a planta

28009 Madrid

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

THIBER, the cybersecurity think tank, nace en 2013 como punto de referencia de la comunidad hispanohablante y generador de ideas, de origen apolítico, con clara vocación internacional en materia de seguridad y defensa del ciberespacio.

Su misión es la de:

- Analizar y estudiar la influencia del ciberespacio en la seguridad y defensa nacional e internacional con el objeto de proponer acciones que posibiliten su dirección y gestión por parte de todos los sectores de la sociedad.

- Crear y fortalecer espacios de diálogo y debate, favoreciendo la creación de un estado de opinión.
- Desarrollar y capacitar a futuros tomadores de decisiones en temas ciber.
- Ofrecer un rol de auditor de los actores públicos.
- Formar y concienciar en materia de ciberseguridad.

PUBLICACIONES Y DOCUMENTACIÓN

CIBER Elcano. Informe Mensual de Ciberseguridad desarrollado para el Instituto por Thiber (The Cyber Security Think Tank), el primer think tank de referencia en lengua castellana en materia de seguridad y defensa en el ciberespacio, perteneciente al Instituto de Ciencias Forenses y de la Seguridad (ICFS), de la Universidad Autónoma de Madrid (Campus Cantoblanco).

DATOS DE CONTACTO

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

https://www.bsi.bund.de

Email: bsi@bsi.bund.de

Godesberger Allee 185-189

53175 Bonn, Germany

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

Las personas cada vez son más dependientes de la tecnología de la información (TI), motivo por el que el tema de la seguridad se vuelve más relevante. La amenaza a nuestra sociedad en este aspecto, por uso indebido o sabotaje, puede causar más complicaciones que con anterioridad. Debido a la complejidad de los problemas de TI, el espectro de tareas de la BSI es extremadamente amplio. El BSI investiga los riesgos de seguridad asociados al uso de las TI y desarrolla medidas de seguridad preventivas. También proporciona información sobre los riesgos y peligros relacionados con el uso de la tecnología de la información y busca soluciones adecuadas. Este trabajo

incluye pruebas de seguridad de TI y la evaluación de los sistemas informáticos, incluyendo su desarrollo, en cooperación con la industria. Incluso en los sistemas de información y telecomunicaciones técnicamente seguras, los riesgos y daños todavía pueden ocurrir como resultado de la administración inadecuada o su uso indebido. Para minimizar o evitar estos riesgos, los servicios de la BSI están destinados a una variedad de grupos objetivo: fabricantes, distribuidores de tecnología de la información. También se analiza el desarrollo y la evolución de la tecnología de la información.

El BSI está organizado en cinco departamentos, uno central y cuatro departamentos especializados. Cada departamento consta de una o dos divisiones, cada una de las cuales a su vez comprende un número de secciones.

PUBLICACIONES Y DOCUMENTACIÓN

BSI Magazine. Esta revista ofrece una visión de proyectos seleccionados sobre la seguridad de las Tecnologías de la Información y la Seguridad Informática, que se están convirtiendo en temas cada vez más importantes en nuestra vida cotidiana.

IT Security Situation. El informe de la Federal Office for Information Security in Germany (BSI) sobre el estado actual de la seguridad de TI en Alemania en 2015, proporciona información sobre el tipo y alcance de las amenazas clave y los riesgos resultantes. El informe se basa en la información procesada por el BSI en relación con las debilidades y vulnerabilidades en tecnologías de la información utilizada en la actualidad, así

como a los ataques a sistemas y redes informáticas. El informe muestra que el número de debilidades y vulnerabilidades en los sistemas de TI sigue incurriendo en un alto nivel. Algunas de estas vulnerabilidades exponen brechas de seguridad graves. El nivel de amenaza asimétrica en el ciberespacio sigue aumentando, lo que significa que la protección de los sistemas informáticos de los usuarios no siempre puede seguir el ritmo de las herramientas a menudo altamente desarrolladas para explotar brechas en la seguridad.

DATOS DE CONTACTO

CENTRO DE CIBERSEGURIDAD INDUSTRIAL (CCI)

https://www.cci-es.org

Calle Maiquez, 18

E-28009, MADRID

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

El Centro de Ciberseguridad Industrial se ha establecido en pro del impulso y contribución a la mejora de la Ciberseguridad Industrial, elaborando actividades de análisis, desarrollo de estudios e intercambio de información sobre el conjunto de prácticas, procesos y tecnologías diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las

organizaciones e infraestructuras industriales y cómo estas suponen una de las bases sobre las que está construida la sociedad actual.

PUBLICACIONES Y DOCUMENTACIÓN

El Boletín Semanal es una recopilación de noticias, documentos técnicos y divulgativos, eventos y reflexiones de actualidad relacionados con la Ciberseguridad Industrial. El boletín evita el carácter comercial y se centra en la divulgación y la información de los hechos más relevantes de la actualidad. El boletín está abierto a la colaboración de los miembros que quieran contribuir con sus propias reflexiones acerca de la Ciberseguridad Industrial. Este boletín tan solo genera un mensaje de correo electrónico a la semana (los lunes) y es enviado a todos los miembros del CCI de forma gratuita.

Una de las principales actividades realizadas desde el CCI es el desarrollo de informes y análisis estratégicos de alta calidad centrados en la Ciberseguridad Industrial. La adquisición de los documentos es exclusiva para sus miembros. Estos documentos son de pago y el coste dependerá de su magnitud.

DATOS DE CONTACTO

NATO COOPERATIVE CYBER DEFENCE
CENTRE OF EXCELLENCE

https://ccdcoe.org

Email: ccdcoe@ccdcoe.org

Filtri tee 12

Tallinn 10132

Estonia

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

NATO Cooperative Cyber Defence Centre of Excellence es un centro de entrenamiento sobre educación, consulta, lecciones aprendidas, investigación y desarrollo en el campo de la seguridad cibernética.

PUBLICACIONES Y DOCUMENTACIÓN

Cyber Defence Library. Esta biblioteca digital reúne libros, artículos, informes y otras publicaciones de la NATO Cooperative Cyber Defence Centre of Excellence, así como el trabajo de sus expertos.

Cyber Security Strategy Documents. Selección de documentos sobre seguridad nacional y las estrategias de defensa en materia de ciberseguridad.

INCYDER (International Cyber Developments Review). Esta herramienta de investigación interactiva se centra en los documentos jurídicos y normativos adoptados por las organizaciones internacionales activas en seguridad cibernética. La colección de documentos es periódicamente actualizada y apoyada por un completo sistema de etiquetas que permiten filtrar el contenido por subdominios específicos. INCYDER también ofrece descripciones y noticias sobre estas organizaciones seleccionadas.

DATOS DE CONTACTO

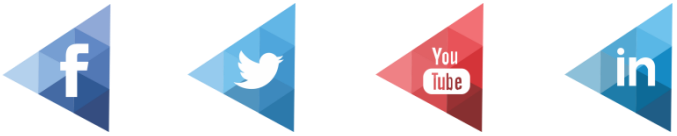
EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY – ENISA

https://www.enisa.europa.eu/

P.O. Box 1309

710 01 Heraklion – Crete – Greece

REDES SOCIALES



OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

La ENISA, Agencia Europea de Seguridad de las Redes y de la Información, es un centro de conocimientos especializados para la seguridad cibernética en Europa. La ENISA ayuda a la UE y los países que la integran a estar mejor equipados y preparados para prevenir, detectar y dar respuesta a los problemas de seguridad de la información.

La ENISA colabora estrechamente con Europol y con el Centro Europeo de Ciberdelincuencia (EC3) en materia de comunicación e investigación conjunta.

PUBLICACIONES Y DOCUMENTACIÓN

La ENISA también publica informes y estudios sobre cuestiones de ciberseguridad. Ha elaborado estudios sobre:

- seguridad de la nube,
- protección de datos,
- tecnologías potenciadoras de la privacidad y cómo garantizar la privacidad de las nuevas tecnologías,
- servicios de identificación y de confianza,
- identificación de ciberamenazas.

La ENISA ayuda a elaborar las políticas y la legislación de la UE sobre seguridad de las redes y de la información.

DATOS DE CONTACTO

EUROPEAN CYBERCRIME CENTRE (EC3)

https://www.europol.europa.eu/ec3

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

La actividad del EC3 se centra en las actividades ilegales en línea de las bandas de delincuencia organizada, especialmente en los ataques dirigidos contra las operaciones bancarias y otras actividades financieras en línea, la explotación sexual infantil en línea y los delitos que afectan a las infraestructuras críticas y a los sistemas de información en la UE.

DATOS DE CONTACTO

US-CERT

https://www.us-cert.gov/

Email: info@us-cert.gov

Mailstop: 0635

245 Murray Lane SW Bldg 410

Washington, DC 20528

REDES SOCIALES

OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

US-CERT se esfuerza para una Internet más segura y más fuerte para todos, respondiendo a incidentes mayores, analizando las amenazas e intercambio de información crítica sobre ciberseguridad con socios de confianza alrededor del mundo.

Entre las actividades de misión crítica de US-CERT figuran:

- Protección de ciberseguridad a través de la intrusión de las capacidades de detección y prevención.

- Desarrollar información oportuna y procesable para su distribución a los departamentos federales y agencias; gobiernos estatales, locales, tribales y territoriales, propietarios de infraestructuras críticas y operadores; industria privada; y las organizaciones internacionales.
- Responder a incidentes y análisis de datos sobre nuevas amenazas cibernéticas.
- Colaborar con los gobiernos extranjeros y entidades internacionales para mejorar la postura de ciberseguridad de la nación.

PUBLICACIONES Y DOCUMENTACIÓN

Current Activity. Proporciona información actualizada sobre los tipos de alto impacto de la actividad de seguridad que afectan a la comunidad en general.

Alerts. Proporcionar información oportuna sobre temas de seguridad, vulnerabilidades y exploits.

Bulletins. Proporcionar resúmenes semanales de nuevas vulnerabilidades. Se facilita información de parche cuando está disponible.

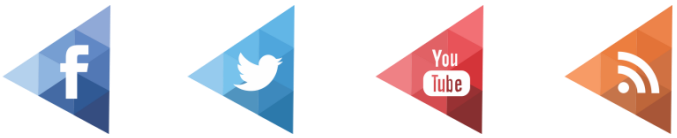
Tips. Asesorar sobre problemas de seguridad comunes para el público en general.

DATOS DE CONTACTO

GRUPO DE DELITOS TELEMÁTICOS DE LA GUARDIA CIVIL

https://www.gdt.guardiacivil.es

REDES SOCIALES



OBJETIVOS Y ÁREAS DE INVESTIGACIÓN

El Grupo de Delitos Telemáticos fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet.

Su origen se remonta al año 1996, cuando se constituyó el Grupo de Delitos Informáticos (GDI) para atender a las pocas denuncias que había entonces por los llamados delitos informáticos.

Su buen hacer y el crecimiento exponencial de usuarios de la red propiciaron el crecimiento del grupo, que pasó a llamarse Departamento de Delitos de Alta Tecnología (DDAT), asumiendo como nueva competencia el fraude en el sector de las telecomunicaciones.

Con la socialización de Internet y el crecimiento de los hechos delictivos, se amplía el abanico de competencias de investigación, que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra estos, lo que se conoce popularmente como el cibercrimen. El departamento cambia de nombre por el actual, Grupo de Delitos Telemáticos (GDT). Estos cambios se acompañaron de la creación de los Equipos de Investigación Tecnológica (EDITE,s) en cada uno de las provincias de España.

El esfuerzo principal del GDT y de los EDITE,s ha sido, desde su creación, la investigación de la delincuencia que se vale de las redes y sistemas de información para delinquir. También cabe destacar los esfuerzos que realizan para fomentar un uso seguro de las nuevas tecnologías, conscientes de que a la larga esta tarea ayudará a minimizar el impacto de la delincuencia.

Cabe destacar, en el trabajo del GDT, su presencia continuada en seminarios y conferencias internacionales, lo que le ha permitido crearse una red de contactos policiales a nivel internacional, esencial en la resolución de determinadas investigaciones.

Actualmente es miembro y participa activamente en los Grupos de Trabajo de Interpol de Europa y Latinoamérica, en el Foro internacional del G-8 para el cibercrimen y en el Grupo de Europol.

Para mayor información:

Centro de Análisis y Prospectiva

Tel. Jefe: 915146538

Tel. Oficina: 915146000/2956

Groupwise: 5904-271REG

Correo electrónico: dg-cap@guardiacivil.org