https://www.basquecybersecurity.eus

Qué es

BCSC, acrónimo de "Basque Cybersecurity Centre", es la organización designada por el Gobierno Vasco para promover la ciberseguridad en Euskadi. Nuestra misión es promover y desarrollar una cultura de ciberseguridad entre la sociedad vasca, dinamizar la actividad económica relacionada con la aplicación de la ciberseguridad y fortalecer el sector profesional.

Somos una iniciativa transversal que representa el compromiso del Gobierno Vasco con sus empresas y ciudadanía en el ámbito de la ciberseguridad

El Basque Cybersecurity Centre está formado por los siguientes agentes:

GOBIERNO VASCO – DEPARTAMENTOS:

- Desarrollo Económico e Infraestructuras
- Seguridad
- Gobernanza Pública y Autogobierno
- Educación

CENTROS TECNOLÓGICOS:

- Tecnalia
- Vicomtech
- Ik4-Ikerlan
- Basque Center for Applied Mathematics

LA IMPORTANCIA DE EVOLUCIONAR EN CIBERSEGURIDAD

La dinamización de la actividad económica relacionada con la aplicación de la ciberseguridad ayuda a **fortalecer el sector profesional**. Con ello conseguimos **promover y desarrollar la cultura de la ciberseguridad** en la sociedad vasca.

Nuestro propósito es ser reconocidos como **punto de encuentro y liderar iniciativas de colaboración**, posicionando a **Euskadi como referente** internacional en la aplicación de tecnologías de ciberseguridad a la industria.

Para hacer frente a estos retos, y con la finalidad de dar respuesta ante posibles incidentes derivados de la seguridad en Euskadi, **nos alineamos con agentes de la red vasca de ciencia, tecnología e innovación**, y con actores públicos clave de Gobierno Vasco como son **EJIE**, la **Ertzaintza** y el **Departamento de Educación**. También trabajamos con otros agentes relevantes de la Administración Pública Vasca como Izenpe, la AVPD o las empresas públicas de informática, así como con numerosas asociaciones profesionales, empresariales y ciudadanas que operan en Euskadi.

Otros colaboradores:

- Colaboramos con multitud de agentes de la industria vasca de ciberseguridad.
- Somos miembros de la **European Cyber Security Organisation (ECSO)** y participamos en varios grupos de trabajo.
- Colaboramos con el **Instituto Nacional de Ciberseguridad (INCIBE)** y con **INCIBE-CERT**, principalmente en la gestión de incidentes de ciberseguridad.
- Colaboramos con varias asociaciones sin ánimo de lucro (vascas, estatales e internacionales) que desean contribuir a promover la ciberseguridad en Euskadi.

MEMBRESÍAS

TF-CSIRT
Trusted Introducer

CSIRT.es

Nuestros servicios: CSIRT

Gestión de incidentes de ciberseguridad.
Apoyo y consejo ante un incidente de ciberseguridad a través del teléfono gratuito **900 104 891** o vía email mediante: incidencias@bcsc.eus / arazoak@bcsc.eus

Gestión de vulnerabilidades.
Facilitamos la comunicación entre quienes descubren vulnerabilidades y los fabricantes, promoviendo así una divulgación responsable a través de una comunicación fluida y honesta.

Análisis de malware.
Llevamos a cabo análisis de malware y desarrollamos estrategias de para detectar, eliminar y protegerse frente a él.

Publicación de Avisos.
Información práctica y relevante para mitigar y remediar vulnerabilidades de seguridad en sistemas tecnológicos.

Alerta temprana: Publicación de Alertas.
Información sobre amenazas y riesgos de especial relevancia.

Diseminación de información.
Elaboramos guías de buenas prácticas e informes situacionales en el ámbito de la ciberseguridad.

Compartición de información para hacer frente a las ciberamenazas.
Compartimos e intercambiamos información de amenazas con otros equipos de respuesta a incidentes, fabricantes, proveedores de servicios de internet y diversas entidades colaboradoras.

Capacitación.

A profesionales.
Realizamos talleres y jornadas para fomentar el aprendizaje en el ámbito de la ciberseguridad a través del portal www.spri.eus/euskadinnova.

Concienciación.

A menores.
Realizamos jornadas con el fin de que sean conscientes de los riesgos derivados del uso incorrecto de las nuevas tecnologías y cómo prevenirlos.

A empresas y asociaciones de entornos industriales.
Organizamos jornadas para sensibilizar a la industria vasca sobre la necesidad de adoptar medidas necesarias, en cuanto a ciberseguridad, para mantener la capacidad competitiva e innovadora en los diferentes mercados internacionales.

Nuestros servicios: De valor añadido

Monitorización de las redes públicas vascas.
Identificamos y tomamos medidas para mitigar ciberamenazas que pongan en riesgo tanto a la ciudadanía como a las empresas de Euskadi.

Colaboración con la Ertzaintza.
Trabajamos para evolucionar las capacidades para perseguir los ciberdelitos y mejorar la protección de las Instalaciones Sensibles.

Promoción de ayudas.
Favorecemos el proceso de implantación de ciberseguridad en entornos industriales.

Promoción de los agentes vascos.
Realizamos una búsqueda activa de socios y contacto con agentes complementarios para desarrollar proyectos en colaboración.

Alineamiento de la especialización.
Coordinamos iniciativas de I+D+i.

Basque Digital Innovation Hub.
Trabajamos para crear infraestructuras y ponerlas al servicio de las empresas.

Apoyo al Emprendimiento en Ciberseguridad.
Trabajamos en la iniciativa BIND 4.0 apoyando a startups vascas en el ámbito de la ciberseguridad.

Apoyo e identificación de talento ante la vocación de ciberseguridad.
Colaboramos en el desarrollo de iniciativas cuyo objetivo es que los jóvenes identifiquen la ciberseguridad como vía de desarrollo profesional.

La "Guía SGCI para el responsable de construir un sistema de gestión de la Ciberseguridad Industrial", disponible para empresas de Euskadi a través del BCSC

12/11/2018 | | RSS

La Industria 4.0 llegó hace ya algún tiempo para quedarse y Euskadi se situó entre las regiones que más rápidamente se adaptó y promovió medidas en este sentido, haciendo de nuestro sector secundario un referente internacional. En la actualidad, la aplicación de ciberseguridad a la industria 4.0 está cobrando cada vez mayor importancia y la inversión en este campo es imprescindible. Con el fin de guiar a las empresas en el proceso de implantar medidas que las protejan de los ciberdelincuentes y que las sitúen en una posición privilegiada por aprovechar la ciberseguridad como valor diferencial, el Centro Vasco de Ciberseguridad (BCSC) pone a disposición de las empresas establecidas en Euskadi la "Guía SGCI para el responsable de construir un sistema de gestión de la Ciberseguridad Industrial".

Un documento de referencia para empresas industriales

BCSC pone a disposición de las empresas industriales establecidas en Euskadi el "Mapa Normativo de la Ciberseguridad Industrial", elaborado por CCI

10/12/2018 | RSS

Conocer las normativas, directrices o leyes dictadas desde Europa, el Estado o Euskadi referentes, directa o indirectamente, a la Ciberseguridad no es una tarea nimia para los responsables de la Ciberseguridad en las empresas industriales. Para facilitar el conocimiento de dichas normas y leyes, el Centro Vasco de Ciberseguridad (BCSC) pone a disposición de las empresas establecidas en Euskadi, de manera gratuita, el documento "Mapa Normativo de la Ciberseguridad Industrial", elaborado por el Centro de Ciberseguridad Industrial (CCI).

Directrices, normas y leyes, reunidas en un único documento

Jornadas de sensibilización en ciberseguridad

Mediante metodología learning-by-doing
Organizadas por Basque Cybersecurity Centre

El contenido de la jornada estará organizado en 5 módulos:

Introducción a la ciberseguridad
Comprensión de la ciberseguridad y ámbitos en los que es aplicable.

Ciberseguridad en la oficina
Aplicación de buenas prácticas en el trabajo diario de oficina.

Ciberseguridad en la planta
¿Cómo afecta la ciberseguridad a una infraestructura OT?

Ciberseguridad en los departamentos de informática e ingeniería
Aplicación de buenas prácticas en el diseño y gestión, para una infraestructura segura.

Gestión de la seguridad
Obtener una visión global de la ciberseguridad y los riesgos a los que se exponen las empresas.

Respuesta a incidentes

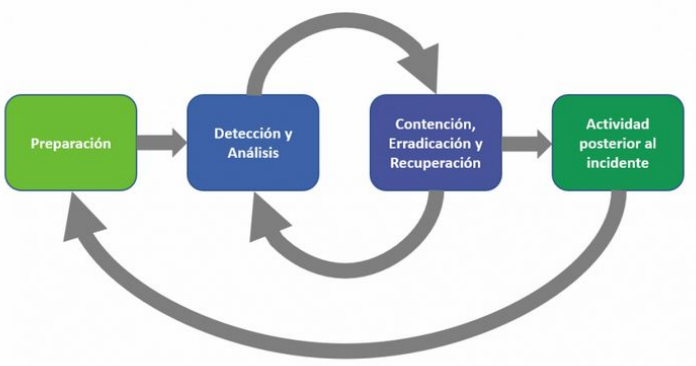


Diagrama basado en el ciclo de respuesta a incidentes propuesto por el NIST

En el BCSC respetamos las pautas de gestión de incidentes propuestas por el National Institute of Standards and Technology (NIST) y el código de buenas prácticas de Trusted Introducer.

Tomando como referencia el documento Computer Security Incident Handling Guide del NIST, un incidente de ciberseguridad es la trasgresión o amenaza de ello, de las políticas de seguridad, políticas de uso o prácticas de seguridad habituales. Algunos ejemplos de incidentes son:

- Un atacante utiliza una botnet para llevar a cabo un ataque de denegación de servicio.
- Usuarios son engañados para abrir un fichero recibido vía email que corresponde a malware, de modo que infecta su equipo y potencialmente los de su red.
- Un atacante obtiene información sensible y amenaza con que los detalles serán publicados si la organización no paga cierta cantidad de dinero.
- Un usuario facilita o expone información sensible a otros a través de servicios de intercambio P2P.

Así mismo, un incidente de ciberseguridad puede ser definido como cualquier evento que amenace la seguridad, confidencialidad, integridad y disponibilidad de un Sistema.

Para hacer frente a este tipo de situaciones, ofrecemos los siguientes servicios:

- **Análisis de incidentes (Incident analysis):** tras la recepción de un incidente realizamos una valoración de la información reportada y de las evidencias relacionadas. Este análisis nos permite categorizar y priorizar el incidente (triage), así como determinar si se trata de un incidente aislado o puede estar relacionado con algún otro que nos hayan reportado. De este modo, podemos afrontarlo de la manera más eficiente.
- **Apoyo a la respuesta a incidentes (Incident response support):** proporcionamos apoyo y consejo a los usuarios que se ven afectados por un incidente de ciberseguridad. Les guiamos sobre las pautas a seguir y, en el caso de que sea necesario, les redirigimos al punto de contacto más adecuado según corresponda.

Ambos servicios se ofrecen mediante una línea de asesoramiento. Se puede notificar un incidente o hacer una consulta técnica o de los servicios que ofrecemos a través de las siguientes vías:

Número de teléfono gratuito:

900 104 891

Correo electrónico:

incidencias @ bcsc.eus
arazoak @ bcsc.eus

Indicando:

- Persona o empresa.
- Nombre y Apellidos o Nombre de la empresa.
- Teléfono.
- Población.
- Provincia.
- Dirección de correo electrónico.
- Asunto.
- Descripción detallada de la consulta. (Rogamos sea lo más detallada y clara posible con el fin de poder ofrecer una asistencia adecuada)

Suscríbete al boletín informativo

Email

Email

He leído y acepto la Política de privacidad

No soy un robot
reCAPTCHA

Privacidad - Condiciones

Basque Cybersecurity Centre como responsable de esta web le informa que sus datos serán tratados para el envío de los boletines a los que se suscribe. Puede ejercer sus derechos a través del correo lopd@bcsc.eus. Para más información sobre el tratamiento de sus datos y los derechos que le asisten pulse en "política de privacidad".

Suscríbete

Publicaciones

Guías, Estudios e Informes

Publicaciones correspondientes al Observatorio Tecnológico sobre tendencias, tecnologías, amenazas, etc. en ciberseguridad.

Boletines de Avisos Técnicos

Recopilación mensual de avisos técnicos publicados.

Boletines de Avisos SCI

Recopilación mensual de los avisos SCI publicados.

Infografías

Consejos básicos para mejorar el nivel de ciberseguridad.

BCSC www.basquecybersecurity.eus

- The European Cyber Security Organisation (ECSO) https://www.ecs-org.eu/
- INCIBE https://www.incibe.es/en
- INCIBE-CERT https://www.incibe-cert.es/en
- SPRI www.spri.eus/euskadinnova
- FIRST https://www.first.org/members/teams/bcsc
- TF-CSIRT https://www.trusted-introducer.org/directory/teams/bcsc.html
- CSIRT https://www.csirt.es/index.php/es/miembros/bcsc
- GLOBALEPIC https://globalepic.org/HomePage

About ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries...

Learn More

LATEST PRESS RELEASES

ECSO convened its first High Level Roundtable on Europe's Cyber Future
5 February 2019, Brussels, Belgium

In his welcoming remarks to 150 participants, Philippe Vannier, Chairman of ECSO, emp...

ECSO and EUNITY Project organised a workshop to foster the EU-Japan cooperation in the field of cyber security and privacy
25 January 2019, Brussels, Belgium

The discussions between the leading cyber security industries and gover...

NEWSLETTER SUBSCRIPTION

Español | Contact | Calendar | Press Room | Site map

INCIBE PORTALS

incibe_
SPANISH NATIONAL CYBERSECURITY INSTITUTE

Protect your business | Events | Other activities | What is INCIBE

INCIBE-CERT

INCIBE-CERT is the CERT for citizens and companies in Spain.
Visit our website and follow the official twitter account.

www.incibe-cert.es | @INCIBE-CERT

protege tu empresa

NO CONVIERTAS LA TECNOLOGÍA EN UN MAL SUEÑO

Conoce INCIBE

¿Qué es INCIBE?

INCIBE es Ciberseguridad. Conoce más acerca del organismo en nuestra sección *¿Qué es INCIBE?*.

Nuestro CERT

INCIBE-CERT es el Centro de Respuesta a Incidentes de Seguridad de INCIBE. Ofrece servicios para profesionales TI.

Empresas

Protege tu empresa ofrece servicios de ciberseguridad para pymes y empresas.

Cybersecurity guide for wireless communications in industrial environments

This cybersecurity guide describes the main wireless technologies used in an industrial environment, and highlights the security features that are implemented by them as well as the recommended good practices to minimise the risks of a cyberincident

More information

Incident reporting

Advisories

- Múltiples vulnerabilidades en Moodle
  03/19/2019
- Validación insuficiente en backend HTTP remoto de PowerDNS
  03/19/2019
- Múltiples vulnerabilidades en VMware
  03/18/2019

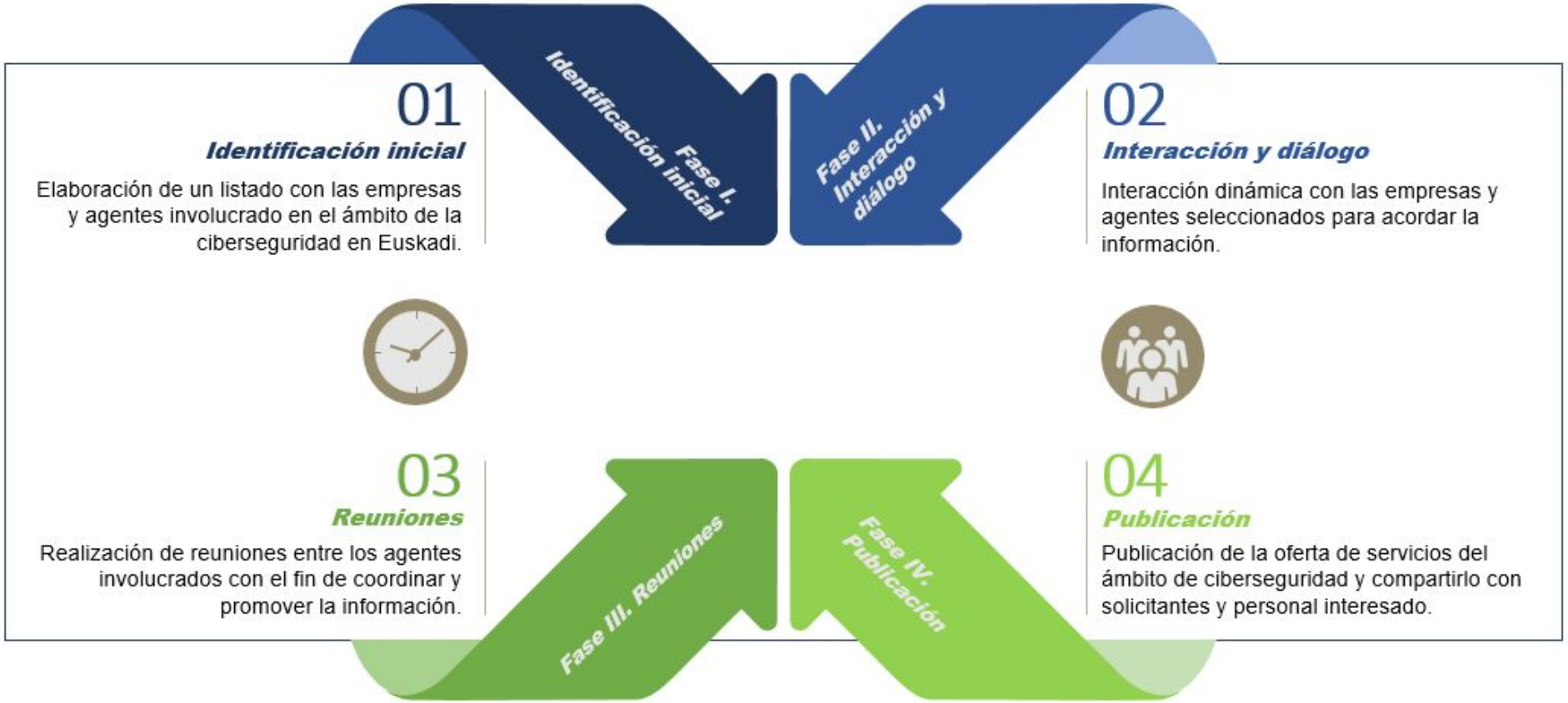
Show more

ICS advisories

- Múltiples vulnerabilidades en Field Xpert de ENDRESS+HAUSER
  03/20/2019
- Múltiples vulnerabilidades en móviles ecom de PEPPERL+FUCHS
  03/15/2019
- Vulnerabilidad de elemento de ruta de búsqueda no controlado en Sentinel UltraPro de Gemalto
  03/15/2019

Show more

BCSC, Metodología aplicada:



01

Identificación inicial

Elaboración de un listado con las empresas y agentes involucrado en el ámbito de la ciberseguridad en Euskadi.

02

Interacción y diálogo

Interacción dinámica con las empresas y agentes seleccionados para acordar la información.

03

Reuniones

Realización de reuniones entre los agentes involucrados con el fin de coordinar y promover la información.

04

Publicación

Publicación de la oferta de servicios del ámbito de ciberseguridad y compartirlo con solicitantes y personal interesado.

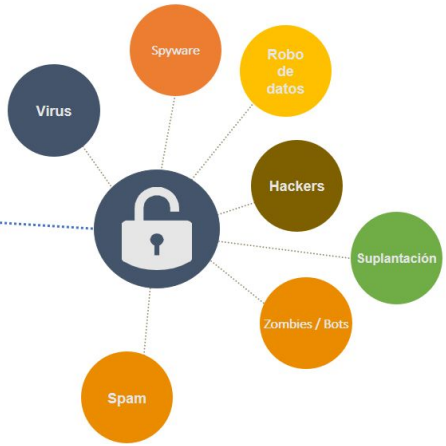
BCSC www.basquecybersecurity.eus

Basque Industry 4.0.

- https://www.spri.eus/es/basque-industry-comunicacion/indussec-2018-ciberseguridad-la-industria/
- https://www.spri.eus/es/basque-industry/

BCSC www.basquecybersecurity.eus

- Amenazas:
  - Virus, spyware, robo de datos, hackers, suplantación, botnets y spam.
- Contramedidas:
  - Antimalware, firewall, antispyware y antispam.
- Consecuencias:
  - Pérdidas económicas
  - Robo de información
  - Destrucción de información
  - Pérdida de prestigio o reputación
  - Suplantación de identidad



Los medios de entrada preferidos de estas amenazas son la navegación web, el correo electrónico y las descargas.

https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

BCSC www.basquecybersecurity.eus

Cibercrimen: https://estadisticasdecriminalidad.ses.mir.es/

- Fraude informático:
  - Estafas bancarias, estafas con tarjetas de crédito, débito y cheques de viaje.
- Delito sexual
  - Pornografía de menores
- Acceso e interceptación ilícita
  - Descubrimiento y/o revelación de secretos

BCSC www.basquecybersecurity.eus

Emprendimiento:

- UP! Euskadi https://upeuskadi.spri.eus/es/aceleradoras-de-startups/
  - https://upeuskadi.spri.eus/es/
- BIND 4.0 https://bind40.com/startups/
  - https://bind40.com/
    - https://www.spri.eus/es/upeuskadi-comunicacion/mas-de-medio-millar-de-startup-de-todo-el-mundo-optan-a-poder-participar-en-la-3a-edicion-del-programa-vasco-de-aceleracion-bind-4-0/
    - https://gem-paisvasco.es/wp-content/uploads/2018/06/GEM_CAPV_2017-18.pdf

Tendencias desde el punto de vista sectorial:

- Sector Industrial y Medio Ambiente
  - Ciberseguridad en Sistemas de Control Industrial
  - Sistemas ciberresilientes para Infraestructuras Críticas
  - Protección de las redes industriales y energéticas
- Sector Movilidad
  - Protección vehículos inteligentes
  - Protección de sistemas de comunicación vía satélite
- Sector Servicios
  - Big Data Analytics
  - Gestión de Información
  - Seguridad en servicios Fintech
- Sector Ciudadanía
  - Protección de dispositivos médicos conectados
  - Cifrado para la investigación
  - Ubicación y transferencia segura de datos médicos
  - Educación y tecnología
- Sector Administración Públicas
  - Distribución de ciberinteligencia
  - Simulación de incidentes y ciberejercicios
- Sector TIC
  - Servicios de seguridad en la nube
  - Cifrado en tiempo real
  - Cifrado homomórfico
  - Hacking ético
  - Certificado de confianza digital

Tendencias desde el punto de vista de evolución del paradigma tecnológico:

- Cloud
- Data Analytics para anticiparse en la detección de amenazas y ataques
- Algoritmos de inteligencia artificial; Sensores (detección del patrones de comportamiento anómalo) y *enforcement* (aplicación de políticas de comportamiento aceptado).
- Sistemas avanzados de autenticación
- Open Source
- RGPD

Prioridades tácticas desde el punto de vista organizativo:

- Determinar el grado de integración eficaz de la seguridad en la organización en su conjunto.
- Aprovechar las competencias profesionales ya existentes.
- La tercera prioridad se basará en ir más allá de las estrategias habituales de reclutamiento en las organizaciones y que las nuevas incorporaciones entiendan las competencias básicas en materia de ciberseguridad.

Actores del mercado:

- Fabricantes
  - Empresas que diseñan, producen, desarrollan y comercializan productos hardware o software. La comercialización de estos productos suele apoyarse en mayoristas y distribuidores. Otros, están operando directamente a través de plataformas web.
- Mayoristas / distribuidores
  - Los mayoristas son empresas que disponen de una selección de productos de fabricantes. Ofrecen las soluciones que mejor se adapten a cada usuario.
  - Los distribuidores son los que comercializan directamente a otras empresas o usuarios finales.
- Integradores / Consultores
  - Los integradores ofrecen una serie de servicios que van desde la instalación hasta la inicialización y posterior servicio.
  - Los consultores son empresas dedicadas al apoyo, consejo y asesoramiento empresarial.
- Otros: Universidades, Centro de Formación Profesional, Centros Tecnológicos, Asociaciones y Clústeres, Administración Pública y otros agentes proactivos.

Taxonomía de ciberseguridad:

- Anti-fraude
- Anti-malware
- Auditoría técnica
- Certificación normativa
- Contingencia y continuidad
- Control de acceso y autenticación
- Cumplimiento legal
- Inteligencia de seguridad
- Prevención de fuga de información
- Protección de las comunicaciones
- Seguridad en dispositivos móviles
- Formación y concienciación
- Gestión de incidentes
- Implantación de soluciones
- Seguridad en la nube
- Soporte y mantenimiento

https://www.incibe.es/sites/default/files/contenidos/guias/doc/taxonomia_ciberseguridad.pdf

Conclusiones www.basquecybersecurity.eus

- El escenario de los riesgos cibernéticos se encuentra actualmente en un proceso de evolución constante. Existe un incremento en cantidad y variedad de las amenazas contra la información y las infraestructuras TIC que afecta a todos los usuarios, incluyendo la ciudadanía, el sector privado y las organizaciones públicas.
- Se requieren cambios determinantes que, atendiendo la diversidad de autores y partes interesadas en los ciberataques (organizaciones privadas y públicas, grupos terroristas, crimen organizado o hacktivistas), deben ser tenidos en cuenta a la hora de desarrollar una estrategia de ciberseguridad adecuada, consistente en un concepto de seguridad integral y una cultura de prevención. No deben obviarse en este punto las recientes trasposiciones de legislación europea (por ejemplo, Directiva NIS y GDPR).

Conclusiones www.basquecybersecurity.eus

- La densidad de startups tecnológicas y de empresas dedicadas a la aplicación de ciberseguridad en Euskadi es muy alta, no solamente si se compara con la globalidad del Estado sino incluso a nivel europeo.
- El carácter eminentemente innovador de Euskadi potenciado por infraestructuras como el Basque Digital Innovation Hub, su tradición en el emprendimiento, su capacidad investigadora y el perfecto banco de pilotaje que supone la fabricación avanzada local crean un nicho para ser referentes, un entorno ideal para la creación de tecnología de ciberseguridad cuyo destino sea la industria estratégica de la Región.

SPRI www.spri.eus

- Basque industry 4.0 https://www.spri.eus/es/basque-industry/
- UP!Euskadi https://upeuskadi.spri.eus/es/
- Basque Trade https://basquetrade.spri.eus/es/
- Investment https://www.spri.eus/invest-in-basque-country/
- https://www.spri.eus/es/basque-industry/basque-digital-innovation-hub/
- Spri Lur http://www.sprilur.eus/es/
- Capital Riesgo https://www.spri.eus/es/capital-riesgo/

Referencias, Bibliografía

- https://www.spri.eus/es/basque-industry-comunicacion/indussec-2018-ciberseguridad-la-industria/
- https://www.w3c.es/Eventos/2016/DiaW3C/Presentaciones/minetur.pdf
- https://www.pwc.es/es/publicaciones/gestion-empresarial/assets/temas-candentes-ciberseguridad.pdf
- https://www.files.ethz.ch/isn/118153/ARI102-2010_Fojon_Sanz_ciberseguridad_Espana.pdf
- https://www.gartner.com/en/information-technology/insights/cybersecurity

El Centro
El Equipo
Sala de Prensa
Decálogo de ética

El Centro de Ciberseguridad Industrial

Antecedentes Misión Visión Objetivos CCI Catalizador

Es sabido que los servicios esenciales y nuestro tejido industrial dependen para el normal desarrollo de su actividad de las Tecnologías de la Información y las Comunicaciones (TIC). Pero no es tan conocido que todos esos servicios esenciales dependen a su vez en mayor medida de los Sistemas Industriales. Son estos últimos los que controlan las torres de refrigeración, los generadores eléctricos que proporcionan la energía necesaria o los sistemas de extinción de incendios, entre otros muchos aspectos.

Los sistemas industriales son la base de las principales Infraestructuras Críticas y Servicios Esenciales en el mundo y por tanto, su seguridad recae finalmente en ellos. Esto ha hecho que se hayan convertido en objetivos de actos de ciber-terrorismo e incluso de ciber-guerra, suponiendo el caldo de cultivo para la aparición de auténticas "ciber-armas" cuyo objetivo es explotar sus vulnerabilidades existentes.

Nuestra sociedad y economía es por tanto, vulnerable y el primer paso debe ser que todas las organizaciones y actores clave tomen conciencia de ello. Tras analizar el mercado de la Ciberseguridad Industrial, sus actores y necesidades, así como los casos de éxito y fracaso de otros países de Europa y Estados Unidos, en Marzo de 2013 hemos puesto en marcha en España el Centro de Ciberseguridad Industrial (CCI).

Se trata del primer centro de estas características que nace desde la industria y sin subvenciones, independiente y sin ánimo de lucro. Nuestra misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial principalmente en España y Latinoamérica, entendiendo por Ciberseguridad Industrial "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, utilizando las perspectivas de personas, procesos y tecnologías".

Clústeres, 9 Industriales

- Energía http://www.clusterenergia.com/
- Fundición www.feaf.es/
- Ferroviaria https://www.mafex.es/
- Movilidad y logística http://www.mlcluster.com/
- Papel http://www.clusterpapel.com/
- Siderurgia https://www.siderex.es/
- Forja https://www.forjas.org/
- Puerto http://www.uniportbilbao.es/es
- Construcción http://www.eraikune.com/

Clústeres, 2 no industriales

- http://www.gaia.es/
- https://www.eikencluster.com/

Conclusiones www.basquecybersecurity.eus

- Claramente la gestión del riesgo en los sistemas de automatización y control está siendo asumida por el área de tecnologías de la información, enfocando sus acciones desde un punto de vista más cibernético que físico o asociado a procesos. Esto es debido a la mayor madurez de estas áreas en materia de ciberseguridad, frente a las áreas técnicas de la operativa industrial. Es decir, en la mayoría de los casos se aborda el problema con una visión parcial, muy informática, por lo que sería conveniente darle una visión más global de gestión de riesgos del negocio.

Conclusiones www.basquecybersecurity.eus

- Es preciso elevar el nivel de concienciación frente a la necesidad y las implicaciones de la Ciberseguridad Industrial a todos los niveles de la organización. De los datos recabados se puede inferir que hay reticencia a la hora de reconocer y notificar los impactos derivados de ciber-incidentes ocurridos en las plantas industriales, lo cual es imprescindible para que la dirección de la organización y las áreas de negocio sean conscientes de la magnitud del problema pudiendo así habilitar las herramientas necesarias para mejorar (por ejemplo, presupuesto).

Conclusiones www.basquecybersecurity.eus

- Se identifican dos factores principales que están acelerando la digitalización de la industria en Euskadi y como consecuencia de ello la necesidad de gestionar el riesgo tecnológico especialmente asociado con la ciberseguridad.
  - En primer lugar, el escenario de regulación impulsado desde Europa, como la protección de infraestructuras críticas o más recientemente la directiva NIS, en el que las empresas vascas pueden verse afectadas por su actividad, determina el modo en que afrontan los retos planteados por los riesgos que afectan a sus sistemas de automatización y control industrial.
  - En segundo lugar, la propia globalización, que provoca una mayor competencia del mercado, especialmente relevante en este estudio dado el perfil de las organizaciones que han decidido responder voluntariamente la encuesta.

Conclusiones www.basquecybersecurity.eus

- El mercado, las empresas y los proveedores de servicios en el ámbito industrial precisan de profesionales especializados en la ciberprotección de los entornos de producción industrial. Los esfuerzos en capacitación en ciberseguridad, en el conjunto de las empresas vascas estudiadas, siguen dedicándose, principalmente, a los departamentos de TI.
- Sería deseable ir aumentando el esfuerzo en capacitar y sensibilizar al resto de áreas de la empresa, especialmente las que operan y mantienen los sistemas de control.

Conclusiones www.basquecybersecurity.eus

- Las tecnologías de ciberseguridad más utilizadas en las redes de control de procesos siguen siendo las de uso habitual en las redes corporativas; aun cuando tales soluciones no sean siempre las óptimas para el entorno industrial.
- Por ello, se recomienda la adopción de medidas más específicas para dicho entorno, tales como la elaboración de listas blancas de aplicaciones (whitelisting, en inglés), los cortafuegos industriales, las pasarelas unidireccionales o los sistemas de prevención y detección de intrusiones (IDS) con características específicas para reconocer protocolos industriales, entre otras.

Conclusiones www.basquecybersecurity.eus

- Una de las razones principales para incorporar la ciberseguridad ha sido la mejora continua.
- Es este un dato muy significativo porque de ello se desprende que, al menos de manera implícita, se percibe la aplicación de ciberseguridad como un camino hacia las mejoras en la calidad, eficiencia y seguridad de los procesos.

Empresas, listado de fabricantes:

- https://www.aliasrobotics.com/
- https://bullhost.es/
- https://www.cc3m.com/
- https://www.countercraft.eu/
- https://www.custarsl.com/
- https://enigmedia.es/
- https://hdivsecurity.com/
- http://www.ibercom.com/
- https://ironchip.net/
- https://keynetic.tech/
- https://www.pandasecurity.com/
- https://redborder.com/
- https://redborder.com/
- https://www.relyum.com/
- http://sealpath.com/
- http://siesoluciones.com/
- https://www.zuratrust.com/
- http://www.aner.com/
- https://www.seguridad-profesional.com/

Empresas, listado de mayoristas/distribuidores:

- http://www.aner.com/
- https://www.seguridad-profesional.com/
- https://www.eitek.net/
- https://www.exclusive-networks.com/
- http://www.ingecom.net/

Empresas, listado de integradores/consultores:

- https://www.accenture.com/
- https://www.adw.es/
- http://www.agpsoftware.com/
- https://akirutek.es/
- https://ambar.es/
- http://www.asitec.es/
- https://beclever.solutions/es/
- http://www.campus-cst.com/
- https://www.comymedia.com/
- http://consulpyme.com/
- http://cv2group.com/
- https://www2.deloitte.com/es/
- https://derten.com/
- https://www.deustosistemas.net/
- https://www.dimensiondata.com/
- https://www.encolaboracion.net/
- https://encriptia.com/
- https://www.innotecsystem.com/
- https://eupraxia.es/
- https://www.euskaltel.com/
- https://www.everis.com/spain/es
- https://gaptain.com/
- https://gfi.world/es-es/
- http://www.globalfactory.es/

Empresas, listado de integradores/consultores:

- https://www.globetesting.com/
- https://www.grupoi68.com/
- https://www.guzcor.com/
- https://hirusec.es/
- https://ibermatica.com/
- https://www.ibm.com/ibm/es/es/
- https://www.idom.com/es/
- https://www.iecisa.com/
- https://www.indracompany.com/
- http://infakt21.com/
- https://www.infoamara.com/
- https://www.its-security.es/
- https://jakincode.com/
- https://home.kpmg/es/es/
- http://www.lks.es/C/CO/MONDRAGON.aspx
- http://www.mangit.es/
- https://www.pantallasamigas.net/
- https://www.p3rs.eus/
- https://www.pkf-attest.es/
- https://www.pwc.es/
- https://www.prosegur.es/
- https://rklintegral.com/
- https://www.s21sec.com/en/

Empresas, listado de integradores/consultores:

- https://www.sarenet.es/
- https://gruposermicro.com/
- http://www.sernivel3.es/es/
- http://www.sqs.es/
- http://www.spcnet.es/
- https://tabiraberezi.com/
- http://www.talio.it/
- http://www.telbask.es/
- https://www.telefonica.com/
- http://www.telenorcomunicaciones.com/
- http://www.titaniumindustrialsecurity.com/
- https://www.viewnext.com/
- https://wsg127.com/

Empresas, listado de institución pública:

- AVPD - Agencia Vasca de Protección de Datos. DBEN – Datuak Babesteko Euskal Bulegoa www.avpd.eus
- Basque CyberSecurity Centre https://www.basquecybersecurity.eus/
- https://www.izenpe.eus/

Empresas, listado de universidades y centros de Formación Profesional:

- https://www.deusto.es/
- https://www.mondragon.edu/
- https://www.tecnun.es/
- https://www.ehu.eus/es/
- https://www.egibide.org/
- http://www.uni.hezkuntza.net/
- www.zubirimanteo.hezkuntza.net/
- http://www.maristak.com/es

Empresas, listado de Red Vasca de Ciencia, Tecnología e Innovación:

- Basque Centre for Applied Mathematics http://www.bcamath.org/es/
- IK4-Ikerlan S.Coop. https://www.ikerlan.es/
- Ceit-IK4 https://www.ceit.es/es/
- https://innovalia.org/
- https://www.tecnalia.com/es/
- http://www.vicomtech.org/

Empresas, listado de Asociación o Grupo de Interés:

- Centro de Ciberseguridad Industrial https://www.cci-es.org/
- Gaia Cluster http://www.gaia.es/
- http://pribatua.org/
- PuntuEus https://www.domeinuak.eus/eu/
- SAE Asociación Vasca de Profesionales de Seguridad Segurtasun Adituen Euskal Elkartea https://www.sae-avps.eus/
- https://stopviolenciadegenerodigital.com/
- VOST Euskadi https://www.vosteuskadi.org/