BASQUE CYBERSECURITY CENTRE

Contribuyendo a un ecosistema industrial más ciberseguro

GRUPO spri TALDEA

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN, JASANGARRITASUN ETA INGURUMEN SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO, SOSTENIBILIDAD Y MEDIO AMBIENTE

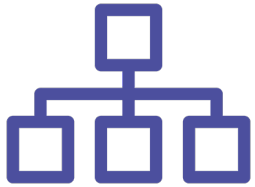
Centro Vasco de Ciberseguridad

Organización designada por el Gobierno Vasco para promover la ciberseguridad en Euskadi.

Análisis del Ecosistema Industrial

Estado de la Ciberseguridad Industrial en Euskadi

Organización de la Ciberseguridad Industrial

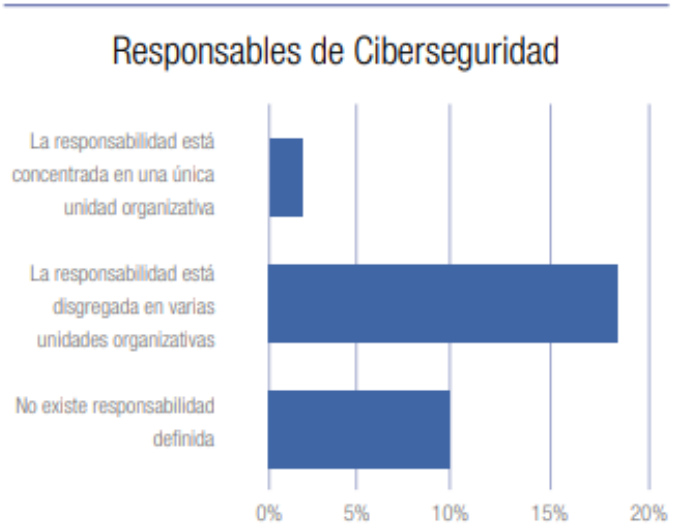


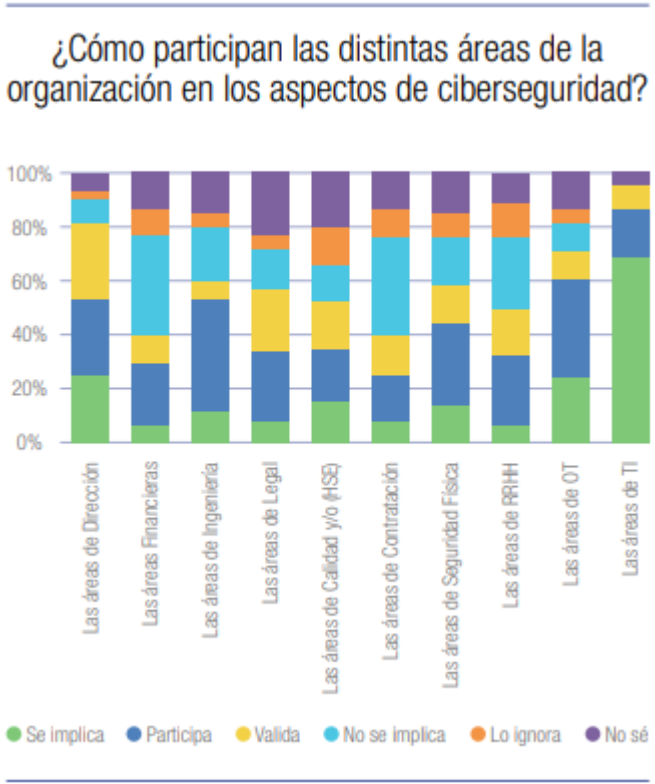
Gestión de la Ciberseguridad Industrial

Aspectos técnicos de la Ciberseguridad Industrial

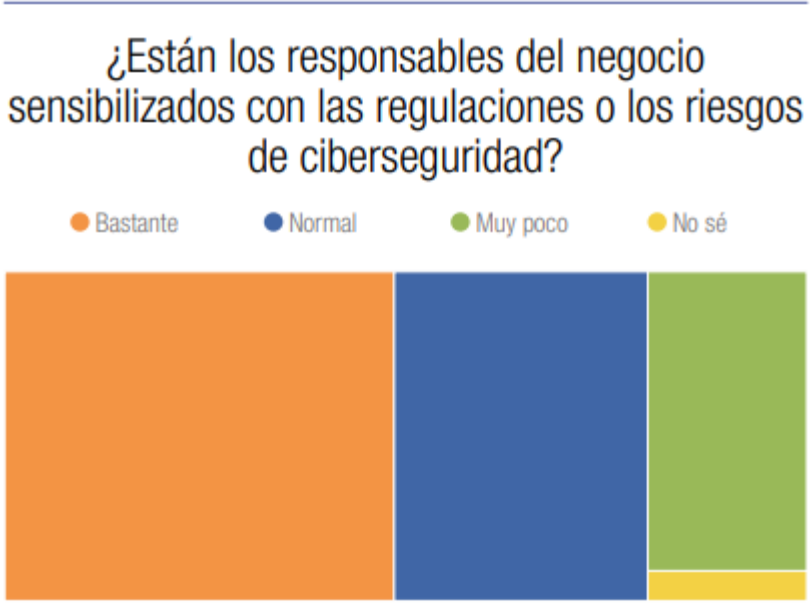
Mercado de la Ciberseguridad Industrial

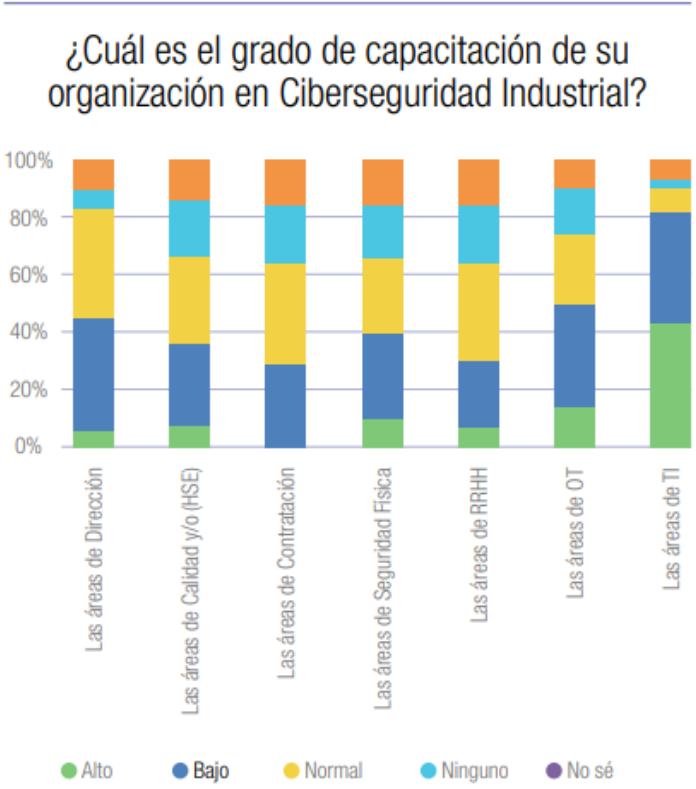
Estado de la Ciberseguridad Industrial en Euskadi





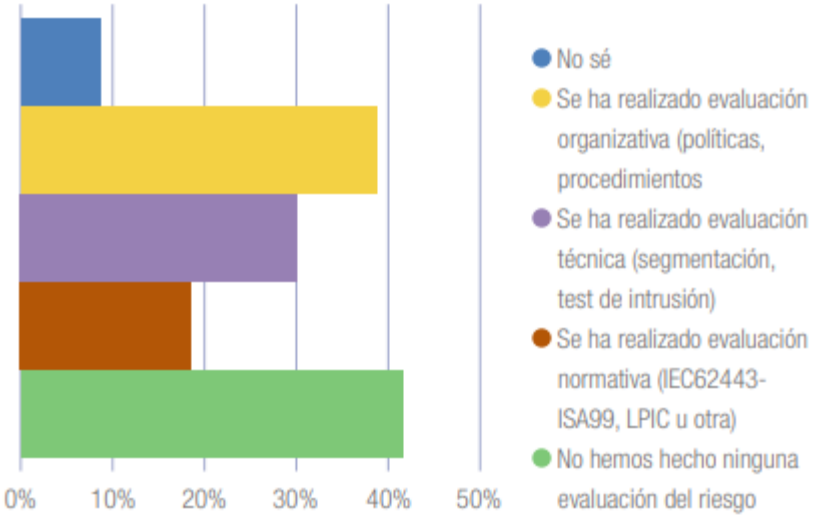
Estado de la Ciberseguridad Industrial en Euskadi



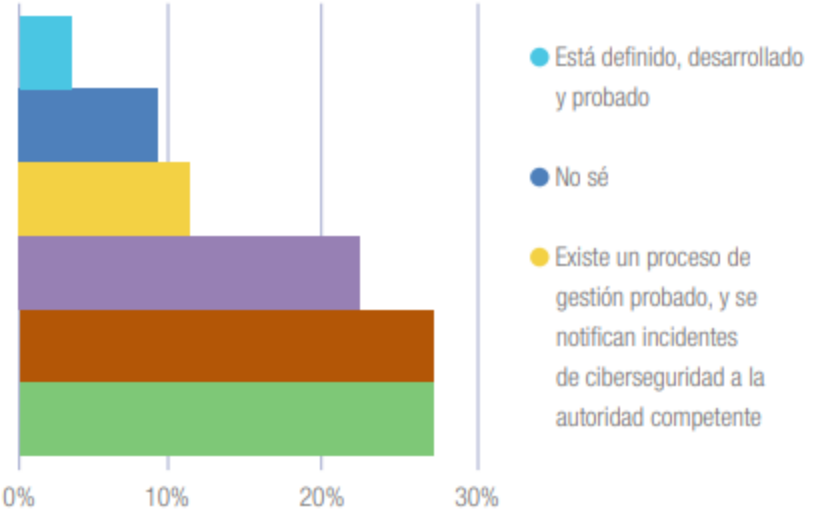


Estado de la Ciberseguridad Industrial en Euskadi

¿Se ha evaluado en su organización el nivel de riesgo de los sistemas de control y automatización?



¿Cómo es el proceso de gestión de incidentes de ciberseguridad en el ámbito industrial de su organización?

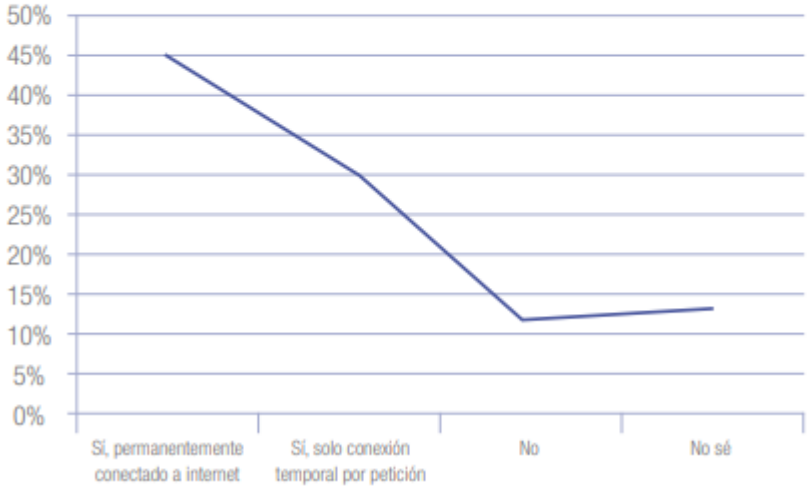


Estado de la Ciberseguridad Industrial en Euskadi

¿Están segmentadas y protegidas las redes en la organización?

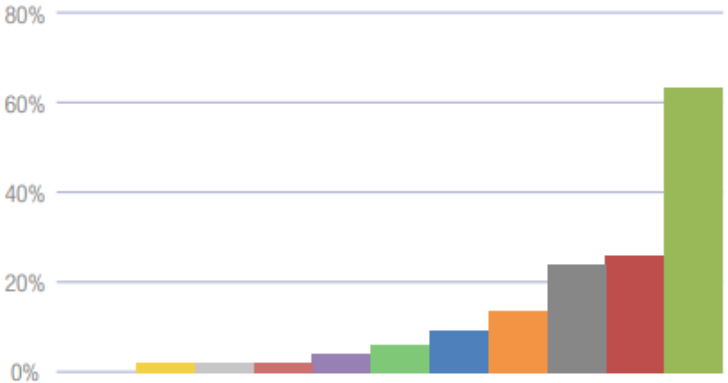
- La red corporativa e industrial están conectadas directamente
- No sé
- La red industrial está total y físicamente aislada de la red corporativa/ofimática
- La red industrial tiene distintos niveles de segmentación
- La red corporativa e industrial están segmentadas por un dispositivo de filtrado

¿Tiene su red industrial, o alguno de los dispositivos o sistemas albergados en ella, conexión a internet (independientemente de los mecanismos de protección aplicados)?



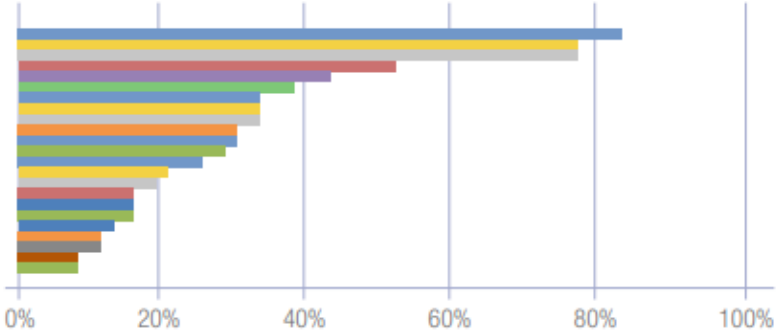
Estado de la Ciberseguridad Industrial en Euskadi

¿Están utilizando normas y estándares en el ámbito industrial?



- SGCI (Elaborado po el CCI)
- NIST 800-53
- NERC CIP
- ENSI (Esquema Nacional de Seguridad Industrial elaborado or el CERTSI)
- NIST 800-82
- Ley de protección de infraestructuras críticas
- Familia ISA 99 - IEC62443
- Otros
- No
- ISO 27001
- Leyes de protección de datos personales

¿Qué medidas tiene implantadas la organización en el ámbito industrial?

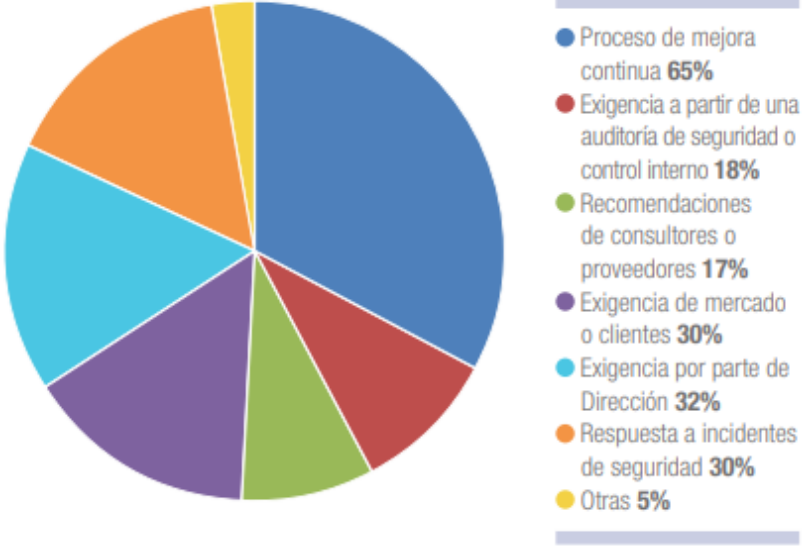


- Antivirus
- Backup/Copias de seguridad
- Firewalls convencionales
- Arquitectura de Red documentada
- Firewalls industriales
- Políticas y Procedimientos Documentados
- Gestión de Recuperación ante desastres

Estado de la Ciberseguridad Industrial en Euskadi

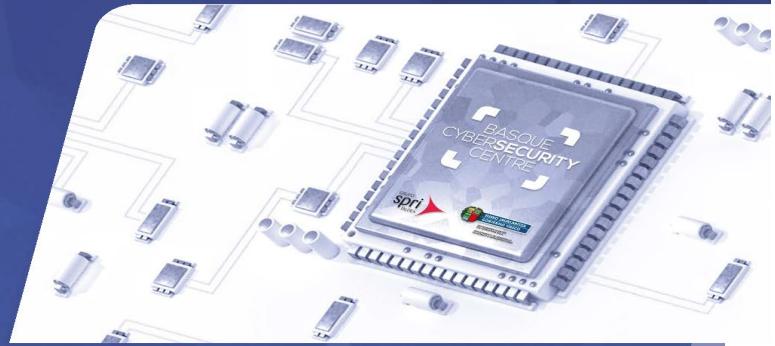
¿Tiene previsto iniciar nuevas actividades en el ámbito de la Ciberseguridad Industrial?

¿Cuales son las motivaciones para la ejecución de proyectos e implantación de soluciones de ciberseguridad en el ámbito industrial?



Catálogo de Ciberseguridad en Euskadi

BASQUE CYBERSECURITY CENTRE



LIBRO BLANCO DE LA CIBERSEGURIDAD EN EUSKADI

2ª Edición

Startups

- Alias Robotics
- Appsamblea
- Araua RegTech
- Barbara IoT
- CodeContract
- Countercraft
- Cras Vigilans Group
- Encriptia
- EnigMedia
- Ensotest
- EuroCybcar
- Gaptain (elasTIC Innovation Hub S.L)
- Globe Testing
- Hdiv
- Ironchip Telco
- Jakin Code
- Keynetic Technologies
- OpenCloud Factory
- Osane
- P3rseus
- Redborder
- Relyum
- RKL Integral
- Saint Intelligence
- Sealpath
- Smowltech
- Titanium Industrial Security
- Wimbitek
- Zuratrust

125
Empresas

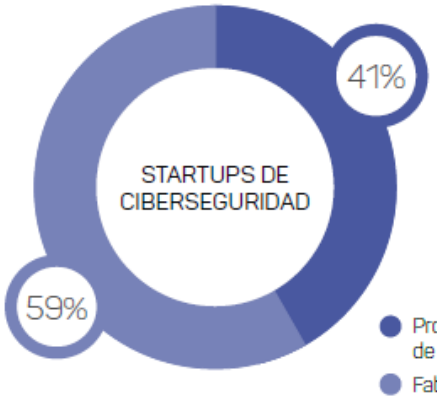
de las cuáles **29** son Startups

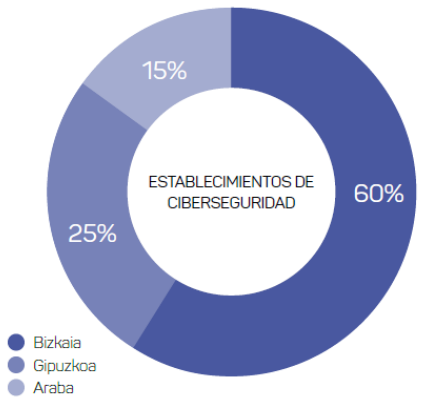
10
Asociaciones

9
Educación y universidades

5
Red vasca de ciencia tecnología e innovación

4
Instituciones públicas





EIBAR·ERMUA

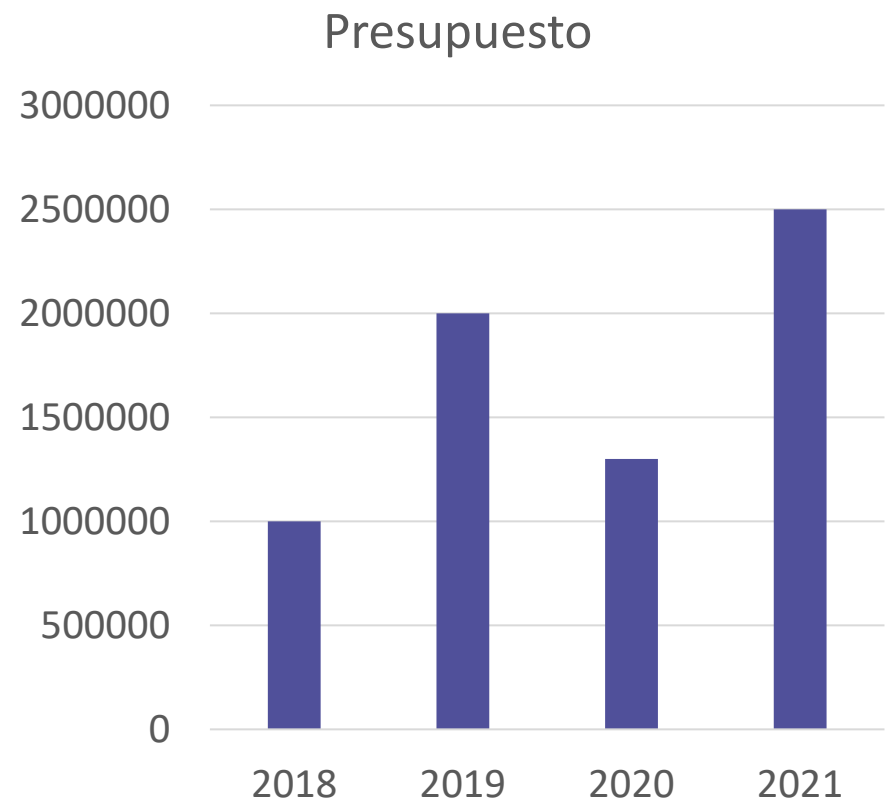
maristak
Durango Ikastetxea

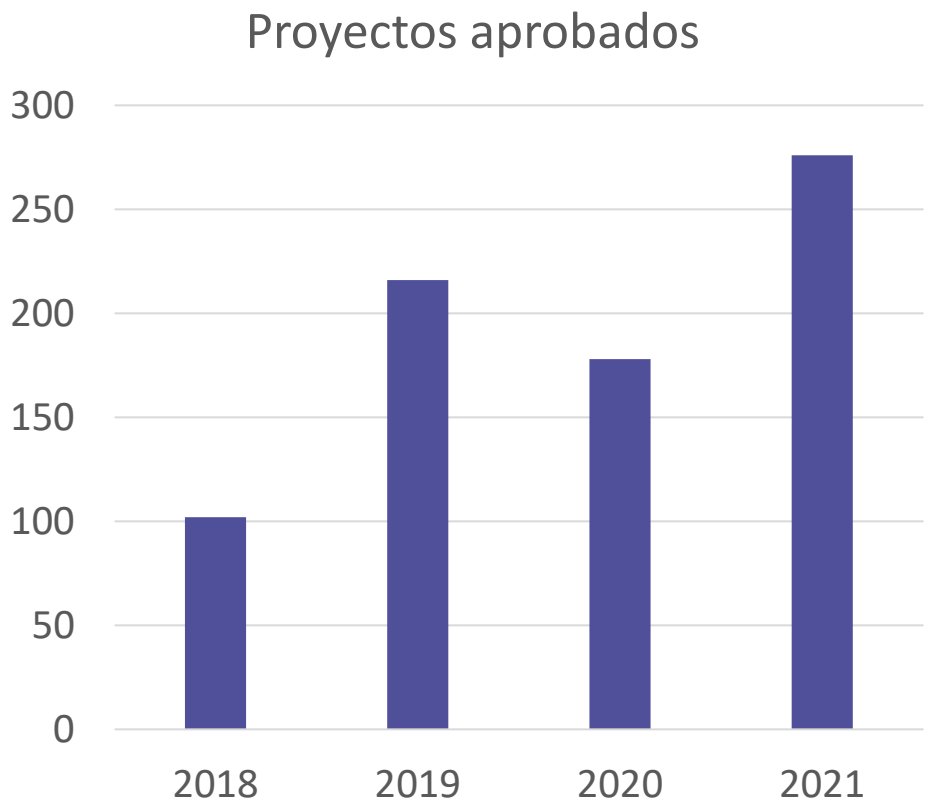
TXURDINAGA
CIFP LHII

ZUBIRI MANTEO

Programa de ayudas de Ciberseguridad Industrial

Programa de ayudas de Ciberseguridad Industrial





Programa de ayudas de Ciberseguridad Industrial

Tipología de proyecto	2018	2019	2020
Diseño y ejecución de arquitecturas seguras y en su caso materialización de la segmentación de redes industriales.	53	121	95
Diagnóstico de situación actual de la industria en materia de ciberseguridad industrial y elaboración de su plan de acción para la mejora de la Ciberseguridad.	17	20	20
Monitorización de dispositivos de seguridad perimetral y de otros dispositivos industriales (Switches, sondas, Appliances, firewalls industriales, PLCs, etc.).	7	20	13
Simulaciones de ataques por personas externas a la organización y auditorias sobre perfiles internos con diferentes niveles de accesos a datos de la compañía.	9	11	X
Securización de los accesos remotos OT a los equipos industriales de la planta productiva requeridos para el mantenimiento de equipo, control y operación de los mismos, tareas realizadas cada vez con más frecuencia de manera remota.	5	12	10

Programa de ayudas de Ciberseguridad Industrial

Tipología de proyecto	2018	2019	2020
Otros proyectos que incrementen de manera significativa el nivel de ciberseguridad de las empresas industriales y reduzcan el riesgo y la vulnerabilidad ante los diferentes tipos de ataques existentes.	4	11	8
Iniciativas para la concienciación de la plantilla de la empresa industrial en el ámbito de ciberseguridad.	4	8	3
Adaptación a estándares de ciberseguridad industrial. Gestión de las normas ISO27001, Esquema Nacional de Seguridad, PIC, mejora continua del proceso de ciberseguridad y similares.	1	7	11
Evaluación de la ciberseguridad del software industrial en las plantas productivas y mejora del mismo.	2	5	7

Jornadas de sensibilización

Sensibilización a empresas y agrupaciones empresariales

Ciberseguridad para desarrolladores

Ciberseguridad en la empresa para directivos

Ciberseguridad en la empresa

Las personas, el eslabón más débil en ciberseguridad

Ciberseguridad en la industria

Ciberseguridad & Pymes ¿Está mi empresa libre de riesgos?

Ciberseguridad en la teleformación

Ciberseguridad en el teletrabajo

Materiales de concienciación

¿QUÉ ES LA VERIFICACIÓN EN DOS PASOS?

Que alguien te robe la contraseña... es más fácil de lo que te imaginas.

BASQUE CYBERSECURITY CENTRE

Con cualquiera de estas acciones habituales, podrías correr el riesgo de que te roben la contraseña:

Acceder con mis credenciales a sitios web estando conectado a una red **WIFI pública**.

Descargar películas, series, software, etc. de **páginas no oficiales**.

Hacer clic en enlaces de mensajes de correo electrónico.

La verificación en dos pasos te ayudará a proteger tu información.

Al activar la verificación de dos pasos, además de tu contraseña, será necesario un paso adicional como:

Un código enviado a tu teléfono, otro dispositivo o una cuenta de correo electrónico.

Un **código enviado a una aplicación** de autentificación como Google Authenticator o Microsoft Authenticator.

Una **llave física**.

De esta manera, aunque te roben tu contraseña, tus cuentas permanecerán seguras.

Activa la verificación de dos pasos en las opciones de configuración, seguridad o privacidad de tus cuentas.

Mayor protección para tu cuenta

Por tu seguridad protege las cuentas de correo, redes sociales y otros servicios que utilizas en internet activando la verificación de dos pasos.

GRUPO spri

ELKO JAURLARITZA GOBIERNO VASCO

DATUEN EZABATZE SEGURUA

Nola ezabatu behar da informazioa gailuak garbi uzteko?

BASQUE CYBERSECURITY CENTRE

Ezabatze ohikoenak

Ezaugarriak

Paperontzia hustu

Artxiboak ezabatu eta **paperontzia hustu**.

Diskoa formateatu?

Ezeztatu Onartu

Formateatu ekipoa.

Desegin gailua.

KONTUZ!!!

Ezabatzeko modu hori **ez da segurua**. Informazioa **ez da guztiz ezabatzen** eta berreskuratu egin daiteke.

Datuak ezabatzeko forma seguruak

Ez bada gailua berriz erabili nahi

DESMAGNETIZAZIOA

Memoria-gailuak kanpo magnetiko handi baten mendean jartzea, gailuan gordetako datuak ezabatzen dituena. Memoria magnetikoko gailuen kasuan bakarrik balio du: disko gogorrak, disketeak, babeskopien zinta magnetikoak, eta abar.

DEUSEZTATZE FISIKOA

Gailuan informazioa gordetzen duen euskarria erabilezin bihurtzea, gerora datuen berreskuratzea saihesteko. Teknika mota desberdinak: desintegrazioa, haustutzea, fusioa, erraustea eta birrintzea. Gailu mota guztientzako balio du: disko gogorra, USB, CD, DVD, etab.

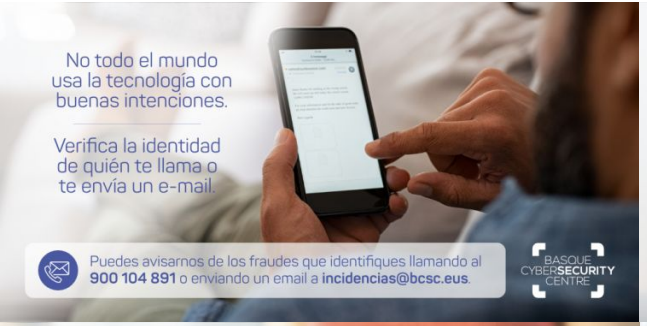
Gailua berriz erabili nahi bada

GAINIDAZTEA

Ezabatze osoa ematen dela bermatzeko, memoriaren azala bere osotasunean gainidatzi behar da. Gailuen edukietara sarbidea eginez eta bildutako balioak aldatuz egiten da; hori horrela, teknika hau ezin da kaltetuak dauden gailuetan erabili, eta ez ere berriz graba ezin diren gailuetan, CD eta DVDetan esaterako. Berriz graba daitezkeen gailuentzako balio du: disko gogorrak, USBak, etab.

GRUPO spri

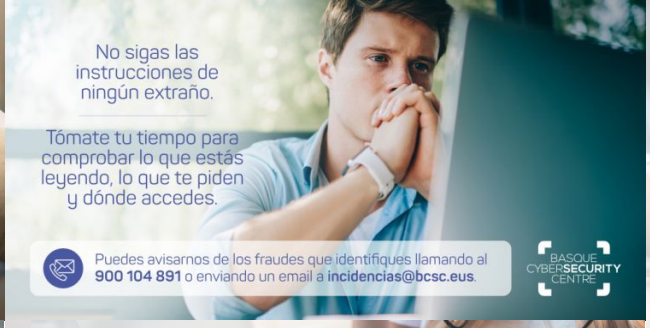
ELKO JAURLARITZA GOBIERNO VASCO


No todo el mundo usa la tecnología con buenas intenciones.
Verifica la identidad de quién te llama o te envía un e-mail.
Puedes avisarnos de los fraudes que identifiques llamando al 900 104 891 o enviando un email a incidencias@bcsc.eus.
BASQUE CYBERSECURITY CENTRE


No todos los enlaces que recibes son de fiar.
No accedas a enlaces sospechosos.
Puedes avisarnos de los fraudes que identifiques llamando al 900 104 891 o enviando un email a incidencias@bcsc.eus.
BASQUE CYBERSECURITY CENTRE

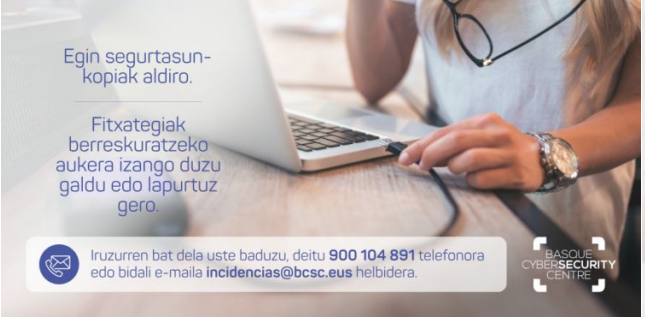

Ninguna fuente oficial te va a solicitar datos personales por e-mail.
Protege tu información personal y antes de compartirla valóralo bien.
Puedes avisarnos de los fraudes que identifiques llamando al 900 104 891 o enviando un email a incidencias@bcsc.eus.
BASQUE CYBERSECURITY CENTRE


No difundas información sin contrastar su veracidad.
No te creas todo lo que lees en Internet. Evita los bulos.
Puedes avisarnos de los fraudes que identifiques llamando al 900 104 891 o enviando un email a incidencias@bcsc.eus.
BASQUE CYBERSECURITY CENTRE


No sigas las instrucciones de ningún extraño.
Tómate tu tiempo para comprobar lo que estás leyendo, lo que te piden y dónde accedes.
Puedes avisarnos de los fraudes que identifiques llamando al 900 104 891 o enviando un email a incidencias@bcsc.eus.
BASQUE CYBERSECURITY CENTRE


Ez exekutatu igorle ezezagunek bidalitako eranskinak.
Ziberdelitugileek gailuak kutsa ditzalete.
Iruzurren bat dela uste baduzu, deitu 900 104 891 telefonora edo bidali e-maila incidencias@bcsc.eus helbidera.
BASQUE CYBERSECURITY CENTRE

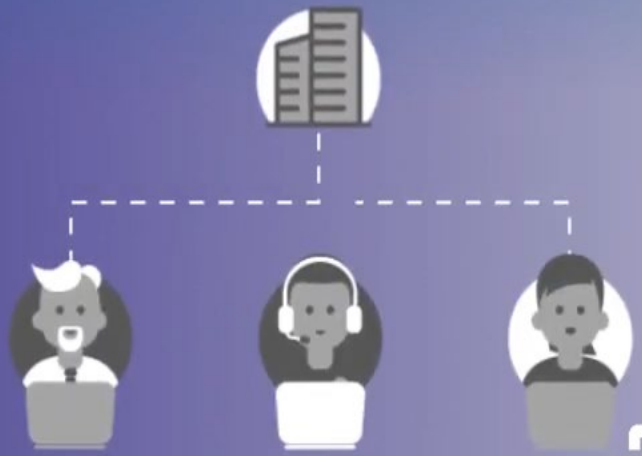

Kontuz ibili COVID19ari buruzko e-mail/ webgune ez ofizialekin.
Ongi begiratu, eta gune ofizialetara bersterik ez sartu.
Iruzurren bat dela uste baduzu, deitu 900 104 891 telefonora edo bidali e-maila incidencias@bcsc.eus helbidera.
BASQUE CYBERSECURITY CENTRE


Egin segurtasun-kopiak aldiro.
Fitxategiak berreskuratzeko aukera izango duzu galdu edo lapurtuz gero.
Iruzurren bat dela uste baduzu, deitu 900 104 891 telefonora edo bidali e-maila incidencias@bcsc.eus helbidera.
BASQUE CYBERSECURITY CENTRE


Gailuak eguneratuta izan.
Informazioa lapurtzea, nortasuna ordezkatzea eta halako arriskuak saihestu.
Iruzurren bat dela uste baduzu, deitu 900 104 891 telefonora edo bidali e-maila incidencias@bcsc.eus helbidera.
BASQUE CYBERSECURITY CENTRE

¿Sabías que...

los ataques a terceros en la cadena de producción han aumentado casi un 80% en el último año?



BASQUE CYBERSECURITY CENTRE

Ba al zenekien...

2020an enpresa askoren lanaren %80 inguru hodeira eraman izan dela dagoeneko?

BASQUE CYBERSECURITY CENTRE

#ciberGaldera

¿Qué son las "botnets"?

Zer dira “botnet”-ak?

A. Redes de trabajo ciberseguras.
Lan-sare ziberseguruak.

B. Redes creadas para la transferencia de documentos cifrados.
Zifratutako dokumentuak transferitzeko sortutako sareak.

C. Red de dispositivos infectados que se utilizan para llevar a cabo ciberataques.
Zibererasoak egiteko erabiltzen diren kutsatutako gailuen sarea.

4

BASQUE CYBERSECURITY CENTRE

#ciberGaldera

¿En que consisten las campañas de spear-phishing?

Zer dira spear-phishing kanpainak?

A. Una estafa de correo electrónico dirigida.
Zuzendutako posta elektroniko bidezko iruzurra.

B. Una estafa mundial a grandes corporaciones.
Mundu osoko korporazio handiei egindako iruzurra.

C. Una campaña de concienciación en ciberseguridad.
Zibersegurtasunaren alorreko kontzientziazio-kanpaina.

6

BASQUE CYBERSECURITY CENTRE

5 PASOS A SEGUIR PARA PROTEGER TUS DISPOSITIVOS

5 PASOS A SEGUIR PARA PROTEGER TUS DISPOSITIVOS

5 PASOS A SEGUIR PARA PROTEGER TUS DISPOSITIVOS

Utiliza contraseñas en todos tus dispositivos.

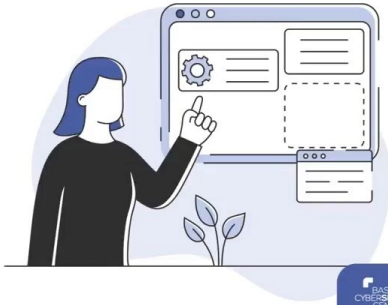
Instala solo apps confiables y que estén autorizadas por la empresa para minimizar el riesgo de malware.

5 PASOS A SEGUIR PARA PROTEGER TUS DISPOSITIVOS

5 PASOS A SEGUIR PARA PROTEGER TUS DISPOSITIVOS

5 PASOS A SEGUIR PARA PROTEGER TUS DISPOSITIVOS

Mantén actualizado el sistema operativo y las aplicaciones.



Instala un antivirus robusto y mantenlo actualizado.

Crea copias de seguridad con regularidad.

Monitorización

Basque Cybersecurity Centre @basquecscentre · 28 abr.

📢¡AVISO! Detectada una campaña de correos electrónicos que suplanta a la Agencia Tributaria. Los e-mails, cuyo asunto es "Medidas Tributarias COVID-19", incluyen un enlace que al pinchar descarga el troyano bancario #Cryxos.
👉bit.ly/2yT75gQ

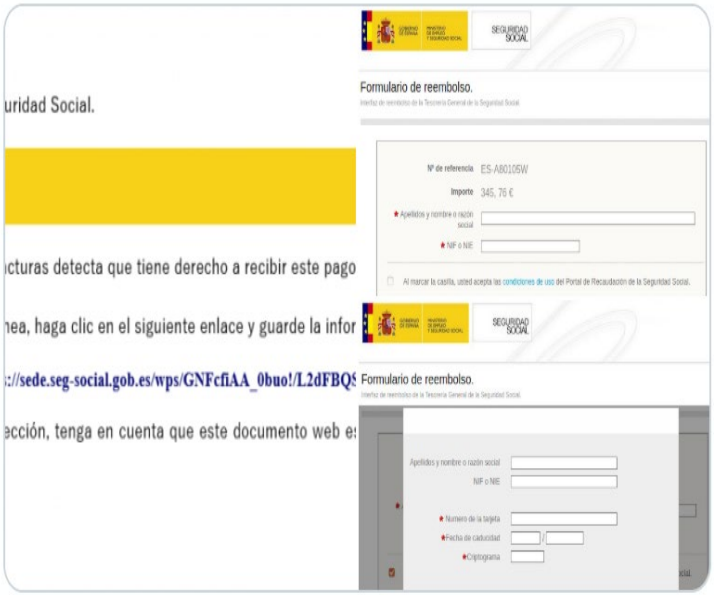
#CiberCOVID19 #StopMalware

Basque Cybersecurity Centre @basquecscentre · 30 abr.

📢¡Aviso! Se ha detectado una campaña de correos electrónicos 📧 que suplantan a la Seguridad Social, con el fin de engañar a los usuarios para que faciliten información personal y bancaria 💰 .

👉 bit.ly/3d3soeB

#StopMalware #MalwareSeguridadSocial #Ciberseguridad




Kr00k


Ghostcat


Starbleed


Thunderspy

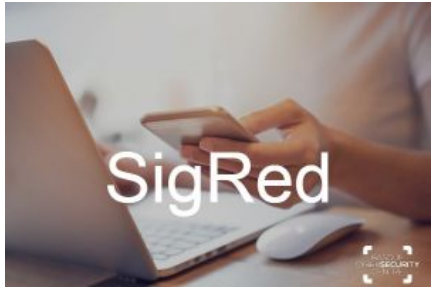

Strandhogg
2.0


SMBleed

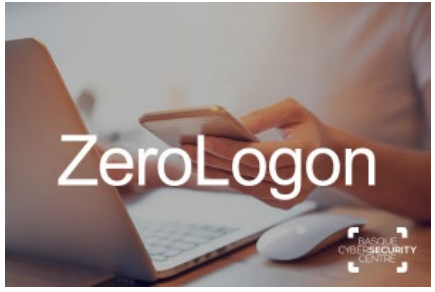

Ripple20


CallStranger


RECON


SigRed


WastedLocker


ZeroLogon

Septiembre 2021

Ciber Eguraldia
BCSC

Noticias generales

Incidentes de ciberseguridad

Estafas y fraudes

Malware y vulnerabilidades

Fugas de información

Ciberseguridad industrial

Estafas y fraudes

Nuevos casos de fraudes detectados a través de WhatsApp

Se han detectado dos tipos de fraudes a través de WhatsApp que podrían estar relacionados. En el primero la víctima es extorsionada y difamada a través de sus contactos de WhatsApp tras solicitar un préstamo por medio de una aplicación. En el segundo caso, los ciberdelincuentes suplantan la identidad de la víctima y solicitan a sus contactos de WhatsApp una cuantía de dinero.

Microsoft explica cómo son los nuevos ataques de phishing que utilizan código Morse

Microsoft ha alertado la existencia de nuevas técnicas empleadas en unos ataques de phishing. Según la compañía, los ciberdelincuentes consiguen adentrarse a través de formas poco conocidas, como guiones y puntos en código Morse, y cambian sus técnicas de ataque cada 37 días.

Desde paquetes perdidos hasta WhatsApp: así están aprovechando el spam para robarte el dinero

Un reciente informa de la empresa de ciberseguridad Kaspersky apunta que España es el país en el que más ataques de este tipo ha detectado la firma durante el segundo trimestre de 2021. Además, comparte algunas nuevas técnicas que están empleando lo cibercriminales.

"Su cuenta quedará bloqueada": el nuevo fraude bancario vía SMS con el que acceden a tu cuenta

La Policía vuelve a alertar de un nuevo intento de estafa y advierte de que jamás debes pinchar el 'link' de este mensaje.

Guías de buenas prácticas

Guías de buenas prácticas

Buenas prácticas para el diagnóstico de ciberseguridad en entornos industriales

Mapa Normativo de Ciberseguridad Industrial

Guía para la creación de un SGCI

Desmantelamiento de campañas maliciosas

¿Cómo reportar incidencias?

Número de teléfono gratuito
900 104 891

Correo electrónico
incidencias@bcsc.eus

El punto de encuentro de la ciberseguridad en Euskadi

www.basquecybersecurity.eus

@basquecscentre

LinkedIn

YouTube