Programa Cultura de Ciberseguridad

Resultados

Julio - Octubre 2022

Gaptain
CYBERSECURITY™
MADE IN EUROPE

CULTURA DE CIBERSEGURIDAD PEOPLE CENTRIC

Durante la implantación en **[EMPRESA]** del programa Cultura de Ciberseguridad se han llevado a cabo las siguientes acciones:

- **Plan de concienciación y capacitación integral** en forma de itinerarios formativos de **20 horas, 10 horas** y **8 horas** para los diferentes colectivos de la organización.
- **Simulacros de ciberataque: 3 campañas** de email phishing (hacking ético)
- **Análisis de resultados**.

PROGRAMA INTEGRAL DE CAPACITACIÓN

COMPETENCIA DIGITAL CIBERSEGURIDAD

Gaptain
CYBERSECURITY MADE IN EUROPE

CAPACITACIÓN: LAS PERSONAS

La **ciberseguridad** es un concepto que **aplica**, además de **a los sistemas informáticos**, a **las personas usuarias** del sistema.

Que éstas conozcan los **protocolos básicos de ciberseguridad**, los **riesgos** y **amenazas**, y que sean capaces de **hacer un uso seguro** de los dispositivos conectados y las herramientas digitales, **depende** en gran medida **la seguridad de todo el sistema**, y el bienestar digital de las personas que integran la organización.

El **80%** de los ciberataques a las organizaciones se realizan a través del factor humano

La 'ingeniería social', el phishing y el malware tipo ransomware son las técnicas más habituales

CAPACITACIÓN: LAS PERSONAS

Con el objetivo de generar una **"Cultura de ciberseguridad"** dentro de la organización se crea y pone en marcha un **plan de capacitación integral y personalizado** para cada uno de los siguientes grupos de empleados/as:

- Dirección
- Administración
- Comercial
- Postventa
- Básico (itinerario reducido)

Plataforma online, 20 y 10 horas en total con cada perfil de empleado/a

La capacitación se completa entre Julio y Octubre de 2022 y se extiende a **52** empleados/as

CAPACITACIÓN: COMPETENCIAS

El plan de capacitación se centra en desarrollar los **conocimientos de ciberseguridad** de cada empleado/a de la organización teniendo en cuenta las **responsabilidades** y **funciones** propias de su puesto de trabajo.

El marco DigComp 2.0 define 5 grandes grupos competenciales. En el programa *Cultura de ciberseguridad People Centric* nos centraremos en el **bloque 4**: **Seguridad Digital**.

1. BÚSQUEDA iNFORMACIÓN
2. COMUNICACIÓN y COLABORACIÓN
3. CREACIÓN de CONTENIDO
4. SEGURIDAD
5. RESOLUCIÓN de PROBLEMAS

COMPETENCIA: SEGURIDAD DIGITAL

1. Información
2. Comunicación y colaboración
3. Creación de contenido digital
4. **SEGURIDAD DIGITAL**
5. Resolución de problemas

4 Área de competencia
SEGURIDAD DIGITAL

- 4.1 PROTECCIÓN DE DISPOSITIVOS
- 4.2 PRIVACIDAD DATOS PERSONALES
- 4.3 PROTECCIÓN DE LA SALUD
- 4.4 PROTECCIÓN DEL ENTORNO

NIVEL GLOBAL COMPETENCIA

Para calcular el **nivel global de conocimientos en materia de ciberseguridad** de la organización, se han tenido en cuenta los siguientes parámetros:

- Tipo de Itinerario: **versión básica** (10 Horas)
- Media de intentos para superar la evaluación: **1.55**
- Porcentaje medio aciertos **94.07%**
- % empleados asignados al Perfil básico: **55.5%**
- % empleados superan capacitación: **95%**

(*) Para obtener la acreditación individual, la plataforma requiere superar la evaluación de cada módulo con un valor mínimo del 75% de respuestas correctas.

Nº empleados acreditados

NIVEL GLOBAL DE COMPETENCIA

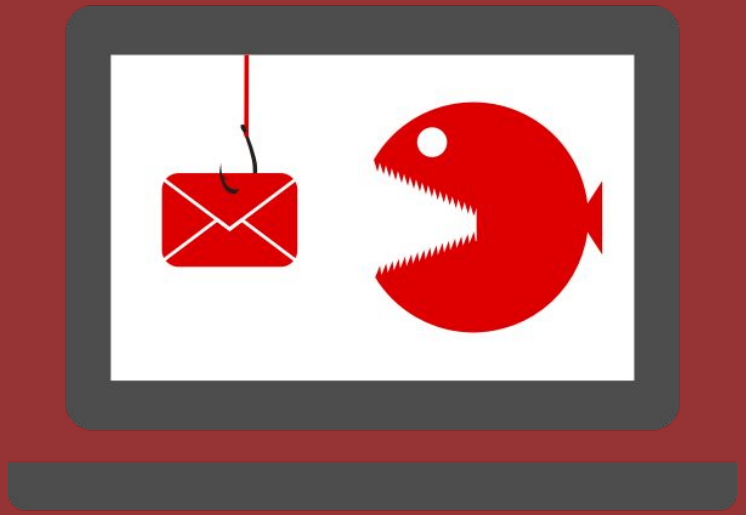
Un bajo nivel de conocimientos en ciberseguridad de los empleados **supone un riesgo para la organización.**

En base a los datos obtenidos durante la capacitación y al análisis de diferentes indicadores (conocimientos sobre ciberseguridad, tipo de itinerario, nº de intentos para superar la evaluación, nº empleados en perfil básico, % empleados capacitados) se calcula el **nivel global de conocimientos en materia de ciberseguridad** de la organización.

Nivel global de conocimientos de ciberseguridad de la organización

*(*) El nivel de competencia en ciberseguridad es una puntuación de 0 a 10 puntos. De 0 a 5 puntos **Nivel Bajo**. De 5 A 8 puntos **nivel Medio**. De 8 a 10 puntos **nivel Alto**.*

SIMULACROS DE CIBERATAQUE



Gaptain
CYBERSECURITY™
MADE IN EUROPE

SIMULACRO de CIBERATAQUE

A lo largo de la capacitación se realizaron **3 simulacros de ciberataque** (hacking ético) durante los días **10 de Octubre**, **31 de Octubre** y **2 de Noviembre**.

Se enviaron campañas de emails phishing a usuarios de diferentes departamentos y con diferentes niveles de responsabilidad dentro de la organización.

[EMPRESA] dispone de un protocolo interno mediante el cual, cuando se recibe un email sospechoso se comunica a toda la organización para que no se abra el correo.

Se ha verificado que **este protocolo se ha activado con éxito** durante los simulacros llevados a cabo y ha frenado la difusión de los emails enviados.

SIMULACRO de CIBERATAQUE

Tras el envío de las diferentes campañas de phishing ético, se recogieron los siguientes **datos globales**.

Total emails enviados: 82
N.º de personas que hacen click en enlace phishing: 5
N.º de personas que aportan sus credenciales: 1

El **6.10%** hace click en el enlace phishing

	Nº Envíos	Clicks	Envío Datos
Campaña 1	28	3	1
Campaña 2	26	1	0
Campaña 3	28	1	0
TOTAL emails	**82**	**5**	**1**

SIMULACRO 1 (10 y 11 de Octubre)

Se enviaron 5 modelos de correos a usuarios de diferentes departamentos de la empresa:

- Gerente
- MKT
- Personal de administración
- Personal de postventa
- Personal comercial

Total emails enviados: 28
N.º de personas que hacen click en enlace: 3
N.º de personas que aportan sus credenciales: 1

El **10.71%** hace click en el enlace phishing

3.57% aportaron datos de acceso

SIMULACRO 2 (31 de Octubre)

Se envió 1 modelo de email phishing a todos los usuarios.
En este caso se opta por un modelo de email phishing de tipo personal, no relacionado con el puesto de trabajo (notificación de pedido de Amazon).

Total emails enviados: 26
N.º de personas que hacen click en enlace: 1
N.º de personas que aportan sus credenciales: 0

El **3.85%** hace click en el enlace phishing.

NADIE proporciona datos de identificación.

SIMULACRO 3 (2 de Noviembre)

Se enviaron 2 modelos de email phishing a usuarios de diferentes departamentos de la empresa:

- Dirección, Administración y Comercial
- Personal de postventa

Total emails enviados: 28
N.º de personas que hacen click en enlace: 1.

El **3.57%** hace click en el enlace
NADIE proporciona datos de identificación.

NIVEL GLOBAL RIESGO CIBERATAQUE

En base a los datos obtenidos durante los simulacros, se calcula el **nivel de riesgo** de ser víctima de un ciberataque tipo phishing así como la **mejora conseguida** tras el programa de capacitación.

Para calcular el nivel de riesgo, se han tenido en cuenta el número de personas que hacen **click en enlaces phishing**, personas que aportan sus **credenciales,** así como el **tiempo de detección** / comunicación del incidente de ciberseguridad.

Pese a la **relevante mejora conseguida**, cabe destacar que los intentos de ciberataque evolucionan día a día, con lo que es necesario **realizar periódicamente** acciones de concienciación y formación.

(*) El nivel del riesgo es una puntuación de 0 a 10 puntos.
De 0 a 4 puntos Riesgo Bajo. De 4 A 7 puntos Riesgo Medio. De 7 a 10 puntos riesgo Alto.

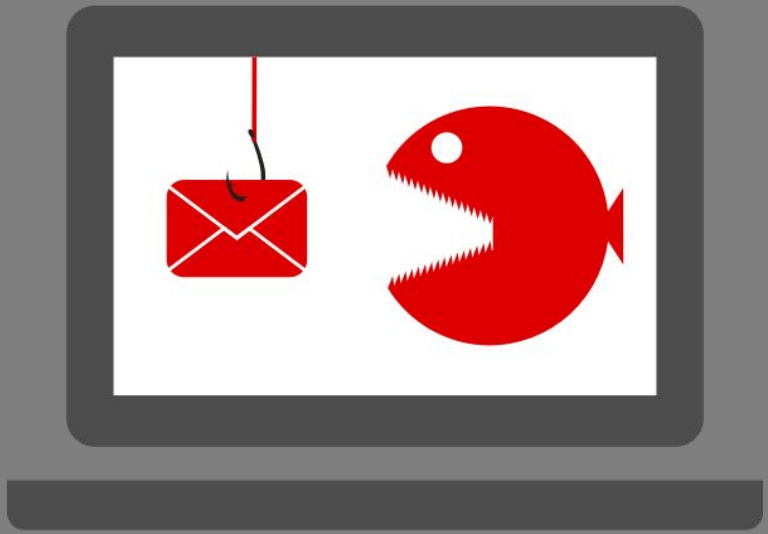
Riesgo ciberataque

62.32%

Mejora conseguida tras el programa de capacitación

MODELOS
emails phishing

CONSIDERACIONES



Gaptain
CYBERSECURITY
MADE IN EUROPE

MODELOS de EMAIL PHISHING

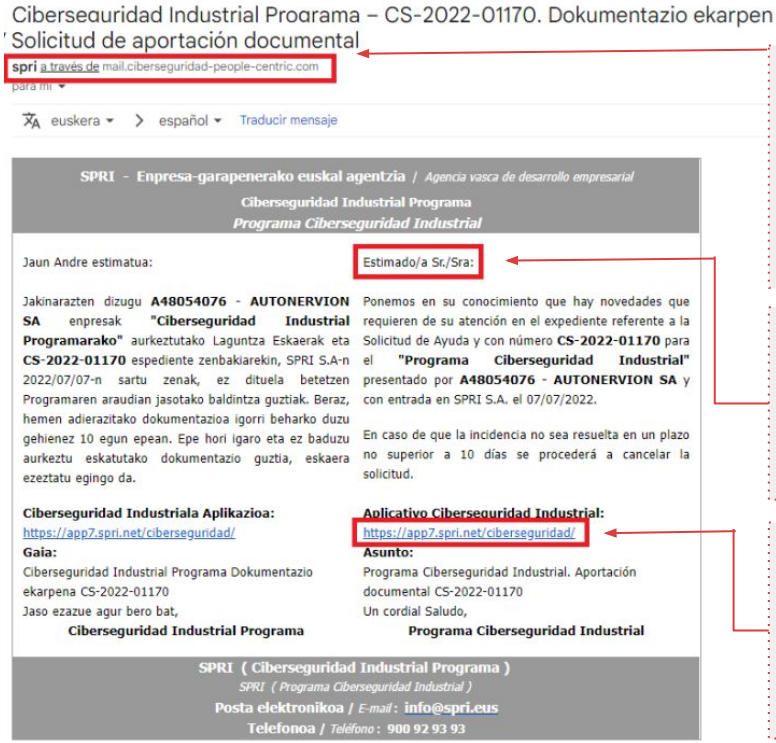
Durante los simulacros de ciberataque se han utilizado varios **modelos de email phishing** similares a los **utilizados por los ciberdelincuentes**.

Para prevenir sus consecuencias negativas, es necesario **conocer las técnicas** habituales y **saber identificar** un intento de **phishing**.

A continuación se indican los '**indicadores de phishing**' en cada uno de los modelos de email utilizados.

El **94%** de todo el malware se envía por correo electrónico

MODELOS de EMAIL PHISHING



Ciberseguridad Industrial Programa – CS-2022-01170. Dokumentazio ekarpen eskaera
Solicitud de aportación documental

spri a través de mail.ciberseguridad-people-centric.com
para mí

euskera › español Traducir mensaje

SPRI - Enpresa-garapenerako euskal agentzia / *Agencia vasca de desarrollo empresarial*
Ciberseguridad Industrial Programa
Programa Ciberseguridad Industrial

Jaun Andre estimatua:

Jakinarazten dizugu **A48054076 - AUTONERVION SA** enpresak **"Ciberseguridad Industrial Programarako"** aurkeztutako Laguntza Eskaerak eta **CS-2022-01170** espediente zenbakiarekin, SPRI S.A-n 2022/07/07-n sartu zenak, ez dituela betetzen Programaren araudian jasotako baldintza guztiak. Beraz, hemen adierazitako dokumentazioa igorri beharko duzu gehienez 10 egun epean. Epe hori igaro eta ez baduzu aurkeztu eskatutako dokumentazio guztia, eskaera ezeztatu egingo da.

Ciberseguridad Industriala Aplikazioa:
https://app7.spri.net/ciberseguridad/
Gaia:
Ciberseguridad Industrial Programa Dokumentazio ekarpena CS-2022-01170
Jaso ezazue agur bero bat,
Ciberseguridad Industrial Programa

Estimado/a Sr./Sra:

Ponemos en su conocimiento que hay novedades que requieren de su atención en el expediente referente a la Solicitud de Ayuda y con número **CS-2022-01170** para el **"Programa Ciberseguridad Industrial"** presentado por **A48054076 - AUTONERVION SA** y con entrada en SPRI S.A. el 07/07/2022.

En caso de que la incidencia no sea resuelta en un plazo no superior a 10 días se procederá a cancelar la solicitud.

Aplicativo Ciberseguridad Industrial:
https://app7.spri.net/ciberseguridad/
Asunto:
Programa Ciberseguridad Industrial. Aportación documental CS-2022-01170
Un cordial Saludo,
Programa Ciberseguridad Industrial

SPRI (Ciberseguridad Industrial Programa)
SPRI (Programa Ciberseguridad Industrial)
Posta elektronikoa / *E-mail*: **info@spri.eus**
Telefonoa / *Teléfono*: **900 92 93 93**

El EMISOR del email no es correcto
El nombre del **emisor del email** es SPRI pero en realidad se envía a través de *mail.ciberseguridad-people-centric.com*

Destinatario genérico
En los servicios que solicitan datos porque somos usuarios, deberían personalizar el destinatario.

El ENLACE no es correcto
El texto del enlace indica que la URL es *https://app7.spri.net/ciberseguridad* pero enlaza a *https://app-secure.net/?keyname=mFoCVfV*

MODELOS DE EMAIL PHISHING

Premios SMART Euskadi: AUTONERVION S.A. - SMART Euskadi SARIAK

GU gunamuno@spri.eus a través de mail.ciberseguridad-people-centric.com

VIE OCT 7 8:28 AM · INBOX

Estimado Jon Lekue,

Soy Guillermo Unamuno, responsable del Dpto. Transformación Digital dentro de SPRI.

Tengo el placer de informarle de que la empresa **AUTONERVIÓN S.A** ha sido nominada para los **premios SMART Euskadi**, cuyo objetivo es reconocer y dar visibilidad a las pymes vascas que han abordado el proceso de transformación digital de forma ejemplar.

En el siguiente enlace encontrarás los detalles de la ceremonia de entrega de los premios SMART, así como y la solicitud de inscripción al evento.

- AGENDA premios SMART Euskadi

Aprovecho para enviarle mi más sincera enhorabuena por su gestión y liderazgo.

Recibe un cordial saludo,

Guillermo Unamuno Enciondo
Ingeniero de Telecomunicaciones – Eraldaketa Digitala / Transformación Digital
Responsable Dpto. SMART SPRI
Tel.: +34 94 403 70 74 / +34 688 674 074 - gunamuno@spri.eus

GRUPO spri TALDEA

EUSKO JAURLARITZA GOBIERNO VASCO

Harpidetu zaitez Suscríbete

BASQUE COUNTRY

El EMISOR del email no es correcto

El nombre del **emisor del email** es Guillermo Unamuno de SPRI pero en realidad se envía a través de *mail.ciberseguridad-people-centric.com*

El ENLACE no es correcto

El texto del enlace indica que la URL pertenece a una noticia relativa a la temática del email pero se proporciona una url genérica.

MODELOS de EMAIL PHISHING

El EMISOR del email no es correcto

El nombre del **emisor del email** es lanbide@euskadi.eus pero en realidad se envía a través de *mail.ciberseguridad-people-centric.com*

No hay destinatario o es genérico

No existe destinatario, es un email genérico.

El ENLACE no es correcto

El texto del enlace indica que la URL enlaza a una página del BOB pero en realidad enlaza a *https://app-secure.net/?keyname=*

Formato del email

La cabecera y pie de página no son muy profesionales, con imágenes no optimizadas y muy genéricas o no relacionadas.

MODELOS de EMAIL PHISHING

Mantenimiento programado

Recibidos x Notificaciones x

Servivio Técnico tecnico@autonervion.com

MANTENIMIENTO INFORMÁTICO PROGRAMADO

Buenos días,

por labores de mantenimiento programado, y con el objetivo de mejorar la calidad de los servicios electrónicos ofrecidos por la empresa, desde el próximo viernes a las 10:00, hasta el domingo a las 20:00 podrían producirse cortes y paradas intermitentes en los equipos y servicios listados a continuación.

Para conocer si tu equipo está entre los afectados por el mantenimiento, pulsa en este enlace e indica tu usuario y contraseña:

> Lista de equipos afectados.

Disculpe las molestias.

Atentamente,

Servicio Técnico

AUTONERVION

Ctra. San Vicente 2
48910 Sestao
Móvil: 621209244
Tel. : +34 9 44 18 80 30
Fax. : +34 9 44 18 81 70
www.autonervion.com

Puedes encontrarnos en:
https://www.instagram.com/autonervionrenault/
https://www.facebook.com/autonervion
https://www.linkedin.com/company/autonervion
AUTONERVION - YouTube

El EMISOR del email no es correcto

El nombre del **emisor del email** es tecnico@autonervion.com pero en realidad se envía a través de *mail.ciberseguridad-people-centric.com*

No hay destinatario o es genérico

No existe destinatario, es un email genérico.

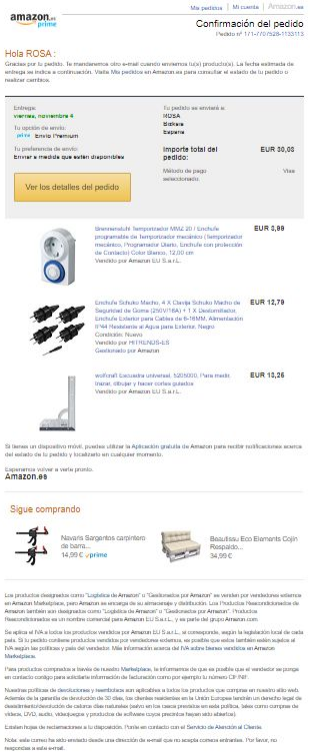
El ENLACE no es correcto

El texto del enlace indica que la URL enlaza a una página que simula ser la web genérica de *Renault España* con un formulario de login.

Formato del email

Se envían mensajes que apremian al usuario para que haga clic. Se usa el formato de pie de página habitual para hacerlo más creíble.

MODELOS de EMAIL PHISHING



Mis pedidos | Mi cuenta | Amazon.es

amazon.es prime

Confirmación del pedido

Pedido nº 171-7070926-7130113

Hola ROSA :

Gracias por tu pedido. Te mandaremos otro e-mail cuando enviemos tu(s) producto(s). La fecha estimada de entrega se indica a continuación. Visita Mis pedidos en Amazon.es para consultar el estado de tu pedido o realizar cambios.

Entrega:
viernes, noviembre 4

Tu opción de envío:
prime Envío Premium

Tu preferencia de envío:
Enviar a medida que estén disponibles

Tu pedido se enviará a:
ROSA
Bizkaia
España

Importe total del pedido: EUR 30,00

Método de pago seleccionado: Visa

Ver los detalles del pedido

EUR 3,89

EUR 12,79

EUR 13,26

Si tienes un dispositivo móvil, puedes utilizar la Aplicación gratuita de Amazon para recibir notificaciones acerca del estado de tu pedido y localizarlo en cualquier momento.

Esperamos volver a verte pronto.
Amazon.es

Sigue comprando

Navaris Sargentos carpintero de barra...
14,99 € prime

Beautissu Eco Elements Cojín Respaldo...
34,95 €

Los productos designados como "Logística de Amazon" o "Gestionados por Amazon" se venden por vendedores externos en Amazon Marketplace, pero Amazon se encarga de su almacenaje y distribución. Los Productos Reacondicionados de Amazon también son designados como "Logística de Amazon" o "Gestionados por Amazon". Productos Reacondicionados es un nombre comercial para Amazon EU S.a.r.L. y es parte del grupo Amazon.com.

Se aplica el IVA a todos los productos vendidos por Amazon EU S.a.r.L. al corresponde, según la legislación local de cada país. Si tu pedido contiene productos vendidos por vendedores externos, es posible que estos también estén sujetos al IVA según las políticas y país del vendedor. Más información acerca del IVA sobre bienes vendidos en Amazon Marketplace.

Para productos comprados a través de nuestro Marketplace, te informaremos de que es posible que el vendedor se ponga en contacto contigo para solicitarte información de facturación como por ejemplo tu número CIF/NIF.

Nuestras políticas de devoluciones y reembolsos son aplicables a todos los productos que compras en nuestro sitio web. Además de la garantía de devolución de 30 días, los clientes residentes en la Unión Europea también un derecho legal de desistimiento/devolución de calcinco días naturales (salvo en los casos precisos en esta política, tales como compras de vídeos, DVD, audio, videojuegos y productos de software cuyos precintos hayan sido abiertos).

Existen hojas de reclamaciones a tu disposición. Ponte en contacto con el Servicio de Atención al Cliente.

Nota: este correo ha sido enviado desde una dirección de e-mail que no acepta correos entrantes. Por favor, no respondas a este e-mail.

El EMISOR del email no es correcto

El nombre del **emisor del email** es Amazon.es pero en realidad se envía a través de *mail.ciberseguridad-people-centric.com*

Destinatario personalizado

Se personaliza con el nombre del destinatario para hacerlo más creíble.

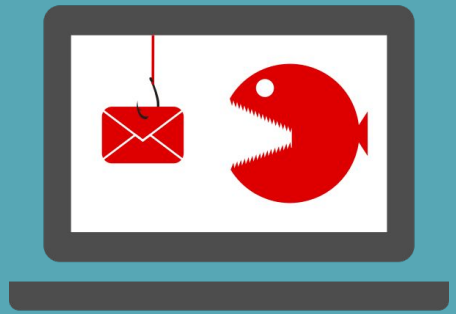
Los ENLACEs no son correctos

Todos los enlaces redirigen a una página que simula el formulario de login de Amazon: *https://app-secure.net/?keyname=*

Tema del email

Se está enviando un email personal a una cuenta empresarial informando sobre un pedido que no se ha realizado.

NIVEL GLOBAL DE EXPOSICIÓN AL RIESGO DE CIBERATAQUE



Gaptain
CYBERSECURITY
MADE IN EUROPE

RIESGO GLOBAL ORGANIZACIÓN

PERSONAS	• Competencia: conocimientos, percepción, puesta en práctica, evangelización... • Riesgo de sufrir ciberataques
PROCESOS	• Protocolos básicos de ciberseguridad • Tratamiento de datos
TECNOLOGÍA / INFRAESTRUCTURAS	• Análisis de vulnerabilidades en la tecnología, los sistemas e infraestructuras de la organización

NIVEL GLOBAL DE EXPOSICIÓN AL RIESGO ORGANIZACIÓN

Para calcular este nivel (0-10) se tienen en cuenta el **nivel de competencia** de todos los miembros de la organización participantes en la capacitación integral así como los **resultados del simulacro de ciberataque**.

Quedan fuera del alcance del proyecto los datos relativos a **procesos** e **infraestructuras** de la organización.

El nivel global de exposición al riesgo de la organización es un valor de 0 a 10 puntos. De 0 a 5 puntos Nivel Bajo. De 5 A 8 puntos nivel Medio. De 8 a 10 puntos riesgo Alto.

RIESGO MEDIO - BAJO

RECOMENDACIONES FINALES

- Los empleados/as tienen una base de conocimientos en ciberseguridad que se debe **actualizar de forma periódica**.
- **Recordar periódicamente las políticas de seguridad** y las **buenas prácticas** que deben seguir los empleados en sus puestos de trabajo.
- Implantar **políticas de uso de dispositivos móviles** y **uso de contraseñas** en la empresa.
- Elaborar un **plan de contingencia** y **recuperación ante desastres** en la empresa.

Cultura de Ciberseguridad

CONTACTO

Isuskiza 195, Plentzia 48620. Bizkaia
Tlf: (+34) 648 281 775
Email: info@gaptain.com
Web: https://www.gaptain.com