

Catálogo de servicios



Índice

01. Introducción	4
1. 1. Objetivo	4
1. 2. Contenido del documento	4
1. 3. Documentos relacionados	4
02. El catálogo de servicios	5
2. 1. Base y fundamento de los servicios del catálogo	5
2. 2. Segmentación de la oferta de servicios	6
2. 3. Ámbitos de actuación de los servicios	6
2. 4. CyberOrratz	7
2. 5. Mantenimiento del catálogo	7
03. Derechos y obligaciones de las entidades	8
3. 1. Derechos de la entidad	8
3. 2. Obligaciones de la entidad	8
3. 3. Notificación de incidentes	9
3. 4. Compromisos y calidad de servicio	9
04. Líneas de servicio	10
4. 1. Auditoría	10
4. 2. Concienciación	11
4. 3. Coordinación estratégica	11
4. 4. Gobierno del riesgo	12
4. 5. Inteligencia de amenazas	12
4. 6. Modelo de seguridad de Euskadi	13
4. 7. Operaciones de seguridad (SOC)	13
4. 8. Respuesta a incidentes (CSIRT)	14
4. 9. Seguridad ofensiva	15
4. 10. Transferencia del conocimiento	15

05. Fichas de servicio	16
5.1. Auditoría	
5.1.1. Evaluación de la seguridad	17
5.1.2. OAT - Órgano de Auditoría Técnica	18
5.1.3. Supervisión de planes de continuidad	19
5.2. Concienciación	
5.2.1. Concienciación	20
5.2.2. Campañas de phishing	21
5.3. Coordinación estratégica	
5.3.1. Despliegue de la Estrategia de Ciberseguridad de Euskadi	22
5.3.2. Oficina de gestión de servicios	23
5.4. Gobierno del riesgo	
5.4.1. Evaluación del riesgo	24
5.4.2. Gestión del riesgo	25
5.4.3. Oficina de armonización	26
5.4.4. Gestión de proyectos especiales	27
5.5. Inteligencia de amenazas	
5.5.1. Alerta temprana	28
5.5.2. Intercambio de información sobre ciber amenazas	29
5.6. Modelo de Seguridad de Euskadi	
5.6.1. Acompañamiento y seguimiento en el despliegue del Modelo de Seguridad de Euskadi	30
5.7. Operaciones de seguridad (SOC)	
5.7.1. SOC	31
5.7.2. Threat hunting	32
5.8. Respuesta a incidentes (CSIRT)	
5.8.1. Asesoramiento Servicio	33
5.8.2. Coordinación	34
5.8.3. DFIR	35
5.8.4. Gestión de crisis	36
5.8.5. Takedown	37
5.8.6. Preparación para la respuesta a incidentes de ciberseguridad	38
5.9. Seguridad ofensiva	
5.9.1. Auditoría técnica	39
5.9.2. EASM	40
5.9.3. Red team	41
5.10. Transferencia del conocimiento	
5.10.1. Formación	42
5.10.2. Entrenamiento	43

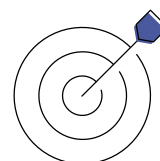
01.

Introducción

1. 1.

Objetivo

Inicialmente, con objeto del **catálogo de servicios** tiene por objetivo presentar una visión global de los servicios prestados por la **Agencia Vasca de Ciberseguridad (Cyberzaintza)**. De este modo, se facilita la comprensión y el acceso a la oferta de servicios, garantizando que cada entidad pueda identificar aquellos que se ajustan a sus necesidades específicas. Además, el catálogo sirve como herramienta de referencia para conocer las características principales, el alcance y los estándares de calidad asociados a cada servicio.



1. 2.

Contenido del documento

Además de este capítulo de introducción, el Catálogo de servicios presenta los siguientes contenidos:



La **descripción** del catálogo de servicios.



Un **conjunto de fichas** que reflejan la definición, características principales y tipologías de cada servicio del catálogo.



La **definición** de cada línea de servicio y de los servicios contenidos en ellas.



Los **acuerdos** de nivel de servicio estándar.

1. 3.

Documentos relacionados

A continuación, se presentan las principales normas de referencia que se han tenido en cuenta para la elaboración del:

Sistemas de gestión de la calidad. Requisitos (UNE-EN ISO 9001).

Tecnología de la información. Sistema de Gestión del Servicio (SGS). Parte 1: Requisitos (UNE ISO/IEC 20000-1).

Cartas de servicios. Requisitos (UNE 93200).

CyberOrratz.

Su aplicación garantiza que los servicios incluidos en el catálogo respondan a estándares reconocidos internacionalmente y se adapten a las mejores prácticas del sector.

02.

El catálogo de servicios

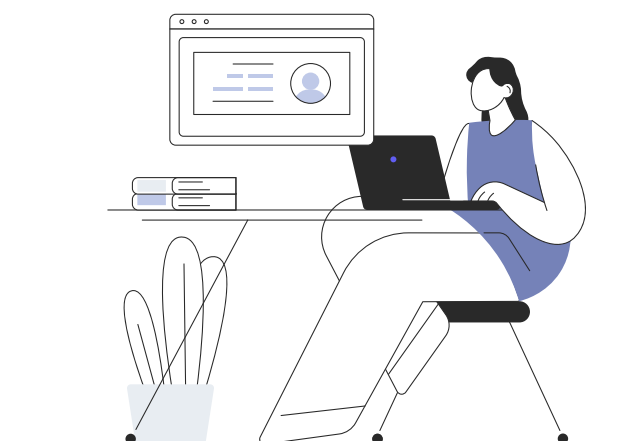
2.1.

Base y fundamento de los servicios del catálogo

Los servicios recogidos en el presente catálogo se fundamentan en el marco competencial, estratégico y operativo de Cyberzaintza, y constituyen el principal instrumento para materializar su misión y funciones en el ámbito de la ciberseguridad en Euskadi.

En primer lugar, dichos servicios se sustentan en la naturaleza y funciones de Cyberzaintza como ente público del sector público de la Comunidad Autónoma Vasca, con personalidad jurídica propia y adscripción al Departamento de Seguridad. De conformidad con lo establecido en la Ley 7/2023, de 29 de junio, de **creación de la Agencia Vasca de Ciberseguridad**, Cyberzaintza tiene encomendadas funciones de promoción, coordinación y apoyo en materia de ciberseguridad, así como el impulso de la capacitación y del desarrollo digital seguro en el ámbito del sector público vasco, el tejido empresarial y la ciudadanía. El Catálogo de servicios constituye, por tanto, la **expresión operativa de dichas funciones**, permitiendo su prestación de forma ordenada, transparente y coherente.

En segundo lugar, los servicios del catálogo se alinean directamente con la **Estrategia Vasca de Ciberseguridad 2024-2029**, que identifica los principales desafíos del País en esta materia y define objetivos estratégicos y líneas de actuación que requieren una ejecución coordinada y sostenida en el tiempo. A través de los servicios incluidos en el catálogo, Cyberzaintza contribuye a la consecución de dichos objetivos, liderando y apoyando acciones de gobernanza, prevención, detección y respuesta frente a ciberamenazas, y facilitando la colaboración entre los distintos agentes implicados.



Asimismo, el catálogo se apoya en la propuesta de valor de Cyberzaintza, **orientada a reforzar la ciberseguridad en Euskadi mediante un enfoque integral y colaborativo**. Los servicios ofrecidos promueven la adopción de buenas prácticas, el desarrollo de estándares y directrices comunes, la protección de los sistemas de información y de los datos, contribuyendo a elevar el nivel global de madurez en ciberseguridad del sector público vasco y de su entorno.



Por último, el catálogo de servicios se concibe como **un instrumento dinámico de referencia**, que permite a las entidades usuarias conocer de forma clara y estructurada los servicios disponibles, su alcance y condiciones de prestación, y que facilita la adaptación progresiva de la oferta de servicios a la evolución de las amenazas, del marco normativo y de las necesidades del ecosistema digital de Euskadi.

2.2.

Segmentación de la oferta de servicios

La oferta de servicios de Cyberzaintza se estructura atendiendo a una segmentación por público objetivo y verticales, con el fin de dar respuesta de manera específica y proporcionada a las distintas necesidades de ciberseguridad existentes en Euskadi.

Esta segmentación permite adaptar los servicios al contexto, nivel de madurez y marco normativo de cada entorno, garantizando una prestación más eficaz y alineada con los riesgos y obligaciones propias de cada ámbito.

En este sentido, los servicios del catálogo se organizan en los siguientes públicos objetivos y verticales:



Sector Público

Orientado al sector público vasco, e incluyendo verticales específicos como administración pública, seguridad, salud y educación.



Empresas

Dirigido al tejido empresarial, con especial atención a: empresas estratégicas, empresas con obligaciones específicas en materia de autoprotección y otras empresas.



Ciudadanía

Con servicios adaptados a distintos colectivos, en particular: menores, personas adultas y grupos en riesgo de exclusión social.

Esta organización por verticales facilita la identificación de los servicios más adecuados para cada tipo de entidad o colectivo, y permite a Cyberzaintza priorizar y especializar su actuación en función de las características y necesidades de cada entorno.

2.3.

Ámbitos de actuación de los servicios

Con independencia del público objetivo o vertical al que se dirijan, los servicios de Cyberzaintza se clasifican en función de su ámbito de actuación en el ciclo de la ciberseguridad, siguiendo un enfoque integral alineado con buenas prácticas y estándares reconocidos internacionalmente.

Los ámbitos de actuación son los siguientes:



Prevención

Comprende los servicios orientados a reducir la probabilidad de incidentes de ciberseguridad mediante la anticipación, la concienciación, la adopción de medidas de protección y el fortalecimiento de capacidades.



Detección

Incluye los servicios destinados a la identificación temprana de incidentes o amenazas de ciberseguridad, mediante el uso de herramientas, sistemas y mecanismos que permitan una respuesta más rápida y eficaz.



Respuesta

Engloba los servicios necesarios para la gestión de incidentes una vez detectados, con el objetivo de contener su impacto, apoyar la recuperación y minimizar las consecuencias para las entidades afectadas.



Gobernanza

Abarca los servicios orientados a establecer marcos, directrices, estándares y estructuras organizativas que permitan gestionar la ciberseguridad de forma coherente, coordinada y sostenible.

Estos ámbitos no solo delimitan los tipos de servicios ofrecidos, sino que **constituyen un marco estructurado de intervención**, que permite abordar de manera integral las distintas dimensiones de la ciberseguridad y asegurar la coherencia del Catálogo con la Estrategia Vasca de Ciberseguridad y el marco normativo aplicable.

2. 4.

CyberOrratz

CyberOrratz es el marco de referencia desarrollado por Cyberzaintza, diseñado específicamente para estructurar, evaluar y fortalecer la ciberseguridad de cualquier organización. Gracias a su metodología basada en controles y niveles de implantación, permite establecer prioridades claras, medir el grado de madurez y planificar actuaciones de mejora continua en áreas clave como la gestión de riesgos, el cumplimiento normativo, la auditoría y la protección integral de sistemas e información. Este modelo responde al mandato de impulsar estándares, directrices y normas técnicas recomendadas para el sector público vasco, garantizando a las entidades una base sólida para consolidar su postura de seguridad.

La estructura de CyberOrratz se articula en dominios de ciberseguridad, cada uno de los cuales agrupa controles y medidas que se implementan a lo largo del modelo. Estos dominios abarcan:

Gobierno de la ciberseguridad

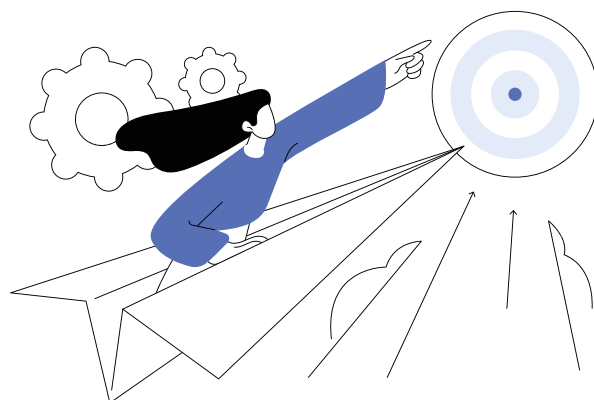
Identificación y clasificación de activos

Protección de activos e infraestructuras

Monitorización, detección y alerta

Respuesta a incidentes

Recuperación y resiliencia



Cada servicio del catálogo se vincula directamente con los controles de estos dominios, garantizando una oferta alineada con las mejores prácticas y adaptada a las necesidades reales de cada entidad.

Sobre esta base, el modelo implementa seis niveles de control progresivos:



Esta estructura permite una implantación ordenada y personalizada de la ciberseguridad, adaptándose al grado de madurez de cada organización y facilitando la integración de los servicios del catálogo en el ciclo de mejora continua. Al asociar cada servicio con un control específico del modelo, se asegura una respuesta eficaz y a medida para cada necesidad.

2. 5.

Mantenimiento del catálogo

El **catálogo de servicios de Cyberzaintza se mantiene actualizado de forma continua** con el fin de garantizar su adecuación a los objetivos estratégicos de la Agencia y a las necesidades de las entidades usuarias.

El Comité de Dirección de Cyberzaintza impulsa y orienta la evolución del catálogo, trasladando los objetivos estratégicos de la organización y las necesidades detectadas en las entidades usuarias a la definición y priorización de los servicios, y participando en la identificación de nuevos servicios y líneas de actuación, en coordinación con las personas responsables de los mismos.

La gestión y supervisión del catálogo de servicios se realiza de manera coordinada dentro de la organización, velando por la coherencia, calidad y adecuación de los servicios incluidos y, en particular:

- Evaluando la adecuación de los servicios definidos en el catálogo en relación con su utilidad, alcance funcional y condiciones de calidad.
- Manteniendo una visión global de los servicios, de los procesos internos de Cyberzaintza, de las infraestructuras que los soportan y de las entidades a las que se dirigen.
- Realizando el seguimiento del catálogo como instrumento de referencia para la prestación de los servicios.

El Comité de Dirección revisa, al menos con periodicidad anual, el contenido del catálogo de servicios, con el objetivo de adecuarlo, en su caso, a la evolución del contexto normativo, estratégico y operativo, así como a las nuevas necesidades detectadas.

03.

Derechos y obligaciones de las entidades

3.1.

Derechos de la entidad

Cualquier entidad que haga uso de alguno de los servicios del presente catálogo tiene adquiridos al menos los siguientes derechos:

- Disponer y tener acceso a los recursos necesarios que le permitan:
 - Acceder al catálogo de servicios para conocer los servicios que Cyberzaintza le ofrece.
 - Consultar las características generales de cada servicio para conocer su objetivo, alcance y colectivo al que va dirigido.
 - Acceder a las condiciones aplicables para el uso del servicio.
 - Conocer las características propias de los acuerdos establecidos con Cyberzaintza respecto a los servicios solicitados.
- Podrá realizar reclamaciones sobre los servicios que recibe.
- Podrá hacer uso de las diferentes opciones existentes en los servicios que recibe para adaptarlos a sus necesidades, según se establece en las características propias del servicio y utilizando para ello canales y procedimientos formalizados.
- Dispondrá de personas de contacto y canales de acceso a los mismos para tratar aspectos sobre su servicio.
- Recibir un tratamiento confidencial de la información que facilite a Cyberzaintza, garantizando que dicha información sea utilizada exclusivamente para la finalidad de los servicios prestados y protegida conforme a la normativa aplicable.
- Exigir que las actuaciones realizadas por Cyberzaintza se ajusten a criterios de necesidad, proporcionalidad y mínima afectación, de conformidad con estándares de buenas prácticas.

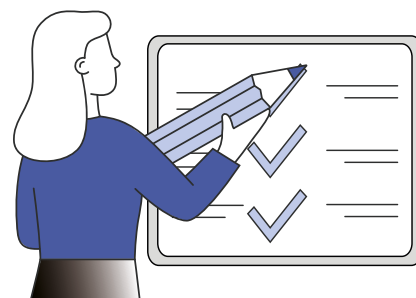


3.2.

Obligaciones de la entidad

Cualquier entidad usuaria que haga uso de alguno de los servicios del presente catálogo tiene adquiridos al menos las siguientes obligaciones:

- Conocer las características de los servicios que recibe, los compromisos de calidad asumidos por Cyberzaintza y cumplir las condiciones de uso y los acuerdos establecidos de forma conjunta.
- Utilizar los servicios y la información asociada de forma diligente, conforme a la normativa que resulte de aplicación, limitando el uso de la información obtenida a la finalidad de los servicios y excluyendo expresamente usos comerciales, con ánimo de lucro, ilegales o no autorizados, comprometiéndose a destruirla cuando deje de ser necesaria.
- Utilizar los canales de acceso y los procedimientos establecidos para solicitar información, gestionar comunicaciones o requerir modificaciones en los términos de prestación de los servicios, así como dar acuse de recibo y gestionar diligentemente las notificaciones remitidas por Cyberzaintza.
- Proporcionar y mantener actualizada la información necesaria para permitir la correcta prestación de los servicios, conforme a lo previsto en el catálogo y en los acuerdos establecidos.
- Cumplir con la legislación vigente en relación con el uso de los recursos tecnológicos que componen los servicios y con el tratamiento de datos de carácter personal.



- Notificar a Cyberzaintza, tan pronto como se tenga constancia, los incidentes de ciberseguridad y ciberamenazas que puedan afectar a la disponibilidad, integridad o confidencialidad de la información de la entidad, de sus usuarios o de otras entidades, incluyendo los incidentes recogidos en la Guía CCN-STIC 817 del Esquema Nacional de Seguridad (ENS).
- Mantener la confidencialidad de la información a la que tenga acceso con motivo de la prestación de los servicios, de conformidad con la normativa aplicable.
- Autorizar a Cyberzaintza a realizar las validaciones necesarias para la adecuada prestación de los servicios, que podrán incluir actuaciones como el descubrimiento y validación de vulnerabilidades, validación de credenciales o comprobación de información expuesta, las cuales se llevarán a cabo conforme a estándares de buenas prácticas y minimizando cualquier impacto potencial.
- Autorizar a Cyberzaintza a compartir la información facilitada con terceros que participen en la prestación de los servicios o con otras entidades del ámbito de Euskadi cuando resulte necesario para la adopción de medidas de protección.

3. 3.

Notificación de incidentes

Salvo disposición en contra, cualquier notificación o comunicación relativa a un incidente de ciberseguridad que deba remitirse a Cyberzaintza, deberá realizarse por escrito y enviarse a la dirección de correo electrónico:



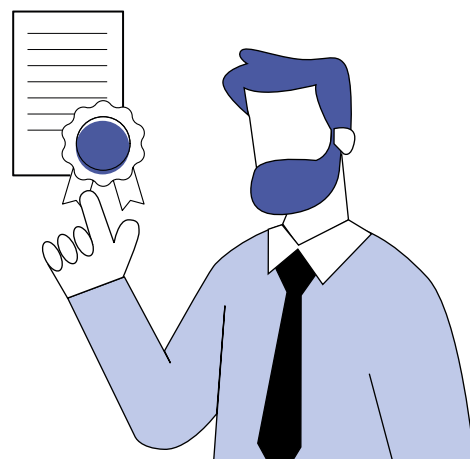
incidencias@cyberzaintza.eus

3. 4.

Compromisos y calidad de servicio

Cyberzaintza asume, en el marco de la prestación de los servicios recogidos en el presente catálogo, los siguientes compromisos y obligaciones:

- Prestar los servicios en los términos y condiciones establecidos en este catálogo y de conformidad con las funciones que, en cada caso, le correspondan.
- Aplicar los medios y esfuerzos razonables disponibles para la prestación de los servicios de forma profesional, diligente y puntual, conforme a los estándares habituales de calidad aplicables.
- Mantener una adecuada comunicación y coordinación con las entidades usuarias en relación con la prestación de los servicios, a través de los canales establecidos.
- Garantizar el tratamiento confidencial de la información a la que tenga acceso como consecuencia de la prestación de los servicios, de conformidad con la normativa aplicable y con la finalidad de los mismos, sin perjuicio de que, por razones de seguridad y prevención, pueda ser necesario compartir determinada información de forma limitada y controlada con otras entidades u organismos, cuando ello resulte imprescindible para la protección de terceros frente a ciberamenazas, aplicando en todo caso el principio de «need to know».
- Cyberzaintza, en el ejercicio de sus funciones, no asume la gestión directa, operación, ni responsabilidad sobre los sistemas de información, ni sobre los sistemas de seguridad de las entidades usuarias, correspondiendo a estas la implantación, gestión y mantenimiento de las medidas de seguridad dentro del ámbito de sus respectivas competencias.



04.

Líneas de servicio

Para facilitar su gestión, los servicios del catálogo se han organizado en **diez categorías principales o líneas de servicio** que agrupan actividades con características similares y un objetivo común. Este enfoque estructurado permite una administración más eficiente y coherente de los servicios, asegurando que cada actividad se alinee con los objetivos estratégicos de Cyberzaintza.

4.1. Auditoría

4.2. Concienciación

4.3. Coordinación Estratégica

4.4. Gobierno del riesgo

4.5. Inteligencia de amenazas

4.6. Modelo de seguridad de Euskadi

4.7. Operaciones de seguridad (SOC)

4.8. Respuesta a incidentes (CSIRT)

4.9. Seguridad ofensiva

4.10. Transferencia del conocimiento

4.1. Auditoría

La línea de acción de auditoría está orientada a la **evaluación objetiva e independiente del grado de cumplimiento normativo, organizativo y técnico en materia de seguridad** de la información y ciberseguridad.

Dentro de la línea de auditoría, se incluyen los siguientes servicios:



Evaluación de la seguridad

El servicio de evaluación de la seguridad se orienta a revisar y asegurar que las organizaciones cumplan con las principales normativas de seguridad y marcos de referencia aplicables. Este proceso incluye la evaluación de la implementación correcta de los controles establecidos, a través de evaluaciones periódicas que buscan identificar posibles áreas de mejora.

OAT (Órgano de Auditoría Técnica)

El servicio de Órgano de Auditoría Técnica se encarga de llevar a cabo auditorías de conformidad con el Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.) para la Administración pública vasca, emitiendo y gestionando, de acuerdo con el reconocimiento emitido por el Centro Criptológico Nacional, los certificados de conformidad correspondientes.

Supervisión de planes de continuidad en materia de ciberseguridad

El servicio de supervisión de planes de continuidad en materia de ciberseguridad se encarga de llevar a cabo el seguimiento, respecto de las organizaciones con obligaciones en materia de planes de autoprotección a las que les aplica la ORDEN de 7 de junio de 2024, del Vicelehendakari Primero y Consejero de Seguridad, por la que se regula la elaboración de planes de continuidad en materia de ciberseguridad para ciertas actividades sujetas a la norma vasca de autoprotección, de que dichas organizaciones registran y mantienen actualizada la información necesaria en relación a los planes de continuidad en materia de ciberseguridad que están obligadas a mantener.

4. 2.

Concienciación

El objetivo principal de la línea de concienciación es **fomentar una cultura sólida de ciberseguridad y elevar el nivel de conocimiento y comprensión**, tanto de personas como de organizaciones, sobre los riesgos digitales presentes en el entorno actual. Además, busca promover comportamientos seguros y responsables en la utilización de la tecnología.

Esta línea incluye una variedad de servicios ofrecidos por Cyberzaintza, diseñados para abordar las necesidades específicas de diferentes públicos objetivos y verticales. Entre estos servicios se encuentran:



Campañas de phishing

El servicio de campañas de phishing realiza ataques de phishing específicamente diseñados para evaluar y fortalecer la capacidad de una organización para detectar y responder ante estas amenazas. Los resultados de estas campañas proporcionan información valiosa sobre las debilidades existentes, facilitando el desarrollo de estrategias de concienciación y mejora continua.

Concienciación

El servicio de concienciación consiste en la organización de jornadas educativas para reforzar el conocimiento y la cultura de ciberseguridad entre la ciudadanía y las organizaciones de Euskadi. Su propósito es aumentar la conciencia sobre los diversos riesgos digitales presentes en el mundo actual y proporcionar a las personas participantes las habilidades necesarias para utilizar internet y las nuevas tecnologías de manera más segura y responsable.

4. 3.

Coordinación estratégica

El objetivo principal de la línea de coordinación estratégica es **coordinar los recursos de ciberseguridad existentes**, desde una perspectiva transversal, con el fin de optimizar y mejorar su eficiencia.

Dentro de la línea de coordinación estratégica, Cyberzaintza cuenta con los siguientes servicios:



Despliegue de la estrategia de Ciberseguridad de Euskadi

El servicio de despliegue de la Estrategia de Ciberseguridad de Euskadi consiste en liderar y apoyar la elaboración, implementación y seguimiento de la estrategia, impulsando su correcta ejecución. Para ello, Cyberzaintza participa activamente en los órganos de gobierno definidos, prestando apoyo técnico mediante la coordinación operativa y la asistencia técnica necesaria, así como mediante la evaluación y supervisión continuas del grado de avance de la estrategia. El servicio se presta a entidades que requieren acompañamiento y soporte en la implementación de la estrategia, facilitando la alineación de sus iniciativas de ciberseguridad con el marco estratégico definido y contribuyendo a la consecución de los objetivos establecidos.

Oficina de gestión de servicios

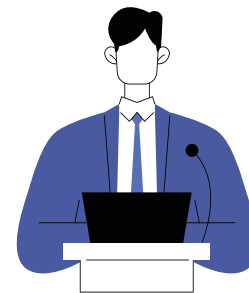
El servicio de oficina de gestión de servicios constituye el canal único y centralizado de relación con las entidades usuarias para la gestión de sus solicitudes vinculadas a Cyberzaintza, proporcionando acompañamiento y una atención integral, coordinada y alineada con sus necesidades específicas en materia de ciberseguridad.

Desde este servicio se realiza la gestión, coordinación y seguimiento de las demandas recibidas, identificando y analizando los requerimientos de los distintos públicos objetivos y verticales, y canalizándolos internamente hacia las áreas responsables para su atención eficaz. Asimismo, la oficina impulsa el desarrollo de las iniciativas desde un enfoque transversal, garantizando la coherencia en la ejecución de las actuaciones y favoreciendo el intercambio de información relevante entre las distintas áreas, de acuerdo con los procedimientos establecidos.

4. 4.

Gobierno del riesgo

La línea de servicios de gobierno del riesgo tiene como objetivos principales **identificar y evaluar los riesgos tecnológicos y organizativos relacionados con la ciberseguridad** de la Comunidad Autónoma del País Vasco y desarrollar actuaciones orientadas a su gestión y mitigación, mediante el desarrollo y despliegue de un marco de gestión del riesgo que permita a las organizaciones obtener una visión clara y transversal de su nivel de riesgo, facilite la comprensión de la problemática en materia de ciberseguridad y la toma de decisiones informadas, así como la implementación de medidas de protección adecuadas, desarrollando iniciativas específicas que promuevan dicha protección.



Dentro de la línea de gobierno del riesgo, Cyberzaintza cuenta con los siguientes servicios:

Evaluación del riesgo	El servicio de evaluación del riesgo se basa en el framework de gestión del riesgo de Cyberzaintza, ofreciendo una visión integral y transversal de los riesgos de ciberseguridad en toda la Comunidad Autónoma del País Vasco. A través de este marco, se identifican los riesgos específicos que deben ser normalizados, asegurando una consideración y evaluación adecuadas de todos los riesgos relevantes. La función predominante de este servicio consiste en analizar tanto los riesgos tecnológicos como organizativos, priorizándolos según su impacto y probabilidad, y comunicando efectivamente dichos riesgos a las partes interesadas. Además, se implementa como un sistema dinámico que actualiza y mejora continuamente la medición para reflejar los cambios en el entorno de amenazas y las mejores prácticas en ciberseguridad.
Gestión del riesgo	El servicio de gestión del riesgo comprende la consideración del nivel de riesgo de cada entidad, de manera continua y teniendo en cuenta sus características particulares y el entorno en el que operan, y la determinación de las medidas de seguridad necesarias para su tratamiento, considerando tanto su posible mitigación como su monitorización continua y la gestión de excepciones. Contempla, así mismo, la definición y priorización de las acciones necesarias para tratar dichos riesgos y la planificación de proyectos específicos para coordinar estas acciones.
Oficina de armonización	El servicio de oficina de armonización incluye el desarrollo de marcos de buenas prácticas para la aplicación de los mecanismos de gestión de riesgos y la elaboración de guías para su aplicación, así como la elaboración de directrices para su aplicación por parte de las entidades. Asimismo, ofrece asistencia en la interpretación de todos los materiales desarrollados, y brinda apoyo en la adopción del resto de servicios de Cyberzaintza.
Gestión de proyectos especiales	El servicio de gestión de proyectos especiales ofrece soporte en la gestión de iniciativas específicas relacionadas con la ciberseguridad dentro del sector público en Euskadi. Asimismo, proporciona ayuda en la gestión de los riesgos vinculados a dichos proyectos y asistencia técnica en la contratación de servicios de ciberseguridad.

4. 5.

Inteligencia de amenazas

La línea de servicios de inteligencia de amenazas tiene como objetivo principal **proporcionar a las organizaciones información relevante y procesable sobre posibles amenazas** en el ámbito de la ciberseguridad. Esto les facilita anticiparse a ataques, tomar decisiones informadas y reforzar su protección.

Esta línea abarca diversos servicios de Cyberzaintza, enfocados en recopilar, analizar y compartir información sobre actividades maliciosas y amenazas. Entre estos servicios se incluyen:



Alerta temprana	El servicio de alerta temprana se centra en la vigilancia digital y monitorización continua. Utilizando un modelo de inteligencia avanzado, se analizan datos de multitud de fuentes para identificar potenciales riesgos e incidentes de ciberseguridad. Al detectar una posible amenaza, se emiten alertas tempranas acompañadas de recomendaciones específicas para prevenir verse afectado y responder de manera efectiva.
Intercambio de información sobre ciberamenazas	El servicio de intercambio de información sobre ciberamenazas facilita la colaboración entre diferentes organizaciones y entidades para compartir datos sobre ciberamenazas de manera ágil y efectiva. Utilizando plataformas especializadas, se recopila y distribuye información sobre indicadores de compromiso, tácticas, técnicas y procedimientos utilizados por los atacantes. Este intercambio de información permite a las organizaciones mejorar su capacidad de detección y respuesta.

4. 6.

Modelo de seguridad de Euskadi

La línea de servicios de modelo de Seguridad de Euskadi tiene como objetivo principal **establecer un marco integral de ciberseguridad** que sirva como base para garantizar un entorno digital seguro y resiliente frente a las ciberamenazas.

Dentro de la línea de modelo de Seguridad de Euskadi, Cyberzaintza cuenta con los siguientes servicios:



Acompañamiento y seguimiento en el despliegue del modelo de seguridad de Euskadi

El servicio de acompañamiento en el despliegue de CyberOrratz, el modelo de ciberseguridad de Euskadi, ofrece apoyo especializado a las entidades usuarias para facilitar la implantación progresiva del modelo. CyberOrratz es el marco común de referencia en ciberseguridad, elaborado y promovido por Cyberzaintza, y se concibe como un conjunto estructurado de principios, controles y criterios técnicos que integra políticas de seguridad, normas técnicas y medidas de protección, alineándose tanto con la normativa vigente como con las necesidades específicas de las administraciones públicas de Euskadi. A través de este servicio, la agencia impulsa la difusión, el conocimiento y la adopción del modelo, proporcionando acompañamiento, asistencia técnica, acciones formativas, guías prácticas y herramientas de apoyo, que facilitan una implantación coherente, homogénea y alineada de la ciberseguridad en el sector público vasco, respetando en todo caso las competencias de cada entidad.

4. 7.

Operaciones de seguridad (SOC)

La línea de servicios de SOC tiene como objetivo principal **proteger las infraestructuras tecnológicas de las organizaciones** mediante la monitorización continua, lo que reduce el tiempo de respuesta ante posibles incidentes de ciberseguridad.

Dentro de la línea de SOC, Cyberzaintza cuenta con los siguientes servicios:



SOC

El servicio de Centro de Operaciones de Seguridad (SOC) está destinado a la monitorización de eventos internos que ocurren dentro de las organizaciones con el fin de detectar y analizar actividades sospechosas en tiempo real. Este servicio permite a las organizaciones responder de manera ágil y eficaz ante potenciales incidentes de ciberseguridad.

Threat hunting

El servicio de threat hunting se centra en la identificación proactiva de amenazas dentro de los entornos corporativos. Su objetivo es detectar y mitigar amenazas desconocidas, previniendo así su impacto antes de que puedan materializarse.

4. 8.

Respuesta a incidentes (CSIRT)

El objetivo principal de la línea de servicios del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) es **asistir a las organizaciones en la gestión de sus incidentes de seguridad**. Con un enfoque integral, se pretende coordinar la respuesta ante incidentes que impacten a múltiples entidades y compartir información crucial para salvaguardar al resto.

Esta línea incluye una variedad de servicios ofrecidos por Cyberzaintza, diseñados para abordar diferentes aspectos de la respuesta a incidentes. Entre estos servicios se encuentran:



Asesoramiento

El servicio de asesoramiento proporciona recomendaciones generales sobre cómo actuar si se ha experimentado un incidente de seguridad informática. Asimismo, cuando es necesario, el equipo técnico especializado en respuesta a incidentes de Cyberzaintza implementa las acciones necesarias para evitar la propagación del incidente y alertar a la comunidad sobre la amenaza.

Coordinación

El servicio de coordinación de incidentes de ciberseguridad se activa cuando estos tienen un impacto múltiple y significativo en los diferentes públicos objetivos de Cyberzaintza. Su propósito es proporcionar asesoramiento técnico especializado y tomar medidas preventivas para evitar que el incidente afecte a otras entidades. Este servicio asegura una respuesta rápida y coordinada, minimizando el alcance y las consecuencias del incidente, garantizando que todas las partes involucradas estén informadas y alineadas en sus acciones.

DFIR

El servicio de análisis Forense Digital y Respuesta a Incidentes (DFIR) consiste en la adquisición remota y el análisis de evidencias digitales ante un incidente de seguridad, con el propósito de dar apoyo en la resolución del incidente.

Gestión de crisis

El servicio de gestión de crisis se encarga de coordinar un plan integral para todo el sector público en Euskadi, asegurando que todas las instituciones estén preparadas para gestionar una crisis derivada de un incidente de seguridad crítico de manera eficaz.

Takedown

El servicio de Takedown se refiere a las acciones que se realizan para retirar contenido malicioso o no autorizado de Internet.

Preparación para la respuesta a incidentes de ciberseguridad

El servicio de preparación para la respuesta a incidentes de ciberseguridad ayuda a las organizaciones a establecer procesos y capacidades preventivas, evalúa su madurez y propone mejoras para optimizar la respuesta ante incidentes.

4. 9.

Seguridad ofensiva

El objetivo principal de la línea de seguridad ofensiva es **identificar amenazas y vulnerabilidades en los sistemas de las organizaciones** antes de que lo haga un atacante, fortaleciendo así su capacidad defensiva frente a posibles ciberataques.

Dentro de la línea de seguridad ofensiva, Cyberzaintza cuenta con los siguientes servicios:



Auditoría técnica

El servicio de auditoría técnica abarca pruebas de penetración (pentesting), auditorías de aplicaciones, redes Wi-Fi y configuraciones, entre otros aspectos. Su objetivo es evaluar el nivel de protección e identificar potenciales aspectos de mejora.

EASM

El servicio de Evaluación de la Superficie de Ataque y Mitigación (EASM) consiste en analizar la superficie de exposición de las organizaciones, con el objetivo de determinar su nivel de riesgo tecnológico. A partir de esta evaluación, se proponen recomendaciones específicas que permitan mitigar los riesgos identificados. Además, el servicio no solo se enfoca en la protección inmediata, sino que también busca aumentar la resiliencia a largo plazo.

Red team

El servicio de Red team se enfoca en realizar simulaciones de ataques reales contra una organización. Este servicio facilita la identificación y corrección de vulnerabilidades en los sistemas y defensas, así como la evaluación de la efectividad de los equipos de protección.

4. 10.

Transferencia del conocimiento

La línea de servicios de transferencia del conocimiento tiene como objetivo principal **fomentar la especialización y el desarrollo de habilidades en ciberseguridad** entre diversos públicos, así como exportar operativas y casos de éxito a los diferentes públicos de Cyberzaintza. Además, se busca exportar maneras de proceder, documentación, clausulado, etc., de entidades con un nivel de madurez mayor a otras con un nivel de madurez menor, promoviendo así un intercambio de conocimientos y prácticas que eleve el estándar general de ciberseguridad.



Entrenamiento

El servicio de entrenamiento se centra en técnicas de operación y de coordinación de ejercicios de simulacros y pruebas de recuperación ante catástrofes. Esto incluye ciberejercicios tanto individuales como colectivos, que preparan a las organizaciones para gestionar crisis de manera eficaz.

Formación

El servicio de formación está diseñado para contribuir a la especialización en ciberseguridad de los distintos públicos objetivos de la agencia. Las capacitaciones pueden llevarse a cabo utilizando los canales establecidos o mediante métodos alternativos cuando se aborden temas específicos que no puedan ser tratados con los medios convencionales.

05.

Fichas de servicio

Para delimitar mejor su ámbito de actuación, se ha incluido una ficha descriptiva por cada servicio ofrecido a una entidad usuaria, a fin de recoger los aspectos básicos que los caracterizan.

5.1. Auditoría

- 5.1.1. Evaluación de la seguridad
- 5.1.2. OAT - Órgano de Auditoría Técnica
- 5.1.3. Supervisión de planes de continuidad

5.2. Concienciación

- 5.2.1. Concienciación Servicio
- 5.2.2. Campañas de phishing

5.3. Coordinación estratégica

- 5.3.1. Despliegue de la Estrategia de Ciberseguridad de Euskadi
- 5.3.2. Oficina de gestión de servicios

5.4. Gobierno del riesgo

- 5.4.1. Evaluación del riesgo
- 5.4.2. Gestión del riesgo
- 5.4.3. Oficina de armonización
- 5.4.4. Gestión de proyectos especiales

5.5. Inteligencia de amenazas

- 5.5.1. Alerta temprana
- 5.5.2. Intercambio de información sobre ciber amenazas

5.6. Modelo de seguridad de Euskadi

- 5.6.1. Acompañamiento y seguimiento en el despliegue del Modelo de Seguridad de Euskadi

5.7. Operaciones de seguridad (SOC)

- 5.7.1. SOC
- 5.7.2. Threat hunting

5.8. Respuesta a incidentes

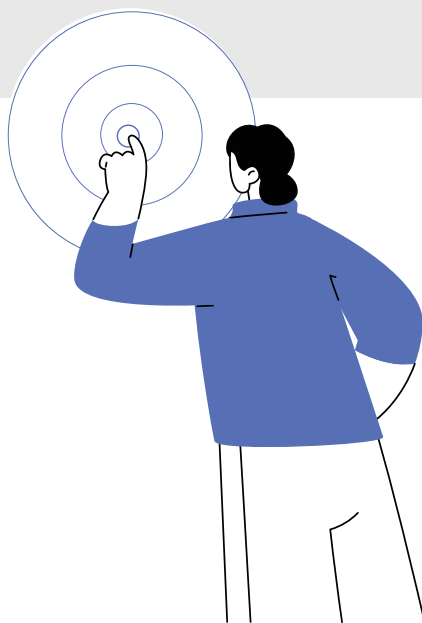
- 5.8.1. Asesoramiento Servicio
- 5.8.2. Coordinación
- 5.8.3. DFIR
- 5.8.4. Gestión de crisis
- 5.8.5. Takedown
- 5.8.6. Preparación para la respuesta a incidentes de ciberseguridad

5.9. Seguridad ofensiva

- 5.9.1. Auditoría técnica
- 5.9.2. EASM
- 5.9.3. Red team

5.10. Transferencia del conocimiento

- 5.10.1. Formación
- 5.10.2. Entrenamiento



5.1. Auditoría

5.1.1.

Evaluación de la seguridad



Línea de servicio
Auditoría

Puntos de contacto
evaluacion@cyberzaintza.eus

El servicio de evaluación de la seguridad se orienta a **revisar y asegurar que las organizaciones cumplan con las principales normativas de seguridad y marcos de referencia aplicables**. Este proceso incluye la evaluación de la implementación correcta de los controles establecidos, a través de evaluaciones periódicas que buscan identificar posibles áreas de mejora.

**Público destinatario**

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✓ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía

**Finalidad**

Permite disponer de una **visión objetiva** del grado de adecuación de la organización en materia de ciberseguridad, facilitando la toma de decisiones y la **priorización de actuaciones de mejora**.

**Características**

- Evaluación del grado de cumplimiento de las normativas de seguridad y marcos de referencia aplicables.
- Obtención de información estructurada a través de reuniones con las personas responsables de los procesos auditados.
- Evaluación in situ o en remoto de los controles de seguridad implementados. Sujeto a necesidad por la naturaleza del servicio a evaluar o normativa aplicable.
- Verificación de la correcta implementación de los controles establecidos.
- Propuesta y seguimiento de las acciones correctoras acordadas.

**Opciones del servicio****Evaluación CyberOrratz.**

Identificación y evaluación del grado de adecuación de los servicios, procesos y sistemas analizados **al modelo de seguridad CyberOrratz**, con informe de resultados y determinación de los niveles de cumplimiento correspondientes.

Evaluación normativa.

Identificación y evaluación del grado de adecuación de los servicios, procesos y sistemas analizados **al marco de ciberseguridad acordado**, con informe de resultados.

**Procedimiento para solicitar el servicio**

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

**Contribución del servicio a CyberOrratz**

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.



Aspecto del modelo que aborda.

Control**G3.4****Programa de auditoría y cumplimiento**

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.1.2. OAT - Órgano de Auditoría Técnica



Línea de servicio
Auditoría

Puntos de contacto
oat@cyberzaintza.eus

El servicio de Órgano de Auditoría Técnica se encarga de llevar a cabo **auditorías de conformidad con el Esquema Nacional de Seguridad** (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.) para la administración pública vasca, emitiendo y gestionando, de acuerdo con el reconocimiento emitido por el Centro Criptológico Nacional, los **certificados de conformidad** correspondientes.



Público destinatario

- ✓ Sector público vasco
- ✗ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

La entidad obtiene una **garantía objetiva e independiente** sobre el cumplimiento del Esquema Nacional de Seguridad, aportando seguridad jurídica y confianza en su nivel de ciberseguridad frente a órganos de control y partes interesadas.



Características

- Determinación del alcance a auditar y, en su caso, certificar.
- Determinación de la categoría de los sistemas o del Perfil de Cumplimiento Específico a considerar como criterio para evaluar la conformidad con el ENS.
- Planificación de la auditoría de conformidad.
- Desarrollo de la fase asíncrona de la auditoría y evaluación preliminar de las medidas de seguridad documentalmente soportadas.
- Desarrollo de la fase síncrona de la auditoría, en remoto o in situ dependiendo de la planificación acordada, y evaluación de las medidas de seguridad.
- Entrega del informe de auditoría.
- Evaluación, en su caso, del Plan de Acciones Correctivas ejecutado.
- Decisión, en su caso, de concesión del certificado.
- Desarrollo, en su caso, de la auditoría extraordinaria.



Opciones del servicio

Auditoría ENS según PCE.

Desarrollo de la auditoría de conformidad con el ENS (y emisión del certificado correspondiente, si procede) **de acuerdo con un Perfil de Cumplimiento Específico** seleccionado por el cliente.

Auditoría ENS según categoría.

Desarrollo de la **auditoría** de conformidad con el ENS (y emisión del certificado correspondiente, si procede) **de acuerdo con la categoría de los sistemas auditados** (básica, media o alta, según corresponda).



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.

1

2

3

4

5



Aspecto del modelo que aborda.

Control

G3.4

Programa de auditoría
y cumplimiento

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.1.3. Supervisión de planes de continuidad



Línea de servicio
Auditoría

Puntos de contacto
jarraipena@cyberzaintza.eus

El servicio de supervisión de planes de continuidad en materia de ciberseguridad se encarga de llevar a cabo el **seguimiento**, respecto de las organizaciones con obligaciones en materia de planes de autoprotección a las que les aplica la ORDEN de 7 de junio de 2024, del Vicelehendakari Primero y Consejero de Seguridad, por la que se regula la elaboración de planes de continuidad en materia de ciberseguridad para ciertas actividades sujetas a la norma vasca de autoprotección, de que dichas **organizaciones registran y mantienen** actualizada la información necesaria en relación a los **planes de continuidad en materia de ciberseguridad** que están obligadas a mantener.



Público destinatario

- ☐ Sector público vasco
- ☐ Empresas estratégicas
- ☒ Empresas con obligación en materia de autoprotección
- ☐ Otras empresas
- ☐ Ciudadanía



Finalidad

Permite a la entidad garantizar el cumplimiento continuado de sus obligaciones en materia de planes de continuidad en materia de ciberseguridad, **asegurando que la información requerida se encuentra registrada y supervisada de forma sistemática.**



Características

- Seguimiento de la obligación de registrar la información relativa a los planes de continuidad en materia de ciberseguridad.
- Evaluación de la información registrada en dicha materia.
- Supervisión de los cambios y actualizaciones sobre la información registrada.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

Para la tramitación de la información de ciberseguridad, una vez que la entidad haya aportado los datos de la actividad en el Registro de Autoprotección, debe cumplimentar el **formulario Ficha con datos específicos para la protección en ciberseguridad**.

Posteriormente se debe remitir el mismo a la Agencia Vasca de Ciberseguridad – Cyberzaintza a través del **Registro Electrónico General**.

Para más información se puede consultar la **“Guía de apoyo para la elaboración de un Plan de Continuidad en materia de Ciberseguridad”**.

Más información relativa a Planes de continuidad en materia de ciberseguridad en las siguientes **FAQs**.

5.2. Concienciación

5.2.1.
ConcienciaciónLínea de servicio
ConcienciaciónPuntos de contacto
csirt@cyberzaintza.eus

El servicio de concienciación consiste en la organización de **jornadas educativas** para reforzar el conocimiento y la cultura de ciberseguridad entre la ciudadanía y las organizaciones de Euskadi. Su propósito es **aumentar la conciencia sobre los diversos riesgos digitales** presentes en el mundo actual y proporcionar a las personas participantes las habilidades necesarias para utilizar internet y las nuevas tecnologías de manera más segura y responsable.

Este servicio se complementa con iniciativas específicas dirigidas a colectivos particulares, como profesionales de la ciberseguridad, personas mayores o menores de edad. Estas iniciativas incluyen la **elaboración de materiales específicos**, la organización de actividades recreativas o el diseño de campañas especializadas, entre otras.

**Público destinatario**

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✓ Empresas con obligación en materia de autoprotección
- ✓ Otras empresas
- ✓ Ciudadanía

**Características**

- Organización de actividades y jornadas educativas de concienciación orientadas a reforzar la cultura de ciberseguridad entre la ciudadanía y las organizaciones de Euskadi.
- Diseño, elaboración y difusión de contenidos formativos dirigidos a la promoción de buenas prácticas en el uso de internet y de las nuevas tecnologías.
- Desarrollo de iniciativas específicas adaptadas a colectivos concretos, tales como profesionales de la ciberseguridad, personas mayores o menores de edad.
- Organización de actividades divulgativas, recreativas o campañas especializadas, adaptadas a las características y necesidades de los distintos públicos objetivo.
- Actualización periódica de los contenidos y mensajes de concienciación, en función de la evolución de los riesgos digitales y de las tendencias emergentes.

**Finalidad**

La persona o entidad usuaria refuerza su nivel de concienciación en ciberseguridad, adquiriendo buenas prácticas y criterios básicos para un uso más seguro y responsable de las tecnologías digitales y reduciendo su exposición a riesgos digitales.

**Opciones del servicio****Desarrollo de materiales.**

Diseño y elaboración de **materiales de concienciación** en materia de ciberseguridad.

Impartición de sesiones de concienciación.

Organización de **jornadas y sesiones de concienciación** dirigidas a los diferentes públicos objetivo del servicio.

**Procedimiento para solicitar el servicio**

Los materiales de concienciación, las campañas y las acciones divulgativas, se ponen a disposición de los diferentes públicos a través de la web y las redes sociales de la Agencia.

La adscripción o participación en el resto de los elementos del servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

**Contribución del servicio a CyberOrratz**

Se recomienda para
todos los niveles de implantación.



Aspecto del modelo que aborda

Control**G1.6****Concienciación
y formación básica**

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.2.2. Campañas de phishing



Línea de servicio
Concienciación

Puntos de contacto
csirt@cyberzaintza.eus

El servicio de campañas de phishing realiza **ataques de phishing específicamente diseñados para evaluar y fortalecer la capacidad de una organización** para detectar y responder ante estas amenazas. Los resultados de estas campañas proporcionan información valiosa sobre las debilidades existentes, facilitando el **desarrollo de estrategias de capacitación** y mejora continua.



Público destinatario

- ☒ Sector público vasco
- ☒ Empresas estratégicas
- ☒ Empresas con obligación en materia de autoprotección
- ☒ Otras empresas
- ☒ Ciudadanía



Finalidad

Permite a la entidad usuaria **conocer su nivel real de exposición frente a ataques de phishing**, identificando debilidades y comportamientos de riesgo y disponiendo de una **base objetiva para reforzar la concienciación** y mejorar la capacidad de detección y respuesta de su organización.



Características

- Prestación del servicio por personal técnico especializado en el diseño y ejecución de campañas de phishing.
- Ejecución del servicio bajo demanda, conforme a los objetivos y alcance definidos por la organización solicitante.
- Configuración de campañas de phishing con distintos niveles de dificultad y realismo, adaptados al grado de madurez en ciberseguridad de la organización.
- Análisis de los resultados obtenidos durante la campaña, con identificación de debilidades y comportamientos de riesgo.
- Elaboración de informes de resultados orientados a evaluar la capacidad de detección y respuesta ante ataques de phishing y a apoyar la definición de acciones de mejora.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.



Aspecto del modelo que aborda

Control

G3.5

Phishing ético

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.3. Coordinación Estratégica

5.3.1.

Despliegue de la estrategia de ciberseguridad de Euskadi



Línea de servicio

Coordinación estratégica

Puntos de contacto

estrategia@cyberzaintza.eus

El servicio de despliegue de la estrategia de ciberseguridad de Euskadi consiste en **liderar y apoyar la elaboración, implementación y seguimiento de la Estrategia**, impulsando su correcta ejecución.

Para ello, Cyberzaintza **participa activamente en los órganos de gobierno definidos**, prestando apoyo técnico mediante la coordinación operativa y la asistencia técnica necesaria, así como mediante la evaluación y supervisión continuas del grado de avance de la Estrategia.

El servicio se presta a entidades que requieren acompañamiento y soporte en la implementación de la estrategia, facilitando la **alineación de sus iniciativas de ciberseguridad con el marco estratégico definido** y contribuyendo a la consecución de los objetivos establecidos.



Público destinatario

- ☒ Sector público vasco
- ☒ Empresas estratégicas
- ☒ Empresas con obligación en materia de autoprotección
- ☐ Otras empresas
- ☐ Ciudadanía



Finalidad

Permite a las entidades obtener acompañamiento especializado para alinear sus iniciativas de ciberseguridad con la estrategia de ciberseguridad de Euskadi, contribuyendo a una implantación coherente y alineada con los objetivos estratégicos comunes.



Características

- Liderazgo en la elaboración, revisión y seguimiento de la Estrategia de Ciberseguridad de Euskadi.
- Impulso de la correcta implementación de la Estrategia en el ámbito regional.
- Participación activa en los órganos de gobierno asociados a la estrategia.
- Prestación de apoyo técnico mediante coordinación operativa y seguimiento de acuerdos.
- Evaluación y supervisión continua del grado de avance de la estrategia.
- Impulso de la alineación de las iniciativas con los objetivos estratégicos definidos.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

5.3.2. Oficina de gestión de servicios



Línea de servicio
Coordinación estratégica

Puntos de contacto
zerbitzuak@cyberzaintza.eus

El servicio de oficina de gestión de servicios constituye el **canal único y centralizado de relación con las entidades** usuarias para la gestión de sus solicitudes vinculadas a Cyberzaintza, proporcionando acompañamiento y una atención integral, coordinada y alineada con sus necesidades específicas en materia de ciberseguridad.

Desde este servicio se realiza la **gestión, coordinación y seguimiento de las demandas recibidas**, identificando y analizando los requerimientos de los distintos públicos objetivo y sectores, y **canalizándolos internamente** hacia las áreas responsables para su atención eficaz.

Asimismo, la oficina impulsa el desarrollo de las iniciativas desde un enfoque transversal, garantizando la **coherencia en la ejecución de las actuaciones** y favoreciendo el intercambio de información relevante entre las distintas áreas, de acuerdo con los procedimientos establecidos.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

Proporciona a la entidad usuaria de un **canal único** de referencia y acompañamiento que le permite simplificar y ordenar la gestión de sus solicitudes, asegurando una **atención coordinada y alineada con sus necesidades en materia de ciberseguridad**.



Características

- Canal único y centralizado de relación con las entidades usuarias de Cyberzaintza.
- Provisión de un acceso ordenado y estructurado a los servicios de ciberseguridad disponibles.
- Gestión, coordinación y seguimiento integral de las solicitudes recibidas.
- Identificación y análisis de las necesidades de los distintos públicos objetivo y sectores.
- Canalización de las demandas hacia las áreas responsables para su atención eficaz.
- Garantía de coherencia en las actuaciones y fomento del intercambio de información entre áreas.



Opciones del servicio

Identificación.

Identificación de las necesidades en materia de ciberseguridad.

Identificación + Soporte.

Identificación de las necesidades en materia de ciberseguridad en Euskadi y **acompañamiento en la implementación**.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, a sí como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

5.4. Gobierno del riesgo

5.4.1.

Evaluación del riesgo



Línea de servicio
Gobierno del riesgo

Puntos de contacto
riesgos@cyberzaintza.eus

El servicio de evaluación del riesgo se basa en el **framework de gestión del riesgo de Cyberzaintza**, ofreciendo una visión integral y transversal de los riesgos de ciberseguridad en toda la Comunidad Autónoma del País Vasco. A través de este marco, se **identifican los riesgos específicos que deben ser normalizados**, asegurando una consideración y evaluación adecuadas de todos los riesgos relevantes. La función predominante de este servicio consiste en analizar tanto los riesgos tecnológicos como organizativos, **priorizándolos según su impacto y probabilidad, y comunicando efectivamente dichos riesgos** a las partes interesadas. Además, se implementa como un **sistema dinámico** que actualiza y mejora continuamente la medición para reflejar los cambios en el entorno de amenazas y las mejores prácticas en ciberseguridad.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Características

- Publicación y actualización del framework de gestión de riesgos de Cyberzaintza.
- Publicación de herramientas, librerías y catálogos para la aplicación del framework de gestión de riesgos de Cyberzaintza.
- Identificación y catalogación de los riesgos de ciberseguridad del público destinatario.
- Análisis de los riesgos de ciberseguridad identificados.
- Normalización y homogeneización de los diferentes análisis de riesgos de ciberseguridad.
- Evaluación de los resultados de los análisis de riesgos de ciberseguridad.
- Análisis y priorización de los resultados de las evaluaciones de los riesgos.
- Comunicación de los resultados de la evaluación y priorización de los riesgos de ciberseguridad.



Finalidad

La entidad obtiene una **visión objetiva, homogénea y priorizada de sus riesgos de ciberseguridad**, que le permite comprender su nivel de exposición, comparar riesgos de forma consistente y disponer de una **base común y actualizada para la toma de decisiones**.



Opciones del servicio

Soporte metodológico.

Habilitación de las herramientas y mecanismos necesarios para que los usuarios del servicio puedan **aplicar de manera eficaz el framework** de gestión del riesgo de Cyberzaintza.

Análisis del riesgo.

Ejecución de **las actividades de evaluación del riesgo** desde la identificación y catalogación de los riesgos hasta el análisis y priorización de los resultados, así como la **correspondiente comunicación**.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Se recomienda para
todos los niveles de implantación.



Aspecto del modelo que aborda

Control G2.9 Metodología de gestión de riesgos

Control G4.1 Gestión cuantitativa del riesgo

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.



5. 4. 2. Gestión del riesgo

Línea de servicio
Gobierno del riesgo

Puntos de contacto
riesgos@cyberzaintza.eus

El servicio de gestión del riesgo comprende la **consideración del nivel de riesgo de cada entidad**, de manera continua y teniendo en cuenta sus características particulares y el entorno en el que operan, y la **determinación de las medidas de seguridad necesarias para su tratamiento**, considerando tanto su posible mitigación como su monitorización continua y la gestión de excepciones. Contempla, así mismo, la definición y **priorización de las acciones** necesarias para tratar dichos riesgos y la planificación de proyectos específicos para coordinar estas acciones. Todo el proceso de seguimiento y gestión de riesgos se lleva a cabo **de acuerdo con el framework de gestión del riesgo de Cyberzaintza**, garantizando una metodología consistente y efectiva.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

La entidad obtiene acompañamiento experto para **convertir su nivel de riesgo en decisiones accionables**, priorizar medidas de seguridad y realizar seguimiento continuo para **reducir su exposición de forma sostenida**.



Características

- Evaluación de los niveles de riesgo de las organizaciones, teniendo en cuenta sus características y contexto.
- Determinación de las estrategias de gestión del riesgo, para cada una de las casuísticas que se consideren.
- Definición y priorización de acciones de tratamiento del riesgo, asociadas a las estrategias de gestión del riesgo que se determinen.
- Articulación de actuaciones de mitigación de riesgos, en aquellos casos que así se determine.
- Seguimiento de la evolución de los riesgos a lo largo de toda su gestión.
- Gestión de excepciones de seguridad, incluyendo su análisis, tratamiento y seguimiento conforme a los criterios establecidos en el framework de gestión de riesgos de Cyberzaintza.
- Diseño y planificación de proyectos específicos destinados a coordinar la ejecución de las acciones de mitigación del riesgo.
- Seguimiento continuo del estado de los riesgos y de las estrategias y acciones asociadas, de acuerdo con el framework de gestión del riesgo de Cyberzaintza.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.



Aspecto del modelo que aborda

Control

G4.1

Gestión cuantitativa del riesgo

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5. 4. 3.

Oficina de armonización



Línea de servicio
Gobierno del riesgo

Puntos de contacto
observatorio@cyberzaintza.eus

El servicio de oficina de armonización incluye el **desarrollo de marcos de buenas prácticas** para la aplicación de los mecanismos de gestión de riesgos y la **elaboración de guías para su aplicación**, así como la elaboración de directrices para su aplicación por parte de las entidades. Asimismo, ofrece **asistencia en la interpretación de todos los materiales desarrollados**, y brinda apoyo en la adopción del resto de servicios de Cyberzaintza.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✓ Empresas con obligación en materia de autoprotección
- ✓ Otras empresas
- ✗ Ciudadanía



Características

- Elaboración y publicación de marcos de buenas prácticas para la aplicación de medidas de seguridad.
- Elaboración y publicación de guías y manuales para la aplicación del framework de gestión de riesgos de Cyberzaintza.
- Elaboración y publicación de guías y manuales para la aplicación de medidas específicas de seguridad.
- Elaboración y publicación de materiales de apoyo para la implementación y articulación de las medidas de seguridad de las organizaciones.
- Asistencia a las organizaciones para la interpretación de los marcos, guías, manuales y materiales de apoyo publicados.
- Asistencia a las organizaciones para la correcta utilización y aplicación interna de los servicios de Cyberzaintza.



Finalidad

Permite a la entidad **avanzar con seguridad en la gestión del riesgo**, disponiendo de referencias claras, homogéneas y contrastadas que reducen la improvisación, aceleran la implantación de medidas de seguridad y mejoran la **coherencia y eficacia del conjunto de actuaciones** en ciberseguridad.



Opciones del servicio

Elaboración de materiales.

Desarrollo de **materiales específicos** a solicitud de necesidades específicas planteadas por las organizaciones.

Asistencia.

Atención a las solicitudes de **apoyo en la interpretación de los materiales** desarrollados y/o en la integración de los servicios de Cyberzaintza.



Procedimiento para solicitar el servicio

Todos los contenidos que se generan a través de este servicio (marcos, guías, manuales y diverso material de apoyo), se ponen a disposición de los diferentes públicos a través de la web y las redes sociales de la Agencia.

La adscripción o participación en el resto de los elementos del servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Se recomienda para
todos los niveles de implantación.



Aspecto del modelo que aborda

- | | | |
|---------|------|---|
| Control | G1.2 | Política de Seguridad de la Información |
| Control | G6.1 | Aplicación de mejores prácticas |

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.



5. 4. 4. Gestión de proyectos especiales

Línea de servicio
Gobierno del riesgo

Puntos de contacto
observatorio@cyberzaintza.eus

El servicio de gestión de proyectos especiales ofrece **soporte en la gestión de iniciativas específicas relacionadas con la ciberseguridad** para el público destinatario al que se dirige el servicio. Asimismo, proporciona ayuda en la **gestión de los riesgos vinculados a dichos proyectos** y asistencia técnica en la contratación de servicios de ciberseguridad.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✓ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

La entidad obtiene **apoyo experto para abordar proyectos complejos de ciberseguridad** con garantías, asegurando una adecuada definición de requisitos y una gestión eficaz de los riesgos, lo que le permite **reducir incertidumbres y avanzar con mayor seguridad**.



Características

- Determinación de requerimientos y exigencias de ciberseguridad en proyectos tipo de sistemas de información, así como de requerimientos y exigencias funcionales en proyectos tipo de ciberseguridad.
- Asesoramiento técnico especializado en los procesos de contratación de servicios y/o proyectos de ciberseguridad, desde el apoyo en la definición de necesidades y requisitos hasta la colaboración en la evaluación de propuestas.
- Colaboración en los procesos de verificación y validación de los requerimientos y exigencias de ciberseguridad aplicables a los proyectos desarrollados.
- Soporte a la gestión de iniciativas especiales y proyectos singulares especialmente complejos en el ámbito de la ciberseguridad.



Opciones del servicio

Fase de requerimiento.

Asistencia para la fase de determinación de requerimientos del proyecto.

Fase de contratación.

Asistencia para la fase de contratación de servicios y/o proyectos de ciberseguridad para el proyecto.

Proyectos singulares.

Colaboración en proyectos singulares e iniciativas especiales en el ámbito de la ciberseguridad.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, a sí como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

5.5. Inteligencia de Amenazas

5.5.1.
Alerta temprana

Línea de servicio
Inteligencia de amenazas

Puntos de contacto
csirt@cyberzaintza.eus

El servicio de alerta temprana se centra en la **vigilancia digital y monitorización continua**. Utilizando un **modelo de inteligencia avanzado**, se analizan datos de multitud de fuentes para identificar potenciales riesgos e incidentes de ciberseguridad. Al detectar una posible amenaza, **se emiten alertas tempranas acompañadas de recomendaciones** específicas para prevenir verse afectado y responder de manera efectiva.

**Público destinatario**

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✓ Empresas con obligación en materia de autoprotección
- ✓ Otras empresas
- ✓ Ciudadanía

**Finalidad**

La persona o entidad obtiene **información anticipada y contextualizada sobre amenazas relevantes**, acompañada de **recomendaciones operativas**, que le permite **prevenir incidentes**, reducir su exposición al riesgo y reforzar su capacidad de respuesta en materia de ciberseguridad.

**Características**

- Monitorización continua de fuentes de información relevantes para la detección temprana de amenazas de ciberseguridad.
- Análisis de datos procedentes de múltiples fuentes, mediante modelos de inteligencia orientados a la identificación de anomalías.
- Detección temprana de posibles amenazas de ciberseguridad, basada en el análisis correlacionado con la información monitorizada.
- Emisión de alertas tempranas acompañadas de recomendaciones específicas para la prevención y respuesta ante las amenazas identificadas.
- Actualización y mejora continua de los modelos de análisis, en función de la evolución del entorno de amenazas.

**Opciones del servicio**

N/A. Este servicio no cuenta con tipologías de servicio.

**Procedimiento para solicitar el servicio**

Se actualiza de manera continuada documentación sobre las ciberamenazas más recientes y se ponen a disposición de los diferentes públicos a través de la web y las redes sociales de la Agencia.

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, a sí como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

**Contribución del servicio a CyberOrratz**

Se recomienda para
todos los niveles de implantación.



Aspecto del modelo que aborda

Control**D2.5****Alerta temprana**

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.



5.5.2.

Intercambio de información sobre ciber amenazas

Línea de servicio

Inteligencia de amenazas

Puntos de contacto

csirt@cyberzaintza.eus

El servicio de Intercambio de información sobre ciberamenazas facilita la colaboración entre diferentes organizaciones y entidades para **compartir datos sobre ciberamenazas** de manera ágil y efectiva. Utilizando **plataformas especializadas**, se recopila y distribuye información sobre **indicadores de compromiso, tácticas, técnicas y procedimientos utilizados por los atacantes**. Este intercambio de información permite a las organizaciones mejorar su capacidad de detección y respuesta.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

La entidad accede a **inteligencia sobre ciberamenazas**, que le permite **mejorar de forma inmediata su detección y respuesta** ante incidentes de ciberseguridad, anticipar patrones de ataque reales y **reforzar su protección** mediante la colaboración activa con otras organizaciones.



Características

- Recopilación de información sobre ciberamenazas procedente de distintas organizaciones y fuentes colaborativas.
- Intercambio ágil y estructurado de información sobre ciberamenazas entre las entidades participantes.
- Compartición de indicadores de compromiso, tácticas, técnicas y procedimientos utilizados por actores maliciosos.
- Distribución de la información intercambiada de forma que facilite la mejora de la capacidad de detección y respuesta de las organizaciones.
- Uso de plataformas especializadas para garantizar un intercambio de información seguro y eficaz.



Opciones del servicio

Intercambio de información estándar.

Participación en el servicio de Intercambio de información sobre amenazas, con **acceso a la información compartida** por la comunidad y posibilidad de consulta.

Intercambio de información avanzado.

Participación activa en el servicio de Intercambio de información sobre amenazas, incluyendo la **aportación de información propia** y la **recepción de información priorizada y contextualizada**.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.

1

2

3

4

5

Aspecto del modelo que aborda

Control

D5.1

Threat Intelligence

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.6. Modelo de Seguridad de Euskadi

5.6.1.

Acompañamiento y seguimiento en el despliegue del modelo de seguridad de Euskadi



Línea de servicio

Modelo de Seguridad de Euskadi

Puntos de contacto

zerbitzuak@cyberzaintza.eus

El servicio de acompañamiento en el despliegue de **CyberOrratz**, el modelo de ciberseguridad de Euskadi, ofrece **apoyo especializado** a las entidades usuarias para **facilitar la implantación progresiva del modelo**.

CyberOrratz es el marco común de referencia en ciberseguridad, elaborado y promovido por Cyberzaintza, y se concibe como un **conjunto estructurado de principios, controles y criterios técnicos** que integra políticas de seguridad, normas técnicas y medidas de protección, alineándose tanto con la normativa vigente como con las necesidades específicas de las Administraciones públicas de Euskadi.

A través de este servicio, la Agencia impulsa la difusión, el conocimiento y la adopción del modelo, proporcionando **acompañamiento, asistencia técnica, acciones formativas, guías prácticas y herramientas de apoyo**, que facilitan una implantación coherente, homogénea y alineada de la ciberseguridad en el sector público vasco, respetando en todo caso las competencias de cada administración.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✓ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

La entidad gana visibilidad objetiva de su nivel de seguridad dentro de su segmento y dispone de una hoja de ruta clara para mejorar de forma gradual, lo que le permite **tomar decisiones basadas en evidencias** y priorizar con eficiencia las actuaciones e inversiones en ciberseguridad.



Características

- Provisión de un marco común de referencia basado en principios, controles y criterios técnicos de ciberseguridad, alineado con la normativa de ciberseguridad vigente y con las necesidades y particularidades del sector público vasco.
- Prestación de apoyo especializado para la implantación progresiva del Modelo de Ciberseguridad de Euskadi.
- Impulso de acciones de acompañamiento, asistencia técnica y formación dirigidas a las entidades usuarias.
- Elaboración y puesta a disposición de materiales tipo, guías y documentación de referencia para facilitar una implantación homogénea del Modelo.
- Evaluación y seguimiento continuo del grado de implantación del Modelo, con identificación de áreas de mejora.
- Promoción de una ciberseguridad coherente, homogénea y alineada entre las administraciones públicas.



Opciones del servicio

Acompañamiento básico.

Soporte en la implantación del Modelo de Seguridad de Euskadi mediante la **provisión de materiales tipo y orientación general** sobre su adopción.

Acompañamiento avanzado.

Soporte en la implantación del Modelo de Seguridad de Euskadi, incluyendo acompañamiento continuado, **seguimiento del grado de implantación y recomendaciones de mejora**.

Acompañamiento integral.

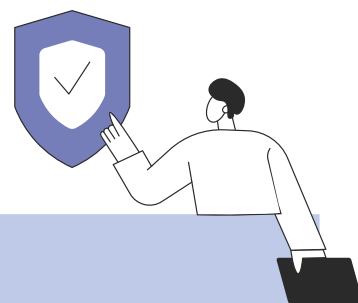
Soporte completo en la implantación del Modelo de Seguridad de Euskadi, incluyendo **acompañamiento continuado, seguimiento, evaluación periódica y apoyo en la mejora continua** del Modelo.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, a sí como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

5.7. Operaciones de seguridad (SOC)

5.7.1.
SOC

Línea de servicio

Operaciones de seguridad (SOC)

Puntos de contacto

csirt@cyberzaintza.eus

El servicio de Centro de Operaciones de Seguridad (SOC) está destinado a la **monitorización de los eventos** internos que ocurren dentro de las organizaciones con el fin de **detectar y analizar actividades sospechosas en tiempo real**. Este servicio permite a las organizaciones **responder de manera ágil y eficaz** ante potenciales incidentes de ciberseguridad.

**Público destinatario**

- ☒ Sector público vasco
- ☐ Empresas estratégicas
- ☐ Empresas con obligación en materia de autoprotección
- ☐ Otras empresas
- ☐ Ciudadanía

**Características**

- Monitorización continua de los eventos de seguridad generados en los sistemas de la organización.
- Detección y análisis en tiempo real de actividades sospechosas y posibles incidentes de ciberseguridad.
- Correlación y análisis de eventos de seguridad para identificar comportamientos anómalos.
- Clasificación y priorización de los incidentes de seguridad detectados en función de su criticidad.
- Comunicación de alertas e información relevante a las organizaciones para facilitar una respuesta ágil y eficaz ante los incidentes.

**Finalidad**

Permite a la entidad obtener **vigilancia continua y análisis en tiempo real de su entorno digital**, lo que le permite detectar de forma temprana actividades sospechosas, reducir el tiempo de respuesta ante incidentes y **mejorar de manera significativa su capacidad de reacción y resiliencia operativa** frente a amenazas de ciberseguridad.

**Opciones del servicio**

N/A. Este servicio no cuenta con tipologías de servicio.

**Procedimiento para solicitar el servicio**

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

**Contribución del servicio a CyberOrratz**

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.

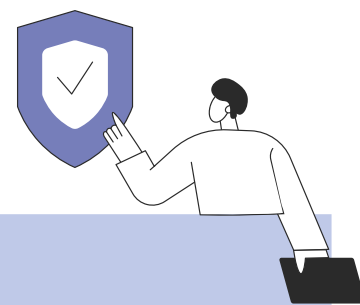


Aspecto del modelo que aborda

Control**D3.4****SOC perimetral**

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.7.2. Threat hunting



Línea de servicio
Operaciones de seguridad (SOC)

Puntos de contacto
csirt@cyberzaintza.eus

El servicio de Threat hunting se centra en la **identificación proactiva de amenazas** dentro de los entornos corporativos. Su objetivo es **detectar y mitigar amenazas desconocidas**, previniendo así su impacto antes de que puedan materializarse.



Público destinatario

- ✓ Sector público vasco
- ✗ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

Permite a la entidad elevar su nivel de protección mediante la **identificación proactiva de amenazas avanzadas y no visibles**, reduciendo el riesgo de incidentes críticos y **fortaleciendo su capacidad defensiva** gracias a análisis especializados y recomendaciones expertas.



Características

- Búsqueda proactiva de amenazas de ciberseguridad en los entornos de la organización, sin depender exclusivamente de alertas predefinidas.
- Análisis avanzado de datos y eventos de seguridad orientado a la identificación de comportamientos anómalos y amenazas no conocidas.
- Desarrollo de hipótesis de búsqueda basadas en técnicas, tácticas y procedimientos utilizados por actores maliciosos.
- Identificación y validación de posibles amenazas detectadas durante los procesos de hunting.
- Comunicación de los hallazgos obtenidos, incluyendo recomendaciones para la mitigación y prevención de las amenazas identificadas.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.



Aspecto del modelo que aborda

Control

D5.3

Threat hunting

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.8. Respuesta a incidentes (CSIRT)

5.8.1.
Asesoramiento

Línea de servicio

Respuesta a incidentes (CSIRT)

Puntos de contacto

incidencias@cyberzaintza.eus

El servicio de asesoramiento proporciona **recomendaciones generales sobre cómo actuar si se ha experimentado un incidente de seguridad informática**. Asimismo, cuando es necesario, el equipo técnico especializado en respuesta a incidentes de Cyberzaintza **implementa las acciones necesarias para evitar la propagación del incidente y alertar a la comunidad sobre la amenaza**.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✓ Empresas con obligación en materia de autoprotección
- ✓ Otras empresas
- ✓ Ciudadanía



Finalidad

La persona o entidad obtiene orientación para la gestión inicial del incidente de ciberseguridad, con recomendaciones claras de contención, respuesta y prevención que permiten reducir su impacto y evitar su propagación.



Características

- Asesoramiento a las organizaciones en metodologías de actuación ante incidentes de seguridad informática, proporcionando recomendaciones generales de contención y respuesta.
- Análisis inicial del incidente comunicado, con el fin de orientar adecuadamente las acciones a realizar.
- Apoyo técnico especializado para evitar la propagación del incidente y reducir su impacto, cuando la naturaleza del incidente lo requiere.
- Emisión de recomendaciones de seguridad derivadas de los incidentes gestionados, orientadas a prevenir situaciones similares en el futuro.
- Comunicación y alerta a la comunidad sobre amenazas relevantes, cuando el incidente pueda tener un impacto más amplio.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Se recomienda para todos los niveles de implantación.



Aspecto del modelo que aborda

Control

R2.4

CSIRT

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5. 8. 2. Coordinación



Línea de servicio

Respuesta a incidentes (CSIRT)

Puntos de contacto

incidencias@cyberzaintza.eus

El servicio de coordinación de incidentes de ciberseguridad se **activa cuando** estos tienen un **impacto múltiple y significativo** en los diferentes públicos objetivo de Cyberzaintza. Su propósito es **proporcionar asesoramiento técnico especializado y tomar medidas preventivas** para evitar que el incidente afecte a otras entidades. Este servicio asegura una respuesta rápida y coordinada, **minimizando el alcance y las consecuencias del incidente**, y garantizando que todas las partes involucradas estén informadas y alineadas en sus acciones.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

Proporciona a la entidad una **respuesta coordinada y experta ante incidentes de alto impacto**, permitiéndole actuar con rapidez, **contener la propagación del incidente**, reducir sus consecuencias y **proteger al conjunto del ecosistema**, mediante una comunicación clara y una alineación efectiva entre los actores implicados.



Características

- Activación del servicio ante incidentes de ciberseguridad con impacto múltiple y significativo en los distintos públicos objetivo de Cyberzaintza.
- Coordinación de la respuesta entre las entidades y actores implicados, con el fin de garantizar una actuación rápida y eficaz.
- Asesoramiento técnico especializado para apoyar la toma de decisiones durante la gestión del incidente.
- Definición y promoción de medidas preventivas orientadas a evitar la propagación del incidente a otras entidades.
- Comunicación estructurada y continua entre las partes implicadas, garantizando que la información relevante se comparta de forma oportuna.
- Seguimiento de la evolución del incidente hasta su estabilización, desde una perspectiva de coordinación y supervisión.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.



Aspecto del modelo que aborda

Control

R4.2

Gestión integrada de ciberincidentes

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.8.3.
DFIR

Línea de servicio

Respuesta a incidentes (CSIRT)

Puntos de contacto

incidencias@cyberzaintza.eus

El servicio de Análisis Forense Digital y Respuesta a Incidentes (DFIR) consiste en la **adquisición remota y el análisis de evidencias digitales ante un incidente de seguridad**, con el propósito de dar apoyo en la resolución del incidente.

**Público destinatario**

- ✓ Sector público vasco
- ✗ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía

**Finalidad**

Permite a la entidad disponer de **apoyo especializado para analizar en profundidad un incidente de seguridad, identificar con su origen, alcance y causas, y resolverlo con garantías, facilitando la recuperación y la implantación de medidas correctoras que refuercen su protección futura.**

**Características**

- Adquisición de evidencias digitales relacionadas con incidentes de seguridad informática.
- Análisis forense de las evidencias digitales adquiridas, orientado a identificar el origen, alcance y causas del incidente.
- Apoyo técnico especializado a las organizaciones en la resolución del incidente.
- Asistencia técnica en la recuperación.
- Elaboración de conclusiones técnicas que contribuyan a la resolución del incidente y a la adopción de medidas correctoras.

**Opciones del servicio**

N/A. Este servicio no cuenta con tipologías de servicio.

**Procedimiento para solicitar el servicio**

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

**Contribución del servicio a CyberOrratz**

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.

1

2

3

4

5



Aspecto del modelo que aborda

Control**R3.3**

DFIR

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.8.4. Gestión de crisis



Línea de servicio

Respuesta a incidentes (CSIRT)

Puntos de contacto

incidencias@cyberzaintza.eus

El servicio de gestión de crisis se encarga de **coordinar un plan integral para todo el sector público en Euskadi**, asegurando que todas las instituciones estén preparadas para gestionar una crisis derivada de un incidente de seguridad crítico de manera eficaz.

Asimismo, ofrece **soporte continuo a entidades estratégicas en la gestión de crisis**, asegurando que dispongan del apoyo necesario para afrontar y mitigar los efectos del incidente que cause dicha crisis.



Público destinatario

- ☒ Sector público vasco
- ☒ Empresas estratégicas
- ☒ Empresas con obligación en materia de autoprotección
- ☒ Otras empresas
- ☒ Ciudadanía



Finalidad

Proporciona a la entidad coordinación y apoyo estratégico **para gestionar con eficacia una crisis de ciberseguridad**, minimizando su impacto y asegurando una respuesta alineada en todo el sector público.



Características

- Definición y coordinación de un plan integral de gestión de crisis en materia de ciberseguridad para el conjunto del sector público en Euskadi.
- Apoyo a las instituciones públicas para garantizar su preparación ante crisis derivadas de incidentes de seguridad críticos.
- Coordinación estratégica de los distintos actores implicados durante la gestión de la crisis, asegurando una actuación alineada y coherente.
- Soporte continuado a entidades estratégicas durante la gestión de la crisis, facilitando la toma de decisiones y la mitigación de los efectos del incidente.
- Seguimiento de la evolución de la crisis desde una perspectiva estratégica, hasta su estabilización.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.



Aspecto del modelo que aborda

Control

C4.1

Plan de continuidad y gestión de crisis

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.8.5. Takedown



Línea de servicio
Respuesta a incidentes (CSIRT)

Puntos de contacto
csirt@cyberzaintza.eus

El servicio de Takedown se refiere a las acciones que se realizan para retirar contenido malicioso o no autorizado de internet.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✓ Empresas con obligación en materia de autoprotección
- ✓ Otras empresas
- ✓ Ciudadanía



Finalidad

Permite a la persona o entidad solicitar la eliminación de contenidos maliciosos de Internet, reduciendo su impacto y reforzando la protección de la organización y de la ciudadanía.



Características

- Identificación de contenidos maliciosos o no autorizados que puedan suponer un riesgo para las organizaciones o la ciudadanía.
- Análisis preliminar del contenido detectado para determinar la viabilidad de las acciones de retirada.
- Gestión de solicitudes de retirada de contenidos maliciosos o no autorizados ante los proveedores de servicios, plataformas o entidades responsables.
- Seguimiento de las acciones de retirada hasta su resolución o cierre.
- Comunicación a las partes interesadas sobre el estado y resultado de las acciones de Takedown realizadas.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Se recomienda para
todos los niveles de implantación.



Aspecto del modelo que aborda

Control

R2.4

CSIRT

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5. 8. 6.

Preparación para la respuesta
a incidentes de ciberseguridad

Línea de servicio

Respuesta a incidentes (CSIRT)

Puntos de contacto

csirt@cyberzaintza.eus

El servicio de preparación para la respuesta a incidentes de ciberseguridad se centra en la fase preventiva, con el objetivo de **ayudar a las entidades a definir los procesos, procedimientos y capacidades necesarias para responder de manera eficaz y coordinada ante incidentes de seguridad**. Asimismo, se evalúa el grado de madurez de la organización para identificar áreas de mejora y fortalecer su capacidad de respuesta.

**Público destinatario**

- ✓ Sector público vasco
- ✗ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía

**Finalidad**

Permite a la entidad **reforzar su preparación frente a posibles incidentes de ciberseguridad**, disponiendo de **procesos, procedimientos y roles** claramente definidos que le permiten responder de manera eficaz y coordinada.

**Características**

- Evaluación del nivel de madurez de la organización en materia de respuesta a incidentes de ciberseguridad, identificando brechas de capacidad y áreas de mejora.
- Diseño y desarrollo de planes de respuesta a incidentes, definiendo roles, responsabilidades, procedimientos de actuación y mecanismos de coordinación.
- Definición de procedimientos operativos y guías de actuación para facilitar una respuesta ágil y consistente ante incidentes de ciberseguridad.
- Alineación de los planes y procedimientos con los marcos normativos y regulatorios aplicables, así como con las buenas prácticas en materia de ciberseguridad.

**Opciones del servicio**

N/A. Este servicio no cuenta con tipologías de servicio.

**Procedimiento para solicitar el servicio**

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

**Contribución del servicio a CyberOrratz**

Se recomienda para
todos los niveles de implantación.



Aspecto del modelo que aborda

Control

G2.3**Gestor de incidentes**

Control

R2.1**Procedimiento de respuesta a ciberincidentes**

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.9. Seguridad Ofensiva

5.9.1.
Auditoría técnica

Línea de servicio
Seguridad ofensiva

Puntos de contacto
csirt@cyberzaintza.eus

El servicio de auditoría técnica abarca **distintos tipos de pruebas**, como pruebas de penetración (pentesting), auditorías de aplicaciones, redes Wi-Fi y configuraciones, entre otros aspectos. Su objetivo es **evaluar el nivel de protección e identificar potenciales aspectos de mejora**.

**Público destinatario**

- ✓ Sector público vasco
- ✗ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía

**Características**

- Evaluación técnica del nivel de seguridad de sistemas, aplicaciones y comunicaciones mediante la realización de pruebas controladas.
- Identificación de vulnerabilidades técnicas, debilidades de configuración y posibles vectores de ataque.
- Ejecución de pruebas de seguridad sobre distintos activos, tales como aplicaciones, redes inalámbricas y configuraciones de sistemas.
- Análisis del impacto potencial de las vulnerabilidades identificadas en el contexto de la organización.
- Elaboración de informes técnicos con los resultados de la auditoría, incluyendo recomendaciones orientadas a la mejora del nivel de protección.

**Finalidad**

La entidad obtiene una **evaluación técnica objetiva** de su nivel de seguridad, identificando vulnerabilidades y debilidades de configuración mediante pruebas controladas, lo que le permite **anticiparse a posibles ataques** y reforzar la protección de sus activos digitales.

**Opciones del servicio**

N/A. Este servicio no cuenta con tipologías de servicio.

**Procedimiento para solicitar el servicio**

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

**Contribución del servicio a CyberOrratz**

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.

1

2

3

4

5



Aspecto del modelo que aborda

Control D3.3 Pentesting externo

Control D4.3 Pentesting interno

Control D5.2 Auditorías de código fuente

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.9.2.
EASM

Línea de servicio
Seguridad ofensiva

Puntos de contacto
csirt@cyberzaintza.eus

El servicio de Evaluación de la Superficie de Ataque y Mitigación (EASM) consiste en **analizar la superficie de exposición** de las organizaciones, con el objetivo de **determinar su nivel de riesgo tecnológico**. A partir de esta evaluación, se **proponen recomendaciones específicas** que permitan mitigar los riesgos identificados. Además, el servicio no solo se enfoca en la protección inmediata, sino que también busca aumentar la **resiliencia a largo plazo**.

**Público destinatario**

- ✓ Sector público vasco
- ✗ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía

**Finalidad**

Permite a la entidad obtener una **visión clara de su exposición en internet**, identificando y priorizando riesgos visibles desde el exterior para **reducir su superficie de ataque y fortalecer su resiliencia tecnológica a largo plazo**.

**Características**

- Identificación y análisis de los activos expuestos en internet que conforman la superficie de ataque de la organización.
- Evaluación del nivel de riesgo tecnológico asociado a la superficie de exposición identificada.
- Detección de configuraciones inseguras, servicios expuestos y posibles debilidades visibles desde el exterior.
- Priorización de los riesgos identificados en función de su criticidad y potencial impacto.
- Elaboración de recomendaciones específicas orientadas a la mitigación de los riesgos detectados.
- Contribución a la mejora de la resiliencia a largo plazo de la organización mediante la reducción de su superficie de ataque.

**Opciones del servicio**

N/A. Este servicio no cuenta con tipologías de servicio.

**Procedimiento para solicitar el servicio**

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.

**Contribución del servicio a CyberOrratz**

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.



Aspecto del modelo que aborda

Control **D3.3** **Pentesting externo**

Control **I3.3** **Identificación de vulnerabilidades**

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.9.3. Red team



Línea de servicio
Seguridad ofensiva

Puntos de contacto
csirt@cyberzaintza.eus

El servicio de Red team se enfoca en realizar **simulaciones de ataques reales** contra una organización. Este servicio facilita la identificación y corrección de vulnerabilidades en los sistemas y defensas, así como la **evaluación de la efectividad de los equipos de protección**.



Público destinatario

- ✓ Sector público vasco
- ✗ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

Permite a la entidad **comprobar cómo resistiría ante un ataque real**, obteniendo una visión clara de la eficacia de sus defensas y equipos, lo que le permite **reducir riesgos críticos**, mejorar la toma de decisiones y **reforzar su capacidad de respuesta** antes de que ocurra un incidente.



Características

- Simulación de ataques reales contra la organización, replicando el comportamiento de actores maliciosos en escenarios controlados.
- Evaluación de la eficacia de las defensas técnicas, organizativas y procedimentales de la organización frente a ataques avanzados.
- Identificación de debilidades en los sistemas, procesos y capacidades de detección y respuesta.
- Análisis del nivel de preparación y reacción de los equipos de protección ante los escenarios simulados.
- Elaboración de informes con los resultados de las simulaciones, incluyendo recomendaciones orientadas a la mejora de las capacidades defensivas.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Nivel de implantación recomendado para asegurar la correcta aplicación del servicio.

1

2

3

4

5



Aspecto del modelo que aborda

Control

D6.1

Red Team

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.10. Transferencia del conocimiento

5.10.1.
Formación

Línea de servicio

Transferencia del conocimiento

Puntos de contacto

csirt@cyberzaintza.eus

El servicio de Formación está diseñado para contribuir a la **especialización en ciberseguridad** de los distintos públicos objetivos de la Agencia. Las capacitaciones pueden llevarse a cabo **utilizando los canales establecidos o mediante métodos alternativos** cuando se aborden temas específicos que no puedan ser tratados con los medios convencionales.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

Permite a la entidad dotar a su personal de criterio y visión en materia de ciberseguridad, asegurando que los equipos clave cuentan con conocimientos alineados con su responsabilidad, lo que reduce el riesgo organizativo y refuerza la protección global de la organización.



Características

- Formaciones especializadas en ciberseguridad, con contenidos adaptados al nivel de conocimiento, rol y necesidades específicas de los distintos públicos objetivo.
- Puesta a disposición de los participantes de materiales y contenidos formativos necesarios para la realización de la formación.
- Actualización continua de los contenidos formativos, garantizando su alineación con las mejores prácticas, la evolución de las amenazas, la normativa vigente y los estándares de referencia en materia de ciberseguridad.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del punto de contacto designado, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Se recomienda para
todos los niveles de implantación.



Aspecto del modelo que aborda

Control

G1.6

Concienciación y
formación básica

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.

5.10.2. Entrenamiento



Línea de servicio

Transferencia del conocimiento

Puntos de contacto

csirt@cyberzaintza.eus

El servicio de entrenamiento se centra en **técnicas de operación y de coordinación de ejercicios de simulacros** y pruebas de recuperación ante catástrofes. Esto incluye ciberejercicios tanto individuales como colectivos, que preparan a las organizaciones para **gestionar crisis de manera eficaz**.



Público destinatario

- ✓ Sector público vasco
- ✓ Empresas estratégicas
- ✗ Empresas con obligación en materia de autoprotección
- ✗ Otras empresas
- ✗ Ciudadanía



Finalidad

Permite a la entidad **poner a prueba y fortalecer su capacidad real de gestión de crisis**, asegurando que sus equipos actúan de forma coordinada y eficaz ante escenarios críticos, identificando mejoras clave y **reforzando la continuidad y resiliencia operativa** antes de que se produzca una situación real.



Características

- Coordinación de ejercicios de simulacro y pruebas de recuperación ante catástrofes, tanto de carácter individual como colectivo.
- Ejecución de ejercicios de simulacro y pruebas de recuperación ante catástrofes, orientados a evaluar la capacidad de respuesta de las organizaciones ante situaciones de crisis.
- Apoyo en la identificación y gestión de mejoras aplicables a los procedimientos y capacidades de respuesta ante situaciones de crisis, a partir de los resultados de los ejercicios realizados.



Opciones del servicio

N/A. Este servicio no cuenta con tipologías de servicio.



Procedimiento para solicitar el servicio

La adscripción o participación en el servicio estará condicionada a su solicitud y gestión a través del **punto de contacto designado**, así como a la determinación de un interlocutor por parte del solicitante que garantice la posibilidad de prestación efectiva del servicio.



Contribución del servicio a CyberOrratz

Se recomienda para
todos los niveles de implantación.



Aspecto del modelo que aborda

Control

R2.1

Procedimiento de respuesta a ciberincidentes

Este servicio proporciona el soporte metodológico necesario para la implantación y refuerzo de este control, asegurando su correcta aplicación en el contexto de la entidad.



Sarean ere, auzolana.
Por ti hacemos red.

Información general:
945 236 636
info@cyberzaintza.eus



www.ciberseguridad.euskadi.eus

EUSKO JAURLARITZA



GOBIERNO VASCO