



Marco de referencia de Ciberseguridad y Gestión Avanzada



EUSKO JAURLARITZA
GOBIERNO VASCO

EKONOMIAAREN GARAPEN
ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO
ECONÓMICO E INFRAESTRUCTURAS

Índice

1. BCSC
2. Marco de referencia
3. Experiencia piloto

1

BCSC

Contexto

Aplicar Ciberseguridad es innovar en la gestión de riesgos corporativos y un ejercicio de responsabilidad.



Cada vez más conectados



No es “un tema informático”



Todos somos visibles



Hay actividades más importantes



Los clientes lo van a exigir

Primeros pasos

La aplicación de medidas no termina con la implantación, es necesario gestionar y mantener la protección.



Identificación de un socio capacitado



Autodiagnóstico



Controles tácticos



Diseño de perímetros



Puesta en marcha del Plan

Somos

Respuesta de un gobierno responsable para:

- Mantener la capacidad competitiva e innovadora de la industria vasca.
- Promover una sociedad con competencias digitales.

No somos

- Competidor de la industria de Ciberseguridad.
- Invasor de la infraestructura interna de las organizaciones.
- Agente duplicador de servicios ya disponibles sufragados con fondos públicos.

Somos SPRI: Nuestra prioridad son las empresas.

Misión

- Promover una cultura de la Ciberseguridad.
- Dinamizar la actividad económica.
- Fortalecer el sector profesional.

Visión

- Euskadi como referente internacional.
- Punto de encuentro entre oferentes y demandantes.
- Liderar iniciativas de colaboración público-privadas.

El Basque Cybersecurity Centre es una iniciativa transversal impulsada por cuatro Departamentos del Gobierno Vasco para alinear todas las actividades relacionadas con la Ciberseguridad en Euskadi.

Servicios CSIRT



- Avisos: Información práctica relevante que facilite la prevención, protección y respuesta ante incidentes de seguridad
- Alertas sobre campañas o eventos de impacto significativo.

Número de teléfono gratuito:

900 104 891

Correo electrónico:

incidencias @ bcsc.eus

arazoak @ bcsc.eus

Para empresas de industria manufacturera

Programa de Ayuda

Catálogo de ciberseguridad

Buscador de empresas



Buscador de soluciones



Publicaciones

↓ [Libro blanco](#) | ↓ [Taxonomía](#)

Alta / Modificación

Para dar de alta o modificar la información de tu empresa, envía un email a info@bcsc.eus

Más de 100 organizaciones ofrecen soluciones en Euskadi

Charlas de sensibilización a asociaciones

El objetivo principal de estas jornadas es concienciar acerca de los riesgos más habituales en el ámbito de la ciberseguridad a los que se enfrentan las empresas del mundo OT y fomentar que estas apliquen medidas de ciberseguridad para que estén más protegidas y, por tanto, menos expuestas a las amenazas existentes. De igual modo, la aplicación de este tipo de tecnologías permitirá tener un valor añadido de cara a mantener la capacidad competitiva e innovadora de Euskadi en los diferentes mercados internacionales

El contenido de la jornada puede incluir uno o varios de los módulos en función de las necesidades de cada organización.

- Introducción a la ciberseguridad
- Ciberseguridad en la oficina
- Ciberseguridad en la planta
- Ciberseguridad en los departamentos de informática e ingeniería
- Gestión de la ciberseguridad

Se pueden solicitar al email de contacto **sensibilizacion@bcsc.eus**

Invertir en concienciación y capacitación es invertir en el futuro del sector industrial.

Objetivos:

- Conocer cuáles son las amenazas actuales en ciberseguridad
- Ser capaz de identificar los riesgos existentes sobre nuestra empresa
- Identificar los pasos a seguir para una gestión óptima de la ciberseguridad

Dirigido a: Gerentes, directivos, responsables de área o negocio

Contenido :

Son jornadas de día completo desde las 9:00 hasta las 19:00 h.

- ¿Qué es esto de la ciberseguridad? ¿Debo estar realmente preocupado? Pasado, presente y futuro de las amenazas
- Cómo actúa un posible atacante: demostración práctica de un ciberataque
- ¿Qué otras amenazas a la seguridad existen? Existen amenazas además de los cibercriminales y suelen ser más habituales de lo que pensamos
- Ciberseguridad en entornos industriales: el nuevo campo de batalla
- El análisis de riesgos
- Aspectos legales de la ciberseguridad
- Decálogo de ciberseguridad para la empresa: qué 10 pautas debo seguir para garantizar la correcta gestión de la ciberseguridad en mi empresa
- Sesión práctica: protejamos nuestro negocio

El Centro Vasco de Ciberseguridad (BCSC) pone a disposición de las empresas establecidas en Euskadi, de manera **gratuita**, el documento "Mapa Normativo de la Ciberseguridad Industrial", elaborado por el Centro de Ciberseguridad Industrial (CCI).

- Siendo sus destinatarios principales operadores industriales, ingenieros, consultores, empresas tecnológicas o bufetes de abogados, para solicitar una copia del documento, los interesados solo tienen que enviar, desde su email corporativo, un correo electrónico a la dirección info@bcsc.eus

MAPA NORMATIVO DE LA CIBERSEGURIDAD INDUSTRIAL

Basque Industry 4.0.: 20-21 Noviembre, BEC



El evento de referencia en Euskadi alrededor de la
4ª revolución industrial y la ciberseguridad.

2

Marco de referencia

Desarrollar un **marco de referencia** para la gestión de la **ciberseguridad** en organizaciones y empresas, basado en el Modelo de Gestión Avanzada (MGA) patrocinado por Euskalit.

Modelo de Gestión Avanzada (MGA)



- Seis elementos fundamentales de la gestión organizativa y empresarial
- Sirven de base para agrupar recomendaciones generales.
- Busca estructurar la competitividad de las organizaciones.

MGA con énfasis en Ciberseguridad



- Sobre el MGA se definirá un catálogo de ejemplos de buenas prácticas en ciberseguridad, para cada uno de los elementos fundamentales del MGA.
- El marco se completará con un glosario en donde se listarán las palabras y las denominaciones técnicas que se utilicen en la descripción de las buenas prácticas.

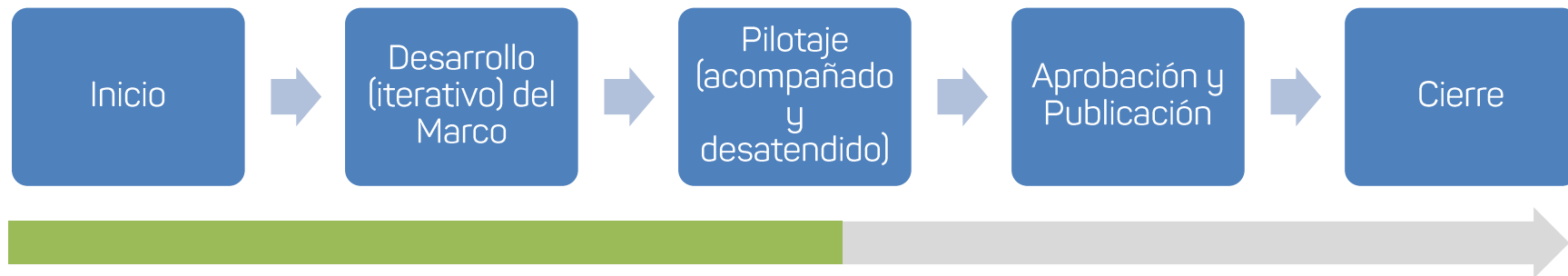
Equipo de Proyecto



KUDEAKETA AURRERATUA
EUSKALIT
GESTIÓN AVANZADA



Cronograma del Proyecto



Contenido del Marco

1. Introducción

2. Cómo utilizar el marco

3. Marco para la Gestión
de la Ciberseguridad

4. Glosario

- Recopilar y analizar la información necesaria para integrar aspectos de ciberseguridad dentro de la estrategia de la empresa.
- Gestionar las amenazas y los riesgos asociados a la ciberseguridad para planificar e implementar medidas acordes a los recursos de la organización y la capacidad de respuesta frente a imprevistos.
- Planificar e implementar la estrategia de la organización, incluyendo las cuestiones relacionadas con la ciberseguridad, reforzando su despliegue y la comunicación de las decisiones y los planes establecidos.

- Conocer de manera sistemática las necesidades y expectativas de los clientes en términos de ciberseguridad.
- Informar a los clientes de las políticas, planes y requisitos de ciberseguridad incorporados tanto en los productos y servicios ofertados como en las relaciones comerciales.
- Incorporar requisitos y especificaciones de ciberseguridad en la fabricación, comercialización y entrega de los productos y servicios ofertados.
- Trasladar, a los proveedores y aliados, los requisitos y especificaciones de ciberseguridad para la fabricación, comercialización y entrega de los componentes de los productos y servicios ofertados

- Implementar las medidas de ciberseguridad en los procesos de gestión de usuarios, gestión de perfiles y permisos de accesos, durante la vida laboral de la persona dentro de la organización.
- Identificar y gestionar los conocimientos y competencias sobre ciberseguridad necesarias para el desempeño de las actividades de las personas de la organización.
- Promover la implicación y el compromiso de las personas para alcanzar los objetivos de ciberseguridad establecidos por la organización.

- Conocer las necesidades y expectativas de los grupos de interés de la sociedad e incorporarlas dentro de la estrategia.
- Participar activamente en la difusión de buenas prácticas en términos de ciberseguridad y cumplir con la entrega de información relevante a los organismos pertinentes.
- Tener en cuenta aspectos de sostenibilidad (energía, reciclaje, medio ambiente, etc.) en el momento de establecer los criterios de ciberseguridad en la organización.

- Sistematizar la gestión de proyectos internos para la generación de nuevas ideas y la puesta en marcha de medidas de ciberseguridad, incorporándolo dentro del sistema de innovación organizacional.

Estratégicos:

- Certificaciones
- Nivel de riesgo asumido
- Consecución de los objetivos

Clientes:

- Grado de satisfacción
- Reclamaciones asociadas a la ciberseguridad
- Rendimiento y eficacia de las medidas de ciberseguridad
- Grado de cumplimiento de los SLA

Personas:

- Revisión de cuentas de usuarios
- Personas formadas y/o concienciadas
- Cumplimiento de políticas y procedimientos de seguridad

Sociedad:

- Incidentes detectados e informados
- Activos tecnológicos sostenibles

Innovación:

- Iniciativas de ciberseguridad
- Éxito de iniciativas implementadas

3

Experiencia piloto

Criterios para las organizaciones del piloto

- Nivel de avance en el MGA
- Madurez en medidas de ciberseguridad
- Territorio histórico
- Tipo de pilotaje
 - Desatendido, basado en la autoevaluación.
 - Acompañado, con un gap análisis in situ.

- Finalizar la fase de pilotaje en el cuarto trimestre del 2019
- Aprobar y publicar el modelo
- Difusión del marco

ESKERRIK ASKO



www.basquecybersecurity.eus

 @basqueCScentre

Linked in

 **YouTube**