MARCO DE REFERENCIA SOBRE LA CIBERSEGURIDAD EN ORGANIZACIONES Y EMPRESA

Modelo de Gestión Avanzada

KUDEAKETA AURRERATUA
EUSKALIT
GESTIÓN AVANZADA

BASQUE CYBERSECURITY CENTRE

Qué es el BCSC

El Basque Cybersecurity Centre (BCSC) es la organización designada por el Gobierno Vasco para promover la ciberseguridad en Euskadi.

El Basque Cybersecurity Centre está formado por

Departamentos del Gobierno Vasco

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

Centros tecnológicos

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

Nuestra misión

La misión del BCSC es promover y desarrollar una cultura de ciberseguridad entre la sociedad vasca, dinamizar la actividad económica relacionada con la aplicación de la ciberseguridad y fortalecer el sector profesional.

Nuestra visión

Posicionar a Euskadi como un referente internacional en la aplicación de tecnologías de ciberseguridad a la industria.

Ser reconocido como punto de encuentro entre oferentes y demandantes locales de ciberseguridad.

Liderar iniciativas de colaboración público-privadas tanto a nivel local como interregional.

Nuestros valores

- Cercanía
- Integridad
- Transparencia
- Innovación
- Compromiso social

Misión

Somos un grupo de organizaciones constituido como fundación, propiciada por el Gobierno Vasco, para promover la Gestión Avanzada en las organizaciones vascas, aportando utilidad, eficiencia y cercanía para contribuir a su competitividad y, así, al desarrollo sostenible de Euskadi, todo ello con un equipo de personas comprometido, profesional y motivado.

Visión

Ser la entidad facilitadora de referencia para las organizaciones y administraciones vascas en su movilización hacia la Gestión Avanzada, que posibilite a Euskadi ser reconocida por ello a nivel internacional.

Valores

COHERENCIA

Con el propósito de poder predicar con el ejemplo, aplicaremos en nuestra propia gestión interna los conceptos y metodologías de Gestión Avanzada.

COOPERACIÓN

Involucraremos a otras personas y organizaciones en la consecución de nuestra Visión, acompañándolas en su avance en la gestión, haciéndolas protagonistas y reconociendo sus logros.

COHESIÓN

Las personas de EUSKALIT orientaremos nuestra actividad personal hacia nuestra Misión y Visión, con compromiso, ilusión y espíritu de equipo, implicándonos con ideas y opiniones en la toma de decisiones, compartiendo la información y el conocimiento, y apoyándonos y reconociéndonos mutuamente para el logro de los objetivos.

AUTORES

Proyecto coordinado por el Basque Cybersecurity Centre (BCSC), con SPRI y EUSKALIT para el Departamento de Desarrollo Económico e Infraestructuras del Gobierno Vasco.

CONTENIDO

CONSEJOS

Alt+ lecha izquierda para volver a la vista anterior después de ir a un hipervínculo.

Haz **click** en **nuestros iconos** y visita nuestra web.

Haciendo **click** en el **número de página** volverás al índice.

1. INTRODUCCIÓN

1.1 MARCO DE REFERENCIA

La adopción tecnológica por parte de la sociedad ha supuesto un desafío para los sectores público y privado, que han tenido que involucrarse en los avances para poder satisfacer los nuevos requerimientos de la sociedad y el mercado, debido a que las nuevas tecnologías se integran, en su desarrollo, con una celeridad cada vez mayor. La transformación digital de la sociedad, las organizaciones públicas y las empresas, ha traído consigo la aparición de **nuevas amenazas y riesgos**.

Debido al entorno interconectado en el que se encuentran tanto la ciudadanía como las empresas, la ocurrencia de incidentes y la materialización de amenazas cibernéticas son una realidad cada vez mayor, aumentando su incidencia tanto a nivel global como en Euskadi. Es importante desterrar la **falsa creencia de que los ataques cibernéticos sólo les suceden a las grandes empresas**, ya que dicho aumento de ataques y/o incidentes cibernéticos está afectando tanto a la grande como a la mediana y pequeña empresa.

La propia Comisión Europea, para minimizar el impacto de las nuevas amenazas y riesgos en la Unión Europea (UE), marca una estrategia de ciberseguridad cuyos objetivos son impulsar los valores europeos de libertad y democracia, y velar por un crecimiento seguro de la economía digital. Para ello, entre las diversas regulaciones y directivas aprobadas recientemente, destaca la Directiva NIS, cuya finalidad es reforzar la **ciber-resiliencia** de los sistemas informáticos, reduciendo los impactos de la delincuencia en la red y fortaleciendo la política de ciberseguridad y ciberdefensa internacional de la UE.

Se desarrolla una guía de interpretación del modelo de Gestión Avanzada para **facilitar la aplicación de la perspectiva de la ciberseguridad**. Se pretende con dicha guía que las organizaciones identifiquen todos los ámbitos de la gestión donde es posible incorporar dicha perspectiva y facilitar su aplicación. Para la elaboración de esta guía se ha seguido el esquema de acción y resultados del Modelo, así como otras buenas prácticas surgidas de diferentes ámbitos y metodologías.

1.2 JUSTIFICACIÓN DEL PROBLEMA

Nos encontramos en una época en la que la integración de la tecnología digital en los procesos de la industria es tan profunda que ha modificado la forma de llevar a cabo dichos procesos, optimizándolos y mejorando su competitividad. Para llevar a cabo este **cambio de forma segura**, es necesario tener en cuenta la ciberseguridad en todas las fases del proceso de transformación.

Para tener una primera aproximación a la gestión de la ciberseguridad dentro de cada organización, nace este marco de referencia para la **gestión de la ciberseguridad en organizaciones y empresas**.

1.3 EL MODELO DE GESTIÓN AVANZADA

El presente marco de referencia para la gestión de la ciberseguridad en organizaciones y empresas se ha diseñado siguiendo la estructura del Modelo de Gestión Avanzada (MGA), ya que es la referencia principal en el ámbito de la gestión organizativa. Este modelo se desarrolló con la participación y el consenso de personas expertas en gestión pertenecientes a relevantes organizaciones e instituciones, coordinados por EUSKALIT.

Este modelo se divide en 6 grandes elementos, que aportan las perspectivas necesarias para el desarrollo de un sistema de gestión sobre el que estructurar la competitividad de las organizaciones, y lograr lo siguiente:

1	Generar una visión de largo plazo que se materialice mediante una estrategia claramente definida.
2	Orientar la organización hacia los clientes realizando una aportación diferencial de valor.
3	Generar en las personas un sentimiento de pertenencia a un proyecto compartido.
4	Aplicar la innovación en todos los ámbitos de la organización.
5	Potenciar el compromiso con la sociedad, importante suministrador de capacidades competitivas relevantes.
6	Alcanzar resultados satisfactorios para los diferentes grupos de interés de manera sostenida y equilibrada.

CÓMO UTILIZAR EL MARCO

2.

2.1 CÓMO UTILIZAR EL MARCO

El presente documento pretende ser un marco de referencia para la gestión de la ciberseguridad en organizaciones y empresas. Un marco que no pretende ser prescriptivo ni obligatorio; más bien, se trata de una recopilación de ideas y buenas prácticas que pueden servir de ejemplo a las empresas para mejorar su compromiso con la ciberseguridad.

La utilización práctica del presente documento, como herramienta de apoyo durante el proceso de reflexión e identificación de áreas de mejora relacionadas con la ciberseguridad, podría ser la siguiente:

1. **Definición del equipo o conjunto de personas que realizarán la reflexión:** Preferiblemente de naturaleza multidisciplinar, con representantes de los principales niveles y unidades organizativas, la alta dirección, personas con actividades directamente afectadas por la ciberseguridad y personas responsables de sistemas informáticos.

2. **Reflexión individual:** Cada participante, utilizando el marco como guía, identifica puntos fuertes y áreas de mejora en cada uno de los 6 elementos. Para ello, analiza cualitativamente las recomendaciones (generales y específicas), su aplicabilidad en la organización, y el nivel y rigor de despliegue. Anota los puntos fuertes que considera que se han implementado con más solidez (identificando las buenas prácticas que las soportan) y las áreas de mejora las que estén en la situación contraria.

3. **Consenso y contraste externo:** Se realiza una reunión del equipo para compartir las reflexiones individuales y consensuar los puntos fuertes y áreas de mejora, seleccionando las más relevantes. Se anotan los dos o tres puntos fuertes y dos o tres áreas de mejora, consensuados en cada elemento. Posteriormente, se realiza una priorización final, utilizando criterios como la potencialidad de reducción de riesgos, optimización de recursos, situación actual, viabilidad, etc., anotando de tres a cinco áreas de mejora en última página del informe. Durante todo este proceso es recomendable la presencia y apoyo de personas externas a la organización, preferiblemente con conocimientos avanzados en organización empresarial y/o ciberseguridad, a las que habrá que hacerles llegar con la suficiente antelación los puntos fuertes y áreas de mejora identificados por los participantes en el paso anterior, para que puedan realizar su análisis y valoración antes de la reunión de consenso.

Tras la reflexión, y basándose en el presente informe, la organización puede establecer equipos y/o responsabilidades para definir, planificar y liderar las acciones que den respuesta a las áreas de mejora priorizadas. Para ello, se pueden utilizar los ejemplos de buenas prácticas, incluidos dentro del propio marco.

MARCO PARA LA GESTIÓN DE LA CIBERSEGURIDAD

3.

3.1 ESTRATEGIA

La ciberseguridad debe ser gestionada como una actividad transversal a toda la organización, que apoye tanto a los procesos de negocio como a los de soporte al mismo. Por ello, consideraciones acerca de la ciberseguridad deben formar parte del desarrollo y la implementación de la estrategia que establezca la organización de cara a su futuro.

La planificación de la ciberseguridad debe estar alineada con los objetivos estratégicos de la organización, recopilando y analizando la información relevante por parte de los distintos grupos de interés, y haciendo un adecuado balance entre las necesidades en materia de ciberseguridad, los requisitos de los clientes y demás partes interesadas, y los objetivos del negocio.

Recomendaciones que pueden ser aplicables:

Recopilar y analizar la información necesaria para integrar aspectos de ciberseguridad dentro de la estrategia de la empresa.
Identificar los grupos de interés (accionistas, dirección, personal, clientes, proveedores, sociedad,...), involucrados y afectados por los riesgos y las medidas de ciberseguridad, para conocer sus necesidades.
Conocer la legislación relevante tanto a nivel europeo, nacional, autonómico y sectorial, así como las principales normas y estándares internacionales en materia de ciberseguridad que afectan a la organización.
Considerar la ciberseguridad dentro de los modelos de negocio, para procurar un adecuado equilibrio entre la usabilidad de los sistemas -que dan soporte a los servicios y los procesos organizacionales-, y las medidas de protección a aplicar en estos sistemas y a la información que procesan.

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.

Identificar los procesos y servicios clave del negocio, además de aquellos que les dan soporte, y establecer criterios de criticidad que indiquen una mayor consideración de unos y otros frente a las amenazas y los riesgos a identificar.

Determinar los recursos y activos relevantes que soportan los procesos y servicios de la organización e identificar su interrelación y dependencia.

Valorar el impacto que supondría una degradación o una interrupción en los procesos y servicios de la organización.

Determinar aquellas amenazas que pueden afectar a los recursos y activos relevantes de la organización y valorar su probabilidad de ocurrencia.

Estimar y priorizar los riesgos, basado en el impacto en los servicios y la probabilidad de ocurrencia de las amenazas.

Acordar entre los órganos directivos y los responsables de las diferentes áreas de la organización, el nivel de riesgo aceptable, de manera de poder priorizar y planificar las medidas de seguridad necesarias para minimizar los riesgos y hacer frente a las amenazas identificadas por el conjunto de la organización.

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.

Establecer planes de acción, a corto, medio y largo plazo, respecto a la implementación de medidas de seguridad dentro de la organización, considerando los recursos humanos, financieros, de información y tecnológicos necesarios para la implementación de estos planes. Definir objetivos e indicadores que permitan medir la eficacia de esta implementación y su contribución al cumplimiento de los objetivos estratégicos.

Establecer una estrategia de comunicación que permita desplegar los objetivos planteados de ciberseguridad, actuar sobre los mismos, y reflejar el valor añadido que la organización está logrando con la implementación de las medidas.

Revisar los objetivos e indicadores al final de cada periodo de gestión, para evaluar el grado de cumplimiento de las metas, la coherencia y la consistencia de los resultados. Tomar estas consideraciones para el establecimiento de los objetivos del siguiente ciclo.

3.2 CLIENTE

Los riesgos asociados con la ciberseguridad pueden afectar a los clientes actuales y potenciales. Por ello, es importante considerar, dentro de los productos y servicios que ofrece la organización, las características relacionadas con la aplicación de medidas de seguridad específicas que aporten confianza a los clientes y que se pueda percibir como un valor añadido.

Las consideraciones sobre ciberseguridad deberían formar parte de la toda la cadena de valor de la organización; los proveedores podrían formar parte de estas actividades por lo que también se hace necesario alinearlos a la estrategia de ciberseguridad.

Recomendaciones que pueden ser aplicables:

Conocer de manera sistemática las necesidades y expectativas de los clientes en términos de ciberseguridad.

Utilizar herramientas y metodologías (por ejemplo, realizar encuestas o entrevistas) para recopilar necesidades y expectativas respecto a los tres aspectos claves de la ciberseguridad: la disponibilidad de los servicios de la organización, la garantía sobre la integridad de los datos y el tratamiento de la confidencialidad de los mismos.

Conocer y tener en cuenta las tendencias sobre medidas de ciberseguridad., relacionadas a productos propios o de la competencia. Recopilar información a través de las noticias, comentarios en las redes sociales, páginas web especializadas, etc.

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. Tener en cuenta estos conceptos como parte de la comercialización y difusión de los mismos.

Dar a conocer las medidas previstas para proteger la privacidad y los derechos fundamentales de las personas, como por ejemplo evitar la recogida excesiva de datos personales y limitar su uso a los servicios y productos contratados.

Informar de las medidas implementadas para mitigar la interrupción de los servicios, así como para la detección a tiempo de incidentes maliciosos y la monitorización de los sistemas.

Evaluar el impacto de esta estrategia en el valor percibido por parte de los clientes, por ejemplo, mediante encuestas de satisfacción, retroalimentación formal e informal, reclamaciones, etc.

Incorporar requisitos y especificaciones de ciberseguridad en la producción, comercialización y entrega de los productos y servicios ofertados.

Considerar las necesidades y las expectativas de los clientes, respecto a la ciberseguridad, dentro del diseño, la producción y/o la puesta en marcha de los productos y servicios de la organización.

Incorporar, en los acuerdos con el cliente, los requisitos y los niveles de seguridad adecuados para los productos y servicios de la organización.

Incorporar medidas de ciberseguridad en los propios procesos de diseño, producción, comercialización y entrega; proteger los sistemas, recursos y activos que soportan los procesos y servicios de la organización.

Monitorizar, detectar y responder oportunamente a anomalías y eventos que comprometan la seguridad; establecer procedimientos de recuperación para asegurar la continuidad de los servicios y las operaciones.

Trasladar, a los proveedores y aliados, los requisitos y especificaciones de ciberseguridad para la producción, comercialización y entrega de los componentes de los productos y servicios ofertados.

Especificar medidas contractuales para cumplir con los requisitos de disponibilidad, integridad y confidencialidad acordados con los clientes.

Coordinar e involucrar a los proveedores en las actividades de monitorización de eventos, identificación de anomalías, respuesta y recuperación de servicios y operaciones, en caso formen parte de la cadena de valor.

Aplicar medidas de seguridad en la relación a la gestión con los proveedores; informar a los proveedores de las medidas implantadas en las actividades de las que forman parte y hacer seguimiento del cumplimiento de las mismas.

3.3 PERSONAS

Para alcanzar los objetivos establecidos por la organización en términos de la ciberseguridad, es importante la implicación de las personas, tanto de aquellos que ocupen puestos directamente relacionados con la gestión y operación de la ciberseguridad, así como del resto de las personas, a quienes las medidas de seguridad impactan o condicionan su labor diaria.

La organización debe fomentar una cultura en la que la ciberseguridad sea una parte importante de la misma y, de esa manera, acompañar a las personas desde su incorporación y durante su desarrollo profesional.

Recomendaciones que pueden ser aplicables:

- 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.
- Informar a la persona, durante su incorporación, de los deberes y responsabilidades que tiene su puesto de trabajo en materia de seguridad, incluyendo las medidas disciplinarias a que haya lugar.
- Garantizar la confidencialidad de la información a la que se pueda tener acceso, tanto durante la ejecución de las funciones del puesto así como a la finalización de las mismas.
- Proceder a la retirada de los permisos, accesos y privilegios otorgados a las cuentas de usuario en caso de cese laboral o de traslado a otro puesto de trabajo.
- En caso de contratación para un puesto específico relacionado con la ciberseguridad, asegurar que la persona tiene la competencia necesaria y que se puede confiar en ella, especialmente si es un rol crítico para la organización.

Identificar y gestionar los conocimientos y competencias sobre ciberseguridad necesarias para el desempeño de las actividades de las personas de la organización.

Sensibilizar a todas las personas de la organización en temas de ciberseguridad. Asimismo, concienciarlas regularmente acerca de su implicación y las responsabilidades que debe asumir con el objetivo de alcanzar los niveles de seguridad establecidos por la organización.

Reforzar la comprensión y el uso de las normativas de seguridad relativas a las buenas prácticas sobre el uso de los sistemas así como la identificación y el reporte de incidencias de seguridad. Preparar a las personas para la actuación en caso de incidentes graves y en tareas relacionadas con la continuidad del negocio y los planes de contingencia.

Dar formación a las personas que requieran temas específicos relacionados con la seguridad para la ejecución de sus funciones (personal técnico, calidad, prevención de riesgos laborales, ...). Incorporar dentro de los planes de formación, las materias necesarias para el desempeño de sus funciones.

Revisar periódicamente la capacidad de las personas en el ámbito de la ciberseguridad, a través de una evaluación de su conocimiento, habilidades y competencias. Definir planes para dar respuesta a las necesidades detectadas.

Favorecer la polivalencia y asegurar la presencia de personas capacitadas que puedan hacerse cargo de funciones claves de la organización en caso de necesidad.

Promover la implicación y el compromiso de las personas para alcanzar los objetivos de ciberse-guridad establecidos por la organización.

Comunicar periódicamente a la organización las medidas de seguridad implementadas y los avances que se están teniendo al nivel organizacional, de equipo e individual.

Fomentar una cultura organizacional en la que se establezca un entorno cooperativo y de confianza para trasmitir y compartir conocimientos y lecciones aprendidas en torno a la ciberseguridad.

Incorporar aspectos de ciberseguridad en el ejercicio de liderazgo para apoyar a otras personas de la organización en la asimilación, compresión y aplicación de las medidas definidas, como por ejemplo, contemplar la asignación de recursos específicos para la gestión de la ciberseguridad en la organización.

Establecer una sistemática para el reconocimiento y/o la compensación de las personas involucradas y comprometidas con los objetivos y las medidas de ciberseguridad.

3.4 SOCIEDAD

La organización, al formar parte de la sociedad, debería convertirse en un actor relevante dentro del contexto en donde opera, extendiendo sus objetivos en materia de ciberseguridad más allá de su propio ámbito de responsabilidad.

Para ello, es importante involucrarse en las necesidades de su entorno, fomentar su participación en la sociedad, y ofrecer su conocimiento y experiencia para mejorar la ciberseguridad en el entorno en el que actúa.

Recomendaciones que pueden ser aplicables:

Conocer las necesidades y expectativas de los grupos de interés de la sociedad e incorporarlas dentro de la estrategia.

Identificar grupos de interés relacionados con la sociedad (consumidores, asociaciones, entes públicos, ...) que podrían ser afectados, en términos de ciberseguridad, por la actividad de la organización.

Determinar áreas de oportunidad para mejorar el conocimiento, la infraestructura y las medidas de ciberseguridad para la sociedad en su conjunto.

Asumir una responsabilidad social y un comportamiento ético de la organización en términos de ciberseguridad, asegurando la transparencia de sus decisiones y la protección de los intereses de todas las partes involucradas.

Participar activamente en la difusión de buenas prácticas en términos de ciberseguridad y cumplir con la entrega de información relevante a los organismos pertinentes.

Brindar información oportuna a los organismos pertinentes acerca del estado de la ciberseguridad en la organización, así como de la detección y respuesta a los incidentes de seguridad en los que se haya visto involucrado.

Establecer canales de comunicación para atender consultas acerca de los aspectos de la ciberseguridad en el desarrollo, operación y entrega de los productos y servicios ofertados.

Tener en cuenta aspectos de sostenibilidad (consumo energético, reciclabilidad de equipos, etc.) en el momento de establecer los criterios de ciberseguridad en la organización.

Hacer uso de sistemas, componentes y/o dispositivos electrónicos con perspectiva medioambiental, es decir, que durante su periodo de vida útil sean energéticamente eficientes.

Reciclar, en la medida de lo posible, los dispositivos y equipos tecnológicos al finalizar su ciclo de vida útil. Tener en cuenta la eliminación de datos e información sensible en esta fase. Llevar los productos obsoletos a puntos limpios autorizados para tal fin.

3.5 INNOVACIÓN

Se entiende como innovación el desarrollo de nuevos productos o servicios, la mejora de los mismos y/o la mejora de los procesos internos de la organización. La innovación puede impulsar la protección frente a las amenazas y los ataques de la ciberdelincuencia -cuya evolución y sofisticación crece día a día-, así como el aumento en la confianza de los clientes y las partes relevantes.

Recomendaciones que pueden ser aplicables:

- 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.
- Valorar la posibilidad de establecer objetivos o políticas de innovación, en el ámbito de la ciberseguridad, que permitan mejorar y/o incorporar nuevos enfoques.
- Facilitar la generación de iniciativas innovadoras en ciberseguridad por parte del personal de la organización, aprovechando su experiencia en la ejecución de sus funciones.
- Identificar mecanismos y recursos externos que promuevan esta innovación, mediante la interacción, por ejemplo, con clientes, proveedores, centros de investigación, clústeres, organismos públicos de ayuda empresarial, etc.
- Evaluar a puesta en marcha de estas iniciativas teniendo en consideración los riesgos asociados y un análisis de coste-beneficio.
- Analizar los resultados de la implementación de estas iniciativas comparándolos frente a las expectativas iniciales, tomando en consideración las lecciones aprendidas para las siguientes propuestas.

3.6 RESULTADOS

Los resultados proporcionan datos e información para evaluar, mejorar e innovar los procesos, las políticas y las operaciones alineadas con la estrategia organizacional para la ciberseguridad.

Medir y analizar cómo se está desempeñando la organización mediante un conjunto integral de indicadores relacionados con la ciberseguridad, ayuda a tomar decisiones que mejoran el rendimiento de las actividades.

RESULTADOS ESTRATÉGICOS

- Certificaciones nacionales y/o internacionales que demuestren el compromiso de la organización con la ciberseguridad.
- Nivel de riesgo asumido por la organización para los activos esenciales.
- Grado de consecución de los objetivos de ciberseguridad de la organización.

RESULTADOS EN CLIENTES

- Grado de satisfacción de los clientes en la relación con la ciberseguridad.
- Número de reclamaciones asociadas a la ciberseguridad (privacidad, disponibilidad, integridad de la información).
- Resultados del rendimiento y la eficacia de las medidas de ciberseguridad implantadas en los procesos de la organización (por ejemplo, respuesta a ciberataques, eficacia en el bloqueo de ataques, medidas de protección de la información, continuidad del negocio, ...).
- Grado de cumplimiento de los acuerdos de nivel servicio tanto hacia los clientes como desde los proveedores.

RESULTADOS EN PERSONAS

Diferencias en la revisión de las cuentas de usuarios, permisos y accesos otorgados respecto a la realidad de la organización.

Porcentaje de personas que han sido formadas y/o concienciadas en temas de ciberseguridad.

Porcentaje de personas que cumplen con las políticas y procedimientos de seguridad (por ejemplo, la renovación de contraseñas o la detección de correos sospechosos).

RESULTADOS EN LA SOCIEDAD

Número de incidentes de seguridad detectados e informados a los órganos competentes.

Porcentaje de activos tecnológicos esenciales que cumplen certificaciones y/o estándares de sostenibilidad

RESULTADOS DE LA INNOVACIÓN

Número de iniciativas, propuestas en el último periodo, relacionadas con la ciberseguridad.

Porcentaje de éxito de las iniciativas de ciberseguridad implementadas.

4.

GLOSARIO

A continuación se presentan una serie de conceptos del que hace uso este modelo, ya sea de forma directa o indirecta. Estas definiciones han sido tomadas del SPRI Hiztegia ***(https://www.spri.eus/hiztegia/)***, diccionario especializado en el ámbito más avanzado del sector industrial, en el que se crean constantemente nuevos conceptos y se actualizan los anteriores. Se recomienda la utilización directa de esta fuente para ampliar información y/o mantenerse actualizado con estas definiciones.

Activo de información
Información —o sistema relacionado con el tratamiento de la información— perteneciente a una empresa u organización, que es susceptible de ser atacada deliberada o accidentalmente provocando consecuencias negativas para la entidad. Puede tratarse de procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

Análisis de riesgos
Proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, con el objeto de determinar los controles necesarios para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Antivirus
Programa de seguridad que se encarga de buscar y eliminar los virus conocidos de un sistema informático. Evita la entrada de virus, o busca y elimina los virus que han conseguido introducirse en el sistema informático. Con la aparición de sistemas operativos más avanzados e Internet, los antivirus han ido evolucionado; actualmente, tienen la capacidad de bloquear virus, desinfectar archivos y prevenir su infección. Además, son capaces de conocer otros tipos de malware: spywares, gusanos, troyanos, etc.

Auditoría de seguridad / Auditoría de seguridad informática
Estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones.

Autenticación
Proceso de verificación de alguien que intenta entrar a un sistema informático o a un servicio online, que constituye una funcionalidad característica para una comunicación segura. La verificación se puede llevar a cabo de muchas maneras: mediante contraseñas, certificados electrónicos, tarjetas inteligentes, sistemas biométricos, etc. Ninguno de ellos verifica totalmente la identidad de la persona usuaria, y se establecen distintos niveles de verificación, en función de la seguridad aportada.

Cadena de valor
Secuencia de actividades que realiza una organización para generar valor, repercutiendo en el valor final del producto y en el coste que supone su oferta a la organización. Las actividades incluyen las diferentes fases de la cadena de suministro, pero también actividades complementarias, como son el marketing, las ventas y el servicio.

Centro Vasco de Ciberseguridad
Centro creado y puesto en marcha por el Gobierno Vasco, con sede en el Parque Tecnológico de Álava. Tiene como cometido promover la incorporación de la ciberseguridad en las empresas vascas, además de convertir a Euskadi en un referente europeo en la aplicación de las nuevas tecnologías de la información y las comunicaciones y dotar a las infraestructuras críticas y a las empresas vascas de una cobertura efectiva y fable de prevención y reacción ante posibles amenazas y/o ataques.

Certificado digital / Certificado electrónico
Fichero electrónico generado por una autoridad de certificación, con el fin de garantizar que una clave pública está asociada a una identidad determinada. Se utiliza para verificar la identidad de la persona titular, verificar su firma o cifrar mensajes dirigidos a ella.

Ciberdelito / Delito informático
Actividad delictiva que se realiza a través de Internet o utilizando recursos tecnológicos. Estos son los principales tipos de delito informático: a) delitos contra la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos; b) delitos de fraude contra el mercado de Internet y telecomunicaciones; c) amenazas y delitos contra el honor; d) delitos relacionados con la pornografía infantil; e) delitos contra la propiedad intelectual e industrial de Internet.

Ciberataque
Acción realizada por una o varias personas por medio de herramientas informáticas, con el fin de dañar un sistema informático o una red informática. Los objetivos del ciberataque pueden ser muy variados: quebrar la seguridad del sistema, obtener datos de forma ilegal o dañar o destruir el propio sistema.

Ciberseguridad
Conjunto de tecnologías y servicios que protegen a una empresa de cualquier agresión o pérdida de datos. En un ámbito digitalizado, cada vez es más importante proteger cualquier información relevante para la empresa.

Ciclo de vida
Secuencia de cambios o fases ocurrido durante el tiempo en que algo (objetos, productos, procesos, etc.) es útil.

Código de conducta
Conjunto de recomendaciones y reglas destinadas a determinar las normas deontológicas aplicables en el ámbito de las tecnologías de la información y la comunicación, con el fin de garantizar la plena confianza y seguridad de las personas usuarias y evitar la vulneración de los derechos fundamentales que les corresponden en tanto que forman parte de la ciudadanía.

Confidencialidad
Propiedad de la información, por la que se garantiza que está accesible únicamente para aquellas personas autorizadas a tener acceso a ella. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. La confidencialidad, la integridad y la disponibilidad conforman las tres dimensiones de la seguridad de la información.

Dato sensible
Categoría especial aplicable a los datos personales, que por su importancia en relación con la privacidad e intimidad de la persona interesada requieren una protección reforzada. De acuerdo con la ley vigente, los datos que se incluyen en esta categoría son aquellos que muestran datos referentes al origen racial o étnico de la persona interesada, sus opiniones políticas, creencias religiosas y filosóficas, afiliación sindical, salud y vida sexual, datos genéticos y biométricos y, por último, datos relacionados con su orientación sexual.

Disponibilidad
Capacidad de un servicio, un sistema, un componente informático o una información para garantizar su accesibilidad y la posibilidad de ser utilizado por los usuarios o procesos autorizados cuando éstos lo requieran. La disponibilidad, la integridad y la confidencialidad conforman las tres dimensiones de la seguridad de la información.

Firma electrónica
Conjunto de datos electrónicos que se utilizan para verificar la identidad de la persona que firma una comunicación o una transacción electrónica, adjunto a otros datos electrónicos o relacionado lógicamente con ellos. Se adquiere mediante una clave pública, y tiene el mismo valor legal que la firma manuscrita, siempre y cuando cumpla los requisitos de la normativa específica correspondiente.

Fuga de datos
Pérdida de la confidencialidad de la información privada de una persona o empresa. Se trata de la filtración de determinada información que, en principio, no debería ser conocida más que por un grupo de personas, por el departamento de una organización... y que termina siendo visible o accesible para otras personas.

Gestión del ciclo de vida del producto
Proceso para gestionar desde el principio el ciclo de vida completo de un producto, incluyendo el diseño de ingeniería, la fabricación, el servicio y la decisión de retirarlo del mercado. La gestión del ciclo de vida del producto engloba personas, datos, procesos y sistemas de negocio, y ofrece información imprescindible para las empresas.

Hacking ético
Trabajo realizado por hackers o personas expertas en seguridad informática, para garantizar la seguridad del sistema de información de una organización. Por ejemplo, tratar de entrar en la red informática de la organización, con el fin de evaluar su solidez.

Incidente de seguridad
Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, como puede ser el acceso o intento de acceso a los sistemas o el uso, divulgación, modificación o destrucción no autorizada de información.

Integridad

Propiedad de la información o de un conjunto de datos, que garantiza que durante su tratamiento, almacenamiento y transmisión por medios electrónicos no sufrirá ninguna alteración, pérdida o destrucción, ya sea de forma intencionada o accidental y ya sea por a errores de software/hardware o por condiciones medioambientales. La integridad de la información constituye la piedra angular de la seguridad de la información. La integridad, la confidencialidad y la disponibilidad conforman las tres dimensiones de la seguridad de la información.

Metadatos

Conjunto de datos relacionados con un documento, en el que se recoge información fundamentalmente descriptiva del mismo (origen, tipo, fecha de introducción, etc.), así como información de administración y gestión. Se trata de un tipo de información que enriquece el documento al que está asociado. A modo de ejemplo, se podría considerar como una analogía al uso de índices que se emplean en una biblioteca, donde datos tales como autor, títulos, etcétera nos permiten localizar un libro en concreto. Los metadatos permiten mejorar las consultas en los buscadores, consiguiendo una mayor exactitud y precisión en los resultados.

Parche de seguridad

Conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente, los parches de seguridad son desarrollados por la empresa fabricante del software, tras la detección de una vulnerabilidad en el mismo. Pueden instalarse de forma automática o manual por parte de la persona usuaria. Siempre que es posible, no modifican la funcionalidad del programa. Se utilizan con frecuencia en aplicaciones que interactúan con Internet.

Procesamiento / Tratamiento de datos

Conjunto de operaciones realizadas para obtener información relevante contenida en un conjunto de datos. Comprende la validación de datos y su ordenación, clasificación, limpieza, combinación y análisis, así como la visualización de los resultados.

Resiliencia

En el ámbito de las tecnologías de la información, capacidad de enfrentarse a siniestros ocurridos a propósito o involuntariamente y volver al estado anterior al siniestro. Los sistemas resilientes son capaces de funcionar sin problemas durante los siniestros y después de haber encontrado una solución y haberlos reparado. Este concepto se emplea, por ejemplo, en el contexto de los ciberataques.

Parque Tecnológico de Álava
+34 945 236 636
info@bcsc.eus
www.basquecybersecurity.eus
@basquecscentre
www.linkedin.com/company/basque-cybersecurity-centre/

Parque tecnológico de Bizkaia
+34 944 209 854
euskalit@euskalit.net
www.euskalit.net
@EUSKALIT
https://www.linkedin.com/company/euskalit/