UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Guía de adaptación a normativa europea NIS2 en el ámbito empresarial

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Pau Sáez, Álvaro

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2023/2024

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Guía de adaptación a la normativa europea NIS2 en el ámbito empresarial

TRABAJO DE FIN DE GRADO

Grado en Ingeniería Informática

Autor: Álvaro Pau Sáez

:

Curso : 2023-2024

Resumen

La Directiva (UE) 2022/2555, conocida como NIS2[1], establece principalmente obligaciones de ciberseguridad para los Estados miembros, medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación. De acuerdo a sus criterios, todas las grandes y medianas empresas de los sectores identificados en la normativas están automáticamente involucradas. De manera previa, algunas de las empresas ya cumplían los requisitos de la norma precedente, la Directiva (UE) 2016/1148 (NIS)[2], que tiene importantes diferencias con la actual. El objetivo principal de esta guía es apoyar en la aplicación de las áreas principales de la nueva normativa NIS2 a partir de sus diferencias con la ya aplicada NIS1 a empresas de tamaño medio, con una plantilla reducida de profesionales informáticos. Como objetivos secundarios se propondrán varias mejoras (buenas practicas) a aplicarse en el ámbito empresarial en general, teniendo en cuenta las obligaciones que la normativa impone.

Palabras clave: Ciberseguridad, NIS2, guía de adaptación, cumplimiento normativo, protección de datos

Abstract

Directive (EU) 2022/2555, known as NIS2[1], mainly establishes cybersecurity obligations for Member States and measures for cybersecurity risk management and notification obligations for entities in its scope. According to its criteria, all large and medium-sized companies in the sectors identified in the regulations are automatically involved. Previously, some of the companies already met the requirements of the previous standard, Directive (EU) 2016/1148 (NIS)[2], which has important differences with the current one. The main objective of this guide is to support the application of the main areas of the new NIS2 regulations based on their differences with the one already applied NIS1 to medium-sized companies, with a small staff of IT professionals. As secondary objectives, several improvements (good practices) will be proposed to be applied in the business environment in general, taking into account the obligations that the regulations impose.

Key words: Cybersecurity, NIS2, adaptation guide, regulatory compliance, data protection

Índice general

Índice de figuras

CAPÍTULO 1
Motivación

La motivación de realizar este trabajo se basa en tres puntos, el primero es la actualidad de la materia en cuestión ya que se trata de una normativa que debe cumplirse el año de la realización de este TFG, el segundo punto sería el impacto empresarial, tanto a nivel académico como profesional es un trabajo del que tanto yo como autor del trabajo, como una empresa que necesite ayuda para implementar la normativa Europea NIS2 pueda beneficiarse y por último estaría el punto del desarrollo profesional y el interés personal ya que me gusta la materia y creo que es una buena idea tratar y aprender sobre temas tan importantes dentro del sector de la ciberseguridad.

CAPÍTULO 2
Objetivos

El objetivo es la realización de una guía aplicable para el seguimiento y cumplimiento de la normativa europea NIS2 que debe cumplirse el 17 de octubre de 2024. Con ello se quiere dejar claro de que trata dicha normativa, los puntos a cubrir y recomendaciones en lo que respecta al cumplimiento de dicha normativa. Finalmente se incluirá un recurso TIC para poder hacer un seguimiento de todo lo tratado en dicho documento.

CAPÍTULO 3
Estado del Arte

En el estado del arte se estudian y analizan algunos documentos ya existentes que tienen una funcionalidad similar, o muy parecida a la del proyecto. En este caso trataré documentos que he encontrado bastante esclarecedores sobre el tema y sobre normativa en general.

3.1 Ciberseguridad Resiliente (CRA)

En este documento se describe como debe ser la estructura a la hora de tratar una normativa en este caso habla sobre una norma actual que se ha aplicado en múltiples entornos empresariales [4].

3.2 Cambios en la normativa de ciberseguridad europea

En este estudio se ejemplifica los cambios consiguiente a la aprobación de la NIS2 y como va a cambiar el paradigma a nivel de ciberseguridad europea [5].

3.3 Taxonomía de los estándares de ciberseguridad

Este es el escrito más ilustrativo por la cantidad de leyes que relaciona y hace ver en el documento, además de una breve explicación realiza mapas conceptuales enlazando las diferentes normativas para agruparlas por bloques [6].

3.4 Auditorías de sistemas de gestión en empresas

Como se puede ver en este articulo docente también se realiza una pequeña guía para la realización de auditorías, así pues definiendo un estándar en uno de los procesos esenciales en los que se basa esta normativa [7].

3.5 Los metadatos en el ordenamiento jurídico español y europeo

El artículo presentado ilustra lo que son los metadatos, pero más importante aún hace una relación con las leyes que afectan a dichos datos y como se debe hacer su tratamiento según las directivas europeas explicando también el marco jurídico y legal [8].

3.6 Análisis de la firma electrónica en el contexto de la Transformación Digital en la Unión Europea

El documento que tratamos ahora es un extracto de un capítulo de un libro en el cual se ejemplifica el método de verificación de el cumplimiento de dicha transformación digital mediante la creación de firma electrónica, además de presentar el marco europeo y realizar un análisis junto al reglamento eIDAS [9].

CAPÍTULO 4
Comprender NIS2

La Directiva NIS2 [1] tiene como objetivo mejorar la ciberseguridad en la UE mediante:

1. La implementación de medidas de seguridad más robustas.
2. La mejora de la colaboración y el intercambio de información entre los Estados miembros.
3. El aumento de la resiliencia de las infraestructuras críticas y los servicios esenciales.

Hay que tener en cuenta, como se ha nombrado en el resumen, que hay ciertos ámbitos y sectores que se ven afectados por la normativa. Estos son algunos de los muchos sectores que deberán adecuarse a la nueva normativa:

1. Energía
2. Transporte
3. Agua
4. Salud
5. Infraestructura digital
6. Administraciones públicas
7. Banca y Finanzas
8. Productos químicos
9. Producción de alimentos

Teniendo en cuenta los puntos en los que la normativa UE NIS2 se centra y los sectores que se ven afectados, debemos tratar las diferencias que esta nueva normativa tiene con respecto a su antecesora, la normativa UE NIS. Subdividiremos las áreas que se ven afectadas por cambios a continuación.

4.1 Alcance y aplicabilidad

Mientras que la NIS se centra en un conjunto limitado de sectores críticos como energía, transporte, banca, salud, agua potable e infraestructuras digitales, la NIS2 amplía significativamente el alcance, incluyendo más sectores y subsectores como los servicios públicos, la gestión de residuos, la producción de alimentos, productos químicos, la fabricación, la gestión de riesgos, y más. Además, introduce criterios de tamaño para definir las entidades cubiertas, afectando así a más organizaciones.

4.2 Requisitos de seguridad

Por un lado, la NIS establece requisitos básicos de seguridad y notificación para los operadores de servicios esenciales y los proveedores de servicios digitales. Por otro lado, la NIS2 refuerza estos requisitos, introduciendo normas más estrictas y detalladas sobre gestión de riesgos, políticas de seguridad, medidas técnicas y operativas, así como plazos más cortos para la notificación de incidentes de seguridad.

4.3 Supervisión y ejecución

En cuanto a la NIS, establece autoridades nacionales de supervisión pero con poderes limitados y enfoques variados entre los Estados miembros. Sin embargo, la NIS2 refuerza las capacidades de supervisión y ejecución de las autoridades nacionales, incluyendo sanciones más severas y armonizadas para el incumplimiento, así como mecanismos de cooperación más sólidos entre los Estados miembros.

4.4 Gestión de incidentes

La NIS exige la notificación de incidentes de seguridad significativos. En contraste, la NIS2 establece procedimientos más claros y uniformes para la notificación de incidentes, incluyendo plazos específicos (por ejemplo, notificación inicial en 24 horas), y promueve la creación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRTs) en cada Estado miembro.

4.5 Cooperación y coordinación

Aunque la NIS introduce el Grupo de Cooperación y la red CSIRT para fomentar la cooperación entre los Estados miembros, la NIS2 refuerza estos mecanismos de cooperación, promoviendo una mayor colaboración y el intercambio de información entre las autoridades nacionales, y estableciendo un marco más sólido para la coordinación en caso de incidentes transfronterizos.

4.6 Impacto y cumplimiento

En términos de cumplimiento y sanciones, la NIS tiene un enfoque más limitado con variabilidad entre los Estados miembros. Por el contrario, la NIS2 introduce sanciones administrativas significativas a nivel europeo para asegurar el cumplimiento, incluyendo multas basadas en el volumen de negocios anual de las entidades no conformes, y obliga a los Estados miembros a aplicar sanciones efectivas, proporcionadas y disuasorias.

4.7 Revisión y actualización

Finalmente, aunque la NIS carece de mecanismos específicos para una revisión periódica integral, la NIS2 incluye disposiciones para la revisión periódica y actualización de las medidas de seguridad, asegurando que la normativa se mantenga relevante y eficaz frente a las nuevas amenazas y tecnologías emergentes.

Teniendo claro cuales son algunos de los sectores afectados por la normativa y las principales diferencias entre la normativa UE NIS[2] y la UE NIS2[1] podemos enfocarnos en los puntos clave para cumplir todos los requisitos que dicha normativa requiere.

CAPÍTULO 5
Evaluación Inicial

Durante este capitulo vamos a presentar los primeros pasos que debemos realizar para conformar nuestra guía.

5.1 Identificación de activos críticos

La identificación de activos críticos es un proceso fundamental en la gestión de riesgos [10] . Este proceso permite a las organizaciones determinar cuáles de sus recursos, infraestructuras o sistemas son esenciales para mantener sus operaciones y alcanzar sus objetivos empresariales. Identificar estos activos críticos ayuda a priorizar las medidas de protección y a asegurar la continuidad del negocio en caso de incidentes. Este proceso involucra varias etapas clave:

5.1.1. Definir los criterios de criticidad

La definición de criterios de criticidad se basa en evaluar y clasificar activos, sistemas o procesos de acuerdo a su importancia y el impacto que su falla o mal funcionamiento podría tener en una organización. Este proceso es esencial para la gestión del mantenimiento, la gestión de activos y la gestión de riesgos. Los criterios de criticidad se definen considerando varios factores clave, entre los que se incluyen:

1. Impacto en la Seguridad
2. Impacto en el Medio Ambiente
3. Impacto en la Producción o la Operación
4. Impacto Económico
5. Impacto en la Calidad
6. Impacto en la Reputación
7. Frecuencia y Probabilidad de Fallo
8. Requerimientos Regulatorios y Legales

Teniendo en cuenta esta lista debemos preguntarnos como de crítico es que se afecte a cada uno de estos factores.

5.1.2. Inventario de activos

Hacer un inventario de activos es un proceso esencial para la gestión eficiente de los recursos de una organización. Hay que tener en cuenta que no todos los activos son físicos y materiales por lo que algunos de los pasos que se vana describir no aplican completamente.

1. **Identificación del activo**
   Se debe definir claramente las categorías de activos (equipos, maquinaria, vehículos, software, mobiliario, etc.). Y proceder a su etiquetado y codificación en un sistema de etiquetado, como se puede ver en la figura 5.1 o codificación único para cada activo, facilitando su seguimiento y gestión.

Figura 5.1: Tipos de etiquetas que se pueden emplear

2. **Recolección de información**
   Debemos realizar una descripción detallada del activo, como su nombre, modelo, fabricante y características principales. Además de registrar el número de serie y cualquier otra identificación específica del activo, la fecha de adquisición y por último la ubicación física del activo, incluyendo edificio, sala o área específica.

3. **Información financiera**
   Se debe registrar el costo original de adquisición del activo e incluir el valor actual en los libros contables, teniendo en cuenta la depreciación, indicando la vida útil esperada del activo y teniendo en cuenta los costos de mantenimiento asociados al activo.

4. **Responsabilidad**
   Se asigna un responsable o propietario del activo dentro de la organización, además de registrar el departamento o unidad al que está asignado el activo.

5. **Sistema de gestión de activos**
   Se puede utilizar un software de gestión de activos para mantener el inventario actualizado y facilitar la gestión(Tanto de activos físicos como software) como se ve en la imagen 5.2. Es recomendable mantener toda la información en una base de datos centralizada y accesible por los usuarios administradores o que se encarguen de este proceso de inventariado en al empresa.

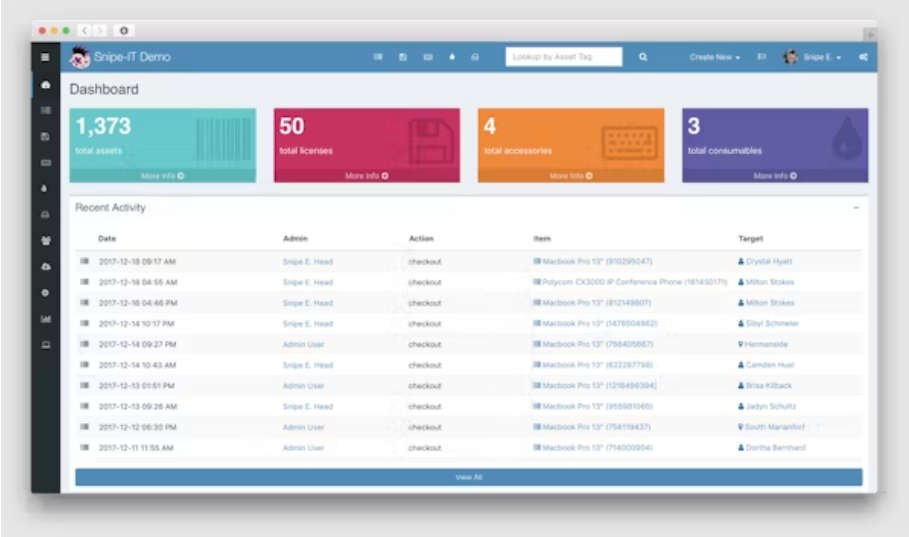

Figura 5.2: Inventario hardware/software con la herramienta SnipeIT

6. **Revisión y actualización**
   Realizar auditorías regulares del inventario para verificar la precisión y actualizar la información además de definir y documentar el proceso para dar de baja activos obsoletos o inservibles.

7. **Seguridad y cumplimiento**
   Asegurar que los activos estén protegidos contra robo, daño o pérdida. Además nos aseguraremos de que el inventario cumpla con las normativas legales y reguladoras aplicables.

5.2 Evaluación de Riesgos

Hay que identificar las amenazas que podrían afectar a cada activo. Determinar las vulnerabilidades que pueden ser explotadas. Evaluar el impacto potencial de la explotación de las vulnerabilidades. Y finalmente estimar la probabilidad de que las amenazas se materialicen. Uno de los aspecto importantes a evaluar es la seguridad de la información para esto podemos aplicar un marco de modelo llamado McCumber Cube creado por Jhon McCumber en 1991 [11] para ayudar a las organizaciones a establecer y evaluar iniciativas de seguridad de la información al considerar todos los factores relacionados que las afectan. Este modelo de seguridad tiene tres dimensiones:

1. Los principios fundamentales para proteger los sistemas de información (fig. 5.3).

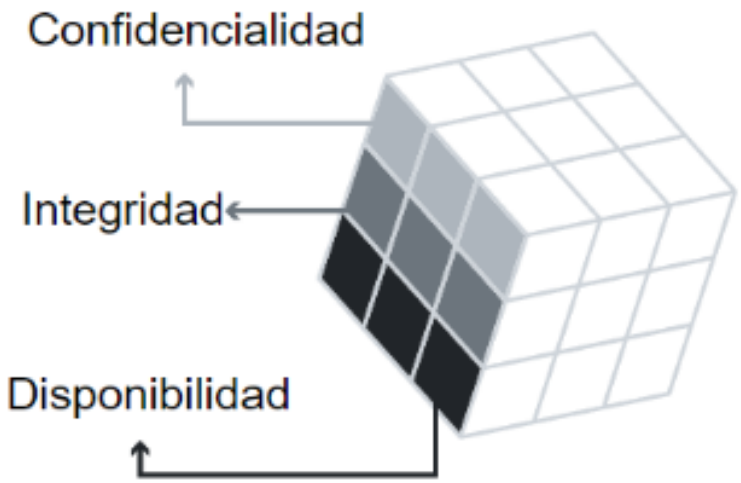

Figura 5.3: Primera cara del cubo de McCumber [3]

La confidencialidad es un conjunto de normas diseñadas para evitar que la información sensible sea divulgada a personas no autorizadas. Los métodos empleados para asegurar la confidencialidad incluyen el cifrado de datos, la autenticación y el control de acceso.

La integridad asegura que la información o los procesos del sistema estén protegidos contra modificaciones tanto intencionales como accidentales. Una manera de garantizar la integridad es mediante el uso de funciones hash o sumas de comprobación.

La disponibilidad implica que los usuarios autorizados pueden acceder a los sistemas y datos cuando y donde lo necesiten, mientras que aquellos que no cumplen con las condiciones establecidas no pueden hacerlo. Esto se logra a través del mantenimiento del equipo, la reparación del hardware, la actualización de los sistemas operativos y el software, y la creación de copias de seguridad.

2. La protección de la información en cada uno de sus estados posibles (fig. 5.4) .

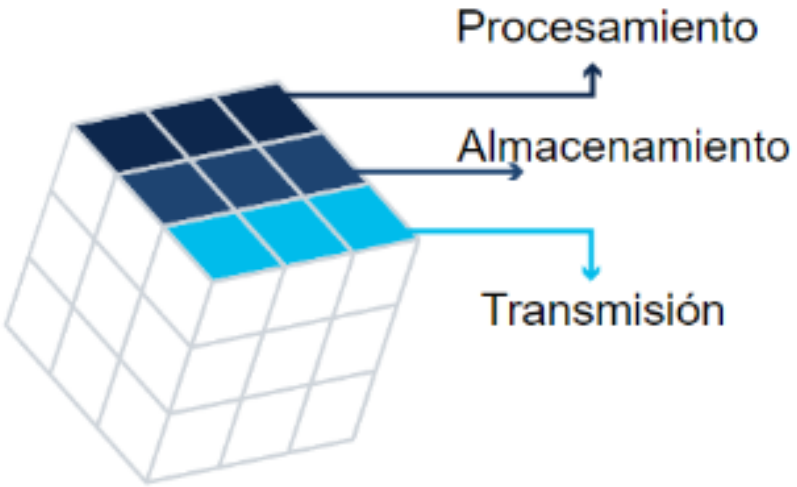

Figura 5.4: Segunda cara del cubo de McCumber [3]

El procesamiento se refiere al uso de datos para llevar a cabo diversas operaciones. Esto puede incluir actividades como la actualización de un registro en una base de datos, la ejecución de cálculos complejos, o la transformación de datos en un formato diferente. Durante el procesamiento, los datos pueden ser manipulados y analizados para obtener resultados específicos que apoyen las decisiones y acciones de la organización.

El almacenamiento se refiere a la retención de datos en diversos medios de almacenamiento. Esto puede incluir la memoria volátil, como la RAM, que se utiliza para el acceso rápido a los datos mientras el sistema está en funcionamiento. También incluye dispositivos de almacenamiento permanente, como discos duros, unidades de estado sólido (SSD) y unidades USB. Estos dispositivos permiten que los datos se guarden de manera segura y se recuperen cuando sea necesario, proporcionando una base sólida para la continuidad y la eficiencia operativa.

La transmisión se refiere al movimiento de datos entre diferentes sistemas de información. Esto puede ocurrir dentro de una red local, entre diferentes oficinas de una misma organización, o a través de internet entre diferentes entidades. La transmisión de datos es crucial para la comunicación y la colaboración efectiva, permitiendo que la información fluya de manera segura y eficiente desde un punto de origen a un destino específico. La integridad y la confidencialidad de los datos durante la transmisión son aspectos críticos que deben gestionarse cuidadosamente para prevenir accesos no autorizados y mantener la precisión de la información.

3. Las medidas de seguridad utilizadas para proteger los datos (fig. 5.5).

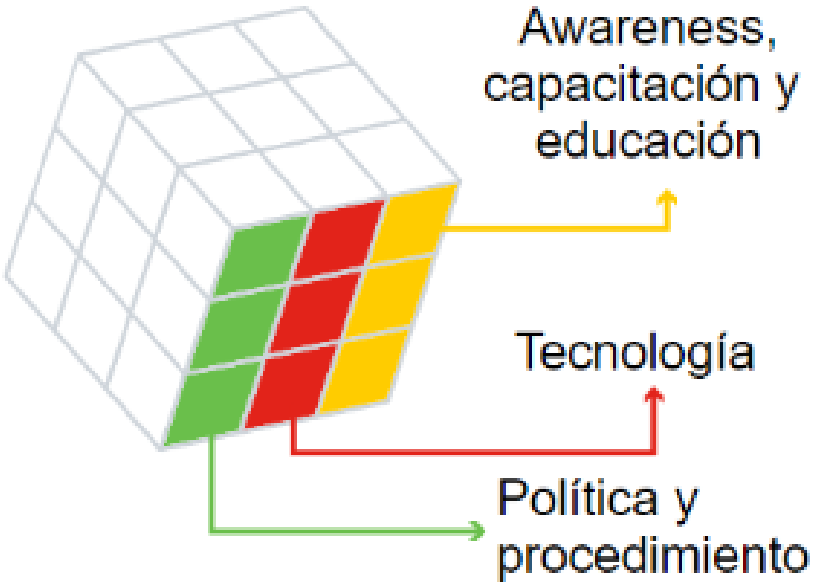

Figura 5.5: Tercera cara del cubo de McCumber [3]

La concienciación, la capacitación y la educación son medidas que una organización implementa para asegurar que los usuarios estén al tanto de las posibles amenazas a la seguridad y las acciones que pueden tomar para proteger los sistemas de información.

La tecnología se refiere a las soluciones basadas en software y hardware diseñadas para salvaguardar los sistemas de información, como los firewalls, que monitorizan continuamente la red en busca de posibles incidentes maliciosos.

La política y los procedimientos se refieren a los controles administrativos que establecen una base para cómo una organización asegura la información, incluyendo planes de respuesta a incidentes y directrices de mejores prácticas.

5.3 Identificación de Brechas de Cumplimiento

La Identificación de Brechas de Cumplimiento es un proceso mediante el cual una organización evalúa sus prácticas, políticas y procedimientos actuales para determinar si cumplen con los requisitos legales, reglamentarios y normativos aplicables. Este proceso es esencial para identificar áreas donde la organización no está cumpliendo completamente con las normas o donde existen riesgos de incumplimiento, permitiendo tomar medidas correctivas para mitigar estos riesgos. A continuación, se describen dos aspectos a tener en cuenta:

1. **Revisión de normativa** Realizar una revisión de las normativas europea, como la Directiva NIS2, es un proceso estructurado para asegurar el cumplimiento y la adaptación a los nuevos requisitos legales.

2. **Informe de Brechas** Un informe de brechas es un documento que identifica y evalúa las discrepancias o deficiencias entre el estado actual de una organización y los requisitos establecidos por normas, regulaciones, políticas internas o mejores prácticas de la industria. Este tipo de informe es crucial para la gestión del cumplimiento y la mejora continua de los procesos dentro de una organización. Aquí se detalla en qué consiste:

   a) Identificar Discrepancias: Detectar áreas donde la organización no cumple completamente con los requisitos.

   b) Evaluar el Impacto: Analizar el impacto potencial de estas brechas en la operación, la seguridad, la calidad y la conformidad legal

   c) Recomendar Acciones: Proponer acciones correctivas para cerrar las brechas identificadas.

CAPÍTULO 6
Medidas de seguridad

6.1 Gestión de Accesos y Autenticación

6.1.1. Establecimiento de Políticas de Acceso y Autenticación

1. Definición de roles y responsabilidades:

   a) Asignar roles específicos y definir claramente las responsabilidades de cada usuario.

   b) Documentar los niveles de acceso necesarios para cada rol dentro de la organización.

2. Política de control de acceso:

   a) Crear y mantener una política de control de acceso que especifique quién puede acceder a qué recursos.

   b) Revisar y actualizar la política regularmente.

3. Autenticación multifactor (MFA):

   a) Implementar MFA para añadir una capa extra de seguridad. Utilizar combinaciones de algo que el usuario sabe (contraseña), algo que el usuario tiene (token, teléfono móvil) y algo que el usuario es (biometría).

6.1.2. Implementación de Controles de Acceso

1. Control de acceso basado en roles (RBAC) [12] [13] :

   a) Configurar los sistemas para que los accesos se basen en los roles y responsabilidades definidos.

   b) Asegurarse de que cada usuario solo tenga los permisos necesarios para realizar su trabajo.

2. Principio de privilegio mínimo:

   a) Asignar los privilegios más bajos posibles que aún permitan a los usuarios realizar sus funciones.

   b) Revisar periódicamente los permisos para asegurarse de que los usuarios no tengan más acceso del necesario.

3. Segregación de funciones (SoD) [14]:

Figura 6.1: Diagrama de la separación de tareas críticas

a) Separar las tareas críticas entre diferentes personas 6.1 para evitar conflictos de intereses y fraude.

b) Implementar controles que requieran la colaboración de más de una persona para realizar tareas sensibles.

6.1.3. Gestión de Identidades

1. Sistema de gestión de identidades (IDM):

   a) Utilizar un sistema de gestión de identidades para centralizar y automatizar la creación, modificación y eliminación de cuentas de usuario.

   b) Integrar el IDM con los sistemas de la organización para un control de acceso coherente.

2. Provisionamiento y desprovisionamiento automatizado:

   a) Automatizar el proceso de alta y baja de usuarios para garantizar que los accesos sean otorgados y revocados oportunamente.

   b) Implementar flujos de trabajo que aseguren la revisión y aprobación antes de conceder o revocar accesos.

6.1.4. Gestión de Contraseñas

1. Política de contraseñas fuertes:
   a) Requerir que las contraseñas cumplan con ciertos criterios de complejidad (longitud mínima, combinación de letras, números y símbolos).
   b) Implementar políticas de caducidad y reutilización de contraseñas.
2. Almacenamiento seguro de contraseñas:
   a) Utilizar técnicas de hashing [15] y salting para almacenar contraseñas de forma segura.
   b) No almacenar contraseñas en texto claro en ningún sistema.
3. Herramientas de gestión de contraseñas:
   a) Fomentar el uso de gestores de contraseñas para que los usuarios puedan manejar contraseñas complejas sin necesidad de recordarlas todas.

6.2 Seguridad de las comunicaciones y redes

6.2.1. Protección de la Infraestructura de Red

1. Segmentación de la red:
   a) Dividir la red en segmentos más pequeños y seguros para limitar el alcance de posibles ataques.
   b) Utilizar VLANs (Virtual Local Area Networks) y subredes para aislar los distintos tipos de tráfico.
2. Firewalls y sistemas de prevención de intrusos (IPS):
   a) Implementar firewalls para controlar el tráfico entrante y saliente basado en reglas definidas.
   b) Utilizar sistemas de prevención de intrusos (IPS) para detectar y bloquear actividades sospechosas en tiempo real.

6.2.2. Seguridad de las Comunicaciones

1. Cifrado de datos en tránsito:
   a) Utilizar protocolos seguros como HTTPS, TLS/SSL para cifrar las comunicaciones a través de la red.
   b) Implementar VPNs (Redes Privadas Virtuales) para asegurar las conexiones remotas y proteger los datos en tránsito.
2. Certificados digitales y PKI (Infraestructura de Clave Pública):
   a) Utilizar certificados digitales para autenticar y cifrar las comunicaciones entre servidores y clientes.
   b) Implementar una infraestructura de clave pública (PKI) para gestionar los certificados y las claves criptográficas.

6.2.3. Monitoreo y Detección de Amenazas

1. Monitoreo continuo:

   a) Implementar soluciones de monitoreo continuo para supervisar el tráfico de red y detectar actividades sospechosas.

   b) Utilizar sistemas de detección de intrusos (IDS) para identificar comportamientos anómalos.

2. SIEM (Security Information and Event Management):

Figura 6.2: Diagrama de SIEM

   a) Implementar una solución SIEM 6.2 para recolectar y analizar logs de eventos de seguridad en tiempo real.

   b) Correlacionar datos de diferentes fuentes para detectar patrones de ataque y responder rápidamente a incidentes.

CAPÍTULO 7
Gestión de Incidentes

7.1 Establecimiento de un plan de respuesta e incidentes

7.1.1. Desarrollo de la Política de Respuesta a Incidentes

1. Objetivos del plan:
   Definir los objetivos principales del plan de respuesta a incidentes, como la minimización del impacto de los incidentes, la protección de los datos y la restauración rápida de las operaciones.

2. Alcance del plan:
   Determinar el alcance del plan, especificando los tipos de incidentes cubiertos, los sistemas y datos afectados y los límites de la responsabilidad del equipo de respuesta.

7.1.2. Formación del Equipo de Respuesta a Incidentes (IRT)

1. Composición del equipo:

   a) Incluir miembros de varias disciplinas, como TI, seguridad de la información, comunicaciones, recursos humanos y asuntos legales.

   b) Definir claramente los roles y responsabilidades de cada miembro del equipo.

2. Capacitación del equipo:

   a) Proporcionar formación regular y específica sobre técnicas de respuesta a incidentes, manejo de herramientas de seguridad y procedimientos de comunicación.

   b) Realizar ejercicios de simulación y escenarios de prueba para evaluar la preparación del equipo.

7.1.3. Identificación y Clasificación de Incidentes

1. Tipos de incidentes:
   Categorizar los incidentes en diferentes tipos, como malware, acceso no autorizado, pérdida de datos, ataques de denegación de servicio (DoS), etc.

2. Clasificación de la severidad:

   a) Definir niveles de severidad (bajo, medio, alto, crítico) basados en el impacto potencial del incidente en la organización.

   b) Establecer criterios claros para la clasificación de incidentes según su severidad.

7.1.4. Procedimientos de Detección y Notificación

1. Detección de incidentes:

   a) Implementar sistemas de monitoreo y detección de intrusos (IDS/IPS) para identificar actividades sospechosas en tiempo real.

   b) Utilizar herramientas de análisis de logs y soluciones de SIEM para correlacionar eventos y detectar patrones anómalos.

2. Notificación de incidentes:

   a) Establecer procedimientos para la notificación inmediata de incidentes a los miembros del IRT y a las partes interesadas relevantes.

   b) Proporcionar canales de comunicación seguros y fiables para reportar incidentes (correo electrónico cifrado, líneas telefónicas seguras, etc...).

7.1.5. Fases del Plan de Respuesta a Incidentes

1. Preparación:

   a) Inventario de activos:
   Mantener un inventario actualizado de los activos críticos y sistemas de información e identificar y documentar los contactos clave y las partes interesadas.

   b) Desarrollo de playbooks:
   Crear playbooks específicos para distintos tipos de incidentes, detallando los pasos a seguir durante la respuesta.

2. Identificación:

   a) Análisis de incidentes:

      1) Verificar y analizar la información del incidente para determinar su naturaleza y alcance.
      2) Utilizar herramientas forenses y de análisis para recopilar evidencias y entender el impacto del incidente.

3. Contención:

   a) Contención a corto plazo:

      1) Implementar medidas inmediatas para limitar el alcance del incidente (e.g., desconectar sistemas afectados, bloquear IPs maliciosas)
      2) Asegurar que las acciones de contención no interfieran con la recopilación de evidencias.

b) Contención a largo plazo:
   1) Aplicar parches, actualizar configuraciones y realizar cambios necesarios para evitar la reaparición del incidente.
   2) Planificar la restauración de los sistemas a su estado normal de operación de manera controlada.

4. Erradicación:

   a) Eliminación de la amenaza:
      1) Identificar y eliminar todas las formas de la amenaza (e.g., malware, accesos no autorizados, cuentas comprometidas).
      2) Realizar análisis completos para asegurarse de que no queden remanentes de la amenaza en el sistema.

5. Recuperación:

   a) Restauración de sistemas:
      1) Restaurar los sistemas y servicios afectados a su estado operativo normal, asegurándose de que estén completamente limpios y seguros.
      2) Verificar que todas las medidas de seguridad estén implementadas correctamente antes de volver a poner los sistemas en línea.
   b) Pruebas de validación:
      1) Realizar pruebas exhaustivas para asegurar que los sistemas funcionan correctamente y que las vulnerabilidades han sido corregidas.
      2) Monitorizar los sistemas restaurados para detectar posibles actividades sospechosas.

6. Lecciones Aprendidas:

   a) Análisis post-incidente:
      1) Realizar una revisión detallada del incidente, documentando los hallazgos, las acciones tomadas y las lecciones aprendidas.
      2) Identificar áreas de mejora en los procedimientos y controles de seguridad.
   b) Actualización de políticas y procedimientos:
      1) Actualizar las políticas, los procedimientos y los playbooks basados en las lecciones aprendidas del incidente.
      2) Implementar mejoras para prevenir futuros incidentes y mejorar la respuesta.

7.1.6. Comunicación y Reporte

1. Plan de comunicación:

   a) Desarrollar un plan de comunicación que especifique cómo se debe comunicar internamente y externamente durante un incidente.
   b) Identificar los puntos de contacto clave y definir los canales de comunicación seguros.

2. Reporte de incidentes:

    a) Mantener registros detallados de todos los incidentes y las acciones tomadas durante la respuesta.

    b) Proporcionar informes regulares a la alta dirección y a las partes interesadas relevantes.

Implementar estos puntos asegurará que la organización esté preparada para manejar incidentes de seguridad de manera eficaz, minimizando el impacto y restaurando rápidamente las operaciones normales.

CAPÍTULO 8
Gobernanza y gestión

8.1 Políticas y procedimientos de ciberseguridad

Trataremos en este apartado las diferentes políticas a aplicar y sus procedimientos todo con el fin de que la normativa NIS2 se aplique lo más rigurosamente posible.

8.1.1. Políticas de Ciberseguridad

1. Política de Gestión de Riesgos de Ciberseguridad:
   - *a*) Evaluación continua de riesgos cibernéticos.
   - *b*) Implementación de medidas de mitigación de riesgos.
   - *c*) Revisión y actualización periódica de la evaluación de riesgos.
2. Política de Seguridad de la Información:
   - *a*) Definición de roles y responsabilidades en seguridad de la información.
   - *b*) Alineación con estándares internacionales (ISO/IEC 27001) [16].
3. Política de Respuesta a Incidentes de Seguridad:
   - *a*) Procedimientos para la detección y respuesta a incidentes de seguridad.
   - *b*) Planes de comunicación interna y externa durante incidentes.
   - *c*) Coordinación con autoridades competentes y CSIRTs (Computer Security Incident Response Teams).
4. Política de Continuidad del Negocio y Recuperación ante Desastres:
   - *a*) Estrategias para asegurar la continuidad de las operaciones críticas.
   - *b*) Planes de recuperación de sistemas y datos después de un incidente.
5. Política de Gestión de Accesos:
   - *a*) Control de acceso basado en roles (RBAC).
   - *b*) Autenticación multifactor (MFA) para accesos sensibles.
   - *c*) Revisión y auditoría periódica de accesos.

6. Política de Seguridad en el Desarrollo de Software:
    a) Integración de prácticas de desarrollo seguro (DevSecOps) [17] .
    b) Evaluación de vulnerabilidades y pruebas de penetración.
7. Política de Concienciación y Formación en Ciberseguridad:
    a) Programas de formación continua para empleados.
    b) Campañas de concienciación sobre ciberseguridad [18].
8. Política de Gestión de Proveedores y Terceros:
    a) Evaluación de riesgos de terceros y proveedores.
    b) Requisitos de seguridad para contratos y acuerdos con terceros.

8.1.2. Procedimientos de Ciberseguridad

1. Procedimiento de Evaluación de Riesgos:
    a) Metodología para identificar y evaluar riesgos cibernéticos.
    b) Registro y seguimiento de los riesgos identificados.
2. Procedimiento de Gestión de Incidentes:
    a) Pasos detallados para identificar, analizar, contener y erradicar incidentes.
    b) Registro y documentación de incidentes y respuestas.
3. Procedimiento de Gestión de Vulnerabilidades:
    a) Identificación y priorización de vulnerabilidades.
    b) Implementación de parches y actualizaciones de seguridad.
4. Procedimiento de Gestión de Accesos:
    a) Proceso para la creación, modificación y eliminación de cuentas de usuario.
    b) Revisión periódica de los derechos de acceso.
5. Procedimiento de Respaldo y Recuperación de Datos:
    a) Frecuencia y métodos de respaldo de datos.
    b) Pruebas periódicas de recuperación de datos.
6. Procedimiento de Gestión de la Configuración y Cambios:
    a) Control de cambios en la configuración de sistemas y redes.
    b) Aprobación y documentación de cambios.
7. Procedimiento de Monitoreo y Detección de Amenazas:
    a) Implementación de sistemas de monitoreo continuo.
    b) Análisis de logs y alertas de seguridad [19].
8. Procedimiento de Formación y Concienciación:
    a) Programas de capacitación para nuevos empleados [20].
    b) Sesiones periódicas de actualización en ciberseguridad.

8.2 Asignación de responsabilidades

La asignación de responsabilidades en una empresa para garantizar la máxima seguridad en el ámbito de la ciberseguridad debe ser clara, estructurada y alineada con las mejores prácticas de gestión de seguridad de la información.Aquí se describe cómo se debe realizar esta asignación de responsabilidades:

1. Gobierno y Liderazgo

   a) Consejo de Administración / Dirección Ejecutiva
   Responsabilidades:
      1) Establecer la visión y la estrategia de ciberseguridad.
      2) Aprobar políticas y procedimientos de ciberseguridad.
      3) Asegurar la asignación de recursos necesarios para ciberseguridad.
      4) Evaluar y gestionar riesgos cibernéticos a nivel estratégico.
      5) Supervisar el cumplimiento de normativas y regulaciones.

   b) Chief Information Security Officer (CISO) / Director de Ciberseguridad
   Responsabilidades:
      1) Desarrollar y implementar la estrategia de ciberseguridad.
      2) Coordinar las políticas, procedimientos y controles de ciberseguridad.
      3) Informar al Consejo de Administración sobre el estado de la ciberseguridad.
      4) Liderar la respuesta a incidentes de seguridad.
      5) Supervisar la evaluación de riesgos y la implementación de medidas de mitigación.

2. Operaciones de Ciberseguridad

   a) Equipo de Seguridad de la Información
   Responsabilidades:
      1) Monitorear y analizar eventos de seguridad.
      2) Gestionar incidentes y vulnerabilidades.
      3) Implementar y mantener sistemas de defensa y detección de intrusiones.
      4) Realizar auditorías de seguridad y pruebas de penetración.
      5) Administrar accesos y permisos.

   b) Equipo de Respuesta a Incidentes (IRT)
   Responsabilidades:
      1) Detectar, analizar y responder a incidentes de ciberseguridad.
      2) Contener y erradicar amenazas.
      3) Recuperar sistemas afectados y restaurar la operación normal.
      4) Documentar y reportar incidentes y lecciones aprendidas.

3. Desarrollo y Mantenimiento de Sistemas

    a) Equipo de Desarrollo de Software / DevSecOps
    Responsabilidades:
        1) Integrar prácticas de seguridad en el ciclo de vida del desarrollo de software (SDLC) [21] .
        2) Realizar revisiones de código y análisis de vulnerabilidades.
        3) Implementar controles de seguridad en aplicaciones y sistemas.
        4) Colaborar con el equipo de seguridad para pruebas de penetración y auditorías.

4. Operaciones de TI

    a) Administradores de Sistemas y Redes
    Responsabilidades:
        1) Configurar y mantener la infraestructura de TI segura.
        2) Aplicar parches y actualizaciones de seguridad.
        3) Implementar y gestionar controles de acceso.
        4) Realizar copias de seguridad y asegurar la integridad de los datos.

5. Usuarios y Formación

    a) Empleados
    Responsabilidades:
        1) Seguir las políticas y procedimientos de ciberseguridad.
        2) Participar en programas de formación y concienciación en ciberseguridad.
        3) Reportar actividades sospechosas o incidentes de seguridad.

6. Gestión de Proveedores y Terceros

    a) Gestores de Relaciones con Proveedores
    Responsabilidades:
        1) Evaluar y gestionar los riesgos de ciberseguridad asociados con proveedores y terceros.
        2) Asegurar que los proveedores cumplan con los requisitos de seguridad establecidos.
        3) Monitorear el desempeño y cumplimiento de los acuerdos de seguridad con proveedores.

7. Cumplimiento y Auditoría

    a) Equipo de Cumplimiento y Auditoría
    Responsabilidades:
        1) Verificar el cumplimiento de políticas y normativas de ciberseguridad.
        2) Realizar auditorías regulares y evaluaciones de conformidad.
        3) Reportar hallazgos y recomendaciones a la alta dirección.

8. Recursos Humanos

    a) Equipo de Recursos Humanos
    Responsabilidades:

1) Integrar la seguridad en los procesos de contratación y desvinculación de empleados.
2) Realizar verificaciones de antecedentes para roles críticos en ciberseguridad.
3) Asegurar la formación continua en ciberseguridad para todos los empleados.

8.3 Formación y concienciación

1. Programas de Formación y Capacitación

   a) Formación Inicial

      1) Orientación de Nuevos Empleados: Incluir módulos de ciberseguridad en la inducción de nuevos empleados.
      2) Entrenamiento Obligatorio: Sesiones formales sobre ciberseguridad que cubran políticas, procedimientos y mejores prácticas [22].

   b) Capacitación Continua

      1) Sesiones Periódicas: Talleres y seminarios regulares para actualizar conocimientos sobre nuevas amenazas y tecnologías de seguridad.
      2) Cursos en Línea: Plataformas de aprendizaje en línea que ofrecen flexibilidad para que los empleados completen cursos a su ritmo.

2. Simulacros y Ejercicios de Ciberseguridad

By Victim Count

Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

*Descriptors**			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

Figura 8.1: Estadística de los ciberataques más comunes en 2022

a) Simulaciones de Phishing

b) Enviar correos electrónicos de phishing 8.1 simulados para evaluar la respuesta de los empleados y proporcionar retroalimentación inmediata.

c) Ofrecer formación adicional para aquellos que caigan en la simulación.

3. Ejercicios de Respuesta a Incidentes

   a) Realizar simulacros de incidentes de ciberseguridad para practicar y mejorar la respuesta de la empresa [23].

   b) Evaluar la eficacia de los procedimientos de respuesta y realizar ajustes según sea necesario.

4. Políticas Claras y Accesible

   a) Documentación de Políticas

      1) Crear y mantener políticas de ciberseguridad claras y comprensibles.
      2) Asegurarse de que las políticas estén fácilmente accesibles para todos los empleados.

   b) Recordatorios Periódicos

      1) Enviar recordatorios regulares sobre políticas clave y procedimientos de seguridad.

CAPÍTULO 9
Colaboración y coordinación

9.1 Cooperación con autoridades nacionales y europeas

La cooperación entre las empresas y las autoridades tanto nacionales como europeas es uno de los puntos claves, ya que ayuda de manera directa a la creación de un espacio seguro para todos los involucrados. Existen varias tareas que se pueden hacer entre otras:

1. Establecer Canales de Comunicación:
   Abre líneas de comunicación con las autoridades competentes en tu país para reportar incidentes y recibir orientación.
2. Participar en Grupos de Trabajo y Foros:
   Involúcrate en grupos de trabajo y foros de ciberseguridad nacionales y europeos para compartir información y mejores prácticas.
3. Plataformas de Intercambio de Información:
   Utiliza plataformas como MISP (Malware Information Sharing Platform) para compartir información sobre amenazas y vulnerabilidades con otras organizaciones y autoridades.

9.2 Plataformas y Herramientas de Apoyo

Además de todas las tareas de cara a la cooperación que se han comentado en el apartado anterior es recomendable colaborar con los Equipos de Respuesta a Incidentes de Seguridad Informática (CERTs) y los Equipos de Respuesta a Incidentes de Seguridad Informática a nivel nacional y europeo (CSIRTs) aquí se describen algunas entidades que pueden ser de vital importancia de cara a un problema en ciberseguridad:

1. ENISA (Agencia de la Unión Europea para la Ciberseguridad)
2. INCIBE [24]
3. CCN-CERT [25]

CAPÍTULO 10
Auditoría y cumplimiento

10.1 Auditorías internas y externas

1. Planificación y Preparación

    a) Definir el Alcance y los Objetivos

        1) Determinar las áreas y sistemas que serán auditados.
        2) Establecer objetivos claros, como evaluar la conformidad con políticas internas y regulaciones, identificar vulnerabilidades y proponer mejoras.

    b) Reunir un Equipo de Auditoría

        1) Formar un equipo con las habilidades y conocimientos necesarios.
        2) Incluir auditores internos de ciberseguridad, expertos en TI y, si es necesario, personal de otras áreas relevantes.

    c) Desarrollar un Plan de Auditoría

        1) Crear un cronograma detallado que incluya todas las actividades de la auditoría.
        2) Identificar las metodologías y herramientas que se utilizarán [26].

2. Entrevistas y Evaluaciones de Cumplimiento

    a) Entrevistar al Personal Clave

        1) Hablar con el personal de TI y otros empleados clave para entender las prácticas y controles actuales.
        2) Evaluar el nivel de conciencia y cumplimiento de las políticas de ciberseguridad.

    b) Evaluación del Cumplimiento Normativo

        1) Verificar la conformidad con leyes y regulaciones aplicables (p. ej., GDPR [27], HIPAA [28]).
        2) Revisar la implementación de controles específicos exigidos por normativas.

3. Análisis y Evaluación

   a) Analizar los Hallazgos

      1) Comparar los resultados de la auditoría con los objetivos y criterios definidos.
      2) Identificar brechas y áreas de mejora en la postura de ciberseguridad.

   b) Evaluar el Impacto de los Riesgos Identificados

      1) Determinar el impacto potencial y la probabilidad de los riesgos identificados.
      2) Priorizar los riesgos según su criticidad.

4. Informe de Auditoría

   a) Documentar los Resultados

      1) Preparar un informe detallado que incluya todos los hallazgos, análisis y recomendaciones [29].
      2) Incluir gráficos y tablas para ilustrar los datos relevantes.

   b) Proporcionar Recomendaciones

      1) Sugerir medidas correctivas y mejoras para mitigar los riesgos identificados mediante guías como las que proporciona el CCN-CERT [30].
      2) Priorizar las recomendaciones según su impacto y urgencia

5. Presentación y Seguimiento

   a) Presentar el Informe a la Alta Dirección

      1) Presentar los hallazgos y recomendaciones al equipo de liderazgo y otras partes interesadas.
      2) Discutir los próximos pasos y obtener aprobación para las acciones propuestas.

   b) Desarrollar un Plan de Acción

      1) Crear un plan detallado para implementar las recomendaciones.
      2) Asignar responsabilidades y establecer plazos para la ejecución.

   c) Monitorear el Progreso

      1) Realizar seguimientos regulares para asegurar que las medidas correctivas se implementen efectivamente.
      2) Re-evaluar los riesgos y ajustar el plan según sea necesario.

6. Revisión Post-Auditoría

   a) Evaluar la Efectividad de las Medidas Implementadas

      1) Revisar el impacto de las acciones correctivas.
      2) Asegurarse de que los objetivos de la auditoría hayan sido alcanzados.

   b) Actualizar Políticas y Procedimientos

      1) Revisar y actualizar las políticas y procedimientos de ciberseguridad según los resultados de la auditoría.
      2) Asegurar que los cambios se comuniquen a todo el personal y se integren en la cultura organizacional.

10.2 Monitoreo continuo

El monitoreo constante de la ciberseguridad en una empresa es esencial para detectar tempranamente amenazas cibernéticas, proteger datos sensibles, cumplir con regulaciones normativas e identificar vulnerabilidades antes de que sean explotadas por ciberdelincuentes. Este monitoreo continuo no solo permite una respuesta rápida a incidentes de seguridad, minimizando su impacto y costes asociados, sino que también fortalece las defensas de la empresa, reduciendo su exposición a riesgos y garantizando la confianza de los clientes y partes interesadas en la seguridad de la información.

10.3 Informes de cumplimiento

1. Introducción

    a) Contexto: Breve descripción del propósito del informe y el alcance del cumplimiento evaluado.

    b) Objetivos: Explicar los objetivos del informe y los estándares o regulaciones a los que se hace referencia.

2. Resumen Ejecutivo

    a) Breve Resumen: Síntesis de los hallazgos clave y el estado general de cumplimiento.

    b) Destacar Conclusiones: Identificar áreas de cumplimiento sólido y aquellas que requieren atención adicional.

3. Marco de Referencia

    a) Normativas y Estándares: Enumerar y describir las regulaciones, políticas internas y estándares de la industria relevantes.

    b) Metodología de Evaluación: Describir el enfoque utilizado para evaluar el cumplimiento.

4. Hallazgos de Cumplimiento

    a) Descripción General: Detallar los hallazgos específicos relacionados con el cumplimiento de cada normativa o estándar evaluado.

    b) Evidencia de Cumplimiento: Proporcionar documentación o evidencia de apoyo, como registros, políticas, procedimientos, etc.

    c) Niveles de Cumplimiento: Clasificar los hallazgos en términos de cumplimiento completo, parcial o no cumplimiento.

5. Conclusiones y Recomendaciones

    a) Conclusiones: Resumir las principales conclusiones derivadas de los hallazgos de cumplimiento.

    b) Recomendaciones: Sugerir acciones correctivas y mejoras para abordar las deficiencias identificadas.

6. Plan de Acción Correctiva

    a) Acciones Propuestas: Detallar las medidas específicas que se tomarán para abordar las áreas de no cumplimiento.

    b) Responsabilidades: Asignar responsabilidades claras para la implementación de cada acción correctiva.

    c) Plazos: Establecer fechas límite realistas para la finalización de cada acción correctiva.

7. Anexos

    a) Documentación de Apoyo: Incluir cualquier documentación adicional que respalde los hallazgos y conclusiones del informe.

    b) Glosario: Definir términos técnicos o acrónimos utilizados en el informe, si es necesario.

8. Firmas y Aprobaciones

    a) Firma del Responsable: Obtener la firma del responsable del informe como evidencia de su revisión y aprobación.

    b) Firma de los Responsables de Área: Si es aplicable, obtener las firmas de los responsables de las áreas evaluadas.

CAPÍTULO 11
Conclusiones

11.1 Beneficios de cumplir con NIS2

Cumplir con la normativa europea NIS2 ofrece a las empresas una serie de beneficios significativos. En primer lugar, mejora la ciberseguridad al implementar medidas más robustas y desarrollar capacidades para una rápida respuesta a incidentes, protegiendo así la infraestructura crítica y los datos sensibles. Además, el cumplimiento evita sanciones legales y facilita la adherencia a otras regulaciones relacionadas. Desde una perspectiva comercial, cumplir con NIS2 fortalece la reputación de la empresa y aumenta la confianza de clientes y socios, quienes valoran el compromiso con la seguridad de la información. En conjunto, estos beneficios no solo protegen a la empresa contra amenazas cibernéticas, sino que también la posicionan favorablemente en el mercado. En definitiva el cumplimiento de la normativa es obligatorio por lo que esta guía puede ayudar de manera positiva a su cumplimiento. Desde mi punto de vista creo que es una normativa necesaria con el auge de tecnologías como la IA que puede ser enfocada a la explotación de vulnerabilidades y que hace la vida mucho mas sencilla para el atacante y mucho más complicada para el defensor. Creo que es un buen rumbo que toda la UE se haya decidido por un marco común y de ayuda conjunta, pero creo que habrá que seguir trabajando conforme a los avances tecnológicos como siempre ha pasado en este campo. Finalmente se ha podido realizar un análisis exhaustivo de la normativa NIS2 y generar un desglose de los temas principales y puntos a tener en cuenta. Así pues proceder en el capítulo 13 Anexo TIC a la construcción de un recurso para la autogestión del cumplimiento de dicha normativa

CAPÍTULO 12
ODS's

12.1 Cumplimiento de las ODS

Trataremos ahora el grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS)[31]

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No procede
ODS 1.- Fin de la pobreza				X
ODS 2.- Hambre cero				X
ODS 3.- Salud y bienestar				X
ODS 4.- Educación de calidad		X		
ODS 5.- Igualdad de género				X
ODS 6.- Agua limpia y saneamiento				X
ODS 7.- Energía asequible y no contaminante				X
ODS 8.- Trabajo decente y crecimiento económico		X		
ODS 9.- Industria, innovación e infraestructuras	X			
ODS 10.- Reducción de las desigualdades				X
ODS 11.- Ciudades y comunidades sostenibles				X
ODS 12.- Producción y consumo responsable				X
ODS 13.- Acción por el clima				X
ODS 14.- Vida submarina				X
ODS 15.- Vida de ecosistemas terrestres				X
ODS 16.- Paz, justicia e instituciones sólidas		X		
ODS 17.- Alianzas para lograr objetivos	X			

Figura 12.1: Cumplimiento de las ODS en relación al proyecto

Como se puede ver en la imagen tiene dos áreas en las que el nivel de involucración es bastante alto como pueden ser la ODS.9 y la ODS.17 ya que es un proyecto que se basa en el cumplimiento empresaria de una normativa europea y la propia normativa esta diseñada para crear un ambiente de colaboración en todo el territorio europeo. Por otro lado tenemos las ODS's 4, 8 y 16 la cuales no llegan a tener un nivel tan alto de involucración pero que también se ajustan a la descripción de este documento, como puede ser la educación de calidad (ODS.4) ya que la normativa incita a educar y a enseñar a los empleados material en el ámbito de la ciberseguridad, por otra parte esta la ODS.8 ya que promueve la seguridad de los trabajadores y la decencia de la empresa de cara a datos personales que puede tratar tanto de empleados internos como de clientes y por último la ODS.16 que recalca el hecho de la justicia y las instituciones solidas que es uno de los pilares sobre los que se redacta la normativa europea que se trata durante todo el documento.

CAPÍTULO 13
Anexo TIC

Como se mencionó en los objetivos al principio del documento, en este apartado se ha desarrollado una solución TIC [32] para facilitar el seguimiento de toda la normativa y los puntos a cumplir dentro de la empresa, mediante un documento de auditoría interna. Esta herramienta ha sido diseñada específicamente para asegurar que se cubren todos los aspectos relevantes de la normativa aplicable y que se realiza un seguimiento exhaustivo del cumplimiento. Se ha optado por utilizar una escala Likert de 5 puntos para evaluar cada uno de los puntos relacionados con la normativa, ya que proporciona una medida clara y comprensible para todos los usuarios, facilitando la comparación de los resultados entre diferentes áreas de la empresa o entre diferentes periodos de auditoría y permitiendo identificar tendencias y áreas que requieren atención. Además, la escala es lo suficientemente flexible como para adaptarse a diversos tipos de normativa y a diferentes contextos dentro de la empresa, equilibrando adecuadamente la complejidad y la utilidad. La amplia aceptación y reconocimiento de la escala Likert en diversas disciplinas garantiza que los resultados serán fácilmente entendidos y aceptados tanto por el personal interno como por auditores externos, contribuyendo a una cultura de cumplimiento y mejora continua dentro de la organización.

Bibliografía

[1] Agencia Estatal Boletín Oficial del Estado. (2022) Directiva (ue) 2022/81963. [Online]. Available: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

[2] ——. (2016) Doue-l-2016-81297. [Online]. Available: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-81297

[3] laprovittera.com.ar, "Ciberseguridad en 2022," 2024. [Online]. Available: https://laprovittera.com.ar/ciberseguridad-en-2022/

[4] I. Kamara, "European cybersecurity standardisation: a tale of two solitudes in view of europe's cyber resilience," *Innovation: The European Journal of Social Science Research*, pp. 1–20, 2024.

[5] P. G. Chiara, "Towards a right to cybersecurity in eu law? the challenges ahead," *Computer Law & Security Review*, vol. 53, p. 105961, 2024.

[6] E.-M. Kalogeraki and N. Polemi, "A taxonomy for cybersecurity standards," 2024.

[7] B. García Ortega, "Auditorias de sistemas de gestión para empresas," 2021.

[8] V. Giménez-Chornet, "Los metadatos en el ordenamiento jurídico español y europeo," *Tábula*, no. 22, pp. 37–50, 2020.

[9] J. V. Oltra Gutiérrez, J. O. Montesa Andrés, D. Stratu Strelet, H. Gil Gómez, R. F. Oltra Badenes *et al.*, "Análisis de la firma electrónica en el contexto de la transformación digital en la unión europea," 2020.

[10] normaiso27001.es, "Iso 27001," 2024. [Online]. Available: https://normaiso27001.es/

[11] "La formación docente en el marco de los desafíos educativos contemporáneos." [Online]. Available: https://www.proquest.com/openview/c445937420fb93e559a46f0a2f542d72/1?pq-origsite=gscholar&cbl=18750

[12] D. Ferraiolo, J. Cugini, D. R. Kuhn *et al.*, "Role-based access control (rbac): Features and motivations," in *Proceedings of 11th annual computer security application conference*, 1995, pp. 241–48.

[13] A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G. Zao, R. Chilro, and L. Antunes, "How to securely break into rbac: the btg-rbac model," in *2009 Annual Computer Security Applications Conference*. IEEE, 2009, pp. 23–31.

[14] R. Kim, J. Gangolly, S. Ravi, and D. J. Rosenkrantz, "Formal analysis of segregation of duties (sod) in accounting: A computational approach," *Abacus*, vol. 56, no. 2, pp. 165–212, 2020.

[15] X. Luo, H. Wang, D. Wu, C. Chen, M. Deng, J. Huang, and X.-S. Hua, "A survey on deep hashing methods," *ACM Transactions on Knowledge Discovery from Data*, vol. 17, no. 1, pp. 1–50, 2023.

[16] Norma ISO 27001, "Iso 27001 - certificado iso 27001 punto por punto - presupuesto online," 2024. [Online]. Available: https://normaiso27001.es/

[17] R. N. Rajapakse, M. Zahedi, M. A. Babar, and H. Shen, "Challenges and solutions when adopting devsecops: A systematic review," *Information and software technology*, vol. 141, p. 106700, 2022.

[18] Instituto Nacional de Ciberseguridad (INCIBE), "Tu ayuda en ciberseguridad - campañas," 2024, accessed: 2024-06-09. [Online]. Available: https://www.incibe.es/ciudadania/campanas

[19] D. C. Merchán, "Análisis de logs del sistema para la realización de un estudio sobre seguridad y comportamiento," 2018. [Online]. Available: https://e-archivo.uc3m.es/entities/publication/1cb4f30a-ddab-4be1-8181-7204a0f5dd4b

[20] Delta Protect, "Capacitación de ciberseguridad para empleados," 2024. [Online]. Available: https://www.deltaprotect.com/modulos/capacitacion-ciberseguridad-empleados

[21] P. Ragunath, S. Velmourougan, P. Davachelvan, S. Kayalvizhi, and R. Ravimohan, "Evolving a new model (sdlc model-2010) for software development life cycle (sdlc)," *International Journal of Computer Science and Network Security*, vol. 10, no. 1, pp. 112–119, 2010.

[22] Cyberzaintza, "Exercise in a box," 2024. [Online]. Available: https://www.ciberseguridad.eus/empresa-segura/exercise-in-a-box

[23] F. Pacheco and D. Staino, "Metodología para ejercicios de simulación de respuesta a incidentes de ciberseguridad," *Memorias de las JAIIO*, vol. 9, no. 8, pp. 15–28, 2023.

[24] Instituto Nacional de Ciberseguridad (INCIBE), "Instituto nacional de ciberseguridad (incibe)," 2024. [Online]. Available: https://www.incibe.es/

[25] Centro Criptológico Nacional, "Centro criptológico nacional - ccn-cert," 2024. [Online]. Available: https://www.ccn-cert.cni.es/es/

[26] Wikipedia contributors, "ISO/IEC 27005," https://es.wikipedia.org/wiki/ISO/IEC_27005, [Accedido: 19 de junio de 2024].

[27] E. Union, "Official journal of the european union," vol. 119, pp. L1–L88, 2016. [Online]. Available: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[28] Microsoft Corporation. (s/f) Cumplimiento normativo de hipaa y hitech. [Online]. Available: https://learn.microsoft.com/es-es/compliance/regulatory/offering-hipaa-hitech

[29] CCN-CERT, "Guía ccn-stic-802: Auditoría del ens," no date. [Online]. Available: https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/502-ccn-stic-802-auditoria-del-ens/file?format=html

[30] CCN-CERT, "Guías de acceso público CCN-STIC," no date. [Online]. Available: https://www.ccn-cert.cni.es/es/series-ccn-stic/guias-de-acceso-publico-ccn-stic?limit=20&limitstart=40

[31] United Nations, “Objetivos de desarrollo sostenible,” 2024. [Online]. Available: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

[32] Álvaro Pau Sáez, “Auditoria de cumplimiento de la normativa europea nis2,” https://form.jotform.com/241683326575362, 2024, formulario de auditoría interna.