APUNTES 05

NORMATIVA VIGENTE DE CIBERSEGURIDAD DE ÁMBITO NACIONAL E INTERNACIONAL

NORMATIVA DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

A lo largo de esta unidad van a desarrollar competencias sobre la aplicación de normativas de ciberseguridad nacionales e internacionales, tales como:

- Establecer plan de revisiones de normativa y jurisprudencia que pueda afectar a la organización.
- Identificar nueva normativa mediante la consulta de las fases de datos jurídicas propuestas.
- Analizar nueva normativa para determinar si aplica a la organización.
- Incluir nueva normativa aplicable.
- Determinar e implementar controles necesarios para garantizar el cumplimiento de las nuevas normativas.

Esta unidad va a tratar fundamentalmente normativas de ciberseguridad en el ámbito nacional e internacional, en ella se desarrollarán los siguientes contenidos:

1. Normas nacionales e internacionales.
2. Sistema de gestión de seguridad de la información (ISO 27001).
3. Planes de continuidad de negocio (ISO 22.301).
4. Acceso electrónico del os ciudadanos a los Servicios Públicos.
5. Esquema Nacional de Seguridad.
6. Directiva NIS.
7. Ley de Protección de infraestructuras públicas.

1.- NORMAS NACIONALES E INTERNACIONALES.

Caso práctico

Son multitud de empresas tanto en España como en el resto del mundo que han sufrido incidentes graves relacionados con la ciberseguridad. Se han dado casos de ransomware, denegaciones de servicio, suplantaciones de identidad, fraude, etc... y todos ellos relacionados con la seguridad de los sistemas de información de las organizaciones.

Ante esta situación la dirección ha decidido contratar a un CISO, que se encargará de mejorar el nivel de madurez en seguridad de la organización.

Para ayudarle a desarrollar la estrategia de ciberseguridad y de continuidad, se van a presentar una serie de normas y estándares ampliamente utilizados con el objetivo de reducir así los riesgos de ciberseguridad de la organización.

Principales estándares internacionales en ciberseguridad.

Modelo COSO - (Committee of Sponsoring Organizations of the Tradeway Commission): es una organización compuesta por organismos privados, establecida en los EEUU, que se dedica a proporcionar un modelo común de orientación a las entidades sobre aspectos fundamentales de gestión ejecutiva y de gobierno, ética empresarial, control interno, gestión del riesgo empresarial, control de fraude y prestación de informes financieros.

Modelo CobIT – (Control Objectives for Information and related Technology): este se trata de un conjunto de buenas prácticas para la gestión de los sistemas de información de las compañías.

Controles de Servicio y Organización 2 (SOC 2) - estándar internacional realizado por el Instituto Americano de Contables Públicos Certificados (AICPA): Estos informes se desarrollan sobre los controles que una organización implementa en sus sistemas y que tienen que ver con la seguridad. Existen dos tipos de informes SOC:

- El SOC tipo 1 consiste en una evaluación puntual en un momento concreto con el objetivo de determinar si los controles implantados por la organización han sido debidamente diseñados y son apropiados.
- En cuanto al SOC 2 tipo 2, se trata de una revisión más duradera, de alrededor de un año. En ella, los controles de la organización son evaluados durante un tiempo acordado para determinar funcionan de manera adecuada durante todo el periodo de evaluación.

Marco CIS CSC: Se trata de 18 Controles de Seguridad Críticos (CSC) desarrollados por el instituto SANS junto con el Centro de Seguridad de Internet (CIS) para mejorar la defensa en ciberseguridad. Estos controles priorizan las acciones más esenciales que una organización puede establecer para mejorar su ciberseguridad.

Marco SCF: El marco Secure Controls Framework (SCF) se trata de un proyecto abierto formado por especialistas voluntarios en ciberguridad, privacidad y Gobierno, Riesgo y Control (GRC) que pretender proveer de una guía gratuita de controles de privacidad y de ciberseguridad que cubran las necesidades estratégicas, tácticas y operacionales de cualquier organización con independencia de su tamaño, sector y país de origen.

NIST Cibersecurity Framework: Es un marco de ciberseguridad creado para ayudar a las empresas de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos, proporcionando un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

Sus resultados se basan en la mejora de los 5 procesos que constituyen el ciclo de la ciberseguridad que presenta el marco:

Id. Función	Función	Id. Cat	Categoría
ID	**Identificar**	ID. AM	Gestión de activos
		ID. BE	Entorno empresarial
		ID. GV	Gobernanza
		ID. RA	Evaluación de riesgos
		ID. RM	Estrategia de gestión de riesgos
		ID. SC	Gestión del riesgo de la cadena de suministro
PR	**Proteger**	PR. AC	Gestión de identidad y control de acceso
		PR. AT	Conciencia y capacitación
		PR. DS	Seguridad de datos
		PR. IP	Procesos de protección de la información
		PR. MA	Mantenimiento
		PR. PT	Tecnología productora
DE	**Detectar**	DE. AE	Anomalías y eventos
		DE. CM	Vigilancia continua de seguridad
		DE. DP	Procesos de detección
RS	**Responder**	RS. RP	Comunicaciones
		RS. CO	Análisis
		RS. AN	Análisis
		RS. MI	Mitigación
		RS. IM	Mejoras
RC	Recuperar	RC. RP	Planificación de recuperación
		RC. IM	Mejoras
		RC.CO	Comunicaciones

El grado de madurez de los controles se evalúa en función a 4 niveles de implementación:

Parcial	No formalizado, realizado puntualmente o de manera reactiva.
Informado	Procesos aprobados pero podrían no ser establecidos como políticas de toda la organización. Actividades de seguridad basadas en objetivos de riesgo.
Repetible	Procesos aprobado y con políticas definidas, actualizados regularmente de acuerdo con el perfil de riesgo de la organización.
Adaptativo	Procesos medidos y mejorados, incluye lecciones aprendidas, la organización se adapta continuamente a un panorama cambiante de amenazas y tecnologías, y responde de manera eficaz.

1.1.- SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

- **Sistemas de Gestión de Seguridad de la Información**

La ISO 27001 es una norma internacional de Seguridad de la Información que pretende mejorar el nivel de seguridad de una organización a través de la implantación de un Sistema de Gestión de Seguridad de la Información que suponga una mejora continua en el nivel de madurez de seguridad y por tanto asegurar la confidencialidad, integridad y disponibilidad de la información de una organización y de los sistemas y aplicaciones que la tratan. Este estándar ha sido desarrollado por la Organización Internacional de Normalización y publicado en su última versión en el año 2013. Es certificable.
Esta norma cuenta con un modo de desarrollo y gestión muy similar al del resto de los estándares ISO que implementan sistemas de gestión vistos anteriormente, por lo que únicamente nos vamos a fijar en los aspectos diferenciales de esta ISO, el marco de controles definidos en la ISO 27002.
Aunque ésta es la más relevante y la mas conocida, la familia ISO 27000 esta compuesta por multitud de normas siempre relacionadas con seguridad de la información, a continuación se presentan varios ejemplos:

- ISO 27000: Contiene las definiciones y los términos que se utilizarán durante toda la serie 27000.
- ISO 27001: Sistema de gestión de seguridad de la información.
- ISO 27002: Manual de buenas prácticas donde se detallan los objetivos de control y las evaluaciones.
- ISO 27003: Información necesaria para la utilización del ciclo PHVA (Planificar, Hacer, Verificar, Actuar).
- ISO 27004: Técnicas de medida y métricas aplicables.
- ISO 27005: Gestión de los riesgos de seguridad de la información.
- ISO 27006: Requisitos para lograr la acreditación de las entidades de auditoría y certificación.
- ISO 27007: Manual de auditoría de un sistema de gestión de seguridad de la información.
- ISO 27011: Gestión de la seguridad de la información específica para el sector de las telecomunicaciones.
- ISO 27017: Seguridad de la información en entornos cloud.
- ISO 27018: Privacidad de la información en entornos cloud.

Además de las organizaciones, existen diversas certificaciones para profesionales enfocados en la seguridad de la información, que deseen auditar o desplegar un SGSI, se trata de la certificación ISO 27001 Lead Auditor (LA) y ISO 27001 Lead Implementer (LI).

- **Estructura de la norma ISO 27001**

Objeto y campo de aplicación: orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.

Referencias Normativas: documentos indispensables para la aplicación de ISO27001.

Términos y Definiciones: Describe la terminología aplicable a este estándar.

Contexto de la Organización: conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI. Como ya hemos visto en temas anteriores en este epígrafe es indispensable:

- Identificación de las partes interesadas dentro del sistema de gestión.
- Identificación de objetivos y requerimientos de las partes interesadas.
- Determinar a que parte del negocio va a afectar el sistema de gestión.
- Analizar los riesgos en seguridad de la información. Este análisis puede estar basado en la norma ISO 31000 o en la 27005 específica de seguridad de la información, ya que son compatibles.

Liderazgo: Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma. Los elementos más relevantes con respecto al apartado de liderazgo son:

- La existencia de una política de seguridad de la información firmada por la dirección, comunicada y disponible para todos los empleados de la organización.
- La definición de un equipo y recursos humanos

Planificación: En esta sección se establece el plan para dar respuesta a los riesgos oportunidades y objetivos establecidos el epígrafe del contexto. Dentro de esta epígrafe debe establecerse el plan de proyectos e iniciativas a acometer, junto el detalle de los parámetros que justifican la priorización elegida.

Soporte: En este epígrafe se deben detallar los recursos necesarios para operar el sistema de gestión de seguridad de la información.
Para los recursos humanos necesarios, se deberá detallar las competencias necesarias con las que debe contar.
Asimismo, el SGSI deberá contar con un plan de comunicación y los documentos relevantes tales como la política de seguridad, deben estar disponibles para todos los empleados de la organización.
Recursos, competencias, conciencia, comunicación e información documentada con la que debe contar la organización para el funcionamiento del SGSI.

Operación: esta parte de la norma indica qué se debe planificar, implementar y controlar los procesos de seguridad de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.
Por cada uno de los procesos implementados dentro del sistema de gestión de seguridad de la información, se ha de hacer un seguimiento y evaluación de los impactos en la madurez y en los riesgos. Como consecuencia de este requerimiento de la norma, se debe realizar una actualización del análisis de riesgos a intervalos planificados, al menos una vez por cada ciclo.

Evaluación del Desempeño: En este punto se establece guías para el seguimiento del sistema, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información.
El sistema de gestión tiene que ser evaluado para facilitar su mejora. La evaluación del sistema puede llevarse a cabo a través de diferentes herramientas, por ejemplo:

- ➢ Evolución de las métricas y los indicadores de seguridad.
- ➢ Auditorías externas del sistema.
- ➢ Auditorías internas del sistema.
- ➢ Revisión por parte de la dirección.

Todas estas revisiones deben ser dejar un soporte documental. Además la información sobre las oportunidades de mejora detectadas, serán utilizadas para la mejora del Sistema de Gestión de Seguridad de la Información.

Mejora: Define obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.
Por lo general, en este último epígrafe se evidencian las decisiones tomadas con respecto a los puntos de mejora y acciones correctivas tomadas tras las evaluaciones de desempeño realizadas en la fase anterior.

- **ISO 27002**

La ISO 27002, proporciona los controles de seguridad de la información, ciberseguridad y privacidad para una organización.
Es un estándar complementario a la ISO 27001 que ayuda a implementar las mejores prácticas y controles más eficaces para prevenir ataques o vulneraciones de privacidad.
En la edición del 2013 contaba con un total de 114 controles divididos en 14 dominios.

- ➢ Políticas de seguridad.
- ➢ Aspectos organizativos de la Seguridad de la Información.Fotografía de un sistema informático
- ➢ Foto de Pixabay (CC BY)
- ➢ Seguridad ligada a los Recursos Humanos.
- ➢ Gestión de activos.
- ➢ Control de accesos.
- ➢ Cifrado.
- ➢ Seguridad física y ambiental.
- ➢ Seguridad en la operativa.
- ➢ Seguridad en las telecomunicaciones.
- ➢ Adquisición, desarrollo y mantenimiento de los sistemas de información.
- ➢ Relaciones con proveedores.
- ➢ Gestión de incidentes en la Seguridad de la Información.
- ➢ Aspectos de la Seguridad de la Información en la gestión de la continuidad de negocio.
- ➢ Cumplimiento.

Actualización iso27001 e iso 27002 versión 2022
El 15 de febrero se publicó una nueva versión de la norma, la ISO 27002:2022, si bien la 27001 aun no se ha publicado, ya se conoce que va a ser publicada durante el año 2022 y que no cambiará el núcleo del sistema de gestión, sino que adaptara sus anexos para alinearse con la nueva ISO 27002.
En relación a la ISO 27002:2022 han sido varios los cambios que ha sufrido:
El número de controles se ha visto reducido de 114 a 93.

El número de dominios se ha reducido asimismo de 14 a 4.

- Controles organizacionales (37)
- Controles de personas (8)
- Controles físicos (14)
- Controles Tecnológicos (34)

La ISO 27002:2022 incorpora 11 nuevos controles para adaptar la norma a las nuevas tecnologías y necesidades surgidas en los últimos años.

- Inteligencia de amenazas.
- Seguridad de la información en la nube.
- Continuidad del negocio.
- Seguridad física y su supervisión.
- Configuración.
- Eliminación de la información.
- Encriptación de datos.
- Prevención de fugas de datos.
- Seguimiento y monitoreo.
- Filtrado web.
- Codificación segura.

Otra de las novedades en la nueva versión es la posibilidad de inclusión de atributos por cada control, lo cual permite su implementación y evaluación para el cumplimiento del estándar ISO y cualquier otro relacionado al que se le puedan asignar controles. Según el listado adjunto:

- Tipos de control: Preventivo, Detectivo y Correctivo.
- Dimensiones: Confidencialidad, Integridad y Disponibilidad.
- Proceso de ciberseguridad: Identificar, Proteger, Detectar, Responder y Recuperar.
- Capacidades Operativas: Gobernanza, Gestión de Activos, Protección de la Información, Seguridad de Recursos Humanos, Seguridad Física, Seguridad de Sistemas y Redes, Seguridad de Aplicaciones, Configuración Segura, gestión de identidades y accesos, gestión de amenazas y vulnerabilidades, continuidad, Seguridad de las relaciones con proveedores, Legal y Cumplimiento, gestión de eventos de seguridad de la información y Aseguramiento/garantía de seguridad de la información.
- Dominios de seguridad: Gobernanza y ecosistema, Protección, Defensa y Resiliencia.

Reflexiona: para obtener la certificación ISO 27001, hay que implementar los controles del anexo A, basados en la norma ISO 27002, sin embargo, no es necesario implementar todos los controles! Uno de los documentos más relevantes del Sistema de Gestión de Seguridad de la Información, es la declaración de aplicabilidad de la norma. En este documento se enumeran todos los controles del anexo ISO 27002 y se ha de justificar cuales aplican al sistema y cuales no.

Para saber más: en el siguiente artículo se pueden consultar de manera detallada los nuevos controles que han aparecido con la nueva versión de la norma ISO 27002. Explicación detallada de los nuevos 11 controles de la ISO 27002 (en ingles)

1.2.- SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO CON ISO 22301.

La continuidad de negocio con ISO 22301

La norma ISO 22301 establece las directrices para el desarrollo de un Sistema de Gestión de Continuidad de Negocio.

Un Sistema de Gestión de Continuidad de un Negocio o SGCN identifica los activos más relevantes para el funcionamiento de una organización y evalúa los efectos que puede tener una interrupción de la actividad para establecer medidas de actuación en caso de que ocurra. Para ello, debe tener en cuenta cualquier tipo de circunstancia adversa que pueda acontecer y que procesos y agentes deben actuar ante dicha situación de riesgo.

Se trata de una norma que mantiene la estructura de sistemas de gestión, basada en el ciclo de Deming. Es una norma certificable, y su última versión data del 2019.

Los cambios con respecto a otros sistemas de gestión son fundamentalmente referentes a los conceptos de continuidad de la información y en operación del sistema. A continuación se presentan los conceptos más relevantes:

Continuidad de negocio: Capacidad de una organización para continuar la entrega de productos o servicios a niveles predefinidos y aceptables tras una interrupción.

Análisis de impacto al negocio (BIA): Proceso de análisis de actividades y el efecto que una interrupción de negocio puede tener sobre ella.

Interrupción: Evento anticipado (por ejemplo, una huelga laboral o un huracán) o no anticipado (por ejemplo, un apagón o un terremoto), que causa una desviación negativa no planificad

Periodo máximo tolerable de interrupción (MTPD): Tiempo para que los impactos adversos, que pueden surgir como resultado de no proporcionar un producto/servicio o realizar una actividad, se vuelvan inaceptable.

Requisitos mínimos de continuidad de negocio (MBCO): Nivel mínimo de servicios y /o productos aceptable para una organización con el fin de lograr sus objetivos comerciales durante una interrupción.

Objetivo de punto de recuperación (RPO): Punto en el que la información utilizada por una actividad puede restaurarse para permitir que la actividad se reanude.

Objetivo de tiempo de recuperación (RTO): Período de tiempo tras un incidente dentro del cual se reanuda un producto, servicio o actividad o se recuperan recursos.

A continuación se detallan las diferentes fases que deben ser llevadas a cabo para la operación del plan de continuidad de negocio.

Análisis de impacto en negocio: El objetivo de esta fase es evaluar las actividades de negocio más críticas que sustenten el negocio. Una vez identificadas, se han de identificar las aplicaciones y sistemas informáticos que les dan servicio, para establecer prioridades y requisitos de continuidad.
Elementos a tener en cuenta:

- Tipos de impacto.
- Actividades clave de negocio.
- Evaluación de impacto en la interrupción de estas actividades.
- Calcular el tiempo máximo tolerable de interrupción (MTPD).
- Calcular un tiempo de recuperación aceptable (RTO).

Evaluación de riesgo: Permite a la organización evaluar la probabilidad de que se materialice una amenaza y cause un impacto negativo en la organización. El objetivo de este proceso es establecer un plan de mitigación de riesgos de continuidad para minimizar los posibles efectos adversos que pueda ocasionar una disrupción en el negocio, y recuperar los procesos de negocio en el menor tiempo posible.
Acciones a llevar a cabo:

- Identificar riesgos para las actividades criticas para la organización.
- Analizar los riesgos identificados.
- Determinar la mejor decisión de tratamiento de riesgos.

Con las evaluaciones de Impacto y Riesgos se determinará la estrategia de continuidad de negocio.
La estrategia y las soluciones de continuidad adoptadas se basaran en los siguientes elementos:

- Capacidad de cumplir con requisitos y continuar actividades.
- Reducir probabilidad y periodo de interrupción.
- Recursos.
- Tolerancia al riesgo de la organización.
- Coste/Beneficio.

Con la estrategia de continuidad, será necesario llevar a cabo una evaluación de los recursos necesarios para completarla, teniendo en cuenta, al menos, los siguientes elementos:

- Personal.
- Información y datos.
- Infraestructura e instalaciones de soporte.
- Equipamiento y bienes.
- Sistemas de TI y telecomunicaciones.
- Transporte y logística.
- Finanzas.
- Socios y proveedores.

Una vez diseñada la estrategia e identificados los recursos, la organización debe establecer un plan y procedimientos de continuidad de negocio, para gestionar la organización en caso de una incidencia que suponga una interrupción y requiera de la activación del plan de continuidad.
Asimismo, se debe crear una estructura organizativa de respuesta con equipos de gestión de crisis responsables de gestionar y responder las interrupciones, con roles y responsabilidades bien definidos, suficiente competencia y procedimientos para comunicarse con partes interesadas, autoridades y medios de comunicación.
Una vez se disponen de los procedimientos de respuesta, se deben generar los planes de recuperación, para volver a la normalidad después de una situación de contingencia.
La organización debe realizar planes de prueba para comprobar la eficacia de los planes diseñados, las pruebas, se basarán en ejercicios de respuesta y recuperación creados a partir de casos reales que podrían ocurrir, verificando la idoneidad de los planes y procedimientos de respuesta y los equipos asignados, estos deben realizarse con la frecuencia necesaria para garantizar su efectividad.
Por lo general, las políticas, planes y procedimientos de respuesta deben ser revisados a intervalos establecidos o ante cambios significativos para mantener su adecuación.

Reflexiona
El valor Return Point Objective, establece el punto a partir del cual no se van a perder transacciones.
¿Qué seria mejor, un RPO alto o bajo?¿Cuál sería el control lógico para dar respuesta aun RPO? ¿Sería posible tener un RPO de cero? ¿Cómo?
El RPO es mejor, cuanto más se acerque a cero, esto significa que no se perderá información en caso de parada de sistemas.
El control más típico y lógico que da respuesta a un RPO, es la elaboración de copias de seguridad. En sistemas muy críticos es posible y necesario tener un RPO de cero, para ello, se deben desplegar sistemas de alta disponibilidad con al menos doble almacenamiento.

1.3.- ACCESO ELECTRÓNICO DE LOS CIUDADANOS A LOS SERVICIOS PÚBLICOS.

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos es la ley que reconoce a los ciudadanos su derecho a relacionarse electrónicamente con las administraciones públicas, así como la obligación de éstas a garantizar ese derecho.

Dentro de un proceso de reorganización y funcionamiento de las administraciones públicas, fue derogada en 2015 surgiendo por dos leyes similares, pero con diferentes enfoques.

Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones Públicas referida a las relaciones externas de la Administración con ciudadanos y empresas.

Ley 40/2015, de 1 de octubre, de régimen jurídico del Gobierno y del sector público referida a las relaciones internas dentro de cada Administración y relaciones entre las distintas Administraciones.

Procedimiento administrativo común de las Administraciones Públicas

El procedimiento administrativo común de las Administraciones Públicas tiene objetivos:

Mejorar la eficiencia con una Administración totalmente electrónica con cero papel e interconectada en sus relaciones con ciudadanos y empresas, facilitar el uso de medios electrónicos y simplificar y agilizar los procedimientos.

Incrementar la seguridad jurídica ganando en certidumbre y predictibilidad al sistematizar en una sola ley la regulación de las relaciones externas de la Administración con los ciudadanos y empresas: procedimiento administrativo y principios aplicables al ejercicio de la iniciativa legislativa y potestad reglamentaria.

Mejorar la calidad normativa del ordenamiento jurídico.

Administración con cero papel. La tramitación de todos los procedimientos se realizará íntegramente a través de medios electrónicos, manteniendo, no obstante, los interesados su derecho a la presentación presencial de documentos.

Todas las Administraciones estarán interconectadas mediante plataformas comunes de intercambio de información.

Se definen los colectivos obligados a relacionarse electrónicamente con la Administración (personas jurídicas, entidades sin personalidad jurídica, empleados públicos, profesionales con obligación de colegiación y representantes de un interesado obligado a relacionarse a través de medios electrónicos con la Administración)

1.4.- ESQUEMA NACIONAL DE SEGURIDAD.

El ENS establece la política de seguridad para la protección adecuada de la información y los servicios prestados a por las administraciones públicas, así como los proveedores del sector privado que prestan servicio a las administraciones publicas.

Estas políticas se estructuran en base a un planteamiento común de principios, requisitos, medidas de protección, mecanismos de conformidad y monitorización para todas las entidades en el alcance.

La última versión esta publicada en el Real Decreto 311/2022, del 3 de mayo de 2022, y sustituye a la versión publicada en enero del 2010.

Objetivos:

- Crear las condiciones necesarias de seguridad en el uso de los medio electrónicos.
- Promover la gestión continuada de la seguridad.
- Promover la prevención, detección y corrección.
- Promover un tratamiento homogéneo de la seguridad.
- Servir de modelo de buenas prácticas.

Implantación del esquema nacional de seguridad:

A continuación se presentan las actividades que se han de llevar a cabo para implantar el ENS en una organización:

- Preparar y aprobar la política de seguridad, incluyendo los objetivos o misión de la organización, el marco regulatorio de las actividades, la definición de roles de seguridad, la estructura y composición del comité para la gestión y coordinación de la seguridad, las directrices de estructuración de la documentación de la seguridad, y los riesgos derivados del tratamiento de datos personales.
- Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados.
- Realizar el análisis de riesgos, incluyendo la valoración de las medidas de seguridad existentes.
- Preparar y aprobar la Declaración de aplicabilidad de las medidas del Anexo II del ENS.
- Elaborar un plan de adecuación para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución.
- Implantar, operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente.
- Auditar la seguridad para verificar el cumplimiento de los requisitos del ENS.
- Obtener y publicitar la conformidad con el ENS.
- Informar sobre el estado de la seguridad.

- **Estructura del ENS**

El real decreto se estructura en cuarenta y un artículos distribuidos en siete capítulos, tres disposiciones adicionales, una disposición transitoria, una disposición derogatoria, tres disposiciones finales y cuatro anexos.
A continuación, vamos a repasar los elementos principales del ENS:

El Capítulo 1 - Disposiciones generales, define el objeto de la norma, ámbito de aplicación, información, elementos y entidades dentro del alcance. Además, también considera elementos como el uso de tecnologías de comunicación 5G y la protección de datos de carácter personal.

El Capítulo 2 – Principios básicos, establece los principios básicos de la norma, enumerados en el artículo 5:

1. La seguridad como proceso integral, formada por todos los elementos relacionados con los sistemas de información, tales como recursos humanos, materiales, técnicos, jurídicos y organizativos, siendo el despliegue del ENS un proceso integral y no un elemento atómico y parcial a la organización.
2. Gestión de la seguridad basada en los riesgos, elaborando un análisis de riesgos como elemento de base para el esquema y evolucionándolo y actualizándolo a medida que se despliegan herramientas y controles.
3. Prevención, detección, respuesta y conservación, con el objetivo de minimizar precisamente las vulnerabilidades que permitan materializar amenazas, o en su defecto, limitar sus daños.
4. Existencia de líneas de defensa, constituyendo una estrategia que permita proteger a la organización en caso de que una capa de seguridad sea vulnerada existiendo capas de seguridad con más profundidad y de alcance acotado.
5. Vigilancia continua, que implica la detección de actividades o comportamientos anómalos y la respuesta ante los mismos.
6. Reevaluación periódica de las medidas de seguridad implementadas, adaptando su implementación a la evolución del nivel de riesgo de la organización.
7. Diferenciación de responsabilidades entre el responsable de información, servicio, seguridad y sistema.

Capítulo 3 - Política de Seguridad y requisitos mínimos para permitir una protección adecuada de la información y los servicios:
La política de seguridad se desarrollará cubriendo los siguientes contenidos mínimos:

- Organización e implantación del proceso de seguridad: La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.
- Análisis y gestión de los riesgos: Cada organización deberá realizar su propia gestión de riesgos, consistente en un proceso de identificación, evaluación y tratamiento de los mismos.
- Gestión de personal: El personal relacionado con los sistemas IT de la organización debe estar formado en sus deberes y responsabilidades en materia de ciberseguridad.
- Profesionalidad: La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido.
- Autorización y control de los accesos: El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los elementos autorizados.
- Protección de las instalaciones: Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales a su riesgo asociado.
- Adquisición de productos de seguridad y contratación de servicios de seguridad: Se utilizarán aquellos que tengan certificada la funcionalidad de seguridad para la que han sido adquiridos.
- Mínimo privilegio: Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño.
- Integridad y actualización del sistema: La inclusión o modificación de cualquier elemento en el inventario de activos, requerirá autorización formal previa.
- Protección de la información almacenada y en tránsito: Se prestará especial atención a la seguridad de la información en reposo y en tránsito enviada a través de dispositivos portátiles. Además, se analizarán los soportes extraíbles de información, y las comunicaciones a través de redes abiertas, para protegerlas convenientemente.
- Prevención ante otros sistemas de información interconectados: Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.
- Registro de la actividad y detección de código dañino: las actividades de los usuarios serán registradas, almacenando la información básica para monitorizar, analizar, investigar y documentar eventos no autorizados o actividades maliciosas.
- Incidentes de seguridad: La organización deberá contar con procedimientos de gestión de incidencias. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis, resolución y comunicación.
- Continuidad de la actividad: Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de disrupción.
- Mejora continua del proceso de seguridad.

El artículo 28 regula el cumplimiento de los requisitos mínimos, según las medidas del anexo II, que podrán no ser implementadas siempre y cuando se establezcan y justifique la implantación de otras medidas compensatorias.
El artículo 29 promueve la utilización de infraestructuras y servicios comunes a las administraciones públicas con el objetivo de fomentar la eficiencia y la compartición de información de ciberseguridad e inteligencia entre administraciones públicas.
El artículo 30 establece la posibilidad de implementar perfiles de cumplimiento específicos estableciendo una serie de medidas de seguridad en función del nivel de riesgos identificado.

Capítulo 4 - Seguridad de sistemas: auditoría, informe e incidentes de seguridad, establece los requisitos de auditoría de seguridad de la organización, debiendo ejecutarse al menos una vez cada dos años siguiendo criterios y métodos de auditoria reconocidos.
Por su parte, el artículo 32, relativo al informe del estado de la seguridad, precisa que este deberá permitir elaborar un perfil general del estado de la seguridad en las entidades.
La prevención, detección y respuesta a incidentes de seguridad se define los artículos 33 y 34, indicando la necesidad de existencia de procesos de gestión de incidencias y designando al CCN-CERT como responsable de la coordinación de respuesta a incidencias en el ámbito de las administraciones y organizaciones dentro del alcance del ENS.

Capítulo 5 – Normas de conformidad, que se concretan en cuatro:
Administración Digital.
Ciclo de vida de servicios y sistemas.
Mecanismos de control y,
Procedimientos de determinación de la conformidad con el ENS.

Capítulo 6 - Actualización del Esquema Nacional de Seguridad
Establece la obligación de actualización de acuerdo con el marco jurídico, la evolución de la tecnología y los estándares en materia de seguridad, nuevas amenazas y vectores de ataque.

Capítulo 7 - Categorización de los sistemas de información.
El artículo 40 establece la categorización de seguridad en función del impacto de un incidente en términos de disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo para ello el procedimiento descrito en el anexo I;
El real decreto se complementa con cuatro anexos:

- El anexo I regula las categorías de seguridad de los sistemas de información, detallando la secuencia de actuaciones para determinar la categoría de seguridad de un sistema;
- El anexo II detalla las medidas de seguridad;
  En particular, este anexo detalla las medidas de seguridad estructuradas en tres grupos:
  1. el marco organizativo, constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
  2. el marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin, y
  3. las medidas de protección, que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.
- El anexo III se ocupa del objeto, niveles e interpretación de la Auditoría de la seguridad y,
- El anexo IV incluye el glosario de términos y definiciones.

Para saber más
Además de la legislación vigente consultable en la web del BOE, el CCN ha habilitado una web específica para consultar las novedades del ENS con multitud de materiales e infografías. Web del ENS CCN-CERT
Asimismo, el CCN, proporciona una serie de herramientas que dan soporte en el proceso de cumplimiento del ENS. Herramientas soporte ENS CCN

1.5.- LA DIRECTIVA NIS.
Bautizada como directiva NIS (Network and Information Security directive), se trata de una directiva aprobada por el Parlamento Europeo, que recoge las medidas para garantizar un nivel de seguridad elevado en entidades tanto del sector privado como del sector público en toda Europa, mejorando su resiliencia y su capacidad de respuesta a incidentes.
Sienta las bases para la gestión de riesgos de ciberseguridad y la obligación de notificación en las organizaciones de los sectores que cubre.
Entre sus objetivos, destacan la homogeneización de las medidas de seguridad entre organizaciones de diferentes países, y el establecimiento de un marco de comunicación común para la respuesta a eventos e incidencias de seguridad, denominado, Red Europea de Organización de Enlace de Crisis Cibernéticas (EU-CYCLONe)
¿Qué organizaciones están afectadas?
1. Aquellas que sean designadas como Operadores de Servicios Esenciales (OSE), en función de si prestan un servicio esencial que dependan de redes y sistemas de información. Y si su pérdida o indisponibilidad causan un perjuicio severo a la sociedad. Son designados equiparando la aplicabilidad a las organizaciones afectadas por la Ley de Protección de Infraestructuras Críticas. Pueden ser entidades públicas o privadas que se activan en sectores específicos, como el de la

energía, el transporte, la banca y la salud, y que al mismo tiempo cumple algunos criterios esenciales que lo califican como servicio esencial.

2. Proveedores de Servicios Digitales (PSD), estos incluyen cualquier persona jurídica que ofrezca un servicio digital y más específicamente un comercio online, un motor de búsqueda o un servicio de computación en la nube. Su regulación se justifica debido al hecho de que muchas empresas dependen de estos proveedores para la prestación de sus propios servicios. Y por ello, una parada del servicio digital podría tener importantes efectos para las actividades económicas y sociales esenciales en la UE. Cabe señalar que la Directiva NIS no exige que los Estados miembros identifiquen a los proveedores de servicios digitales, lo que garantiza un enfoque global.

Tres tipos de proveedores de servicios digitales entran dentro del alcance de la Directiva NIS:

- proveedores de mercados en línea,
- proveedores de motores de búsqueda en línea y
- distribuidores de servicios de computación en la nube.

Autoridades relevantes:

Se trata de las autoridades competentes, que serán quienes ejerzan las funciones de vigilancia y apliquen el régimen sancionador.

Según el tipo de entidad, se distinguen los siguientes:

- Centro Nacional de Protección de Infraestructuras Críticas (CNPIC): para todos aquellos OSE que sean Operadores Críticos.
- Centro Criptológico Nacional (CCN): para todos aquellos OSE y PSD que no sean Operadores Críticos y formen parte del sector público.
- Autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente: para todos aquellos OSE que no sean operadores críticos y no formen parte del sector público.
- Secretaría de Estado para el Avance Digital, del Ministerio de Energía, Turismo y Agenda Digital: para todos aquellos PSD que no sean operadores críticos y no formen parte del sector público.

Elementos relevantes definidos en la directiva NIS:

Equipos de respuesta a incidentes de seguridad informática de referencia (CSIRT), que serán los encargados de analizar los riesgos y supervisar los incidentes a escala nacional, difundiendo alertas y aportando soluciones para mitigar sus efectos.

Según el tipo de entidad, se distinguen los siguientes:

- CCN-CERT: para los OSE que formen parte del sector público, y aquellos PSD que forman parte de la comunidad de referencia del CCN-CERT.
- INCIBE-CERT: para los OSE que no formen parte del sector público, y aquellos PSD que no forman parte de la comunidad de referencia del CCN-CERT.
- ESPDEF-CERT: cooperará con CCN-CERT e INCIBE-CERT cuando lo requieran para apoyar a los OSE, y siempre que tenga incidencia en la Defensa Nacional.

Punto de Contacto Único, que será el encargado de garantizar una cooperación transfronteriza con las autoridades competentes y los CSIRT de otros estados miembros, y que será ejercido por parte del Departamento de Seguridad Nacional del Consejo de Seguridad Nacional.

Requisitos de seguridad a cumplir por OSE y PSDs:

1. Designar a una persona, unidad u órgano, como responsable de Seguridad como punto de contacto y coordinador técnico.
2. Establecimiento de desarrollos reglamentarios, órdenes ministeriales, instrucciones y guías que permitan detallar las obligaciones específicas.
3. Definición de medidas técnicas y de organización para gestionar los riesgos.
4. Proporcionar información necesaria para evaluar la seguridad de las redes y los sistemas de información.
5. Proporcionar información sobre la implantación de las políticas de seguridad.
6. Ser sometido a una auditoría sobre la seguridad de las redes y sistemas de información.
7. Ser requerido a solucionar las deficiencias detectadas.
8. Notificación al órgano supervisor de Incidentes de seguridad significativos, según los siguientes parámetros:
    - 8.1. Número de usuarios afectados.
    - 8.2. Duración del incidente.
    - 8.3. Área geográfica afectada.
    - 8.4. Nivel de perturbación del servicio.
    - 8.5. Impacto en actividades económicas y sociales cruciales.
    - 8.6. Criticidad del sistema o de la información afectada por el incidente en un OSE.
    - 8.7. Daño reputacional.

1.5.1 ESTRUCTURA DE LA DIRECTIVA NIS

La última versión de la directiva NIS puede ser consultada en el portal de publicación de regulaciones de la unión europea, a través de este enlace: Directiva NIS
La directiva cuenta con un total de 27 artículos distribuidos en 7 capítulos:

El capítulo 1, es de disposiciones generales, cuenta con los siguientes artículos:

El artículo 1 define el objeto de la norma y su ámbito de aplicación, en él, se detalla la finalidad de la norma y los diferentes objetivos que persigue.

El artículo 2 habla del tratamiento de los datos personales, especificando que debe ser realizado de acuerdo a la directiva 95/46/CE.

El artículo 3 establece que la normativa supone un mínimo común en seguridad en las redes y sistemas de información de los estados miembros, no obstante, permite a los Estados miembros establecer medidas adicionales.

El artículo 4 define y describe diferentes términos utilizados en la normativa.
Los artículos 5 y 6 define que son Operadores de Servicios Esenciales y efecto perturbador definitivo.

El capítulo 2 versa sobre marcos nacionales de seguridad de las redes y sistemas de información, compuesto por los siguientes artículos:

El artículo 7 habla sobre la estrategia nacional de seguridad de las redes y sistemas de información.
Los Estados miembros tienen la obligación de aprobar una estrategia nacional sobre seguridad. El enfoque específico de la transposición nacional de la Directiva NIS, corresponde a cada Estado miembro. Para que las disposiciones nacionales sobre requisitos de seguridad se alineen en la mayor medida posible, la Comisión alienta a los Estados miembros a seguir el documento de orientación desarrollado por el Grupo de Cooperación. En este documento se establecen algunos principios generales que todos los Estados miembros deben tener en cuenta al adoptar medidas de seguridad. Estas medidas deben ser efectivas, personalizadas, compatibles, proporcionadas, concretas y verificables.

El artículo 8 define las autoridades nacionales competentes y el punto de contacto único.

El artículo 9 habla sobre los equipos de respuesta a incidentes (CSIRT).

El artículo 10 introduce conceptos de cooperación a escala nacional y sirve de introducción al capítulo 3.

El capítulo 3 trata sobre la cooperación en materia de seguridad, esta conformado por los siguientes artículos:

El artículo 11 trata de la construcción de grupos de cooperación entre los diferentes Estados miembros.

El artículo 12 habla sobre la construcción de una serie de CSIRT nacionales y la colaboración entre los diferentes CSIRT de los Estados miembros.

El artículo 13 versa sobre la cooperación internacional.
El Grupo de Cooperación, establecido por la directiva NIS, estará presidido por la Presidencia del Consejo de la Unión Europea y conformado por diferentes representantes de los Estados miembros, la Comisión (en calidad de secretaría) y ENISA.
Dentro de sus funciones, están posibilitar el intercambio de información y la cooperación estratégica y confianza entre los Estados miembros.
También se establece la creación de una red de CSIRT nacionales. La red CSIRT estará compuesta por representantes de los CSIRT de los Estados miembros y del CERT-EU (el Equipo de respuesta ante emergencias informáticas para las instituciones, agencias y organismos de la UE).
Entre las tareas dentro de las competencias de la red CSIRT están:

- Intercambio de información sobre los servicios, las operaciones y las capacidades de cooperación de los CSIRT.
- Intercambio de información relacionada con incidentes y riesgos asociados.
- Identificación de una respuesta coordinada a un incidente.
- Prestación de apoyo para los Estados miembros al abordar incidentes transfronterizos.

El capítulo 4 establece las normas de seguridad de las redes y sistemas de información de los operadores de servicios esenciales, lo forman los siguientes artículos:

El artículo 14 trata sobre requisitos en materia de seguridad y notificación de incidentes y el artículo 15 sobre la observación y seguimiento de las mismas.
Los requisitos de seguridad para los OSE y para los PSD implican la obligación de notificar a las autoridades competentes cualquier incidente que tenga un impacto en la continuidad de los servicios (esenciales) que proporciona un operador. Ambos, no deben notificar incidentes menores, sino solo incidentes graves que afecten la continuidad del servicio esencial.
Se establece una lista de parámetros que deben tenerse en cuenta al determinar la importancia del impacto de un incidente:

- Número de usuarios afectados.
- Duración del incidente.
- Extensión geográfica con respecto al área afectada por el incidente.

El capítulo 5 establece las normas de seguridad de las redes y sistemas de información de los proveedores de servicios digitales, lo forman los siguientes artículos:

El artículo 16 trata sobre requisitos en materia de seguridad y notificación de incidentes y el 17 sobre la observación y el seguimiento de las mismas.

El artículo 18 trata sobre la jurisdicción y territorialidad de los prestadores de servicios digitales.

La Directiva describe las medidas de seguridad que los proveedores de servicios digitales deben tomar para mitigar los riesgos que amenazan la seguridad de la red y los sistemas de información que utilizan para la prestación de su servicio.
Los elementos que un proveedor de servicios digitales debe tener en cuenta al identificar y adoptar medidas de seguridad para su red son:

- Seguridad de los sistemas e instalaciones.
- Manejo de incidentes.
- Gestión de la continuidad del negocio.
- Monitoreo, auditoría y pruebas.
- Cumplimiento de las normas internacionales.

Los proveedores de servicios digitales deben notificar a la autoridad competente o al CSIRT cualquier incidente con un impacto sustancial en la prestación de su servicio.
Los parámetros que deben tenerse en cuenta para determinar si el impacto de un incidente es sustancial son:

- número de usuarios afectados por el incidente, en particular usuarios que confían en el servicio para la prestación de sus propios servicios;
- duración del incidente;
- distribución geográfica con respecto al área afectada por el incidente;
- alcance de la interrupción del funcionamiento del servicio;
- alcance del impacto en las actividades económicas y sociales.

El capítulo 6 trata sobre la normalización y notificación voluntaria, cuenta con los siguientes artículos:
El artículo 19 habla sobre la normalización, la utilización de normas agnósticas a la tecnología.
El artículo 20 trata de la notificación voluntaria de incidentes por cualquier entidad con independencia de su nombramiento como operador de servicio esencial.

El capítulo 7 comprende las disposiciones finales, consta de diferentes artículos en los que se establecen elementos como el régimen sancionador, procedimientos de comité, la revisión de la interpretación y ejecución de la directiva por los estados miembros, medidas transitorias, entrada en vigor, y destinatarios.

1.5.2. REGLAMENTO DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

El Reglamento de Seguridad de las Redes y Sistemas de la Información (Reglamento NIS) tiene como objetivo desarrollar en el territorio nacional lo establecido en la Ley NIS europea, con respecto al marco institucional en la materia, la cooperación y coordinación, la gestión y notificación de incidentes, las medidas a implantar, la supervisión de los requisitos de ciberseguridad o la función del CISO.
Estarán sometidos a este real decreto,

- Los operadores de servicios esenciales (OSE) y los proveedores de servicios digitales (PSD) que realicen su actividad en España.
- Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no se consideren como operadores críticos.
- Los proveedores de servicios digitales cuando sean microempresas o pequeñas empresas, según las definiciones establecidas en la Recomendación 2003/361/CE de la Comisión.

El Reglamento especifica asimismo, que las autoridades competentes en ciberseguridad serán, con carácter general, las que recoge la Ley:

- Secretarías de Estado de Seguridad.
- Defensa y para el Avance Digital a través de diferentes órganos.

Para los operadores privados de servicios esenciales que no sean críticos, establece que serán autoridades competentes, los organismos responsables para los sectores de transporte, energía, TIC, sistema financiero, espacio, industria química, instalaciones de investigación, salud, agua, alimentación e industria nuclear.
La cooperación entre los CSIRT de referencia y las autoridades competentes, se llevará a cabo mediante la Plataforma Nacional de Notificación y Seguimiento de Ciber incidentes.
El Departamento de Seguridad Nacional es el punto de contacto único para actuar como enlace entre autoridades nacionales y la Unión Europea, el Grupo de Cooperación Europeo y la red de CSIRT.
El reglamento especifica las funciones de este organismo, entre las que se encuentran:

- Comunicar a la Comisión Europea la lista de operadores de servicios esenciales nacionales.
- Transmitir los puntos de contacto de otros Estados miembros, información sobre incidentes con impacto transfronterizo.
- Enviar a los CSIRT de referencia y a las autoridades competentes nacionales información sobre incidentes con efectos perturbadores en los servicios esenciales que supongan la interrupción de dichos servicios.

Uno de los aspectos destacados del Reglamento NIS es la función que desempeñará el CISO en este marco normativo:
Los operadores de servicios esenciales tendrán que designar a una persona como responsable de la seguridad de la información para que ejerza las funciones de punto de contacto y coordinación con las autoridades competentes y CSIRT de referencia. El objetivo principal de estos profesionales es el de elaborar las políticas de seguridad para gestionar los riesgos para la seguridad de las redes y sistemas de información y reducir el impacto de los ciber incidentes.

Las funciones del responsable de seguridad son:

- Supervisar y desarrollar políticas de seguridad, normativas y procedimientos.
- Redactar una Declaración de Aplicabilidad de las medidas de seguridad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Comunicar los incidentes perturbadores a la autoridad competente.

El Reglamento NIS recoge asimismo el procedimiento de gestión de incidentes de seguridad, el proceso de notificación a través de la Plataforma Nacional de Notificación y Seguimiento de Ciber incidentes, así como el sistema de supervisión de cumplimiento de obligaciones de seguridad y notificación de incidentes.
Los OSE y PSD están obligados a implantar las medidas de seguridad técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información que usan para prestar sus servicios, ya sean redes y sistemas propios, o de proveedores externos. Además, se tienen que aprobar unas políticas de seguridad de las redes y sistemas de información, teniendo en cuenta los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas.
Dichas políticas tendrán en cuenta, como mínimo, los siguientes aspectos:

- Análisis y gestión de riesgos.
- Gestión de riesgos de terceros.
- Catálogo de medidas de seguridad.
- Gestión del personal.
- Adquisición de productos o servicios.
- Detección de eventos de seguridad
- Gestión de incidentes.
- Planes de recuperación y continuidad de las operaciones.
- Mejora continua.
- Interconexión de sistemas.
- Registro de la actividad de los usuarios.

En el capitulo 4 del reglamento se define que los OSE y los PSD deben gestionar los incidentes de seguridad que afecten a las redes y sistemas de información que usan para la prestación de sus servicios. En el caso de las redes y sistemas sean propiedad de proveedores externos, deben aplicarse las medidas necesarias para garantizar que dichas acciones serán llevadas a cabo.
La obligación de gestionar y resolver los incidentes de seguridad afecta tanto a aquellos detectados por el operador o un tercero que le proporcione servicio como a los que sean señalados por el CSIRT de referencia, que podrá prestar ayuda. La notificación de los incidentes, debe ser realizada al CSIRT de referencia, cuando puedan tener efectos perturbadores significativos en los servicios. Igualmente, tendrán que dar cuenta de los sucesos o incidencias que pudiesen afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, aunque no hayan tenido aún un efecto adverso real sobre aquellos.
La notificación de los incidentes es una función del responsable de la Seguridad de la Información designado.
Los CSIRT de referencia, el CCN-CERT, el INCIBE-CERT y el ESP-DEF-CERT del Mando Conjunto del Ciberespacio, podra facilitar los actores involucrados el acceso a la Plataforma Nacional de Notificación y Seguimiento de Cibe rincidentes, con el objetivo de intercambiar información y hacer un seguimiento de incidentes entre los operadores o proveedores y las autoridades competentes.

1.6.- LEY DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS.

Una Infraestructura Crítica es aquella cuyo funcionamiento es indispensable y no permite soluciones alternativas. Estas incluyen instalaciones, redes, sistemas y equipos físicos y de tecnología de comunicaciones sobre los que funcionan los servicios esenciales para la población. Los servicios esenciales son aquellos necesarios para el funcionamiento de las funciones sociales básicas: Salud, seguridad, bienestar social y económico y sector público.
La protección de infraestructuras críticas consiste en el conjunto de actividades destinadas a garantizar el funcionamiento, continuidad e integridad de las infraestructuras críticas y prevenir, reducir o neutralizar el daño causado por un ataque deliberado contra las mismas.
La Ley 8/2011, de 28 de abril, establecen las directrices para la protección de las infraestructuras críticas y que esta ampliada por el reglamento de medidas de protección descritas en el real decreto 704/2011. Esta normativa, surge como consecuencia de la transposición española de la directiva europea Directiva 2008/114/CE.
Los dos principales objetivos de esta norma son:
Identificar el conjunto de infraestructuras que prestan servicios esenciales a nuestra sociedad.
Diseñar un plan de prevención y protección eficaz contra las posibles amenazas físicas y tecnológicas sobre dichas infraestructuras.
La Ley 8/2011 de protección de infraestructuras críticas, consta de 18 artículos, estructurados en 3 Títulos.

- Disposiciones generales (artículos 1 al 4): Definiciones de los términos acuñados por la Directiva 2008/114/CE, así como a establecer las cuestiones relativas al ámbito de aplicación y objeto. Entre las definiciones establecidas, cabe destacar:

- Servicio esencial: Se considera como el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.
- Sector estratégico: Cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial.
- Infraestructuras estratégicas: Instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.
- Infraestructuras críticas: Infraestructura estratégica cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
- Criterios horizontales de criticidad: Parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica, en base al potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública, el impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios, el impacto medioambiental, y por último, el impacto público y social, que va relacionado con la confianza del ciudadano en sus Instituciones Públicas, el sufrimiento físico o la alteración de la vida cotidiana por el grave deterioro de servicios esenciales.

- **El Sistema de Protección de Infraestructuras Críticas** (artículos 5 al 13): Describe como se regulan los órganos e instrumentos de planificación que se integran en el Sistema de Protección de las Infraestructuras Críticas, compuesto por una serie de instituciones, órganos y empresas, procedentes públicas o privadas con responsabilidades en el correcto funcionamiento de los servicios esenciales. La Ley involucra a los siguientes agentes:

- La secretaría de Estado de Seguridad es nombrada responsable del Sistema de Protección de las infraestructuras críticas nacionales y es la encargada de dirigir la estrategia nacional de protección de infraestructuras críticas y aprobar los planes de seguridad.
- El Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante CNPIC) encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la protección de las Infraestructuras Críticas en el territorio nacional, además corresponderá la realización de altas, bajas y modificaciones de infraestructuras en el Catálogo, así como la determinación de la criticidad de las infraestructuras estratégicas incluidas en el mismo.
- Por cada sector estratégico, se designará al menos, un ministerio, organismo, entidad u órgano de la Administración General del Estado integrado en el Sistema, que será el encargado de impulsar, en el ámbito de sus competencias, las políticas de seguridad del Gobierno sobre los distintos sectores estratégicos nacionales y de velar por su aplicación, actuando igualmente como puntos de contacto especializados en la materia.Fotografía de Banco de España
Julio Irrazabal. Banco de España (Dominio público)
- Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades intervendrán, a través de las Fuerzas y Cuerpos de Seguridad en la implantación de los diferentes planes de las infraestructuras críticas de su demarcación.
- Para las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público participarán en la implantación de los planes a través de sus respectivos cuerpos policiales, y serán miembros de la Comisión Nacional para la Protección de las Infraestructuras Críticas. Las Comunidades Autónomas no incluidas en los apartados anteriores participarán en el Sistema de Protección de Infraestructuras Críticas y en los Órganos previstos en esta Ley, de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía.
- Otro órgano de nueva creación es la Comisión Nacional para la Protección de las Infraestructuras Críticas, que es un órgano colegiado competente para aprobar los diferentes Planes Estratégicos Sectoriales así como para designar a los operadores críticos a propuesta del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, al que le corresponderá la elaboración de los diferentes Planes Estratégicos Sectoriales y la propuesta a la Comisión de la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.
- Especial atención merecen la figura de operadores críticos que son los encargados de proveer un servicio esencial a través de sus infraestructuras críticas.

- **Instrumentos y comunicación del Sistema** (artículos 14 al 18): Define las medidas de protección y los procedimientos que deben derivar de la aplicación de la norma.

- Los operadores considerados críticos en virtud de esta Ley deberán colaborar con las autoridades competentes del Sistema, con el fin de optimizar la protección de las infraestructuras críticas y de las infraestructuras críticas europeas por ellos gestionados y deberán, entre otras obligaciones, elaborar el Plan de Seguridad del Operador y un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo, así como designar a un Responsable de Seguridad y Enlace, que será el interlocutor con el CNPIC en esta materia, y a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas.
- El sistema de planificación comprende los siguientes planes:
    - El Plan Nacional de Protección de las Infraestructuras Críticas, elaborado por la Secretaría de Estado de Seguridad, es un documento para dirigir y coordinar las actuaciones en esta materia en la lucha contra el terrorismo.

- Los Planes Estratégicos Sectoriales, elaborados por el Grupo de Trabajo Interdepartamental, que incluyen por sectores los criterios de las medidas a adoptar frente a una situación de riesgo.
- Las empresas que sean designadas como operadores críticos deberán presentar un PSO (Plan de Seguridad del Operador). En el, se define la política general de seguridad del operador y su marco de gobierno; identificando los servicios esenciales que presta; implantando una metodología de análisis de riesgo y desarrollando los criterios de aplicación de medidas de seguridad integral. Los Planes de Seguridad del Operador son documentos de alto nivel que contemplan aspectos relativos a la seguridad organizativa y procedimental del operador crítico. Deberán contener, al menos, aspectos relacionados con la política de seguridad del operador, marco de gobierno de la seguridad, identificación y estudio de los servicios esenciales que presta, la metodología de análisis de riesgos empleada, los criterios de aplicación de las medidas de seguridad empleadas y documentación complementaria.
- Asimismo, también deberán presentar un PPE (Plan de Protección Específico) respecto a todas sus infraestructuras clasificadas como críticas, en el que se defina la organización de la seguridad asociada al operador crítico; describiendo los datos generales, activos, elementos e interdependencias de las infraestructuras que hayan sido designadas como críticas; identificando las amenazas internas o externas, físicas o lógicas, intencionadas o aleatorias; detallando las medidas de seguridad y valores de riesgo y proponiendo las medidas a aplicar para proteger los activos críticos como consecuencia de los resultados obtenidos en el análisis de riesgos. Los Planes de Protección Específicos son documentos de seguridad de cada una de las infraestructuras críticas, donde se establecen las medidas de seguridad adoptadas por los operadores críticos para su protección.
- Los Planes de Apoyo Operativo son planes de carácter táctico, elaborados por el Cuerpo Policial con competencia en la demarcación, para cada una de las infraestructuras críticas, que deberán contener, al menos, los aspectos organizativos de la seguridad de la infraestructura, la descripción de la misma, un análisis de riesgos y un plan de acción con las medidas de seguridad a implementar.

Las entidades y organizaciones consideradas infraestructuras críticas, no están publicadas, no obstante, pertenecen a los siguientes sectores, considerados críticos:

- Salud.
- Sistema Financiero y Tributario.
- Industria Química.
- Espacio.
- Instalaciones de Investigación.
- Administración.
- Energía.
- Industria Nuclear.
- TIC.
- Transporte.
- Agua.
- Alimentación.

Para saber más: El CNPIC ha desarrollado unas guías de buenas prácticas para el desarrollo del Plan de Seguridad del Operador y del Plan de Protección Específico. Estas pueden ser visitadas en el apartado de Guías y metodologías del CNPIC

1.6.1. El Centro Nacional de Protección de Infraestructuras Críticas

El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) es un organismo creado mediante Acuerdo de Consejo de Ministros, el de 2 de noviembre de 2007. Sus competencias, están reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

El CNPIC depende de la Secretaría de Estado de Seguridad, del Ministerio del Interior, máximo responsable del Sistema de Protección de las Infraestructuras Críticas nacionales, asignándole al CNPIC la dirección y coordinación de cuantas actividades relacionadas con la protección de infraestructuras críticas frente a cualquier tipo de amenaza, como por ejemplo pueden ser aquellas procedentes de ataques terroristas u organizaciones criminales.

El Centro Nacional para la Protección de Infraestructuras Críticas desempeña las siguientes funciones:

Asiste al Secretario de Estado de Seguridad en la ejecución de sus funciones en materia de protección de infraestructuras críticas, actuando como órgano de contacto y coordinación con los agentes del Sistema.

Ejecuta y mantiene actualizado el Plan Nacional de Protección de las Infraestructuras Críticas.

Determina la criticidad de las infraestructuras estratégicas incluidas en el Catálogo.

Mantiene operativo y actualizado el Catálogo de Infraestructuras Estratégicas.

Dirige y coordina los análisis de riesgos de los Planes Estratégicos Sectoriales.

Establece los contenidos mínimos de los Planes de Seguridad de los Operadores, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo.

Analiza los Planes de Protección Específicos facilitados por los operadores críticos respecto a las diferentes infraestructuras críticas que propone, en su caso, para su aprobación, al Secretario de Estado de Seguridad.Logo CNPIC CNPIC. Logo del CNPIC (Todos los derechos reservados)

Validar los Planes de Apoyo Operativo diseñados para cada una de las infraestructuras críticas existentes en el territorio nacional por el Cuerpo Policial estatal o autonómico competente.

Implanta mecanismos permanentes de información, alerta y comunicación con todos los agentes del Sistema.

Recopila, analiza, integra y valora la información sobre infraestructuras estratégicas procedente de instituciones públicas, servicios policiales, operadores y de los diversos instrumentos de cooperación internacional para su remisión al Centro Nacional de Coordinación Antiterrorista del Ministerio del Interior o a otros organismos autorizados.

Participa en la realización de ejercicios y simulacros de protección de las infraestructuras críticas.

Coordina los trabajos y la participación de expertos en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas, en los ámbitos nacional e internacional.

El Servicio de Planes y Seguridad es el responsable de coordinar todos aquellos asuntos relacionados con la seguridad integral de las infraestructuras críticas y estratégicas nacionales, llevando a cabo las labores de implantación del sistema de planificación de la normativa relativa a la protección de infraestructuras críticas. Además, es el encargado de la custodia, mantenimiento y explotación del Catálogo Nacional de infraestructuras estratégicas que es el registro con la información completa, actualizada y contrastada de todas las infraestructuras estratégicas ubicadas en el territorio nacional, incluyendo las críticas y de la explotación de la herramienta de mensajería instantánea ALERTPIC.
El servicio está dividido en tres secciones: Análisis, Estudios sobre Infraestructuras y Centro de Coordinación y Alerta.
Para el desempeño de sus cometidos, se apoya en los servicios transversales siguientes:

- Servicio de Coordinación, que tiene como función el auxilio y cooperación con el titular del centro sobre el cumplimiento de sus funciones, asistida por la Sección de Relaciones Internacionales, encargada de las relaciones internacionales, especialmente con la Unión Europea.
- Servicio de Normativa que tiene como misiones principales las relativas al ámbito normativo en todo lo relacionado con la protección de las infraestructuras críticas y servicios esenciales.

Reflexiona: ACME se ha convertido en una empresa de telecomunicaciones, que da servicio a una o varias Fuerzas y Cuerpos de Seguridad del Estado (FCSE). Como tal, ¿Podría ser considerada ACME como infraestructura crítica?
Esta claro que ACME puede ser considerado un Proveedor de Servicios Digitales e incluso un Operador de Servicios Esenciales en el sector de telecomunicaciones.
Teniendo en cuenta que esta prestando servicio a FCSEs, una caída de su servicio podría ocasionar consecuencias graves para la población, por lo que podría ser considerado en el análisis de designación de infraestructuras críticas.

Respuesta
Autoevaluación I: c)
Autoevaluación II: a) c) d)
Autoevaluación III: a)El CCN-CERT es el CERT de referencia para entidades del sector público, b) Como ACME es una empresa privada, INCIBE-CERT debe ser su CERT de referencia
TEST I 10/10: 1 a), 2 a), 3 a), 4 c), 5 b), 6 a), 7 a), 8 a), 9 c), 10 b)
TEST II 10/10: 1 c), 2 c), 3 c), 4 a), 5 d), 6 d), 7 a), 8 a), 9 a), 10 a)

Autoevaluación I
El auditor del SGSI, quiere analizar que proyectos se han acometido durante el presente ciclo del SGSI ¿En qué epígrafe del sistema de gestión podría encontrar esta información?

a) Contexto de la organización
b) Operación
c) Planificación
d) Mejora

Autoevaluación II
¿Qué herramientas proporciona el CCN específicamente para el soporte al cumplimiento del ENS? (Multirespuesta)

a) AMPARO
b) CLARA
c) INES
d) VANESA

Autoevaluación III
En el caso en que ACME sufra un incidente de seguridad grave, y requiera soporte de un CERT. ¿Cuál sería su CERT de referencia?

a) CCN-CERT:
b) INCIBE-CERT:

TEST I

1- ¿Cual de las siguientes NO es una actividad necesaria para la adecuación al ENS?
   a. Desplegar un Centro de Operaciones de Seguridad.
   b. Realizar el análisis de riesgos.
   c. Preparar y aprobar la política de seguridad.
   d. Construir una declaración de aplicabilidad.

2- ¿Cuál de los siguientes procesos no forma parte de la evaluación de riesgos de continuidad?
   a. Minimizar los riesgos.
   b. Identificar riesgos para las actividades criticas para la organización.
   c. Analizar los riesgos identificados.
   d. Determinar la mejor decisión de tratamiento de riesgos.

3- Los requisitos mínimos a cumplir con el ENS estan definidos en el anexo 2 de la norma. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

4- ¿Cuál de los siguientes no es un objetivo de la directiva NIS?
   a. El establecimiento de un marco de comunicación entre las diferenes instituciones para la compartición de información de seguridad.
   b. La homogeneización de las medidas de seguridad entre organizaciones de diferentes países.
   c. La formación de un conjunto de profesionales que dara servicio a las administraciones públicas europeas.
   d. La mejora de los procesos de respuesta a eventos e incidencias de seguridad.

5- La directiva NIS existe un listado de proveedores de servicios digitales. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

6- La directiva NIS exige nombrar a un responsable de seguridad a las organizaciones en las que aplica. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

7- Tanto las personas como las organizaciones nos podemos certificar en ISO 27001. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

8- La última versión del Esquema Nacional de Seguriad es del año 2022. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

9-¿Cuál de las siguientes organizaciones no esta obligada a cumplir con el Esquema Nacional de Seguridad?
   a. Ministerio de industria, turismo y comercio.
   b. ACME, como empresa de telecomunicaciones dando servicio a Fuerzas y Cuerpos de Seguridad del Estado.
   c. Banco Santander.
   d. Banco de España.

10- El período de tiempo permitido tras un incidente dentro del cual se reanuda un producto, servicio o actividad o se recuperan recursos se denomina:
   a. Objetivo de punto de recuperación (RPO).
   b. Objetivo de tiempo de recuperación (RTO).
   c. Requisitos mínimos de continuidad de negocio (MBCO).
   d. Periodo máximo tolerable de interrupción (MTPD).

TEST II

1- ¿Cuál de las siguientes organizaciones esta afectada por la directiva NIS?
   a. Meliá.
   b. Mercadona.
   c. Amazon.
   d. Ferrovial.

2- ¿Qué tipo de control de los siguientes no es válido?
   a. Preventivo.
   b. Detectivo.
   c. Responsivo.
   d. Correctivo.

3- ¿En que proceso podriamos incluir la formación y capacitación en ciberseguridad?
   a. Detección.
   b. Identificación.
   c. Protección.
   d. Respuesta.

4- La ultima versión de la ISO 27002 es del año 2022. ¿Verdadero o falso?
   a) Verdadero

b) Falso

5- Un proceso Procesos aprobado y con políticas definidas, actualizados regularmente de acuerdo con el perfil de riesgo de la organización. ¿En que nivel de madurez se encuentra?

a. Informado.
b. Parcial.
c. Adaptativo.
d. Repetible.

6- ¿Que tres grupos de medidas hay en el anexo 2 del Esquema nacional de seguridad?

a. Medidas de protección, deteccion y organización.
b. Marco preventivo, detectivo y operativo.
c. Marco detectivo, operativo, y organizativo.
d. Marco Organizativo, operacional y medidas de protección.

7- La norma ISO 22301 es certificable. ¿Verdadero o falso?

a) Verdadero
b) Falso

8- ¿En qué epigrafe del SGSI podemos encontrar el listado de partes interesadas de la organización?

a. Contexto.
b. Liderazgo.
c. Soporte.
d. Planificación.

9- Los procesos de identificar, proteger, detectar, responder y recuperar... ¿a que marco pertenecen?

a. NIST cibersecurity framework.
b. Modelo CobIT
c. ISO 27001.
d. Marco SCF.

10- La directiva NIS recoge las medidas para garantizar un nivel de seguridad elevado en entidades tanto del sector privado como del sector público en toda Europa. ¿Verdadero o falso?

a) Verdadero
b) Falso

Caso práctico

La compañía ACME S.A. se encarga de proveer servicios de telecomunicaciones enfocados en comunicaciones internacionales tanto a particulares como a empresas.

ACME tiene una cartera de 300.000 clientes en España a los que ofrece estos servicios y por los cuales cobra una tarifa media de 23,5 € mensuales.

ACME está presente en 32 países, y se aprovecha de esta situación para dar servicio a multinacionales. Durante el año 2022 ACME ha logrado adjudicarse el servicio de telecomunicaciones de todas las embajadas en España.

Uno de sus clientes multinacionales es una entidad bancaria, con un nivel de madurez en seguridad elevado, uno de los requisitos que establece es la certificación ISO27001 en los servicios de comunicaciones.

La sede central de ACME se encuentra en Madrid, fue abierta en el año 2020, sus oficinas cuentan con climatización inteligente, jardines en las azoteas para mejorar la climatización y aprovechar el agua de la lluvia para los riegos de sus zonas verdes y paneles solares para mejorar la eficiencia energética.

Además, parte de los terrenos de la organización, han sido convertidos en parques públicos que pueden ser utilizados por los residentes de la zona, y los accesos por carretera a la zona han sido acondicionados, mejorados y reasfaltados.

En los últimos meses ACME esta de enhorabuena, ha logrado la adjudicación de un contrato mayor para la prestación de servicios de comunicaciones a una institución de las Fuerzas y Cuerpos de Seguridad del Estado. Dado el servicio que provee ha sido designado como proveedor de servicio esencial.

Dados los compromisos existentes hasta la fecha y con los nuevos contratos adjudicados, ACME va a abordar el proyecto de despliegue de un Sistema de Gestión de Seguridad de la Información, así como un Sistema de Gestión de Continuidad de Negocio. Asimismo, con el contrato otorgado para Fuerzas y Cuerpos de Seguridad del Estado, debe cumplir con la normativa del Esquema Nacional de Seguridad y con la Directiva NIS.

Apartado 1: Normas nacionales e internacionales

¿Podrías proponer tres controles de cada proceso de seguridad de la normativa NIST?

Procesos de seguridad de la normativa NIST

1. Identificación:

Asset Management, inventario y clasificación de activos.
Business Environment, identificar el entorno empresarial y sus dependencias.
Governance, políticas y procedimientos de seguridad.

2. Protección:

Access Control, control de acceso (roles y privilegios mínimos).
Data Security, encriptación de datos.

Maintenance, mantenimiento y actualización de sistemas.

3. Detección:

Anomalies and Events, monitoreo continuo para detectar anomalías.
Security Continuous Monitoring, implementar sistemas de monitoreo continuo.
Detection Processes, procedimientos para detectar y reportar incidentes.

4. Respuesta:

Response Planning, planes de respuesta ante incidentes.
Communications, comunicación interna y externa durante incidentes.
Analysis, análisis forense después de incidentes.

5. Recuperación:

Recovery Planning, planes de recuperación ante desastres.
Improvements, mejora continua en base a las lecciones aprendidas.
Communications, comunicación durante la recuperación.

Apartado 2: Sistema de gestión de seguridad de la información basado en ISO 27001

- Contexto descriptivo de la organización alineado con los requisitos del estándar:

ACME S.A. es una empresa dedicada a dar servicios de telecomunicaciones internacionales, con 300,000 clientes en España, localizada en 32 países. La sede central está ubicada en Madrid, con instalaciones modernas que incluyen climatización inteligente, jardines en las azoteas, y paneles solares. ACME ha sido designada como proveedor esencial para las Fuerzas y Cuerpos de Seguridad del Estado, lo que implica cumplir con normativas como el Esquema Nacional de Seguridad y la Directiva NIS.

- Propuesta de tres controles para la mitigación de riesgos identificados:

1. Establecer controles de acceso físicos y lógicos, implementando sistemas biométricos y autenticación multifactor para acceder a áreas críticas y sistemas informáticos o a información sensible.
2. Utilizar encriptación avanzada, utilizar algoritmos robustos para proteger datos sensibles tanto en tránsito como en reposo.
3. Programar auditorías periódicas tanto internas como externas de forma regular para asegurar el cumplimiento continuo con las normativas ISO 27001.

- Desarrollo de tres métricas de seguridad para ACME:

1. Media de incidentes detectados al mes: recopilar el número total de incidentes detectados y dividirlo por el número total de meses y así poder hacer un estudio de cuando hubo más, y donde se debe reforzar la seguridad.
2. Tiempo medio para resolver incidentes: saber el promedio del tiempo que se tarda desde la detección hasta la resolución completa del incidente, para poder mejorar los procedimientos.
3. Porcentaje de sistemas actualizados: calcular los sistemas utilizados por la organización que tienen los últimos parches de seguridad o actualizaciones realizadas y compararlo con el número total de sistemas, para mantener los sistemas actualizados y reducir las posibles vulnerabilidades.

Apartado 3: Sistema de gestión de continuidad de negocio basado en ISO 22301

El escenario a utilizar para este análisis de impacto es el de los sistemas centralizados que dan servicio a la red de comunicaciones de manera centralizada. En caso de indisponibilidad de estos sistemas, la red completa no podría funcionar.
Lucro cesante, provocado por la incapacidad de facturación ocasionada por la parada de los servicios de red. Se estima que la organización factura 100.000 € por hora.
Compensaciones, provocadas por los perjuicios que pudieran ocasionar a las empresas a las que ACME da servicio. Según los contratos firmados con los clientes de la empresa, se garantiza un 99% de servicio, y únicamente se debe compensar en caso de que la caída dure más de 30 minutos, y si el cliente corporativo lo reclama. Se ha estimado que, a partir de la primera hora, las compensaciones supondrían 500.000€ por cada hora de caída.
Imagen, la confianza en la organización y en los servicios que provee se vería afectada. Esto supondría una pérdida de un 1% de la cartera de clientes por cada incidencia. Además, se estima que habría una caída de altas nuevas. Este tipo de perjuicios se ha cuantificado en 200.000€ por incidencia.
Sanciones, la comisión del mercado de las telecomunicaciones puede actuar en caso de una pérdida de servicio elevada, además al haber un designio de operador de servicio esencial, una caída prolongada podría ocasionar pérdidas económicas por sanciones.
Se estima que esta situación se daría únicamente en caso de caídas repetidas y de larga duración.
La organización no está dispuesta a asumir pérdidas mayores a 1,5 millones de €.

- Análisis de impacto en continuidad sobre los sistemas asociados al servicio de telecomunicaciones:

El análisis de impacto en la continuidad del negocio es crucial para identificar y evaluar los efectos de una interrupción en las actividades críticas de la organización. Para ACME, los sistemas centralizados que dan servicio a la red de comunicaciones son esenciales. En caso de indisponibilidad, la red completa podría no funcionar y enfrentar pérdidas significativas debido a:

- Lucro cesante, se perderían ingresos por la incapacidad de facturar, la empresa factura alrededor de 100,000 € por hora, si se da una interrupción prolongada podría resultar en pérdidas importantes.
- Compensaciones, se deberán dar compensaciones a los clientes por perjuicios tras la caída del servicio. Debido a los contratos se garantiza el 99% de servicio, si la caída dura más de 30 minutos y es reclamada, serían de 500,000 € por hora.
- Pérdida de confianza, los clientes podrían perder la confianza en la organización y en sus servicios, se estima que un 1% de clientes se pierden por cada incidencia, además de un descenso en las nuevas altas. El daño se aproxima a 200,000 € por incidencia.

- Sanciones regulatorias, por parte de la comisión del mercado de las telecomunicaciones se pueden recibir sanciones económicas debido a que ACME es considerada proveedora de servicio esencial.

- Establecimiento del valor justificado para los parámetros MTPD, RPO Y RTO:

1. MTPD (Maximum Tolerable Period of Disruption): 24 horas, considerando el impacto financiero y reputacional. Una interrupción más prolongada podría resultar en pérdidas significativas y daños en la imagen de la empresa.
2. RPO (Recovery Point Objective): 1 hora, minimizar la pérdida de datos críticos es esencial para mantener la continuidad del negocio y la confianza de los clientes. Se asegura que la información perdida sea mínima..
3. RTO (Recovery Time Objective): 5 horas, para asegurar una rápida restauración del servicio. Este valor permite una rápida restauración del servicio minimizando el impacto en los clientes y las operaciones.

Apartado 4: Esquema nacional de seguridad

Categoriza los sistemas asociados al servicio de telecomunicaciones en función al escenario definido en el caso práctico, por la prestación de servicios a FCSEs.

Desarrolla una declaración de aplicabilidad justificada.

- Categorización de los sistemas asociados al servicio de telecomunicaciones:

Los sistemas asociados al servicio de telecomunicaciones de ACME deben ser categorizados como críticos debido a su rol esencial en las comunicaciones para las Fuerzas y Cuerpos de Seguridad del Estado (FCSE). La declaración se basa en el impacto de un incidente en términos de disponibilidad, autenticidad, integridad, confidencialidad…

- Debe incluir controles específicos:

- Autenticación robusta, implementar sistemas de autenticación Multifactor, protege contra accesos no autorizados y asegura que solo las personas que autorizadas puedan acceder a la información sensible
- Monitoreo continuo, implementar sistemas de monitoreo continuo para vigilar de forma constante los sistemas, detectando anomalías y amenazas en tiempo real.
- Planes detallados de respuesta ante incidentes, desarrollar planes de respuesta ante incidentes que incluyan procedimientos y roles bien definidos y claros, para asegurar respuestas rápidas y efectivas ante cualquier incidente, minimizando el impacto en las operaciones.

Para desarrollar las respuestas de manera clara y detallada es importante seguir una estructura, primero se realiza una introducción describiendo el problema y los objetivos de la respuesta, en el segundo paso analizamos los elementos involucrados, las propuestas de solución y cada una de sus justificaciones, por último en la conclusión hacemos un resumen de los puntos clave y las recomendaciones finales .