Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

El perito ante el ENS

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Alejandro Zafont Armengol

Tutor: Juan Vicente Oltra Gutiérrez

2017-2018

Resumen

En estos últimos años la tecnología avanza muy rápido y con ellos más ataques informáticos, para solventar esa amenaza se necesita gente cualificada para evitar daños de estos ciberataques. En este trabajo se va presentar una herramienta metodológica para los peritos que tengan que trabajar en una infraestructura crítica.

Se hablará del oficio de perito, como se trabaja, a que normativas y éticas está sujeto el perito profesional y la demanda de peritos cualificados. Por otra parte, se presentará las infraestructuras críticas: que son, la importancia en nuestra sociedad y su seguridad en todas las entidades del mismo ámbito. Conoceremos la tendencia actual que sufre una nación con los ciberataques, mostraremos unos ejemplos de las consecuencias de cualquier ataque a estas entidades que consigan atravesar la seguridad y unos casos prácticos donde veremos al perito trabajar, los pasos que sigue en su trabajo con las infraestructuras críticas.

Palabras clave: Perito, Infraestructura Crítica, Seguridad Nacional, ciberseguridad, resiliencia, ciberataque, normativa, amenazas, ataques informáticos

Abstract

In these last years, technology is advancing very rapidly and with it comes more cyberattacks. To solve this threat, qualified people are needed to avoid damages from these cyberattacks. This project will present a methodological tool for security experts which have to work in a critical infrastructure.

This project will contain information about the profession, what are the methodologies, the ethics and regulation they have to follow as well as the demand for qualified professionals. On the other hand, this project will also present critical infrastructures: what they are and the importance they have in our society; as well as their safety in every entity of the same scope. We'll be getting acquainted with the current tendencies of cyberattacks on nations, we'll be showing some examples of the consequences of any attack to these entities that are able to breach security. We'll also get acquainted with how the professionals work through some practical cases and the steps he follows when he works within critical infrastructures.

Key words: Expert, professional, critical infrastructure, national security, cybersecurity, resilience, cyberattack, regulation, threats, computer attack

Tabla de contenidos

Tabla de contenido

1. Introducción

Este trabajo de fin de grado (TFG) trata sobre el tema de los peritos informáticos y las Infraestructuras Críticas (IC). Cada vez hay más ciberataques a medida que la tecnología avanza y unos de los objetivos son entidades que son fundamentales para el día a día de las personas (hospitales, centrales eléctricas, centrales hidráulicas), por ello se tiene que brindar la máxima protección y estar constantemente con la última tecnología descubierta. Se presentará el oficio de perito informático que ayudará a las tareas de prevención de estas infraestructuras y actuación en caso de ataque.

1.1 Motivación

He elegido este tema para mi proyecto por dos razones. La primera es que durante la carrera se me presento el oficio del perito y cuáles eran sus funciones. Era la primera vez que oía el trabajo de un perito informático y me gusto, porque estamos muy acostumbrados a tener en mente como informático a esa persona delante del ordenador escribiendo código. También es gracias al profesor que me imparto esa materia que le dio un enfoque desde su experiencia que hizo que me atrajera más. La segunda razón es el desconocimiento de las personas a este oficio y como su labor es sumamente importante, cuando actualmente estamos rodeados de tecnología, por eso hay que dar a conocer el perfil de perito con este trabajo.

1.2 Objetivos

El principal objetivo de este TFG es tener una herramienta metodológica para futuros peritos que vayan a ejercer este oficio en un caso específico, en este caso de las infraestructuras críticas. Otros objetivos que quiere cubrir este TFG es la importancia de la seguridad en IC y su relevancia para la sociedad de hoy en día. También dar a conocer el oficio de perito informático y su desempeño en la sociedad actual.

1.3 Estructura

Mi trabajo está dividido en 3 grandes apartados:

- **El perito:** Hablaremos de lo que es un perito, cuál es su objetivo y que clases de perito nos podemos encontrar. También hablaremos sobre que norma se rige el perito y su metodología.
- **Seguridad nacional:** Detallaremos la situación actual que tiene España con la seguridad, en un término general hacia las posibles amenazas que pueden ocurrir. En este apartado nos centraremos en las IC y explicaremos que son y porque tiene que estar protegida severamente.

- **Casos prácticos y hechos reales:** Este apartado se expondrá unos ejemplos de cómo actúa un perito en 2 casos concretos y hechos que ha sucedido respecto a las IC o la Seguridad Nacional y sus consecuencias.

2. Estado del arte

La informática avanza a pasos agigantados, nuevas tecnologías se van creando o descubriendo y con ellos futuros puestos de trabajo que hay que cubrir. En el ámbito de la informática nos centraremos en los peritos informáticos, ya que es el tema de este trabajo de fin de grado. El perito cada vez se hace más visible para las empresas y la sociedad, como pasa con la profesión de auditor y consultor que cada vez está más demandada y un futuro cercano pasará con el perito, más adelante hablaremos de esas 3 profesiones y la conexión que existen entre ellas. No obstante, el oficio de perito ha crecido menos comparado al de auditor y consultor.

Dentro de la ETSINF existe un trabajo de TFG de ALBERTO JOSÉ PEDRERA ROS titulado: *Clasificación y estudio de herramientas para periciales informáticas* (2015-10-08), por ello mi trabajo complementará este trabajo de una forma más técnica con un ampliación del conocimiento del perito y una herramienta metodológica para un futuro perito.

No hay mucha información documentada reciente del perito informático y este trabajo sería un añadido más a esta profesión para futuros peritos y demostrar la importancia del perito informático.

3. Perito

3.1 ¿Qué es un perito?

La palabra perito, heredera del término latino ***peritus***, ha ido variando en su significado a lo largo de la historia. En la edición actual en vigor del diccionario de la RAE, 23º (2017), define perito como:

- Experto o entendido en algo
- Ingeniero técnico

Esta definición es algo pobre, para dar una definición más detalla hay que saber el significado de "*pericia".*

Según la RAE, edición 23º, la pericia se le denomina como **<<La sabiduría, práctica, experiencia y habilidad en una ciencia o arte>>.** Con esta definición podemos concluir que el perito es una persona experimentada, hábil o entendida en una ciencia o arte, es decir un experto en una determinada materia.

Según (Juan Vicente) el perito debe ser independiente e imparcial. Cuando decimos que un perito tiene que ser independiente nos referimos al contexto de la ausencia de vínculos con el conflicto y la imparcialidad al estado mental que permite emitir una opinión en libertad y sin prejuicios. También es necesario que aporte un enfoque analítico y honesto, que le permita discernir y plantear ante el juzgador aquellos aspectos que puedan favorecer o perjudicar a las partes, siempre centrado en aquellos que se le está encargando.

Hay que destacar un aspecto importante del perito, cuando recibe un encargo para que emita un informe, realice unas acciones o comprobaciones, el perito comprueba con el debido celo y diligencia, pero no investiga; de lo contrario convertiría a los peritos en una especie de inquisidores que se sale de su competencia.

En el caso de nuestra actividad es muy importante la prudencia y la discreción. El perito puede verse expuesto a un volumen importante de información, a veces sensible, pero deberá tratar de ceñirse a aquella imprescindible para cumplir el encargo y evitar cualquier otra irrelevante al mismo. Deberá guardar así misma confidencialidad de la misma y está obligado como cualquier otro profesional a poner los medios adecuados para que la información relativa a los asuntos que trata esté protegida y se mantenga privada.

3.2 Informática forense

Un aspecto importante de un perito es la parte forense, analizar pruebas y sacar evidencias, es crucial. Cuando se contrata un perito es para que haga esa función en la mayoría de casos. Como estamos en un trabajo sobre perito informático vamos hablar sobre informática forense.

La Informática Forense es considerada una rama de las ciencias forenses que se encarga de adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital. Es el uso de las Tecnologías de la Información para recuperar evidencia digital.
Hablamos de evidencias digitales a aquellas evidencias no físicas, que albergan información en forma binaria. La evidencia se convierte luego en elemento material probatorio cuando el perito la somete a examen, pues de manera separada, evidencia, dictamen pericial y testimonio del perito, serán cada uno elemento material probatorio. La presentación de estos en audiencia pública ante autoridad judicial y contradicción de las partes será la prueba.

El perito con su sabiduría y experiencia, debería analizar las evidencias.

El ámbito donde actúa la informática forense engloba todo un sistema informático tanto, si es el fin de un delito o es una forma de cometerlo, estos sistemas son objeto de análisis y estudio para a posteriori presentarlo como prueba, en su mayoría de caso será ante un tribunal, aquí el perito se ayudará con una normativa, **UNE 197001**, que más adelante explicaremos.

A la hora de actuar con el análisis de forense el perito suele usar una metodología que ayuda a la hora de trabajar y además cumplir con la denominada **cadena de custodia.**

La cadena de custodia, es este caso de las evidencias informáticas, tiene como objetivo guardar un registro de acciones y accesos, de tal forma que esté protegido de una posible manipulación y que no se descarte esa prueba como una evidencia; ningún jurado aceptará una prueba si se ha roto la cadena de custodia.

Para que el perito se asegure que se cumple la cadena de custodia, utilizará la siguiente metodología que consta de 5 fases para hacer un análisis forense.

3.2.1 Identificar

Se debe identificar las fuentes de datos a analizar y aquello que deseas encontrar. Hay que tener en mente la premisa de que se debe conservar las evidencias, por ello, no hay que hacer nada que pueda modificarlas.

3.2.2 Adquirir

En esta fase recopilaremos todas las evidencias que encontremos. Esta fase hay que ser muy cuidadoso y dejar constancia de todo lo que hacemos y como encontramos las cosas, es aconsejable tomar fotografías de los equipos o de cómo se encuentra el área y anotar todo lo que haces con la fecha, la hora de inicio y fin de cada de los pasos que se den. También es aconsejable que haya otra persona

que sea como un testigo y si es un notario, mejor que mejor. A continuación, daremos un formulario para tener un control de las acciones que se debe hacer y qué elementos debemos que observar, este formulario pretende ser una aproximación de las acciones más cotidianas que hace un perito.

Entorno

- Fotografiar y/o grabar el escenario o área donde se encuentren las evidencias o donde se produjo el ataque.
- Comprobar medidas de seguridad (cámaras, llaves, guardias).
- Preguntar si alguien ha tocado algo y por qué.
- Entrevistar a los responsables.
- Saber quién tiene acceso al sistema o al área.

Evidencias físicas

- Obtener ordenadores afectados.
- Obtener discos duros implicados.
- Comprobar la instalación eléctrica, ventilación y cableado.
- Obtener USB implicados.
- Móviles afectados.

Evidencias electrónicas

- Recopilar correo y mensajes.
- Registros y contenidos de la cache.
- Estados de las conexiones de red, tabla de rutas, puertos abiertos.
- Estado de los procesos en ejecución.
- Usuarios conectados remota y localmente.
- Información eliminada que se pueda recuperar.
- Bases de datos.
- Programas instalados.

3.2.3 Preservar

Aquí preservaremos las evidencias para que sean una prueba legal, así que lo primero que haremos será hacer una copia de esas evidencias, es recomendable etiquetar con la fecha y la hora de creación de la etiqueta.

Otro aspecto a tener en cuenta y que está relacionado con la **cadena de custodia** será preparar un documento en el que se registren los datos de todos los implicados en el proceso de manipulación, además sería interesante documentar:

- Dónde, cuándo y quién manejó o examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fecha, hora, etc.
- Quién estuvo custodiando la evidencia, durante cuánto tiempo y donde se almaceno.

- Cuando se cambie la custodia de la evidencia también deberá documentarse cuándo y como se produjo la transferencia y quien la transportó.

Todas estas medias harán que el acceso a la evidencia sea muy restrictivo y quede claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas o intentos de acceso no autorizados.

3.2.4 Analizar

Esta fase es el más laboriosa, donde se deberá recrear o teorizar la cadena de acontecimiento que tuvo lugar. Esta fase finalizará cuando sepamos responder a las siguientes preguntas **Qué, Cómo, Quién, Dónde y Cuándo**. Puede ser que alguna de estas preguntas no podamos contestar.

3.3.5 Presentar

Aquí elaboraremos nuestro informe pericial detallando todo lo descubierto, más adelante hablaremos en profundidad de los informes periciales.

3.4 Clase de perito y sus funciones

Cada vez más la presencia del perito es más importante ya sea en la parte judicial ayudando al juez o como árbitro para resolver un conflicto, por ello vamos a explicar lo tipos de peritos que hay y las funciones que realizan (Emilio, 2001)

3.4.1 Perito judicial

La ley de Enjuiciamiento Civil dedica sus artículos, 335 al 352 al dictamen de los peritos.

Los peritos (Art. 340 LEC) deberán tener títulos de tales en la ciencia o arte a que pertenezca el punto sobre el que han de dar su dictamen, si su profesión está reglamentada por las leyes o por el Gobierno. No habiendo peritos de aquella clase, deberán ser nombrados cualesquiera personas entendidas o prácticas en aquella materia, aunque no tengan título.

Según el Art.336 LEC, indica que las partes litigantes acompañen con sus escritos de demanda y de contestación a la demanda los informes periciales que pretendan aportar al proceso, con la posibilidad (Art 337) de aportarlos en un momento posterior.

Ello implica que quien quiera aportar un dictamen pericial a un proceso judicial, no necesita acudir al Juez o Tribunal para que le designen un perito, sino que puede dirigirse libremente al profesional que considere más oportuno para la emisión de la opinión técnica en la que sustentará su demanda o su oposición a la formulada por otro litigante. Aspectos generales de la designación directa del perito son su libre elección, por el propio litigante o por su abogado que dirige el asunto y la exigencia de idoneidad para la realización del dictamen.

3.4.2 Arbitraje

El arbitraje es un instrumento para la resolución de conflictos, basado en el acuerdo muto de las partes involucradas para conseguir una solución rápida y eficaz sin acudir a los Tribunales.

En un arbitraje el árbitro puede considerar necesaria la ayuda de un perito que dictamine sobre lo que se precise para un mejor conocimiento de los hechos. Parece que la necesidad de un perito en un arbitraje se dará más cuando se trate de un arbitraje de derecho, pues en el caso de los arbitrajes de equidad los árbitros suelen ser peritos en la materia sobre la que actúan.

Un árbitro pueden ser personas naturales que se hallen en el pleno ejercicio de sus derechos civiles, siempre que no se lo impida la legislación a la que puedan estar sometidos en el ejercicio de su profesión.

Como añadido, existe el “Arbitraje Institucional” (Art 14 L.A), que es el realizado por Corporaciones de Derecho público y Entidades públicas que puedan desempeñar funciones arbitrales, según sus normas reguladoras, así como Asociaciones y entidades sin ánimo de lucro en cuyos estatutos se prevean funciones arbitrales. Estas instituciones ejercerán sus funciones conforme a sus propios reglamentos y velarán por el cumplimiento de las condiciones de capacidades de los árbitros y por la transparencia en su designación, así como su independencia.

3.4.3 Mediación/particulares

Según la ley: “Se entiende por mediación aquel medio de solución de controversias, cualquiera que sea su denominación, en que dos o más partes intentan voluntariamente alcanzar por si mismas un acuerdo con la intervención de un mediador”.

El dictamen puede ser solicitado por dos partes enfrentadas que no desean acudir a los Tribunales ni a un arbitraje y quieren conocer la opinión de un tercero sobre el tema en litigio al objeto de dirimir su contencioso en función de la que diga un perito.

Asimismo, puede suceder que una parte desee conocer las posibilidades que tiene de obtener una sentencia favorable antes de presentar una demanda o querella y evitarse con ellos los problemas que un procedimiento judicial conlleva de tiempo, gastos y para ello solicita el dictamen de un perito.

3.5 Responsabilidad y deontología profesional

Según nos comenta (Emilio, 2001) un perito tiene que tener las siguientes consideraciones cuanto a la responsabilidad y deontología asociada a sus acciones, como elementos que van más allá de lo que las leyes u otras normas le imponen:

1. Cuando un perito ejerce su actividad es responsable ante el cliente, las partes en conflicto, el colectivo de peritos y la sociedad en general.
2. El perito deberá ser consciente de sus capacidades, carencias y circunstancias cuando acepta un encargo profesional. Todas las conclusiones que exprese deben ser objetivas, estar soportadas por evidencia al respecto y alinearse con las prácticas y usos del sector de actividad.
3. Cuando el peritaje no sea a instancia de una parte, el perito mantendrá a ambas partes debidamente informadas por igual de la evolución del encargo, especialmente de aquellos hechos que pueden ser relevantes al desarrollo del mismo. Por lo demás, velará por la confidencialidad para con la otra parte. El perito considerará todo lo que favorezca o perjudique a las dos partes ciñéndose a lo que se le solicita.
4. El perito deberá inhibirse en cuanto conozca alguna circunstancia que pueda comprometer su imparcialidad. Debe comprometerse también en la medida de lo posible a evitar que terceros tengan conocimiento de hechos relativos a su trabajo como perito que puedan vincularse con personas o entidades concretas y que no sean públicos y notorios por otros cauces.
5. El coste del peritaje ha de ser razonablemente proporcional al volumen de trabajo que suponga. El perito deberá exponer a la parte que realiza el encargo en la medida de lo posible, el coste aproximado y las posibles desviaciones para que pueda dicha parte evaluar su idoneidad con el objeto de litigio.

Por último, el perito se abstendrá de realizar y facturar tareas que no aporten valor en la línea de lo que se indica es el objeto del encargo.

3.6 Peritaje informático

El peritaje en informática tendría una visión eminentemente probatoria de los indicios y no se quedaría en hechos simples, sino que estaría en disposición de extraer hechos complejos y de alto nivel de las evidencias observadas, incluso cuando estos hechos de alto nivel requieren de una capacitación para su interpretación o valoración. El perfil del perito debe incluir conocimientos de los sistemas de información sobre los que tenga que actuar, las técnicas de informática forense y siendo el objeto de su trabajo la introducción de hechos en un litigio, un mínimo conocimiento de las reglas que operan en el procedimiento a este respecto.

Cabe reseñar que el perito en informática interviene siempre que es necesaria la opinión de un experto en informática en un litigio, por lo que su actividad no se limita a la captación, interpretación y presentación de indicios, bien sea en

conflictos con objeto tecnológico u otros. Como experto está en disposición de opinar y valorar elementos y circunstancias como por ejemplo el grado de cumplimiento de una obra o servicio informático.

Las causas por las que se comenzaron a realizar peritajes en esta área, es la cantidad de infracciones que se producían en este ámbito: infracciones a la propiedad intelectual del software, revelación de secretos, vulneración de la intimidad, estafa, fraudes, daño, incumplimiento en contratos de programación o de implantación de sistemas informáticos, valoración de bienes informáticos, investigación del contenido de ordenadores en soportes magnéticos, etc.

Relación entre informática y delito (Darahuge y Arellano, 2008):

- **Delitos informáticos:** Son los delitos que provocan daño sobre la información, afectando a la integridad y confiabilidad, sobre la confidencialidad, afectando a la privacidad, autenticidad y control de accesos.
- **Delitos por medios informáticos:** Son los delitos que están tipificados en la legislación vigente, lo que se cometen con el auxilio de medios físicos o lógicos, generalmente computacionales.
- **Prueba informático forense:** Resulta del empleo de técnicas informáticas y criminalísticas para detectar, proteger, documentar, analizar y evaluar los indicios probatorios que aparecen en un sistema de información para poder reconstruir los hechos, ya sean delictivos o no.

Según la empresa **Recovery Labs,** empresa dedicada a los servicios de peritaje informático, para ayudarles a resolver aquellos litigios relacionados con la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, el servicio que más cubre es **investigaciones informáticas** por cuestiones alusivas a delitos informáticos relacionados con el ámbito empresarial. A continuación, vamos a mostrar las estadísticas de los servicios que piden sus clientes del 2015.

- Un **46.71%** son **Delitos Informáticos** como la falsificación o fraude informático mediante la introducción, borrado o supresión de datos informáticos, o la interferencia en sistemas informáticos.
- Un **43.11%** son **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos**. Dentro de esta categoría las conductas que más se repiten son con un 63.89% delitos relacionados con el acceso ilícito a sistemas informáticos, y con un 36.11% todas aquellas conductas delictivas relativas a la interferencia en el funcionamiento de un sistema informático.
- Un **10.18%** son **Delitos relacionados con el contenido,** como la producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos (Forensic, 2015).

Para más información sobre los tipos de delitos informáticos en el **Anexo 2**.

3.7 Informe pericial

El informe pericial es el documento redactado por el perito informático, en el que se exponen las conclusiones obtenidas por el experto, tras la investigación de un caso de delito informático o una revisión de las normativas a las instalaciones.

El Informe pericial debe incluir, al menos:

- Los datos del cliente.
- Los objetivos de la investigación.
- La declaración previa del perito informático, en la que se establecen los principios de profesionalidad, veracidad e independencia.
- Documentación sobre el proceso de adquisición de pruebas.
- Detalle de las acciones que el perito informático lleva a cabo durante la investigación.
- Resultados de la investigación informática y conclusiones.

La elaboración del informe consta a su vez de tres fases:

1. **Fase de adquisición de las pruebas:**

   Recogida de todos elementos que van a intervenir en la investigación. Es importante que el proceso de intervención de los equipos informáticos se lleve a cabo con todas las garantías para las partes. La documentación del proceso de adquisición de las pruebas es una información que debe formar parte del informe pericial.

2. **Fase de la investigación:**

   El perito informático realiza un análisis exhaustivo de los equipos informáticos, especialmente de las unidades de almacenamiento de datos en busca de todos aquellos elementos que puedan constituir prueba o evidencia electrónica en el caso en cuestión.

   Constarán en el informe todas las acciones realizadas durante la fase de investigación, como las herramientas empleadas para la adquisición de la evidencia electrónica y el detalle y resultado de los procesos efectuados sobre el dispositivo o unidad que se está analizando.

3. **Fase de elaboración de la memoria.**

   Tras el minucioso estudio de la información almacenada en los dispositivos, intervenidos en la fase de adquisición de pruebas, el perito informático analiza los resultados obtenidos con el fin de extraer las conclusiones finales de la investigación.

   En esta última fase, el perito informático recopila la información que ha obtenido durante todo el proceso de investigación y redacta el informe o memoria que se presentará ante los Tribunales o la persona que le han contratado: jefes de una empresa, alto cargo del estado.

El creciente número de actuaciones periciales profesionales, lleva la necesidad de establecer una garantía para asegurar que aquellas son adecuadas al uso a que se destinan, por eso se creó la normativa **UNE197001**
Criterios generales para la elaboración de informes y dictámenes periciales.

Esta normativa establece los requisitos formales que deben de tener los informes y dictámenes periciales, así se aseguran una metodología para la creación de informes y dictámenes. Hace hincapié sobre la estructura que tiene que tener un informe, el cuerpo del informe estará constituido por:

- Objeto
- Alcance
- Antecedentes
- Consideraciones preliminares
- Documentos de referencias
- Terminología y abreviaturas
- Análisis
- Conclusiones

Todos estos apartados están incluidos en la normativa **UNE 50132,**
Numeración de las divisiones y subdivisiones en los documentos escritos.

Vemos que la normativa **UNE 50132** ayuda a la normativa **UNE 197001** a tomar una metodología a la hora de elaborar el informe pericial y subdividir los apartados correctamente. No obstante, la **UNE 50132** no solo sirve para informes periciales sino para cualquier escrito o documento de carácter formal, es más, este trabajo tiene parte de la UNE 50132 que se está cumpliendo.

3.8 Consultor y Auditor

Cuando hablamos del perito y de sus funciones puede llevar a confusión, puesto que la diferencia entre un perito, un consultor y un auditor son leves, ya que hay una línea muy fina que les separa. Las funciones de esas 3 profesiones son muy similares, pero tantos sus metas y su impacto en una empresa o institución son diferentes. Ya hemos hablado del perito y de sus labores anteriormente, a continuación, hablaremos del Consultor y del Auditor veremos cuáles son las diferencias entre estas profesiones.

3.8.1 Consultor

Antes de dar una definición de un consultor vamos tener en mente una hipotética situación. Imaginamos que tenemos una empresa mediana e importante durante varios años. Tenemos nuestros empleados y nuestro sistema de información. La empresa se ha mantenido con altibajos, a veces el sistema no presentaba bien el stock que teníamos en almacén o con las nuevas políticas implantadas en estos años se retrasaban los envíos o peor aún el sistema de información estaba obsoleto y no podía cubrir todos los aspectos que tú quieres cubrir. En este punto necesitas alguien externo que te ayude a rediseñar tu sistema de implantación y analizar los posibles fallos y solventarlos, es ahí cuando entra el consultor.

Un consultor, según la RAE, es aquella persona experta en una materia sobre la que asesora profesionalmente. Si recordamos la definición que daba al perito es casi idéntica salvo la parte de “asesora”, ya vemos la primera pequeña diferencia entre un perito y un auditor. El consultor debe ser un experto en su campo (igual que del perito), asesora correctamente y da soluciones viables para la empresa.

Según (Ribeiro Soriano, 1998) apunta que la consultoría opera sobre la capacidad de aumentar la efectividad organizacional.

(Garzón Castrillón, 2005) Formula que los lineamientos generales de la consultoría son los siguientes:

- **Es un servicio independiente**. Se caracteriza por la imparcialidad del consultor, que es un rasgo fundamental de su papel. Esta independencia significa al mismo tiempo una relación muy compleja con las organizaciones (clientes) y con las personas que trabajan en ellas. El consultor no tiene autoridad directa para tomar decisiones y ejecutarlas. Pero esto no debe considerarse una debilidad si el consultor sabe actuar como promotor de cambio y dedicarse a su función, sin por ello dejar de ser independiente. Por consiguiente, debe asegurar la máxima participación del cliente en todo lo que hace de modo que el éxito final se logre en virtud del esfuerzo de ambos.
- **Es, esencialmente, un servicio consultivo**. No se contrata a los consultores para dirigir organizaciones o para tomar decisiones en nombre de directores en problemas. Su papel es actuar como asesores, con responsabilidad por la calidad e integridad de su consejo; los clientes asumen las responsabilidades que resulten de la aceptación de dicho consejo. No solo se trata de dar el consejo adecuado, sino de darlo de manera adecuada y en el momento apropiado. Esta es la cualidad fundamental del consultor. El cliente, por su parte, debe ser capaz de aceptar y utilizar esa ayuda del consultor.
- **Proporciona conocimientos y capacidades profesionales para resolver problemas prácticos**. Una persona llega a ser consultor de empresas en el pleno sentido del término después de haber acumulado una masa considerable de conocimientos sobre los diversos problemas y situaciones que afectan a las empresas y adquirido la capacidad necesaria para identificarlos, hallar la información pertinente, analizar y sintetizar, elegir entre posibles soluciones, comunicarse con personas, etc. Cierto es que los dirigentes de las empresas también tienen que poseer estas capacidades. Lo que distingue a los consultores es que pasan por muchas organizaciones y que la experiencia adquirida en las tareas pasadas puede tener aplicación en las empresas en las que se realizan nuevas tareas. Además, los consultores profesionales se mantienen al tanto de los progresos en los métodos y técnicas, señalan estos progresos a sus clientes y contribuyen a su aplicación.
- **No proporciona soluciones milagrosas**. Sería un error suponer que, una vez contratado el consultor, las dificultades desaparecen. La consultoría es un trabajo difícil basado en el análisis de hechos concretos y en la búsqueda de soluciones originales, pero factibles. El empeño decidido de la dirección de la empresa en resolver los problemas de ésta y la cooperación entre cliente y consultor son, por lo menos, tan importantes para el resultado final como la calidad del consejo del consultor.

(Valles Romero, 2008) Propone el siguiente modelo de cinco fases, con sus correspondientes actividades, como proceso de consultoría, hay que tener en cuenta que cada empresa es distinta y la función que debe desempeñar un consultor puede variar, esto es solo una forma de organizarse el trabajo.

1. **Iniciación (Preparación inicial)**
    a. Primeros contactos con el cliente
    b. Diagnóstico preliminar
    c. Planear el cometido
    d. Propuesta de tareas
    e. Contrato
2. **Diagnóstico**
    a. Descubrir los hechos
    b. Análisis y síntesis
    c. Examen detallado del problema
3. **Planificación de medidas (Plan de acción)**
    a. Elaborar soluciones
    b. Evaluar opciones
    c. Propuesta al cliente
    d. Planear la aplicación de medidas
4. **Aplicación (Implementación)**
    a. Contribuir a la aplicación
    b. Propuesta de ajustes
    c. Capacitación
5. **Terminación**
    a. Evaluación
    b. Informe final
    c. Establecer compromisos
    d. Planes de seguimiento
    e. Retirada

Como podemos observar los dos primeros apartados serian idénticos al de perito en una pericia, sin embargo, los apartados 3 y 4 no se le incluiría al perito porque ya comentamos anteriormente que el perito solo esta para encontrar los fallos y los hechos en que sucedido eso, no está en su labor dar soluciones o quien fue el responsable de los errores. El último apartado también es acorde en una pericia, pero en algunas partes.

Como hemos ido observando sí que existen diferencias de funciones y objetivos entre un perito y un consultor, pero las diferencias son mínimas. Se puede dar el caso que una persona haga una labor pericial y esa misma persona luego haga una labor de consultoría, no sería nada raro tal como hemos estado observando

3.8.2 Auditoria

Como hemos hecho en el apartado de “Consultor” vamos a coger ese mismo ejemplo que hemos explicado y vamos cambiarlo un poco. Tenemos la empresa y queremos comprobar que todos los protocolos de seguridad, licencias, contabilidad etc.… se esté haciendo correctamente como dicta la normativa, para esa función se le llama a un Auditor para que realice ese trabajo.

Según La RAE un auditor es el que realiza auditorías. Esta definición es muy pobre así que daremos una definición un poco más técnica. Un auditor es una persona experta, cualificada e independiente, designada por una autoridad competente, para revisar y evaluar los resultados de una gestión administrativa o financiera de una institución, una empresa o sociedad pública o privada. Como podemos observar la definición es muy parecida a la de perito y al consultor, su labor viene a ser muy similares. Suele llamar a un auditor cuando quiere que se certifique alguna certificación o comprobar que se está realizando el trabajo correctamente, para ello se hace una auditoria.

La misión de una auditoria consiste en proporcionar los elementos técnicos que puedan ser utilizados por el auditor para obtener la información y comprobación necesaria que fundamente su opinión profesional sobre los aspectos de una entidad sujetos a un examen. Consiste en apoyar a los miembros de la organización en relación al desempeño de sus actividades, para ello la auditoria les proporciona análisis, evaluaciones, recomendaciones, asesoría y toda aquella información relacionada con todas las actividades revisadas por el auditor, la auditoria se encarga de promocionar un control efectivo o un mecanismo de prevención (Alvin A. Arens, Randal J Elder, Mark S. Beasley,Prentice Hall, 2007)

Norma ISO 19011, *Directrices para la auditoría de los sistemas de gestión*
Las cualidades que deben definir a un auditor son las siguientes:

- Ser imparcial y honesto.
- Ser discreto y comprender el concepto de confidencialidad.
- Tener la mente abierta para considerar ideas y puntos de vista alternativos.
- Ser diplomático y tener tacto con el trato con las distintas personas.
- Ser firme y estar seguro de sí mismo. En este punto es importante destacar que en la auditoría el auditor no debe negociar con el auditado sobre la inclusión o eliminación de una determinada no conformidad en el informe final ya que, de esta forma, desvirtúa la eficacia de esta. Es decir, aunque se actúe de manera responsable y ética, algunas decisiones tomadas por el auditor pueden no ser populares, pudiendo llegar a causar desacuerdos y confrontaciones que no deben llevar a la negociación para la aceptación del informe.
- Tener una alta capacidad de observación.
- Tener instinto para ser consciente y comprender las situaciones.
- Adaptarse fácilmente a los distintos contextos, es decir, ser versátil.
- Tener una clara orientación hacia la consecución de los logros definidos como metas.
- Alcanzar conclusiones basadas en razonamientos lógicos y el análisis de las distintas evidencias.
- No tener prejuicios que limiten o eliminen su objetividad.

El auditor sigue una metodología para hacer la auditoria, observaremos que los pasos que siguen son similares al de una consultoría (Alvin A. Arens, Randal J Elder, Mark S. Beasley,Prentice Hall, 2007)

1. **Análisis General y Diagnostico**
    a. Evaluación preliminar

   b. Plan de trabajo
   c. Ejecución
   d. Diagnostico
2. **Planeación especifica**
   a. Determinación de objetivos
   b. Elaboración de programas
   c. Determinación de recursos
   d. Seguimiento del programa
3. **Realización**
   a. Ejecución
   b. Obtención de evidencias
   c. Técnicas y Recurso
   d. Coordinación y supervisión
4. **Informes**
   a. Observaciones y oportunidades de mejora
   b. Estructura, contenido y presentación
   c. Discusión con el cliente y definición de compromisos
   d. Informe ejecutivo
5. **Fase final**
   a. Diseño
   b. Implementación
   c. Evaluación

Esta metodología es muy parecida al de un consultor con sus pequeñas variantes y también al de un peritaje con sus pequeñas diferencias también.

Como resumen de este apartado concluiremos que las figuras de perito, consultor y auditor tienen una misma base donde sale su metodología y las características de estas profesiones, pero en la práctica cada oficio se utiliza para determinadas situaciones y diferentes fines.

4. Seguridad nacional

4.1 ¿Qué es la seguridad nacional?

La seguridad nacional es la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizas la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos.

El concepto de seguridad ha evolucionado en consonancia con las transformaciones globales, para hacer frente a los crecientes desafíos que presentan las circunstancias del mundo en que vivimos.

El mundo globalizado actual se encuentra en un proceso de cambio continuo, debido a factores como la evolución constante de los centros de poder, con nuevas potencias en ascenso, la consolidación de nuevos actores internacionales, la mayor capacidad de influencia adquirida por parte de los individuos, los cambios demográficos, la mayor competencia por los recursos energéticos, alimenticios y económicos, así como el papel de las tecnologías en la sociedad del conocimiento o la mayor interdependencia económica, política y jurídica.

Existen, en consecuencia, nuevos riesgos y amenazas que afrontar. Junto a los tradicionales, como los conflictos armados, surgen otros de naturaleza esencialmente transnacional, que se retroalimentan y, al interactuar, potencian su peligrosidad y la vulnerabilidad del entorno. Otros elementos que suman complejidad a los riesgos y amenazas del contexto estratégico actual son su impacto transversal en distintas estructuras y actores del Estado y de la sociedad o la difícil identificación de su origen y la ausencia de un centro de gravedad único. El terrorismo internacional, la proliferación de armas de destrucción masiva, el crimen organizado, los ciberataques o el espionaje son solo algunos ejemplos.

El concepto de seguridad en el siglo XXI debe ser amplio y dinámico, para cubrir todos los ámbitos concernientes a la seguridad del Estado y de sus ciudadanos, que son variables según las rápidas evoluciones del entorno estratégico y abarcan desde la defensa del territorio a la estabilidad económica y financiera o la protección de las infraestructuras críticas.

Por otra parte, la respuesta a los riesgos y amenazas que comprometen la seguridad en nuestros días precisa de cooperación tanto en el plano nacional como en el multilateral. Las respuestas unilaterales y aisladas no son eficaces, por su carácter incompleto y parcial, frente a unos retos que exigen un enfoque multidisciplinar y una acción conjunta. Solo esta perspectiva abarca todos los aspectos potencial o realmente afectados.

Los cambios y tendencias relativos al entorno de la seguridad, sus dimensiones, y las respuestas que pide su preservación, son factores que inciden en la visión de la Seguridad Nacional. España se sitúa junto a los países más avanzados en la materia y concibe la seguridad de una manera integral, acorde con las transformaciones globales que repercuten en el Estado y la vida diaria del ciudadano. En esta línea, la crisis financiera y económica que actualmente afecta a

España, a la zona euro y a parte importante de las economías mundiales representa uno de los mayores retos para la Seguridad Nacional y extrema la necesidad de ser eficientes en la respuesta.

Para brinda que la seguridad nacional no sea amenaza, el gobierno traza una Estrategia de Seguridad Nacional para cumplir estos objetivos.

Dentro de la Seguridad Nacional cubre un amplio abanico de ámbitos donde detalla cuáles son y cómo actúa sobre ese ámbito, como nuestro trabajo es sobre el ámbito de las infraestructuras críticas, nos centraremos exclusivamente en ellas.

4.2 Infraestructuras críticas

La definición de infraestructuras críticas (IC) se basa no tanto en el sistema si no en la función que este desempañe o el servicio que presta, es decir, las infraestructuras críticas son aquellas que desempeñan una función esencial para el correcto funcionamiento de un país. Hay una entidad que es el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) donde detallaremos cuando se formó y cuales es su función.

4.3 El Centro Nacional para la Protección de las Infraestructuras Críticas

4.3.1 Historia

A raíz de los atentados del 11 de marzo de 2004, España tuvo que tomar las medidas oportunas para evitar que algo similar a lo que acababa de suceder pudiera volverse a producir. Así fue que en 28 de mayo de 2004 nace el Centro Nacional de Coordinación Antiterrorista (CNCA)-No operativo- para contrarrestar los posibles ataques terroristas. Sus funciones eran muy amplias y no se enfocaba a las Infraestructuras Criticas por ello en 2007, cuando se diseña y desarrolla el Plan Nacional de PIC (PNPIC) y se crea el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) (GrupoS2, 2011)

4.3.2 Qué es y cuáles sus funciones

El CNPIC es el órgano ejecutor de la mayoría de las políticas que sobre esta materia lleva a cabo el Gobierno a través de la Secretaría de Estado del Ministerio del Interior, y por ello, está presente en toda la normativa de Protección de Infraestructuras Criticas (PIC) a lo largo de todo su articulado. Como determina la Ley 8/2011, es el «órgano ministerial encargado del impulso, la coordinación y la supervisión de todas las actividades en el campo de las PIC». Es, por tanto, el motor del Sistema PIC. (GrupoS2, 2011)

El CNPIC responde a un patrón muy concreto que, a nivel internacional, ha sido implantado en muchos de los países de nuestro entorno, que no es otro que el de constituirse como el órgano nacional competente en materia de PIC (en España esa responsabilidad cae en el Ministerio del Interior), por el ámbito de actuación

escogido por el legislador, que no es otro que el prevenir/responder ataques deliberados en el marco de la seguridad nacional.
A tal fin, el CNPIC destaca, en primer lugar, por su condición de ser un órgano de coordinación, y en este sentido hay que tener en cuenta que es el departamento oficialmente designado para representar a nuestro país en el campo de la PIC ante las instituciones comunitarias y supranacionales. (GrupoS2, 2011)

En segundo lugar, el CNPIC es el órgano responsable del Catálogo Nacional de Infraestructuras Estratégicas a la hora de gestionar su contenido, explotarlo, dar accesos y custodiar su seguridad. Esta tarea, junto con la necesidad de proporcionar una seguridad integral, con una focalización cada vez mayor en la ciberseguridad, es clave a la hora de plasmar el rendimiento operativo del CNPIC y su traslado a los organismos y unidades encargadas de proporcionar seguridad y protección sobre el terreno. (GrupoS2, 2011)

Finalmente, la tercera, y no menos importante labor que el CNPIC está llamado a ejercer en el marco de la legislación sobre PIC, son sus funciones de estudio, información, desarrollo, colaboración, supervisión y revisión del sistema de planificación que más tarde se estudiará en mayor profundidad y que, comenzando por el Plan Nacional PIC, finaliza con los Planes de Apoyo Operativo. Su participación en todo el proceso de vida de dichos planes es clave para el desarrollo e impulso de un proceso que necesita de la involucración de todos los actores representativos.

Los ejes de trabajo, o pilares, sobre los que el CNPIC desarrolla sus cometidos son, de esta forma, tres fundamentales:

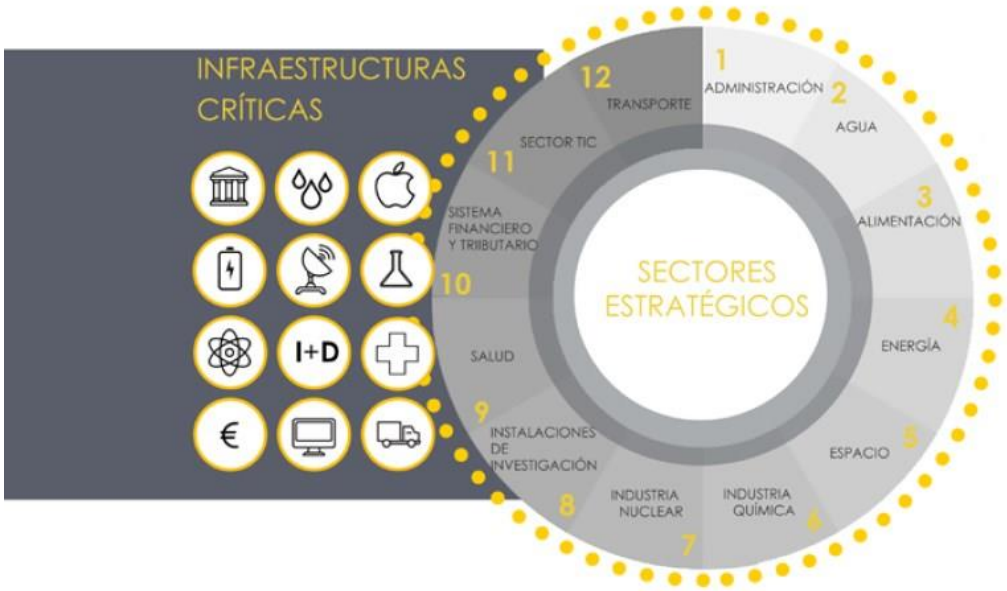
- Su función de coordinación, integración e impulso del Sistema PIC y su labor de desarrollo y seguimiento de los instrumentos de planificación (basado todo ello en la cooperación público-privada y en la regulación normativa).

- Sus actividades de gestión y mantenimiento del Catálogo Nacional de Infraestructuras Estratégicas, como base operativa y de conocimientos del Sistema.

- Su misión de búsqueda de una seguridad integral, proyectándose en la ciberseguridad de forma muy especial, sobre la base de herramientas y metodologías específicas.

En nuestra sociedad cada vez está más vinculada o depende en gran medida de un sector estratégico para su funcionamiento. Los sectores estratégicos se dividen en doce (Valles Romero, 2008):

- Administración
- Agua
- Alimentación
- Energía
- Espacio
- Industria Química
- Industria Nuclear
- Instalaciones de investigación
- Salud
- Sistema Financiero y Tributario
- Tecnologías de la Información y las comunicaciones
- Transporte



(Imagen 01 Sectores Estratégicos, imagen sacada de documento, ESTRATEGIA DE SEGURIDAD NACIONAL)

Estos sectores son de vital importancia, porque constituyen los pilares principales de nuestra sociedad y cualquier ataque contra estos sectores pondría en peligro la estabilidad del país y su funcionamiento (Valles Romero, 2008). Más información en el **Anexo 3** y **5**

Cualquier organismo, institución o empresa, tanto pública como privada, que gestione al menos una infraestructura considerada como crítica para la clasificación del CNPIC, podrá ser considerado como un operador crítico.

La designación de un operador critico es un proceso que comenzó en 2011 con la aprobación de la Ley "*PIC*" (Protección de Infraestructuras Críticas) en septiembre de 2011 y la designación de los primeros operadores críticos, a los que recientemente se han unido 54 más en los sectores del agua y el transporte, a los que próximamente se unirán operadores críticos en el sector alimenticio y sanitario.

En el **BOE Núm. 102 de viernes 29 de abril de 2011 Sec. I. Pág. 43370 Art 13** se nos habla que los operadores críticos 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.

4.4 Ley PIC

La Ley PIC define como IC aquellas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Estos a su vez, se definen como los servicios necesarios 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 Publicas

Por último, define como infraestructuras estratégicas las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

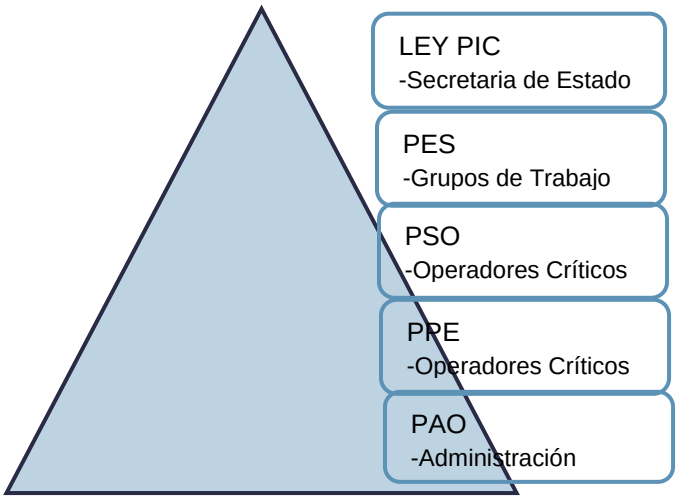
Principales aportaciones de la Ley PIC:

1. **Creación del sistema nacional de Protección de Infraestructuras Críticas:** Este sistema crea una estructura organizativa a nivel nacional en la que se distribuyan las funciones y responsabilidades que los diversos agentes tantos públicos como privados, deben tener en el marco de la seguridad de las IC que proveen a la sociedad de los servicios esenciales, contando como organismo centralizador al CNPIC, como entidad director y coordinador. Trata de establecer el concepto de asociación público-privada y una base de confianza mutua entre entidades CNPIC, ministerios, comunidades autónomas, corporaciones locales, grupos de trabajo sectoriales y empresas privadas.
2. **Sistema de planificación PIC:** Es un conjunto de textos normativos que definen una serie de medidas para la protección de las infraestructuras críticas, que se concretan en actuaciones que deben llevar a cabo los integrantes del sistema de protección de infraestructuras críticas.

   Según la ley PIC se definirán tantos PES (Planes Estratégicos Sectoriales) como sectores haya definidos. El desarrollo de estos planes permite conocer cuáles son los servicios esenciales proporcionados a la sociedad, su funcionamiento general, las infraestructuras estratégicas sobre las que se asistan estos servicios esenciales, los operadores, propietarios o gestores de las mismas, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento.

   Las empresas que sean designadas como operadores críticos deberán presentar y mantener actualizado un PSO (Plan de Seguridad del Operador) y un PPE (Plan de Protección Especifico) para todas sus infraestructuras clasificadas como críticas. La administración competente apoyada por los cuerpos y fuerzas de seguridad del estado, deberá desarrollar un PAO (Plan de apoyo orientativo).

   En un modo de resumen y esquemático la organización se representaría con el siguiente esquema.



(Imagen 2: Organización Ley PIC)

A continuación, explicaremos brevemente los PSO, PPE, PAO

PSO

Los Planes de Seguridad del Operador son los documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión y deberá como mínimo contener:

1. Política general de seguridad del operador y marco de gobierno
2. Relación de servicios Esenciales prestados por el operado crítico.
3. Metodología de análisis de riesgo (amenazas físicas y lógicas)
4. Criterios de aplicación de Medidas de Seguridad Integral.
5. Documentación Complementaria.

PPE

Son documentos operativos donde se definen las medidas concretas a poner en marcha por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas y deberá contener:

1. Organización de la seguridad
2. Descripción de la infraestructura
3. Resultado del análisis de riesgo.
4. Plan de acción propuesto.

PAO

Los Planes de Apoyo Operativo son los documentos operativos donde se deben plasmar las medidas concretas a poner en marcha por las Administraciones Públicas en apoyo de los operadores críticos para la mejor protección de las infraestructuras críticas.

3. **Catálogo Nacional de infraestructuras Estratégicas:** Contiene la información relativa a las características específicas de cada una de las infraestructuras existentes en el territorio nacional. Con ánimo de establecer

una buena comunicación entre las partes fue desarrollado el proyecto Hermes, a través de cual los operadores críticos podrán dar de alta, acceder y modificar la información relativa a aquellas infraestructuras críticas que gestionen.

4. **Gestión de incidentes.** En colaboración con el CNPIC, INTECO se convierte en el CERT especializado en la gestión de incidentes a nivel nacional.

4.5 Medidas y amenazas para la Seguridad Nacional

Cada vez hay más peligro de cualquier acto de agresión hacia el país, el gobierno se ha puesto en marcha con medidas para evitar daños severos a la seguridad del País. El gobierno aprobó para el 2017 un boletín de “Estrategias de Seguridad Nacional 2017” donde recopila el estado en que se encuentra el mundo y la situación en España, aparte podemos encontrar las diferentes amenazas y sus consecuencias. También podemos encontrar los objetivos separados por los ámbitos más importantes y las medidas que recurren. Nosotros nos centraremos en la protección de las infraestructuras críticas.

(Imagen 3: Diferentes ámbitos de la seguridad nacional, sacado de documento Informe anual de seguridad nacional)

El objetivo principal en la protección de las infraestructuras criticas es asegurar la correcta provisión de los servicios fundamentales para la sociedad, haciendo más

robusto y resiliente el sistema de IC sobre el que se sustenta. Por ellos el gobierno aplicará las siguientes líneas de acción:

- Avanzar en el cumplimiento de la normativa sobre protección de infraestructuras críticas y en el proceso de planificación escalonada previsto en dicha normativa.
- Mejorar la seguridad integral de las IC a través de todas aquellas actuaciones de planificación, prevención, reacción, mitigación de daño y restitución del servicio que resulten más oportunas.
- Incrementar la capacidad y resiliencia de los sistemas asociados a las infraestructuras críticas, impulsando la implantación de programas de gestión de riesgos siguiendo los acuerdos de prioridades establecidas en el Plan Nacional de Protección de las IC.
- Promover la coordinación en materia de protección de IC, lucha contra el terrorismo y ciberseguridad entre todas las organizaciones responsables.
- Estimular la cooperación público-público y público-privada en el marco del Sistema Nacional de Protección de las infraestructuras críticas, incentivando el intercambio de información con el establecimiento de procedimientos y canales seguros y de confianza.
- Favorecer la innovación en seguridad, equipando progresivamente a las IC de sistemas y componentes de seguridad apostando por la tecnología y el desarrollo I+D+i español.
- Impulsar la colaboración internacional y avanzar en el desarrollo de las estructuras y sistemas de intercambio de información y alerta temprana entre países sobre todo en los miembros de la Unión Europea.

La seguridad de una nación puede verse comprometida por factores medioambientales, sociales, políticos, religiosos, entre otros. Llamamos amenazas a aquellas acciones o eventos que pueden hacer peligrar la seguridad de un país. Vamos analizar aquellas amenazas puede tener como objetivo las IC

- **Conflictos armados:** Estos últimos años ha habido mucha tensión política entre varios países, ya sea EEUU y Rusia o Corea del Norte y la ONU, es por ello que se considera estos como una de las amenazas más significativas para la Seguridad Nacional. Este punto engloba muchas acciones que puede ser objetivo para IC como por ejemplo el espionaje, que hablaremos en otro punto, ataques militares, sabotajes, ciberataques, etc.
- **Terrorismo:** Los actos de terrorismo ha sido un tema muy importante en España por el grupo terrorista ETA y por el atentado del 11 de marzo de 2004. Actualmente el grupo Yihadista es el que más impacto tiene por los múltiples ataques terroristas en Europa. Es por eso que hay que maximizar las defensas contra este grupo para que no ataque a ninguna IC que pueda perjudicar al funcionamiento del país.
- **Espionaje:** El espionaje se ha adaptado muy rápido a las nuevas tecnologías y eso implica estar siempre al día en las nuevas tecnologías para poder detener cualquier acto de espionaje. Si una IC está expuesta al espionaje sería un riesgo para seguridad de todos los ciudadanos y al propio sistema de Seguridad Nacional.

4.6 Resiliencia

Hemos hablado de las amenazas existentes y cómo prevenirlas, del perito en su trabajo, de constatar que se cumple con el reglamente vigente para la seguridad de las IC y las normativas ISO para garantizar la protección, pero ¿Qué pasa si consiguen superar las barreras y atacar con éxito las IC? ¿Tenemos un plan para estos casos? Es aquí cuando hablaremos de la resiliencia.

La resiliencia, según la RAE (edición 23º), es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. Este es un concepto global a la definición de residencia, para este trabajo aclararemos la definición de resiliencia para infraestructura y tecnológica.

- **Resiliencia (infraestructura):** La capacidad que tiene el edificio para resistir una amenaza y recuperarse de sus efectos de la mejor manera posible y eficiente, para recuperar lo antes posibles las funciones básicas que se realizaban en esa infraestructura.
- **Resiliencia (Tecnología):** La capacidad de un sistema de soportar y defenderse antes amenazas y desastres y volver a sus funciones lo antes posible.

La resiliencia se ha tenido que intensificar estos años por los avances tecnológicos de esos últimos años y el aumento de ciberataques y virus, es por ello que hay mucho esfuerzo en cubrir todos los aspectos de la seguridad, pero hay cierta incertidumbre en este tema. Con estos aumentos de ciberataques tenemos que hablar sobre la ciber-resiliencia

La ciber-resiliencia se ha definido partiendo de la definición de resiliencia y restringiendo las posibles fuentes de crisis a eventos tecnológicos y procedentes del ciberespacio, o también se ha definido limitando la dimensión afectada de la empresa, a lo que son sus sistemas de proceso de datos y sus comunicaciones. Dado la complejidad de las entidades y diferentes elementos que las formas: Empleados, suministros, infraestructuras TIC, etc. Es muy difícil trazar la división en lo que suponía resiliencia y ciber-resiliencia, una y otra están íntimamente relacionadas, es más, son un mismo concepto. No se puede crear una infraestructura tecnológica ciber-resiliente si la organización en sí no es resiliente. La organización es un todo, y el departamento TIC no es un ente independiente que puede sobrevivir o pretender ser inmune a los eventos que pueden sacudir a su personal y sus usuarios.

Cuando hablamos de que una entidad será resiliente cuando se enfrente de forma exitosa tanto a los cambios que se desarrollan de forma progresiva, como a los que se desaten de forma violenta. Las alteraciones del entorno pueden ser desde ciberataques hasta catástrofes naturales, y podrían tomar cualquier otra forma: problemas energéticos, de suministros, políticos, financieros, contractuales, etc. Por otro lado, considerar que la única fuente de problemas puede ser un ataque externo es un gran error. El origen de una crisis que afecta de forma traumática a dicho organismo puede ser de origen

interno. Centrar la estrategia en repeler ataques externos, subrayando la palabra ataques, es enfocar el problema de forma errónea. Una crisis interna puede generarse por la influencia de agentes externos o tener carácter mixto. Puede ser el caso de la crisis que se genera debido a una prolongada situación de estrés, condicionada por factores ambientales, que desgasta los recursos propios. En ese caso, los recursos más críticos son fundamentalmente humanos, sensibles a los fenómenos sociales. El personal en riesgo no es solo el equipo clave de toma de decisiones, puede ser parte del personal menos cualificado pero que son parte necesaria de los procesos de soporte de la organización.

Un aspecto importante que también mide el grado de resiliencia de una organización es su capacidad de anticipación a las crisis. Una justificación fácil es que las crisis o los ataques no son previsibles, que es imposible conocer cuándo se van a materializar, pero esto no es cierto. Excepto algunas catástrofes naturales y muy contados ataques, la mayor parte de las crisis de una organización se pueden prever, bien mediante un análisis de las series históricas, bien prestando atención a los sucesos en organizaciones similares, bien llevando a cabo una tarea efectiva de inteligencia o tan solo asumiendo lo que todos los días se lee en los periódicos.

Finalmente, una organización no será igual de resiliente a cualquier tipo de crisis. No es una cualidad que se pueda aplicar de forma homogénea en todas sus actividades o cada una de sus dimensiones. Un organismo puede ser muy resiliente a ataques técnicos, pero no a ataques sociales, o no muy preparada para crisis a corto plazo, pero demasiado rígida para cambios del entorno a largo plazo.

4.6.1 Medidas para alcanzar la ciber-resilencia

Es muy complicado que una entidad este 100% seguro y preparado para cualquier incidente, no obstante, se puede seguir unas medidas para tener un alto índice de protección, existes muchas medidas y medidas muy específicas. Aquí hablaremos de las más genéricas.

- **Conocer la entidad:** El primer paso ante de tomar alguna medida es conocer la entidad, su organización y su entorno. Parece obvio, pero se suele idealizar demasiado la propia entidad y no dar una visión crítica de la organización, aparte tenemos no solo que tener conocimiento de que ocurre dentro de ella, sino también de fuera y como las perciben los demás
- **Adecuada gestión de cambio, riesgo, medida preventivas:** La organización tiene que tener una sólida gestión de cambio, riesgo y medidas preventivas para aumentar la resiliencia. Una organización resiliente es la que incorpora el concepto de cambio como parte de sus principios de su funcionamiento.
- **Factor humano:** Concienciar al personal de la organización es de suma importancia, ya que estadísticamente lo fallos producidos vienen a raíz de un error humano. También es clave el compromiso del personal. Si se abandona el compromiso de la organización con los trabajadores, estos abandonan el compromiso con la organización y se convierte en una

relación de carácter utilitarista a corto plazo y en ambos sentidos. Los resultados son aún peores cuando la falta de fidelización se produce a nivel directivo. Para crear este compromiso mutuo la organización ha de ofrecer una carrera profesional a sus trabajadores, más aún, un plan de vida, una seguridad, un sentimiento de grupo, en algunos casos un ideal, y una proporcionar una serie de valores añadidos que vayan más allá del estímulo económico directo.

- **Incertidumbre:** Según Manuel Sanchez Gomez, “la incertidumbre es un ingrediente que aporta variables imprevisibles, debido a la dificultad de conocer de antemano el total de las amenazas y riesgos a los que se enfrenta la sociedad en cada situación, dificultando con ello la selección de medidas para combatirlas.”. Es difícil anticiparse al evento que puede venir, ya que el abanico de posibilidades es muy amplio. Por ello, se tiene que atacar a aquellos eventos o amenazas que pueden hacer mucho daño o en los que estadísticamente es más probable que pase.
- **Menor dependencia de los interfaces externos:** Hay que tener control del entorno de la entidad. Los interfaces con el exterior son de muchos tipos, pueden abarcar desde aspectos sociales a las redes de suministro eléctrico, pasando por el outsourcing y los servicios en la nube. Una estrategia de ciber-resiliencia ha de estar dirigida a disminuir las dependencias externas. Esto no quiere decir que una organización sea autárquica en su operativa diaria, es imposible imaginar una organización completamente aislada, y el aislamiento no tiene que ser el objetivo de una organización, ya que perdería su sentido. Pero ha de ser capaz de resistir durante un periodo de tiempo tan prolongado como sea posibles cortes en los suministros, en especial en los suministros de energía, y no ha de depender en su operativa de servicios proporcionados a la propia empresa a través de Internet. **(Ejemplos: los hospitales tienen generadores de energía, empresas se crean su propia nube para tener menos dependencia de estos servicios**)
- **Analizar los procesos claves.** Tendrá mejor resiliencia si los procesos continúan operativos en cualquier circunstancia, con un grado de eficacia que tal vez no alcance el cien por cien del rendimiento deseable, pero que sí permita mantener la vida de la organización. Ante una incidencia es necesario distinguir aquellos procesos que son imprescindibles, frente a los que se pueden detener temporalmente, clasificando estos últimos en función del tiempo que pueden estar suspendidos (algunos podrán estar detenidos durante minutos, otros indefinidamente) desarrollando un plan de continuidad de negocio a largo plazo y con una visión amplia. Para ello es necesario identificar cuáles son los recursos claves, y en particular los recursos TIC, que son imprescindibles para mantener el funcionamiento de cada uno de ellos.

5. Normativas e ISO

Para un perito es muy importante estar a la última de nuevas normativas e ISO que están en vigor, ya que una parte de su trabajo será garantizar que tanto empresa o como una infraestructura crítica estén dentro de la norma actual. Por lo tanto, ambos aspectos importantes de mí TFG tiene relación con las normativas y las ISO. Hemos hablado de normativas en apartado más atrás porque era más acorde al ámbito que se encontraba, aquí hablaremos de las normativas más genéricas que a partir de esa se crean las demás o que atañe a ambos, pero antes hablaremos de la **Asociación Española de Normalización y Certificación (AENOR)**

5.1 AENOR

La Asociación Española de Normalización y Certificación (AENOR) se constituyó en 1986, coincidiendo con la incorporación de España a la Comunidad Económica Europea, la apertura de fronteras que suponía era al mismo tiempo una gran oportunidad y un tremendo reto para los productos españoles.

Hasta esta fecha, las labores de normalización eran responsabilidad del Instituto de Racionalización y Normalización (IRANOR). En el primer año se crearon los primeros 24 comités técnicos de normalización, en su mayoría traspaso de las actividades técnicas de IRANOR, y se partió de un cuerpo normativo de 7.810 normas, también heredado de aquel organismo. Un año más tarde, la Asociación Española de Normalización y Certificación asumía la representación de España ante los organismos europeos (CEN, CENELEC y ETSI) e internacionales (ISO e IEC).

La Asociación Española de Normalización, UNE, es el organismo legalmente responsable del desarrollo y difusión de las normas técnicas en España. Las normas indican cómo debe ser un producto o cómo debe funcionar un servicio para que sea seguro y responda a lo que el consumidor espera de él. UNE pone a disposición de todos uno de los catálogos más completos, con más de 31.500 documentos normativos que contienen soluciones eficaces.

5.2 ISO27001

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa, con o sin fines de lucro, privada o pública, pequeña o grande.
La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad, es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la

información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

Una organización necesita identificar y administrar cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas puede ser considerada como un “proceso”. A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos.

A raíz de la importancia de la norma ISO 27001, muchas legislaciones han tomado esta norma como base para confeccionar las diferentes normativas en el campo de la protección de datos personales, protección de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, etc.

6. Tendencias actuales

Los delitos informáticos han tendido a crecer, durante los últimos años, no únicamente en nuestro país, sino también en todo el mundo. Sin duda, son muchas las causas de esta realidad, pero el hecho de que cada vez nuestras vidas confluyan a través del uso de las TIC, es decir, de las redes sociales e Internet, y a una mayor facilidad para acceder a la red por parte de los usuarios, independientemente del lugar en el que se encuentren, facilita y conlleva que los delincuentes desde el anonimato pretendan obtener resultados criminales con éxito.

Para concienciar a los ciudadanos españoles el Ministerio de Interior ha ido lanzando informes sobre Cibercriminalidad para dar a conocer la realidad delictiva que gira en torno a la Cibercriminalidad. Los datos extraídos provienen fundamentalmente del sistema estadístico de criminalidad (SEC), registrados por las Fuerzas y Cuerpos de Seguridad. El estudio correspondiente al año 2015, fija como objeto fundamental, mostrar los datos que envuelven a la Cibercriminalidad desde diferentes perspectivas y ámbitos.

Este informe (Interior, 2015) también señala la parte jurídica. Con las nuevas tecnologías están apareciendo nuevos delitos cibernéticos, se tienen que adaptar e las Leyes Orgánicas 1/2015 y 2/2015 a estas nuevas tendencias, cuya vigencia tuvo lugar a partir del día 01 de julio del año 2014, vino a regular nuevos tipos penales en el ámbito de la Cibercriminalidad.

En resumen, la ciberdelincuencia avanza y evoluciona mediante la aparición de nuevos delitos informáticos y de comportamiento constitutivos de esta clase de ilícitos, que son detectados y conocidos día a día por las Fuerzas y Cuerpos de Seguridad, así igualmente la legislación española, tanto nacional como internacional se va perfeccionando, para evitar, y actuar contra la actividad delictiva en este ámbito. La siguiente imagen nos muestra la cantidad ciberataques que se han producido en España en los 2012-2015, dividido en subcategorías de delitos.

>> 4.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2012	2013	2014	2015
ACCESO E INTERCEPTACIÓN ILÍCITA	1.701	1.805	1.851	2.386
AMENAZAS Y COACCIONES	9.207	9.064	9.559	10.112
CONTRA EL HONOR	1.891	1.963	2.212	2.131
CONTRA PROPIEDAD INDUST./INTELEC.	144	172	183	167
DELITOS SEXUALES	715	768	974	1.233
FALSIFICACIÓN INFORMÁTICA	1.625	1.608	1.874	2.361
FRAUDE INFORMÁTICO	27.231	26.664	32.842	40.864
INTERFERENCIA DATOS Y EN SISTEMA	298	359	440	900
Total HECHOS CONOCIDOS	42.812	42.403	49.935	60.154

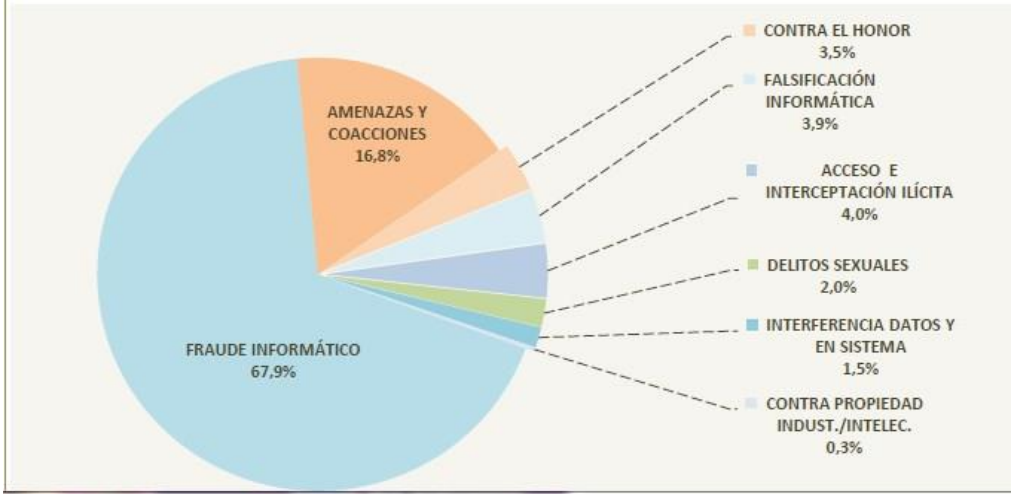


Imagen 4. Evolución de hechos conocidos por categorías delictivas (fuente estudio sobre la Cibercriminalidad en España 2015)

A lo largo de la serie histórica 2012-2015, se aprecia un incremento de la delincuencia comprendida dentro del concepto de Cibercriminalidad. En concreto, durante el año 2015, se ha conocido un total de 60.154 hechos, de los cuales el 67,9% corresponde a fraudes informáticos (estafas) y el 16,8% a amenazas y coacciones. Las diferentes categorías presentan una estabilidad con respecto a los años anteriores, con la excepción de los delitos de falsificación informática, que este año superan en porcentaje a los delitos contra el honor, hecho que no ocurría el pasado año.

Vemos que cada año se incrementa el número de ataques cibernéticos y esto puede afectar también a las Infraestructura Criticas.

>> 3.2. Incidentes gestionados en relación con las infraestructuras críticas

Tipo de incidente	INCIDENTES GESTIONADOS 2014	2015
Acceso no autorizado	2	15
Fraude	6	8
Virus, troyanos, gusanos, spyware	31	75
SPAM	0	0
Denegación de servicio	2	10
Escaneos de red	1	7
Robos de información	9	2
Otros	12	13

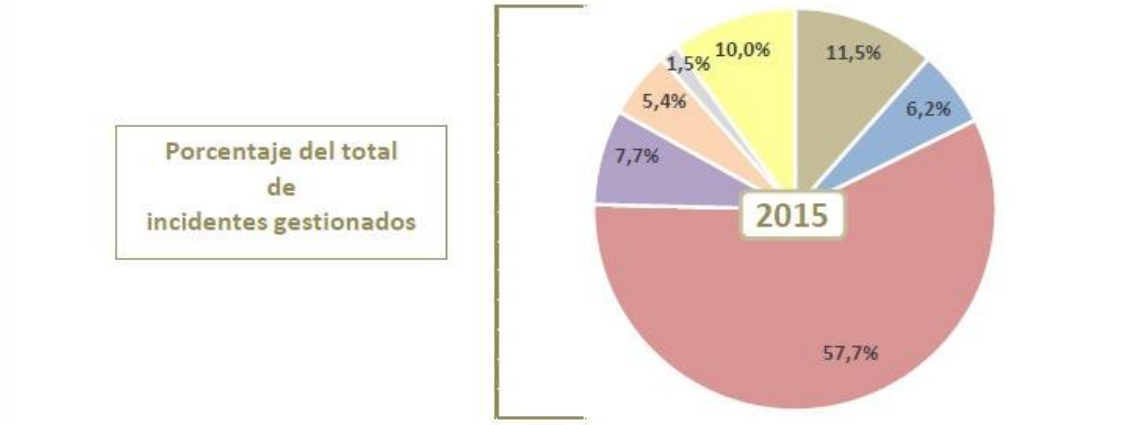


Imagen 5. Incidentes gestionados en relación con las infraestructuras críticas (fuente estudio sobre la Cibercriminalidad en España 2015)

>> 3.3. Incidentes gestionados por comunidad de referencia

Incidentes por público objetivo	INCIDENTES GESTIONADOS 2014	2015
Ciudadanos y empresas	14.715	45.693
Red académica (RedIris)	3.107	4.153
Infraestructuras Críticas (IICC)	63	130

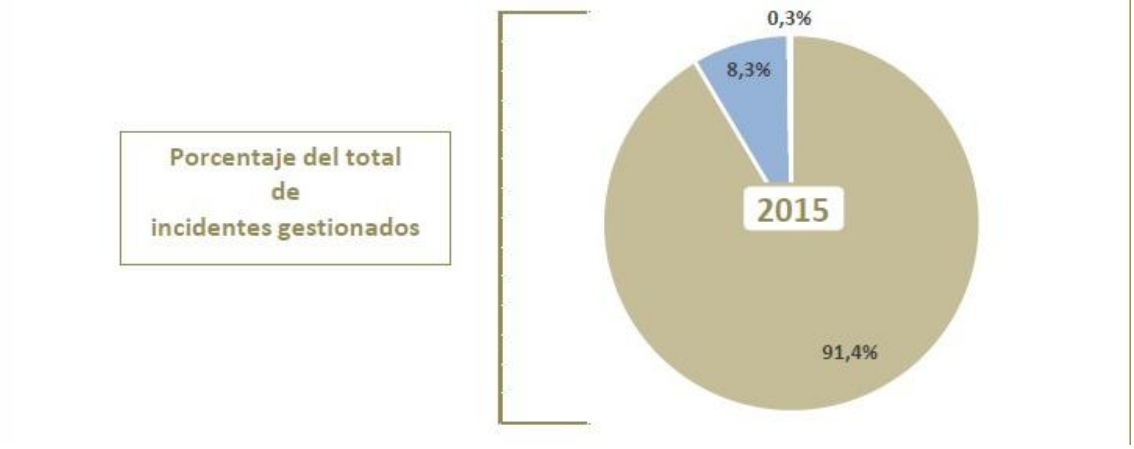


Imagen 6: Incidentes gestionados por comunidad de referencia (fuente estudio sobre la Cibercriminalidad en España 2015)

>> 3.4. Incidentes gestionados por sector estratégico

Sector estratégico	INCIDENTES GESTIONADOS 2014	2015
Energía	34	46
Transporte	14	24
Tegnologías Información y Comunicac. (TIC)	6	17
Sistema tributario y financiero	3	17
Alimentación	0	12
Agua	0	5
Industria nuclear	4	5
Administración	2	1
Espacio	0	0
Industria química	0	0
Instalaciones de Investigación	0	0
Salud	0	0
Todos los sectores afectados	0	3

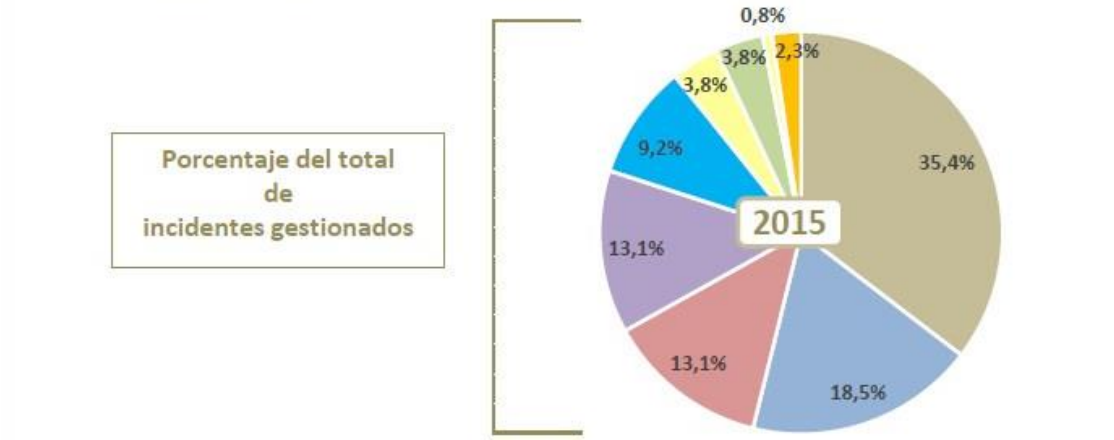


Imagen 7. Incidentes gestionados por sector estratégico (fuente estudio sobre la Cibercriminalidad en España 2015)

Como hemos observado en las últimas imágenes, las infraestructuras críticas también sufren ataques cibernéticos, aunque tengan unas cifras muy pequeñas comparadas a los ataques que reciben los ciudadanos y empresas, no hay que menospreciar esos números. Un ataque a una IC puede causar graves daño tantos a los ciudadanos (ataques a las centrales eléctricas, agua, salud etc.) o a las administraciones españolas (sistemas Tributarios y Financieros, Administración, Investigación etc.). Por ello, se tiene que dar todos los recursos posibles para proteger las IC y que los incidentes ocasionados por ciberataques tiendan a 0.

7. Casos prácticos y hechos reales

Hemos hablado del perito, las infraestructuras críticas y su importancia y las tendencias actuales sobre los ataques informáticos. A continuación, se explicará con dos ejemplos cómo actúa un perito, en prevención y actuación, para mayor entendimiento del trabajo. No hay que olvidar que la finalidad de este TFG es tener una herramienta metodológica para los peritos en infraestructuras críticas y tener más documentación al respecto.

Por otra parte, mostraremos dos casos reales sobre ataques a IC que han tenido éxito y han tenido consecuencias para el país afectado. Adelantamos que hablaremos sobre el caso del primer ciberataque documentado en Estonia en 2007 y el otro caso será el reciente ataque global que sufrió a mano de Ramsonware **WannaCry.**

7.1 Caso practico

7.1.1Un perito en una Infraestructura Critica. Prevención

El perfil del perito informático en la PIC puede ser variado: iría desde hacer una auditoria a la seguridad de las instalaciones (redes, bases de datos, accesos del personal…) hasta realizar un ataque a la instalación para evaluar las vulnerabilidades que se encuentren y resolverlas, como si fuera un hacker Sombrero Blanco[1] . Normalmente estos peritos informáticos trabajan para el estado español o son contratados por el jefe de la infraestructura. Lo primero será tener claro los siguientes aspectos (Joaquin, 2011).

- El objetivo
- El ámbito
- La profundidad
- Evaluar la situación actual

La asignación del perito está relacionada con el conocimiento del perito en cuestión al objetivo. Como el perito trabaja para estado, sus honorarios y la tasación de costas ya están estipulados, pero no la provisión de fondo.

La provisión de fondo es una cantidad avanzada, solicitada antes de la práctica de la prueba, que normalmente se aproxima al importe de la misma, sin perjuicio de la ulterior liquidación. Según **el Art. 342** de la LEC regula la Provisión de fondos al perito, disponiendo en su apartado 3 que: (Juan Vicente)

[1]El término **Sombrero Blanco** en Internet se refiere a un hacker (o pirata informático) ético, o un experto de seguridad informática, quién se especializa en pruebas de penetración y en otras metodologías para asegurar la seguridad de los sistemas informáticos de una organización

"El perito designado podrá solicitar, en los tres días siguientes a su normalmente, la provisión de fondos que considere necesaria, que será a cuenta de la liquidación final. El secretario judicial, mediante decreto, decidirá sobre la provisión solicitada y ordenará a la parte o partes que hubiesen propuesto la prueba pericial y no tuviese derecho a la asistencia jurídica gratuita, que procedan a abonar la cantidad fijada en la Cuenta de Depósitos y Consignaciones del Tribunal, en el plazo de cinco días."

Transcurrido dicho plazo, si no se hubiere depositado la cantidad establecida, el perito quedara eximido de emitir el dictamen, sin que pueda procederse a una nueva designación.

Al calcular la cantidad hay que tener en cuenta:

- La complejidad de trabajo encomendado
- Su duración
- Gastos para cubrir desplazamientos y estancias
- Ensayos de laboratorios y otros e intervención de terceros

Una vez establecido la provisión de cobro, y cobrado, estamos listos para empezar.

Para que la **lección o documento** sea lo más clara posible usaremos un ejemplo para un mejor entendimiento. Recientemente ha salido una actualización de la norma UNE**-EN ISO/IEC 27001 mayo 2017,** así que nuestro perito va seguir la norma y comprobar que la Infraestructura Critica que le haya sido asignada, cumple la nueva normativa. Para más información sobre la nueva normativa **UNE-EN ISO/IEC 27001** en el **Anexo 3**

En este trabajo nos vamos a fijar en el apartado **A11 Seguridad física y entorno** para ver cómo trabaja un perito.

Cuando lleguemos al complejo lo primero será recopilar información, debemos ver las instalaciones para ver su estado y su funcionamiento normal. Nuestro objetivo será certificar si la infraestructura es robusta con acceso físico no autorizado, daños e interferencia a la información de la organización y evita la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización. El perito ira apartado por apartado para comprobar el buen cumplimiento de la nueva normativa. Empezaremos la inspección con el apartado **A.11.1 Áreas seguras** y su subapartado:

11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos
11.1.4 Protección contra las amenazas externas y ambientales
11.1.5 El trabajo en áreas seguras
11.1.6 Áreas de carga y descarga

Empezaremos con la **11.1.11,** hay que comprobar que utilizan perímetros de seguridad para proteger las áreas que contienen información sensible. Para ello iremos a la zona donde guardan la información sensible y analizaremos la

seguridad: si solo tienen acceso personal autorizado, tienen cámaras de seguridad, si utilizan un sensor biométrico… Si encontramos evidencias de que hay una seguridad robusta para la protección de la información sensible daremos como bueno este apartado.

La **11.1.2** consiste en controlar los accesos a las áreas seguras para que solo el personal autorizado pueda acceder a esas zonas, ya sea con tarjetas de acceso, sensores biométricos o un guarda protección la zona.

La siguiente es las **11.1.3** tenemos que verificar que se aplica la seguridad física en las oficinas, despachos y recursos.

El siguiente apartado es el **11.1.4**, en el cual nos aseguraremos que existe protección física para desastres naturales, como puede ser cajas fuerte contra incendios y terremotos y ataques provocados por el hombre, como puede ser tener todo el cabreado oculto para no tropezarse.

El punto **11.1.5** tendremos que comprobar que se sigue unos protocolos y procedimientos para trabajar dentro de las áreas seguras.

Por último, la **11.1.6**, en el caso que la infraestructura tenga una zona carga y descarga tendremos que demostrar que existe seguridad en esas zonas para que no accedan persona no autoriza, ya sea contratando un vigilante hasta cameras de seguridad.

Para más información sobre las medidas de seguridad, en el **Anexo 1**

Si en nuestra revisión hemos dado el visto bueno (vamos imaginar que ha cumplido todo apartado) podemos decir con toda la certeza que cumple que con los requisitos de **áreas seguras.** El siguiente paso será hacer lo mismo con el siguiente apartado de **1.2 Seguridad de los equipos** y si concluimos que este apartado también lo cumple con la normativa, podemos garantizar que esta infraestructura cumple con el apartado **A11 de seguridad física y del entorno.**

Una buena forma de recopilar información del buen uso de las instalaciones y su uso correcto, es haciendo entrevistas a los empleados para que nos cuente como trabajan ellos, si respetan los protocolos a seguir, si hacen suficientes copias de seguridad, no acceden a sitios web potencialmente peligrosos, etc. Se puede dar que los empleados mientan, ya que estamos en una inspección y eso puede dar algo de nervios y pensar que estamos buscando un culpable, en estos casos hay que concienciar a la gente que estamos aquí para saber cómo se trabajar y no buscamos culpables, pero en ocasiones eso no servirá. Así que la entrevista será un refuerzo para realizar el dictamen y tener más pruebas. Está claro que se puede dar caso que en que encontremos evidencia que no se relaciona a que nos cuenta un empleado. Ejemplo: Un empleado nos cuenta que las llaves de la caja fuerte se guardan en un lugar seguro, pero en tu inspección te has encontrado esas llaves colgadas en un colgador de llaves. Ante esta situación tienes que presentar las evidencias que has visto porque es la situación con la que te has encontrado.

Con la información recopilada comenzaremos a redactar el dictamen.

Un dictamen es un documento sobre una determinada materia donde el perito pondrá por escrito las evidencias encontradas, tiene que cubrir el objetivo y dar su opinión. El dictamen tiene que ser claro, conciso, fundamentado, justificado.

Hay que matizar que no es lo mismo un informe que un dictamen. Un **informe pericial** es totalmente aséptico. En el mismo, el perito se limita a exponer y a argumentar, pero sin dar una valoración profesional ni una opinión al respecto. El **dictamen pericial** incluye, además, la opinión del experto que ha realizado el informe. Puede incluir también recomendaciones sobre acciones a tomar para mejorar los posibles problemas detectados. Para elaborar el informe pericial utilizaremos la normativa **UNE 197001** explicado anterior mente en el apartado de informe pericial

Cuando terminamos de escribir el dictamen podemos incluir alguna opinión sobre lo que hemos visto durante nuestra inspección o algunos aspectos que queramos resaltar. Este dictamen será presentado para la persona que te lo ha encargado, ya sea el jefe de la infraestructura como un abogado.

Como hemos visto en ningún momento hemos incluido una solución a los problemas que hemos encontrado porque el trabajo de un perito es dar parte de lo que se ha encontrado y del funcionamiento que ha visto y de su juicio redactar el dictamen. Este trabajo se le puede dar a un consultor, ya que él se encargará de dar el abanico de posibilidades que tiene un problema concreto. En ningún momento cruzaremos esa línea que separa entre el trabajo del perito y del consultor.

Como hemos hablado a lo largo de este punto siempre daremos una visión de lo que hemos encontrado, que partes se cumple y que parte las incumplen. Nuestro dictamen puede ser da gran ayuda al consultor ya que permitirá hacer su trabajo de una forma más efectiva y rápida.

7.1.2 Un perito en una Infraestructura Critica. Actuación

Hemos explicado con un ejemplo de trabajo de un perito revisando la nueva normativa **UNE-EN ISO/IEC 27001 a** una IC para comprobar si cumple con la nueva normativa, ese ejemplo sería como una **prevención**; el perito comprueba el estado de la IC para evitar futuras amenazas. Pero a veces con toda la prevención, la seguridad y el anticiparse a los acontecimientos, la amenaza se manifiesta y rompe toda la seguridad haciendo daño (acto terrorismo) o accede a la base de datos de la infraestructura (Ciberataque) en cualquier cosa hay que saber que ha pasado y como han logrado llegar, y aquí entra el perito.

Como ha ocurrido con el anterior ejemplo vamos a suponer que nos llama el estado para que hagamos una peritación a una IC que ha sido atacada y han conseguido acceder a las bases de datos de la entidad. Este caso es una

actuación donde ha sucedido algo y debemos de buscar evidencias de como lo han hecho. Vamos a suponer que han atacado a un hospital.

Lo primero, como en el anterior caso, negociaremos la provisión de cobro, y cobraremos y estaremos listos para empezar.

Cuando lleguemos al hospital tenemos que tener en mente que vamos a ser como detective y resolver las típicas preguntas:

- Qué ha pasado.
- Quién lo ha hecho.
- Cómo lo ha hecho.
- Desde dónde lo han hecho.
- Cuándo ha sucedido.

Con esta idea empezamos preguntar el **"Qué"** ¿Qué ha pasado? ¿Qué ha ocurrido? Se nos confirmará que han accedido a la base de datos del hospital, en este momento tenemos que averiguar la gravedad del ataque porque es diferente que haya accedido a la información de los pacientes y médicos, que a las listas de turnos de guardias. Lo mejor en estos casos es preguntar al informático que lleva la base datos y preguntarle si aparte de acceso a esa información previa, han accedido a más sitio, en cualquier caso, nuestra labor es buscar evidencias de que haya accedido a más sitios: Código de software, sistema de seguridad, ordenadores de los médicos etc. Por otra parte, se descubrimos que hay parte de la base de datos que esta corrompido o borrado, en este punto entraría el apartado de resiliencia del hospital. También tenemos que estar anotando la escala de daño que ha sufrido el hospital en el ataque. La siguiente tabla nos ayudara a conocer el nivel de impacto que ha sufrido la entidad en los diferentes aspectos.

Nivel de impacto	Descripción
I0 – IRRELEVANTE	No hay impacto apreciable sobre el sistema. No hay daños reputacionales apreciables.
I1 – BAJO	La categoría más alta de los sistemas de información afectados es BÁSICA. El ciberincidente precisa para resolverse menos de 1 JP2. Daños reputacionales puntuales, sin eco mediático.
I2 – MEDIO	La categoría más alta de los sistemas de información afectados es MEDIA. Afecta a más de 10 equipos con información cuya máxima categoría es BÁSICA. El ciberincidente precisa para resolverse entre 1 y 10 JP. Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
I3 – ALTO	La categoría más alta de los sistemas de información afectados es ALTA. Afecta a más de 50 equipos con información cuya máxima categoría es BÁSICA.

	Afecta a más de 10 equipos con información cuya máxima categoría es MEDIA. El ciberincidente precisa para resolverse entre 10 y 20 JP. Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
I4 – MUY ALTO	Afecta a sistemas clasificados RESERVADO. Afecta a más de 100 equipos con información cuya máxima categoría es BÁSICA. Afecta a más de 50 equipos con información cuya máxima categoría es MEDIA. Afecta a más de 10 equipos con información cuya máxima categoría es ALTA. El ciberincidente precisa para resolverse entre 20 y 50 JP. Daños reputacionales a la imagen del país (marca España). Afecta apreciablemente a actividades oficiales o misiones en el extranjero. Afecta apreciablemente a una infraestructura crítica.
I5 - CRÍTICO	Afecta a sistemas clasificados SECRETO. Afecta a más de 100 equipos con información cuya máxima categoría es MEDIA. Afecta a más de 50 equipos con información cuya máxima categoría es ALTA. Afecta a más de 10 equipos con información clasificada RESERVADO. El ciberincidente precisa para resolverse más de 50 JP. Afecta apreciablemente a la seguridad nacional. Afecta gravemente a una infraestructura crítica.

Tabla 1: Nivel de impacto de un incidente, la tabla fue inspirada en el documento (españa, 2017)

Una vez que aclarado el apartado de **"Qué"** tenemos que preguntarnos el **"Cómo"** ¿Cómo lo ha hecho? ¿Vía Online o física? En este punto se puede dividir el enfoque de la peritación, si descubrimos evidencias de que ha sido vía online, rompiendo los cortafuegos y los protocolos de seguridad o de lo contrario alguien ha accedido a la sala de los servidores y ha accedido por ahí, otra opción es que esa persona ha usurpado la identidad de cualquier personal que pueda acceder a la habitación. Como podemos observar dependiendo de lo que descubramos tenemos dos vías de investigación, para una mejor compresión del trabajo hablaremos de ambas vías

Si han accedido vía online tenemos que averiguar si se infiltro por alguna vulnerabilidad que esta al descubierto o por el contrario rompió todas las protecciones. Un buen método seria meterte en el papel del atacante e intentar romper las barreras de seguridad o colarte en el sistema buscando vulnerabilidad y recorrer el mismo camino que hizo. Tenemos que buscar

indicios de si en los días anterior el servicio estuvo bajo ataque y ver lo que estaba haciendo, así podemos teorizar que el atacante estaba probando nuestra seguridad y encontró un punto débil por dónde atacar. Si encontramos un punto débil en la seguridad tenemos que investigar de porque hay una vulnerabilidad e informar. La otra opción es que hayan accedido a la sala de servidores y haber accedido desde allí, entonces tenemos que analizar la seguridad que tienen para entrar a la sala de ordenadores y ver sus medidas de seguridad: Si hay cameras de vigilancia, hay un escáner dactilar para acceder a la sala, hay un guardia vigilando etc.… También tenemos que analizar el registro de entrada de personal y comprobar por entrevistas o con cámaras de seguridad que confirman que ellos mismo entraron a la sala y no un extraño con su acreditación. Esto solo descarta de gente externa al personal del hospital, si ha sido la propia gente del hospital que entraron en la sala de ordenador para provocar ese ataque, la cosa ya se complica. Hay que dejar claro que nuestro cometido es buscar lo que ha pasado y no buscar al culpable exclusivamente.

A continuación, será preguntarnos el **“Cuándo”** ¿Cuándo ocurrió el ataque? ¿Fue reciente o el ataque es anterior y se manifestó recientemente? Nuestra tarea será aclarar estas preguntas para un mejor entendimiento de lo sucedido. Habrá que buscar evidencias de que el sistema de base de datos funcionaba algo diferente, para ello tendremos que entrevistar a los empleados del hospital y mirar las copias de seguridad de las bases de datos para ver alguna anomalía entre las diferentes versiones de la base de datos. Si encontramos alguna prueba de que la base de datos fue comprometida por algún agente externo: Virus, Script, persona no autorizada... etc. y se manifestó hace pocos días entonces tenemos que averiguar qué sucedió entre un periodo de días e investigar. Por otro lado, si no encontramos ninguna prueba de anomalía en la investigación podemos asegurarnos que la base de datos estaba bien y solo fue comprometida en el día del ataque.

Lo siguiente seria preguntarnos el **“Quién”** ¿Quién lo hizo? ¿Algún empleado despedido, algún espionaje de alguna empresa o país, terrorismo, algún hacker que solo quería ver hasta dónde podía llegar? Las posibilidades son muy amplias y algunas opciones, como el terrorismo, se nos escapa de nuestras responsabilidades y entrarían otros factores de seguridad nacional. Para encontrar al culpable nos ayudará saber el **“Dónde”** ¿Desde dónde nos atacó? En el caso de que haya sido por acceder a la sala de servidores esta parte ya la sabríamos; en cualquier otro caso tendremos que averiguar el **“Dónde”**. Para averiguar desde donde nos atacó tendremos que rastrear los registros y ver desde donde procede el ataque. Se puede dar el caso que el atacante uso una aplicación para ocultar su IP como el programa Tor, entonces estaremos ante un obstáculo difícil, ya que no hay forma de rastrear cualquier evidencia que deje el atacante.

Durante todos estos procesos de investigación iremos recopilando evidencias que nos pueda servir para el dictamen, sin romper la cadena de custodia que hemos hablado anteriormente. Es importante que el perito anote y fotografié todo pasos que vaya haciendo y tener un registro de todas las acciones que ha

realizado y cuales falta por realizar. En el apartado de informática forense comentamos, con unos ejemplos, las acciones que suele realizar, pero claro hay acciones que no se puede hacer tan fácilmente como por ejemplo si el servidor ha sufrido el ataque y debemos detener la ejecución para comprobar el arranque del servidor será lento el realizarlo porque detendría todo el funcionamiento del hospital y eso no bueno. Por ellos el formulario es una orientación y un ayuda al perito que con su sabiduría sabrá adaptar y atacar a los objetivos más rápidamente.

Una vez que hayamos concluido todos nuestros análisis, procederemos a redactar el informe con toda la información y evidencias que hemos encontrado y en el mejor de los casos al autor del ataque. Aquí dejamos el camino ya establecido para otras personas, como consultores, analistas o auditores, eviten la parte de análisis y se concentre en asegurarse que las vulnerabilidades sean cerradas e intentar prevenir futuros ataques. Para elaborar el informe usaremos la normativa **UNE 197001**.

Durante este caso de ejemplo a modo de ver a un perito en un caso de ataque, hemos visto al perito como tiene que buscar evidencia y recopilar información sobre el evento ocurrido, no hemos hablado de las técnicas que usa el perito para recopilar, pues este trabajo se extendería demasiado y se perdería el propósito de este trabajo, que sea una herramienta metodológica.

7.2 Caso reales

7.2.1 El ciber-ataque a Estonia 2007

En el 2007 Estonia sufrió ataques cibernéticos a gran escala paralizando a todo el país durante 3 semanas. Antes de hablar lo sucedido vamos explicar brevemente como estaba Estonia a nivel tecnológico. Estonia fue el primer país en votar a través de internet, el 97% de toda su actividad bancaria se realiza por internet, la amplia mayoría de entidades gubernamentales era accesibles por vía online. Es ese momento pocos países tenían un despliegue tecnológico tan amplio como lo tenía Estonia. Nos podemos hacer una idea de que casi todo se podía acceder por internet.

Ahora que conocemos el estado que se encontraba Estonia, narraremos el desencadenante del ciberataque. En 15 de abril el gobierno de Estonia decidió remover el monumento del Soldado de Bronce en Tallin que homenajeaba a los soviéticos caído durante la Segunda Guerra Mundial cuando liberaron Estonia de los Nazis, parte de los soviéticos se quedaron a Estonia a vivir y convivieron juntos tanto estonios y soviéticos. Los rusos estaban en contra de la retirada del monumento y hubo muchas revueltas. El primer ciberataque empezó el 26 abril a las 22:00 cuando el monumento había sido recolocado a un cementerio militar, en la mañana del 27 de abril los estonios notaron algo raro pasaba, las paginas gubernamentales estaban colapsados y el acceso a la banca estaba bloqueado, las páginas de noticias estaban caídas. Durante esa semana los ataques crecían exponencialmente, de los 1000 paquetes por segundo, a los 4 millones de paquetes por segundo que se registró la segunda semana del 2 de mayo, bloqueando todos los medios de comunicación, estaban aislados. El 9

de mayo tumbaron todos los sistemas bancarios y los cajeros dejaron de funcionar. Durante tres semanas Estonia sufrió unos de los peores ciberataques que se haya documentado hasta la fecha.

Un año después, en 2008, la OTAN decidió crear en Tallin el Centro de Excelencia para la ciberdefensa, un proyecto en el que participa España junto a otros seis países para diseñar estrategias de defensa contra ataques por Internet. En el centro trabajan dos españoles, uno militar y otro civil, y funciona con presupuesto de Defensa de los países participantes. Los ataques quedaron grabados y documentados y sirvieron para probar la importancia de la ciberseguridad.

7.2.2 Ataque Global: Ramsonware WannaCry

El 12 de mayo de 2017 España fue atacada por un ciberataque a varias empresas importante: Telefónica, Gas Natural, Iberdrola etc. Este ataque sorpresa obligó a esas empresas a apagar los ordenadores para evitar más contagios, en Telefónica, en torno a un 85% de los ordenadores de la compañía han sido afectados por el gusano informático.

Aparte de España más países sufrieron ese mismo ataque y se propagó a grandes empresas y ha Infraestructura Criticas. En Inglaterra el ciberataque afectó a los ordenadores de 16 hospitales y centro de salud. El ataque ha obligado a apagar todos los sistemas informáticos en diversos hospitales y los médicos han tenido que utilizar lápiz y papel, según testimonios recogidos por la BBC. Varios hospitales han tenido que cancelar citas y han pedido a los pacientes que eviten acudir salvo en casos de verdadera urgencia.

En Francia, Renault tuvo que suspender la producción de varias plantas al estar los ordenadores infectados. En Alemania el ciberataque afectó el sistema informático de la compañía de trenes alemana, Deutsche Bahn (DB); el ataque provocó alteraciones técnicas en los paneles de información digitalizada en estaciones y otros sistemas de aviso al pasajero, pero no derivó en "restricciones en el tráfico ferroviario". Y en Rusia fue el país donde más ordenadores fueron infectados; el Ministerio de Interior y entidades financieras fueron infectados por el virus, el principal banco de Rusia Sberbank fue uno de muchos.

Con los últimos acontecimientos cada vez los ciberataques van más dirigido a grandes empresas e infraestructura críticas e intentan hacer el mayor daño posible. Por ello, tenemos que estar protegidos y estar siempre alertar para cualquier incidente. Un ejemplo de lo que podía pasar si un ataque tuviera éxito a una infraestructura critica seria lo que le sucedió en Ucrania. El 23 de diciembre de 2015 un ataque informático provocó un corte de suministro eléctrico masivo, dejando a 600.000 hogares de la región de Ivano-Frankivsk, al sureste de Ucrania, sin corriente eléctrica en pleno invierno.

El martes 25 de junio de 2017 un nuevo virus ha atacado a empresas, instituciones y bancos de varios países como: Ucrania, Rusia, Reino Unido e

India. En Ucrania fue el país más afectado de ese ciberataque, el Banco Central fue atacado dejando sin servicio, también en la capital de Ucrania, Kiev, el ataque llego a los metros de Kiev y al gobierno de Ucrania dejando a los ministros sin poder ejercer su labor. El aeropuerto más grande de Ucrania, el de Boryspil, también han caído. La web oficial del aeropuerto y la pantalla con los horarios de los vuelos no funcionaban dejando el aeropuerto sin servicio a los clientes.

Una noticia reciente de 24 de mayo del 2018 nos informa que una IC de Alemania fue objetivo de un ciberataque por parte de agente del extranjero, su objetivo era implantar un malware para preparar un ataque de sabotaje y perpetrarlo algún día cuando se suscite un conflicto político.

8. Conclusiones

Durante todo este trabajo hemos abarcado muchos aspectos del perito informático para tener una imagen apropiada de esta profesión y que salida puede tener un perito. También otros aspectos como que cualidades son importantes para un perito. No obstante, la documentación que se puede encontrar es escasa, la gran mayoría de libros son del 1900-2000 aproximado, así que parte de esa información, en gran parte todo relacionado a las tecnologías y como tratar, está obsoleta y las que son recientes no están abiertas para cualquier persona. Estos contratiempos se resolvieron gracias a mi tutor, ya que es un perito profesional, es la mejor forma de saber con certeza como trabaja un perito.

Otra parte importante de este TFG es Seguridad Nacional, era el caso contrario a la documentación del perito, había en abundancia. La gran mayoría venia del gobierno y de los ministerios, más fiable no puede ser, ya que son directrices que se tiene que seguir el buen cumplimiento de la normativa y evitar amenazas posibles. Ahora bien, el que haya documentación ha sido una odisea muchas veces, el tener tanta información era abrumadora y muchas ocasiones había que sintetizar los documentos para plasmarlo en el trabajo. Había aspectos que se nombraban, pero se explicaba de una forma muy genérica, como por ejemplo la resiliencia. La resiliencia fue difícil de encontrar contenido que me sirviera para este TFG, si ser demasiado ambiguo. Otro aspecto de la resiliencia era que no te contaba que hacían para devolver una entidad a su funcionamiento, me temo que esa información es clasificada.

Ha sido una buena experiencia el combinar el peritaje, tema que me agrada y me gustaría profundizar más en ese mundillo, y la parte de Infraestructuras Críticas que desconocía su procedencia y las medidas de seguridad que lleva. Durante el desarrollo del trabajo se actualizo la norma española **UNE-EN ISO/IEC 27001** y aprovechamos para dar un nuevo enfoque al trabajo dándole un apartado más práctico para un mejor entendimiento.

9. Referencia

Alvin A. Arens, Randal J Elder, Mark S. Beasley,Prentice Hall. (2007). *Auditoría un enfoque integral.*

Bruno, T. (12 de 5 de 2017). *El mundo*. Recuperado el 18 de 6 de 2017, de http://www.elmundo.es/tecnologia/2017/05/12/59158a8ce5fdea194f8b4616.html

Carrasco, L. d. (2015). *CIBER-RESILIENCIA.* IEEE.

Consejo de europa. (2001). *Convenio sobre ciberdelicuencia.*

Daniel, L. a. (2012). *Digital Forensics for Legal Professionals.* Elsevier.

Detica Limited. (2011). *The Cost of Cybercrime.* Cabinet Office., Office of Cyber Security and Information Assurance, Guildford. Recuperado el 14 de Enero de 2014, de www.baesystemsdetica.com/resources/the-cost-of-cyber-crime/

EC. (27 de 6 de 2017). *El confidencial.* Recuperado el 31 de 6 de 2017, de http://www.elconfidencial.com/tecnologia/2017-06-27/ucrania-ransomware-ataque-gobierno-banco-nacional_1405916/

Emilio, d. P. (2001). *Peritajes Informáticos.* IEE.

españa, G. d. (2017). *INFORME NACIONAL DEL ESTADO DE SEGURIDAD.* Centro Criptológico Nacional.

Félix, P. (28 de 5 de 2017). *El País*. Recuperado el 20 de 6 de 2017, de https://elpais.com/tecnologia/2017/05/18/actualidad/1495108825_274656.html

Forensic, C. (2015). *Computer Forensic.* Recuperado el 23 de 6 de 2017, de http://www.delitosinformaticos.info/peritaje_informatico/estadisticas.html

Gálvez, J. J. (29 de 5 de 2017). *El País*. Recuperado el 20 de 6 de 2017, de https://politica.elpais.com/politica/2017/05/24/actualidad/1495619175_136537.html

Garzón Castrillón, M. A. (2005). *El desarrollo organizacional y el cambio planeado.* Universidad del Rosario.

Gobierno de España. (2013). *Estrategia de Seguridad Nacional.* Madrid.

GrupoS2. (2011). *Protección de Infraestructuras Críticas.* S2 Grupo.

Guimón, P. (12 de 5 de 2017). *El País*. Recuperado el 22 de 6 de 2017, de https://elpais.com/tecnologia/2017/05/12/actualidad/1494602389_458942.html

Guimón, P. (12 de Mayo de 2017). Un ciberataque a Reino Unido. *Un ciberataque paraliza 16 hospitales de Reino Unido y les exige dinero*, pág. 1.

Interior, M. d. (2015). *ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA.*

Joaquin, A. (2011). *Peritaje Informática. Escenario, conceptos y técnicas básicas.* Janguas.

Juan Vicente, O. G. (s.f.). Curso básico de periciales informáticas. Marco Legal y normativo. Autoeditado.

Luis Muñoz López, P. A. (2015). *CARACTERIZACIÓN DEL SUBSECTOR Y EL MERCADO DE LA CIBERSEGURIDAD.* ONTSI.

Michael Noblett, A. F. (2000). *Computer Forensics:Tools & Methodology.* IATAC.

Ministerio de Defensa. (2018). *Resiliencia: del individuo al Estado yy del Estado al individuo.* IEEE.

Nacional, C. C. (2017). *INFORME NACIONAL DEL ESTADO DE SEGURIDAD DE LOS SISTEMAS TIC.*

ONTSI. (2017). *Estudio sobre la Ciberseguridad y Confianza en los hogares españoles.* ONTSI.

Ribeiro Soriano, D. (1998). *Asesoramiento en dirección de empresas: la consultoría.* Díaz de Santos.

Sahuquillo, M. R. (28 de 6 de 2017). *El País.* Recuperado el 31 de 6 de 2017, de https://internacional.elpais.com/internacional/2017/06/27/actualidad/1498568187_011218.html

tapia, P. n. (2009). *Tasacion y peritaciones judiciales.* Euroinnova editorial .

vacca, J. R. (2005). *Computer Forensics:Computer Crime Scene Investigation.* CHARLES RIVER MEDIA, INC.

Valles Romero, J. A. (2008). *Consultoria en la Logística y Transporte.* Avyasa Editores. Recuperado el 14 de 6 de 2017, de http://www.cnpic.es/

9.1 Glosario

- **Perito:** Persona hábil o experimentada en una determinada materia
- **Informática forense:** Parte de la ciencia de la forense que se encarga de adquirir, analizar, preservar y presentar datos en el ámbito electrónico.
- **Evidencias:** Prueba determinante para un proceso o para un tribunal
- **Cadena de custodia:** Metodología para controlar los materiales, relacionado por un delito, para evitar alteraciones, sustituciones, contaminaciones o destrucciones.
- **Dictamen:** Opinión o juicio que una persona experta se forma y emite sobre una cosa.
- **Consultor:** Persona experta que asesora los problemas de una entidad.
- **Auditor:** Persona experta que revisa y analiza una entidad.
- **Infraestructura Crítica:** Son aquellas infraestructuras que desempeñan una función esencial para el correcto funcionamiento de un país.
- **Resiliencia:** Capacidad que tiene una entidad para volver a su estado original

9.2 Índice de Imagen

9.3 Índice de tabla

9.4 ANEXO 1

Medidas de seguridad

Son programas o acciones utilizadas por el usuario para proteger el ordenador y los datos que se encuentre en este. Estas herramientas y acciones pueden ser realizadas con la intervención directa del usuario (automatizables y no automatizables) y pueden ser también medidas anteriores o posteriores a que ocurra la incidencia de seguridad (proactivas, reactivas o ambas)

Medidas automatizables: Son aquellas medidas de carácter pasivo que no requieren de ninguna acción por parte del usuario, o cuya configuración permite una puesta en marcha automática.

Medidas no automatizables: Son aquellas medidas del carácter activo que, si requiere una actuación especifica por parte del usuario para su correcto funcionamiento.

Medidas proactivas: Son aquellas medidas utilizadas para prevenir y evitar las incidencias de seguridad y minimizar las posibles amenazas desconocidas y conocidas.

Medidas reactivas: Son las medidas que se utilizan para subsanar una incidencia de seguridad, es decir, eliminar amenazas conocidas o incidencias ocurridas.

A continuación, mostraremos una tabla de contenidos donde se puede ver los algunos ejemplos de medidas vistas recientemente y su tasa de uso de estas medidas:

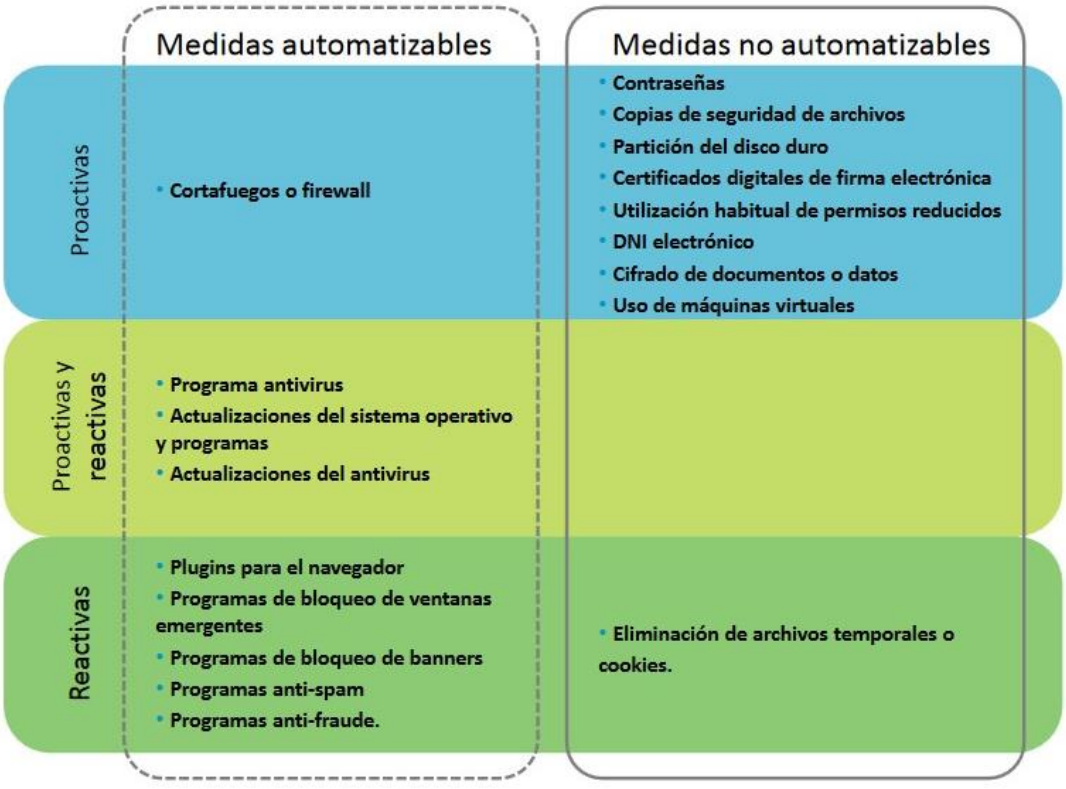


Imagen 8. Clasificación de las medidas de seguridad

Medidas de seguridad automatizables

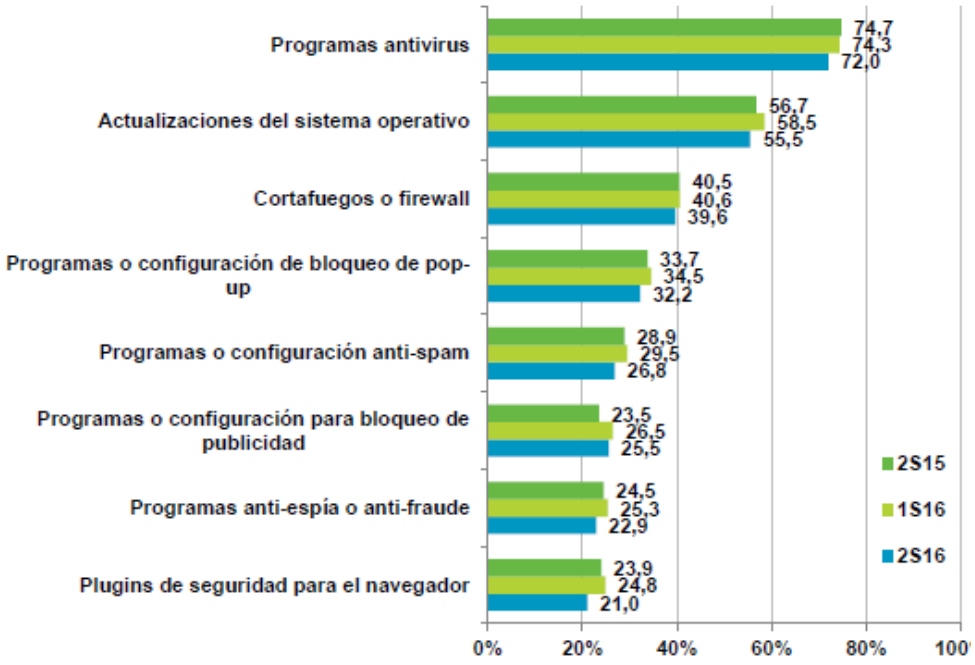


Imagen 9. Porcentaje de uso de medidas de seguridad automatizables

Medidas de seguridad no automatizables o activas

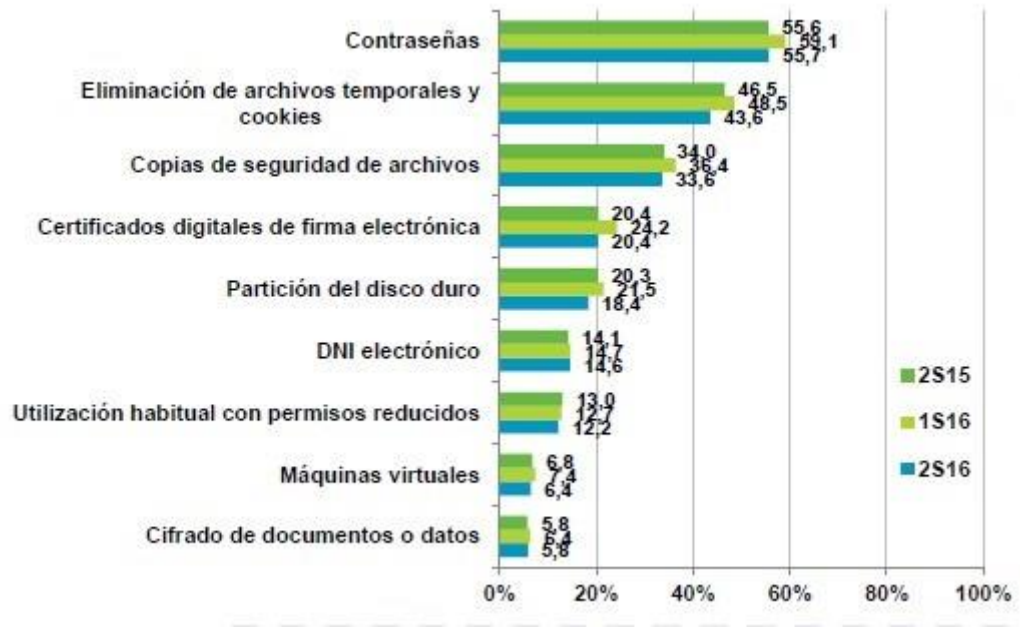


Imagen 10. Porcentaje de uso de medidas de seguridad no automatizables o acticas.

Como se puede observar en las dos últimas imágenes, se aprecian una tendencia a la baja en el uso de las medidas de seguridad automatizables con respecto al estudio anterior. Las principales medidas son el **software antivirus** (**72,0%**) y las **actualizaciones del sistema operativo** (**55,5%**). Por otra parte, en las medidas no automatizables o activas, prácticamente todas las medidas decrecen.

9.5 ANEXO 2

Tipos de delitos informáticos

Existen muchos tipos de delitos informáticos que es imposible de enumerar cada una de ellas y sus variantes, por ello hemos creado una lista de los delitos más habituales de este sector:

a) **Robo de Identidad**, conocido como *identity theft*, supone la sustracción de información personal a las victimas (pe. Nombres, fechas de nacimiento o cuentas bancarias) para, a posteriori, explotarla de manera deliberada en búsqueda de beneficio. En la mayoría de los casos las víctimas no saben de su condición hasta que el daño es demasiado grande como para poder prevenirlo.
b) **Estafas electrónicas**, en inglés *online scams*, que se traducen en la obtención de información financiera o de otro tipo a través de medios fraudulentos (pe. *Phishing*, *pharming*, *spoofing*, etc.). Esta información es empleada a posteriori con otras finalidades, normalmente la obtención de dinero.
c) ***Scareware***, del inglés *scare*, miedo, y *software*, abarca diferentes tipos de programas desarrollados con la finalidad de infectar los equipos. Habitualmente implica convencer al usuario de que se encuentra en situación de peligro, siendo el software malicioso a única alternativa para protegerse frente a esas amenazas (pe. Un banner publicitario que informa al usuario de que ha sido infectado por un virus o similar, redirigiéndolo a una tienda online donde adquirir un software antivirus caracterizado por su inutilidad, al no existir amenaza alguna).
d) **Fraude Fiscal**, en ingles *fiscal fraud*, con los consecuentes impactos en la esfera pública y las arcas del Estado vinculado a las TIC.
e) **Blanqueo de Dinero** o *money laundering*, actividad vinculada a grandes organizaciones o conglomerados criminales con presencia internacional. El medio más habitual es el diseño y establecimiento de sistemas de transferencias bancarias fraudulentas a nivel mundial que permiten mover el dinero de forma rápida e inadvertida para las autoridades fiscales a través de las TIC.
f) **Robos a Negocios**, *theft from bussines*, mediante el acceso a cuentas bancarias u otro tipo de activos de información. Es habitual la participación de un topo o *insider*, una persona con acceso a cierto tipo de información desde la misma organización a cambio de una comisión determinada.
g) **Extorsión**, *extortion*, dirigida fundamentalmente a empresas. Los cibercriminales mantienen a una empresa o comercio en una situación crítica, por ejemplo, saturando sus servidores con peticiones o modificando la página web corporativa incluyendo material sensible o poco adecuado (pe. Enlaces a páginas web pornográficas) hasta que se abona la cantidad demandada por aquellos.
h) **Robo de Cartera de Clientes**, *customer data loss*, donde el objetivo es la información sobre clientes, sobre todo aquella de naturaleza sensible, con el fin de emplearla en sus actividades comerciales o revenderla al mejor postor.
i) **Robo de Propiedad Intelectual**, *intelectual property theft*, que por diferencias jurídicas entre diferentes regímenes jurídicos incluye la propiedad industrial, patentes o marcas. En nuestra casuística, este tipo de información es muy valiosa ya que constituye el núcleo de los beneficios directos de grandes corporaciones o conglomerados comerciales (pe. Sector farmacéutico o de alta tecnología).

En términos generales, las prácticas anteriores constituyen el núcleo duro de los delitos informáticos en la actualidad (Detica Limited, 2011).

9.6 ANEXO 3

Normal Española UNE-EN ISO/IEC 27001

ISO (Organización Internacional de Normalización) e IEC (la Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en los campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, públicas y privadas, en coordinación con ISO e IEC, también participan en el trabajo. En el campo de tecnologías de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1.

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las Directivas ISO/IEC.

La tarea principal de los comités técnicos es preparar normas internacionales. Los proyectos de normas internacionales adoptados por los comités técnicos se envían a los organismos miembros para votación. La publicación como norma internacional requiere la aprobación por al menos el 75% de los organismos miembros que emiten voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO e IEC no asumen la responsabilidad por la identificación de cualquiera o todos los derechos de patente.

La Norma ISO/IEC 27001 fue preparada por el Comité Técnico conjunto ISO/IEC JTC 1 *Tecnología de la Información,* Subcomité SC 27 *Técnicas de seguridad*.

Esta segunda edición anula y sustituye a la primera edición (ISO/IEC 27001:2005) que ha sido revisada técnicamente.

Esta norma internacional se ha preparado para proporcionar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de la seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de la seguridad de la información por una organización está condicionado por sus necesidades y objetivos, sus requisitos de seguridad, los procesos organizativos utilizados y su tamaño y estructura. Lo previsible es que todos estos factores condicionantes cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos.

Es importante que el sistema de gestión de la seguridad de la información forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles. Es de esperar que la

implementación del sistema de gestión de la seguridad de la información se ajuste a las necesidades de la organización.

Esta norma internacional puede ser utilizada por partes internas y externas para evaluar la capacidad de la organización para cumplir con sus propios requisitos de seguridad.

El orden en que esta norma internacional presenta los requisitos no es reflejo de su importancia ni implica el orden en el cual deben implementarse. Los diferentes elementos de cada listado se enumeran sólo a título de referencia.

La Norma ISO/IEC 27000 describe la visión de conjunto y el vocabulario de los sistemas de gestión de la seguridad de la información, haciendo referencia a la familia de normas de sistemas de gestión de la seguridad de la información (incluyendo las Normas ISO/IEC 27003[2], ISO/IEC 27004[3] e ISO/IEC 27005[4]), junto con los términos y definiciones relacionados.

1. Compatibilidad con otras normas de sistemas de gestión

Esta norma internacional emplea la estructura de alto nivel, texto esencial idéntico, términos y definiciones esenciales comunes contenidos en el anexo SL de la Parte 1 de las Directivas ISO/IEC, Suplemento ISO consolidado y por lo tanto mantiene la compatibilidad con otras normas de sistemas de gestión que han adoptado el anexo SL.

Este enfoque común definido en el anexo SL será útil para aquellas organizaciones que deciden implantar un sistema de gestión que cumpla con los requisitos de dos o más normas de sistemas de gestión.

2. Objeto y campo de aplicación

Esta norma internacional especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información en el contexto de la organización. Esta norma también incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de información a la medida de las necesidades de la organización. Los requisitos establecidos en esta norma internacional son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño o naturaleza. No se acepta la declaración de conformidad con respecto a esta norma internacional habiendo excluido alguno de los requisitos especificados en los capítulos 4 al 10.

3. Normas para consulta

Los documentos indicados a continuación, en su totalidad o en parte, son normas para consulta indispensables para la aplicación de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición (incluyendo cualquier modificación de ésta).

ISO/IEC 27000, *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.*

4. Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones incluidos en la Norma ISO/IEC 27000.

5. Contexto de la organización

5.1. Comprensión de la organización y de su contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.

NOTA La determinación de estas cuestiones se refiere al establecimiento del contexto externo e interno de la organización considerando el apartado 5.3 de la Norma ISO 31000:2009[5].

5.2. Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información; y

b) los requisitos de estas partes interesadas que son relevantes para la seguridad de la información.

5.3. Determinación del alcance del sistema de gestión de la seguridad de la información

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Cuando se determina este alcance, la organización debe considerar:

a) las cuestiones externas e internas referidas en el apartado 4.1;

b) los requisitos referidos en el apartado 4.2;

c) las interfaces y dependencias entre las actividades realizadas por la y las que se llevan a cabo por otras organizaciones.

El alcance debe estar disponible como información documentada.

5.4. Sistema de gestión de la seguridad de la información

La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta norma internacional.

6. Liderazgo

6.1. Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información:

a) asegurando que se establecen la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización;

b) asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;

c) asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles;

d) comunicando la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de la seguridad de la información;

e) asegurando que el sistema de gestión de la seguridad de la información consigue los resultados previstos;

f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información;

g) promoviendo la mejora continua; y

Apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

6.2. Política

La alta dirección debe establecer una política de seguridad de la información que:

a) sea adecuada al propósito de la organización;

b) incluya objetivos de seguridad de la información (véase 6.2) o proporcione un marco de referencia para el establecimiento de los objetivos de seguridad de la información;

c) incluya el compromiso de cumplir con los requisitos aplicables a la seguridad de la información; e

d) incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.

La política de seguridad de la información
debe:

e) estar disponible como información documentada;

f) comunicarse dentro de la organización; y

g) estar disponible para las partes interesadas, según sea apropiado.

6.3. Roles, responsabilidades y autoridades en la organización

La alta dirección debe asegurarse que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de esta norma internacional; e

b) informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información.

NOTA La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el comportamiento del sistema de gestión de la seguridad de la información dentro de la organización.

7. Planificación

7.1. Acciones para tratar los riesgos y oportunidades

7.1.1. Consideraciones generales

Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar las cuestiones a las que se hace referencia en el apartado 4.1 y los requisitos incluidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar con el fin de:

a) asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos;

b) prevenir o reducir efectos indeseados; y

c) lograr la mejora continua

La organización debe planificar:

d) las acciones para tratar estos riesgos y oportunidades; y

e) la manera de:

1) integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información, y

2) evaluar la eficacia de estas acciones.

7.1.2. Apreciación de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de apreciación de riesgos de seguridad de la información que:

a) establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo:

   1) los criterios de aceptación de los riesgos, y

   2) los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información;

b) asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables;

c) identifique los riesgos de seguridad de la información:

   1) llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información,

   2) identificando a los dueños de los riesgos;

d) analice los riesgos de seguridad de la información:

   1) valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse,

   2) valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en el punto 6.1.2 c) 1),

   3) determinando los niveles de riesgo;

e) evalúe los riesgos de seguridad de la información:

   1) comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos en el punto 6.1.2 a),

   2) priorizando el tratamiento de los riesgos analizados.

La organización debe conservar información documentada sobre el proceso de apreciación de riesgos de seguridad de la información.

7.1.3. Tratamiento de los riesgos de seguridad de la información

La organización debe definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información para:

a) seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos;

b) determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

c) comparar los controles determinados en el punto 6.1.3 b) con los del anexo A y comprobar que no se han omitido controles necesarios;

d) elaborar una “Declaración de Aplicabilidad” que contenga:

- los controles necesarios [véase 6.1.3 b) y c)];
- la justificación de las inclusiones;
- si los controles necesarios están implementados o no; y
- la justificación de las exclusiones de cualquiera de los controles del anexo A.

e) formular un plan de tratamiento de riesgos de seguridad de la información; y

f) obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información por parte de los dueños de los riesgos.

La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

7.2 Objetivos de seguridad de la información y planificación para su consecución

La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

Los objetivos de seguridad de la información deben:

a) ser coherentes con la política de seguridad de la información;

b) ser medibles (si es posible);

c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos;

d) ser comunicados; y

e) ser actualizados, según sea apropiado.

La organización debe conservar información documentada sobre los objetivos de seguridad de la información.

Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar:

f) lo que se va a hacer;

g) qué recursos se requerirán;

h) quién será responsable;

i) cuándo se finalizará; y

j) cómo se evaluarán los resultados.

8. Soporte

8.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

8.2 Competencia

La organización debe:

a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información; y

b) asegurarse que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;

c) cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo; y

d) conservar la información documentada apropiada, como evidencia de la competencia.

8.3. Concienciación

Las personas que trabajan bajo el control de la organización deben ser conscientes de:

a) la política de la seguridad de la información;

b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información;

c) las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información.

8.4. Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan:

a) el contenido de la comunicación;

b) cuándo comunicar;

c) a quién comunicar;

d) quién debe comunicar;

e) los procesos por los que debe efectuarse la comunicación.

8.5. Información documentada

8.5.1. Consideraciones generales

El sistema de gestión de la seguridad de la información de la organización debe incluir:

a) la información documentada requerida por esta norma internacional;

b) la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información.

8.5.2. Creación y actualización

Cuando se crea y actualiza la información documentada, la organización debe asegurarse, en la manera que corresponda, de lo siguiente:

a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);

c) la revisión y aprobación con respecto a la idoneidad y adecuación.

8.5.3. Control de la información documentada

La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta norma internacional se debe controlar para asegurarse que:

a) esté disponible y preparada para su uso, dónde y cuándo se necesite;

b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:

c) distribución, acceso, recuperación y uso;

d) almacenamiento y preservación, incluida la preservación de la legibilidad;

e) control de cambios (por ejemplo, control de versión);

f) retención y disposición.

La información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación del sistema de gestión de la seguridad de la información se debe identificar y controlar, según sea adecuado.

9.7 ANEXO 4

La ciberseguridad en el Sistema de Seguridad Nacional

La visión integral de la ciberseguridad plasmada en esta Estrategia, los riesgos y amenazas detectados que le afectan y los objetivos y líneas de acción trazados, para dar respuesta conjunta y adecuada a la preservación de la ciberseguridad bajo los principios que sustentan el Sistema de Seguridad Nacional, explican la necesidad de contar con una estructura orgánica precisa a estos efectos, que estará constituida por los siguientes componentes bajo la dirección del presidente del Gobierno:

El Consejo de Seguridad Nacional

El Consejo de Seguridad Nacional configurado como Comisión Delegada del Gobierno para la Seguridad Nacional, asiste al presidente del Gobierno en la dirección de la Política de Seguridad Nacional.

El Comité Especializado de Ciberseguridad;

El Comité Especializado de Ciberseguridad dará apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad. Además, reforzará las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilitará la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

La composición del Comité Especializado de Ciberseguridad reflejará el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de ciberseguridad, para coordinar aquellas actuaciones que se deban abordar de forma conjunta con el fin de elevar los niveles de seguridad.

En el Comité podrán participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria.

En el cumplimiento de sus funciones el Comité Especializado de Ciberseguridad será apoyado por el Departamento de Seguridad Nacional en su condición de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional.

El Comité Especializado de Situación, único para el conjunto del Sistema de Seguridad Nacional.

El Comité Especializado de Situación será convocado para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la ciberseguridad que, atendiendo a la acentuada transversalidad o dimensión e impacto de sus efectos, produzcan el desbordamiento de los límites de capacidad de respuesta eficaz por parte de los mecanismos habituales previstos, siempre respetando las competencias asignadas a las distintas Administraciones Públicas y a los efectos de garantizar una respuesta inmediata y eficaz a través de un solo órgano de dirección político-estratégica de la crisis.

El Comité Especializado de Ciberseguridad y el Comité Especializado de Situación actuarán de forma complementaria, cada uno en su ámbito de competencias, pero bajo la misma dirección estratégica y política del Consejo de Seguridad Nacional presidido por el presidente del Gobierno.

El Comité Especializado de Situación será apoyado por el Centro de Situación del Departamento de Seguridad Nacional con el fin de garantizar su interconexión con los centros operativos implicados y dar una respuesta adecuada en situaciones de crisis, facilitando su seguimiento y control y la trasmisión de las decisiones.
Para el cumplimiento eficaz de sus funciones de apoyo al Comité Especializado de Situación, el Centro de Situación del Departamento de Seguridad Nacional podrá ser reforzado por personal especializado proveniente de los departamentos ministeriales u organismos competentes, los cuales conformarán la Célula de Coordinación específica en el ámbito de la Ciberseguridad.

La puesta en marcha del Comité Especializado de Ciberseguridad y del Comité Especializado de Situación, y la armonización de su funcionamiento con los órganos existentes, se realizará paulatinamente mediante la aprobación de las disposiciones normativas necesarias y el reajuste de las vigentes, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes del Sistema de Seguridad Nacional.

9.8 ANEXO 5

Reglamento de Protección de Infraestructuras Críticas

El Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, desarrolla, concreta y amplía los aspectos contemplados en la LPIC con la articulación de un sistema compuesto por órganos y entidades tanto de las Administraciones Públicas como del sector privado y el diseño de todo un planeamiento orientado a prevenir y proteger dichas infraestructuras críticas.

El texto contempla la elaboración de diferentes planes que deben ser desarrollados tanto por las Administraciones Públicas —en el caso del Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales y los Planes de Apoyo Operativo como por las empresas, organizaciones o instituciones clasificadas como operadores críticos, para la elaboración de los Planes de Seguridad del Operador y los Planes de Protección Específicos.

El Reglamento consta de 36 artículos y está estructurado en cuatro títulos.

Título I

En este Título se define el objeto del Reglamento como el establecimiento de medidas para la protección de las infraestructuras críticas y la regulación de las obligaciones que deben asumir tanto el Estado como los operadores de aquellas infraestructuras que se determinen como críticas. El ámbito se establece para las infraestructuras críticas en territorio nacional, a excepción de las dependientes del Ministerio de Defensa y de las FFCCSS.

También se referencia el Catálogo Nacional de Infraestructuras Estratégicas, registro de carácter administrativo que contiene información de todas las infraestructuras estratégicas, incluyendo tanto las críticas como las críticas europeas, y cuya finalidad es valorar y gestionar los datos que se dispone de ellas para diseñar los mecanismos de planificación, prevención, protección y reacción ante una eventual amenaza.

Según se indica en el Reglamento, el Catálogo contendrá todos los datos necesarios (relativos a la descripción de las infraestructuras, su ubicación, titularidad y administración, servicios que prestan, medios de contacto, nivel de seguridad) aportados por el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y los operadores, así como el resto de sujetos responsables y tendrá la clasificación de SECRETO; su gestión y mantenimiento corresponde al Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.

Título II

En este Título se enumeran y definen los agentes del Sistema de Protección de Infraestructuras Críticas; se establecen las funciones para la Secretaría de Estado de Seguridad, órgano superior responsable del Sistema de Protección de las IICC nacionales, entre las que destacan el diseño y dirección de la estrategia nacional de protección de IICC, la aprobación del Plan Nacional de Protección de las IICC declarando los niveles de seguridad, en coordinación con el Plan de Prevención y Protección Antiterrorista, los Planes de Seguridad de los Operadores, los Planes de

Protección Específicos y los Planes de Apoyo Operativo, así como la aprobación de declaración de zona crítica o la identificación de los ámbitos de responsabilidad en la protección de IICC; dentro también de este Título, se define y establece el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), dependiente de la Secretaría de Estado de Seguridad, cuyas funciones principales son las de asistir al Secretario de Estado de Seguridad en materia de protección de IICC actuando como contacto y coordinador entre los agentes del Sistema, mantener el Plan Nacional de Protección de las IICC, determinar la criticidad de las IICC y mantener el Catálogo.

Respecto a los instrumentos de planificación, el CNPIC dirige y coordina los análisis de riesgos realizados por los organismos especializados en los Planes Estratégicos Sectoriales, establece los mínimos de los Planes de Seguridad de los Operadores, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo, y evalúa los Planes de Seguridad del Operador y los propone al Secretario de Estado de Seguridad para su aprobación. Otras funciones asignadas son la propuesta de declaración de zona crítica al Secretario de Estado de Seguridad, la recopilación y valoración de la información sobre infraestructuras estratégicas para su remisión al Centro Nacional de Coordinación Antiterrorista del Ministerio del Interior, la participación en la realización de ejercicios y simulacros y el establecimiento del Punto Nacional de Contacto con organismos internacionales en el ámbito de la protección de IICC.

Las principales competencias de los Ministerios y organismos integrados en el Sistema de Protección de IICC son la participación en los Planes Estratégicos Sectoriales a través del Grupo de Trabajo Interdepartamental y la verificación de su cumplimiento, la colaboración en la designación de los operadores críticos y el asesoramiento técnico en la catalogación de las infraestructuras y su clasificación como crítica; todo ello, dentro de su sector de competencia correspondiente. Se establecen adicionalmente facultades para las Delegaciones del Gobierno en las Comunidades Autónomas y Ciudades Autónomas, como la coordinación de las FFCCSE ante una alerta de seguridad o el velar por la aplicación y cumplimiento del Plan Nacional de Protección o de los Planes Sectoriales, entre otras. Las competencias para las Comunidades Autónomas y las Ciudades Autónomas con competencias para la protección de persona y bienes y para el mantenimiento del orden público son similares a las de las Delegaciones del Gobierno; para aquellas que no tengan competencias, se les reconoce la participación en el Sistema y en los órganos colegiados.

Las funciones de la Comisión Nacional para la Protección de las Infraestructuras Críticas pasan por preservar, garantizar y promover una cultura de seguridad de las IICC en las Administraciones Públicas, promover la aplicación efectiva de las medidas de protección e impulsar acciones de cooperación interministerial. Esta Comisión estará presidida por el Secretario de Estado de Seguridad y tendrá representación de los organismos implicados con rango Director General, así como un representante por Comunidad Autónoma con competencias de seguridad. Se reunirá una vez al año y será asistida por el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, grupo entre cuyas funciones está elaborar los diferentes Planes Estratégicos Sectoriales, proponer a la Comisión la designación de operadores críticos y la creación de grupos de trabajo sectoriales.

Los últimos agentes del sistema reconocidos en el Reglamento son los Operadores Críticos, aquellos en los que al menos una de las infraestructuras gestionadas por él reúna la consideración de crítica; deberán prestar colaboración técnica en la valoración de las infraestructuras, colaborar con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales y en el análisis de riesgos, así como elaborar el Plan de Seguridad del Operador, un Plan de Protección Específico y designar a un

Responsable de Seguridad y Enlace y un Delegado de Seguridad, entre otras funciones.

Título III

Este Título recoge los instrumentos de planificación; define el Plan Nacional de Protección de las Infraestructuras Críticas como el instrumento de programación dirigido a mantener seguras las infraestructuras españolas que proporcionan servicios esenciales.

Este Plan establece criterios y directrices para asegurar la protección del sistema de infraestructuras estratégicas y prevé distintos niveles de seguridad e intervención policial, en coordinación con el Plan de Prevención y Protección Antiterrorista.
Se definen además los Planes Estratégicos Sectoriales indicando que se trata de instrumentos de estudio y planificación que permitirán conocer los servicios esenciales, el funcionamiento general de éstos, sus vulnerabilidades, las potenciales consecuencias de su inactividad y las medidas necesarias para su mantenimiento. El Grupo de Trabajo, con la participación de los operadores afectados, elaborará un Plan Estratégico por cada sector o subsector de actividad que estará basado en un análisis general de riesgos cuyo contenido mínimo será un análisis de riesgos, vulnerabilidades y consecuencias a nivel global y una serie de propuestas de implantación de medidas para los diferentes escenarios, medidas de coordinación con el Plan Nacional PIC.

Los Planes de Seguridad del Operador vienen recogidos en el Capítulo III de este Título y tienen como finalidad definir las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión. Estos planes deberán establecer una metodología de análisis de riesgos que garantice la continuidad de los servicios y recoger los criterios de aplicación de las diferentes medidas. Dentro del Capítulo IV se desarrollan los Planes de Protección Específicos como los documentos operativos donde se definen medidas concretas para garantizar la seguridad integral de sus infraestructuras críticas. Deberán contemplar la adopción tanto de medidas permanentes de protección como de medidas de seguridad temporales y graduadas. En un plazo de dos meses tras su recepción, la Secretaría de Estado de Seguridad notificará al interesado su resolución de la aprobación, proponiendo un calendario de implantación gradual. Las Delegaciones del Gobierno mantendrán un registro de los Planes que afecten a su demarcación y el CNPIC mantendrá un registro central de todos ellos. La revisión de estos planes se realizará cada dos años y deberá ser aprobada por la Delegación del Gobierno, quien velará también por la correcta ejecución de los Planes de Protección Específicos.

Ésta tendrá facultades de inspección y podrán requerir del responsable de las IICC la situación actualizada de la implantación de las medidas propuestas. Estos Planes se efectuarán sin perjuicio del obligado cumplimiento de lo exigido para instalaciones nucleares y radiactivas, portuarias, aeroportuarias, aeródromos e instalaciones de navegación aérea.

Finalmente, en este mismo Título III, el Capítulo V recoge los Planes de Apoyo Operativo donde se deben plasmar las medidas concretas para la mejor protección de las IICC; su realización será supervisada por la Delegación del Gobierno y para la elaboración de estos planes se dispone de cuatro meses tras la aprobación del respectivo Plan de Protección Específico, debiendo contemplar las medidas planificadas de vigilancia, prevención, protección y reacción, cuando se produzca la activación del Plan Nacional de Protección de las IICC. El contenido mínimo será

establecido por el CNPIC, así como el modelo en el que fundamentar la estructura y desarrollo de éstos.

Título IV

El último Título del Reglamento versa sobre las comunicaciones entre los operadores críticos y las Administraciones públicas, donde se designa al CNPIC como responsable de administrar los sistemas de información y comunicaciones diseñadas para la protección de las IICC, y cuya seguridad será acreditada y certificada por el Centro Criptológico Nacional; cada infraestructura crítica deberá contar con un Responsable de Seguridad y Enlace y en caso de ser necesario, con un Delegado de Seguridad.

El nombramiento y comunicación de ambos se hará en el plazo de tres meses al CNPIC y a la Delegación del Gobierno, respectivamente. Durante este año 2011 se ha publicado el documento que tiene por título “Estrategia Española de Seguridad, una responsabilidad de todos”. Esta estrategia expone la necesidad de una estrategia de seguridad para España, sitúa el estado de la seguridad de España en el mundo y analiza los potenciadores del riesgo para la seguridad del país, así como los principales riesgos y amenazas. Propone además un modelo institucional integrado, que requiere una serie de cambios orgánicos para ofrecer una respuesta a las necesidades de seguridad del país.