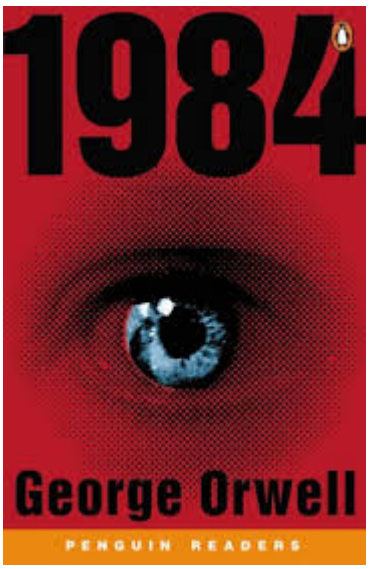
INSTITUTO VASCO DE ESTADÍSTICA (EUSTAT)

Política de Seguridad en un Instituto de Estadística

Autor: Aitor Iriarte Goikoetxea

1.-Breve historia de la protección de datos en Europa

A partir del final de la segunda guerra mundial, en pleno desarrollo público y privado de la era de la información, diferentes organismos, principalmente en Europa, han visto la necesidad de poner límites legales a las enormes posibilidades en el tratamiento de la información.



En 1948 George Orwell imagina una sociedad constantemente vigilada por el Gran Hermano. La novela se ambienta en un momento futuro que el autor sitúa en 1984 (resultado obtenido al intercambiar los últimos dígitos de 1948).

En esta novela, los ciudadanos tienen una cámara y un micrófono que registra todas sus actividades en su propia vivienda. Además, la policía utiliza autogiros para observar a través de las ventanas y balcones.

Se trata por lo tanto una sociedad sin derecho a la intimidad.

La novela 1984 se publica en 1949, y no pasará mucho tiempo hasta que el primer organismo internacional europeo desde el final de la guerra mundial, el Consejo de Europa, constituido en 1949, elabore el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que en su art.º 8 se refiere al "Derecho al respeto a la vida privada y familiar".

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

A lo largo de la década de 1970, el Consejo de Europa emite diferentes resoluciones para proteger los datos individuales frente al aumento de tratamientos de datos en el sector privado. Finalmente, en 1981 se publica el **Convenio 108** para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Podemos destacar brevemente las principales exigencias de este Convenio:

- Obtención leal y legítima de los datos.
- Finalidades legítimas y determinadas.

- Datos exactos y puestos al día.
- Medidas de seguridad contra la pérdida, acceso, modificación, difusión no autorizados.
- Conocimiento de la existencia del fichero, las finalidades.
- Autoridad controladora.
- Lograr la rectificación o el borrado de los datos cuando se hayan tratado con infracción del derecho.
- Régimen de sanciones.

Como trasposición de dicho Convenio, se aprueba en el Estado Español la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD), y unos meses más tarde, ya en 1993, se crea la Agencia Española de Protección de Datos.

En 1995 se aprueba en el Parlamento Europeo la Directiva 95/46/CE que posibilita la libre circulación de datos personales en un contexto europeo con protección de datos. Finalmente en 1999 se traspone la Directiva por aprobación de la **Ley Orgánica 15/1999**, de 13 de Diciembre, de Protección de Datos de Carácter Personal que viene ahora a proteger también los tratamientos manuales además de los automatizados.

Este mismo año 2016, se ha aprobado el **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE. Y lo que es importante destacar es que al tratarse de un Reglamento Europeo, no requiere de trasposición, sino que directamente es de obligado cumplimiento para los Estados miembros.

2.-La Seguridad, el Esquema Nacional de Seguridad (ENS), y las obligaciones legales

Respecto al ámbito estadístico, ya en 1945 cuando se crea el Instituto Nacional de Estadística, se observa la gran importancia que tiene un principio propio como es el **Secreto Estadístico**. Desde entonces, en cada una de las Leyes de Estadística autonómica se ha incluido un capítulo, o varios artículos, para desarrollar dicho principio.

Además de este principio tan particular del ámbito de la **Confidencialidad**, en todos los sistemas informáticos, tradicionalmente, se han considerado otras dos dimensiones de la seguridad, como son la **Integridad** y la **Disponibilidad**.

Hoy en día, tratar de asegurar como buenamente se pueda estos tres aspectos, ya no es suficiente. Existen **metodologías para la gestión de riesgos**, que sirven para analizar y valorar los riesgos a los que estamos expuestos, evaluar el estado de la seguridad en cada momento, y señalar donde debemos destinar nuestros esfuerzos para reducir progresivamente el riesgo.

Así mismo, desde un punto de vista más amplio, la propia **gestión de la seguridad** se ha estandarizado, permitiendo utilizar una terminología común, y unos procedimientos y certificaciones encaminados a lograr, por una parte la implicación de todo el personal empezado por la Dirección, y por otra, lograr el aumento de la seguridad en una dinámica de mejora continua.

Desde un punto de vista Legal, se han aprobado Leyes que obligan al sector público a poner en marcha estas iniciativas, y a cumplir con el Esquema Nacional de Seguridad:

- Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. En su art. 1, garantiza el derecho de los ciudadanos a relacionarse por medios electrónicos, y por otra parte obliga a las administraciones públicas a asegurar la disponibilidad de acceso, la integridad, la autenticidad, la confidencialidad y la conservación. En el art. 42 menciona el Esquema Nacional de Seguridad (ENS), y el Esquema Nacional de Interoperabilidad (ENI).

- RD3/2010, de 8 de Enero, por el que se regula el ENS en el ámbito de la Administración electrónica. Había un plazo para la adecuación al ENS, pero dicho plazo venció el 30 de Enero de 2014.

- Ley 39/2015, de 1 de Octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Esta Ley deroga la Ley 11/2007 el 2/10/2016. Algunas disposiciones son de aplicación a partir del 2/10/2016. Para otras, la fecha límite es el 2/10/2017.

- Ley 40/2015, de 1 de Octubre, de Régimen Jurídico del Sector Público. Los plazos de adecuación son también el 2/10/2016 y el 2/10/2017, dependiendo del caso.

3.-La política de seguridad

El Esquema Nacional de Seguridad (Real Decreto 3/2010) es obligatoria para todas las Administraciones Públicas (art. 1). Para los sistemas que ya se encontraban en funcionamiento en el momento de la aprobación del Real Decreto, en su disposición transitoria, de título “Adecuación de Sistemas”, establece un plazo de 12 meses para su cumplimiento. Si hubiera dificultades para su aplicación, obliga a redactar un plan de adecuación con el objetivo de lograr su cumplimiento en el plazo de 48 meses desde su aprobación.

- Fecha de publicación del ENS: 29 de Enero de 2010.
- Primera fecha límite para el cumplimiento: 30 de Enero de 2011.
- Fecha límite (con un plan de adecuación): 30 de Enero de 2014.

En el año 2016, la **Política de Seguridad es obligatoria** para todos los organismos públicos (Anexo II del ENS). Aunque no todos los organismos públicos han aprobado un documento con esa denominación, disponen de numerosos planes estratégicos, procedimientos normalizados, medidas de seguridad, normativas internas, nombramientos en el ámbito de la seguridad, etc.

A continuación, vamos a enumerar unos apartados básicos que entendemos que debe reunir un documento de seguridad:

3.1 Situación de la organización, infraestructura básica, y gestión de los sistemas de información

Una descripción del organismo, su misión, y sus valores. ¿Es un Instituto de Estadística con forma de organismo autónomo?, ¿A qué Departamento está adscrito?, ¿Es una Consejería?, ¿Un órgano estadístico?, o ¿un servicio con su propio sistema de información?

Es relevante también mencionar quién gestiona la infraestructura básica como son las comunicaciones, la conexión a Internet, el servicio de correo electrónico. ¿Se hace con medios propios?, ¿Está externalizado?, ¿Se encarga un Departamento trasversal?

Por último, y lo más importante, ¿Quién gestiona los sistemas de información que realmente contienen los datos y ofrecen los servicios? ¿Dónde están físicamente albergados los sistemas?

Un capítulo de la Política de Seguridad tiene que ir destinado a aclarar todos estos aspectos que tanto varían de un organismo a otro.

En el caso concreto de EUSTAT, la certificación ISO9001 del área de sistemas de información, ha supuesto recoger toda esta información en el **manual de calidad** del organismo. Por lo tanto, se introduce una referencia a dicho manual en la política de seguridad.

3.2 Los nombramientos

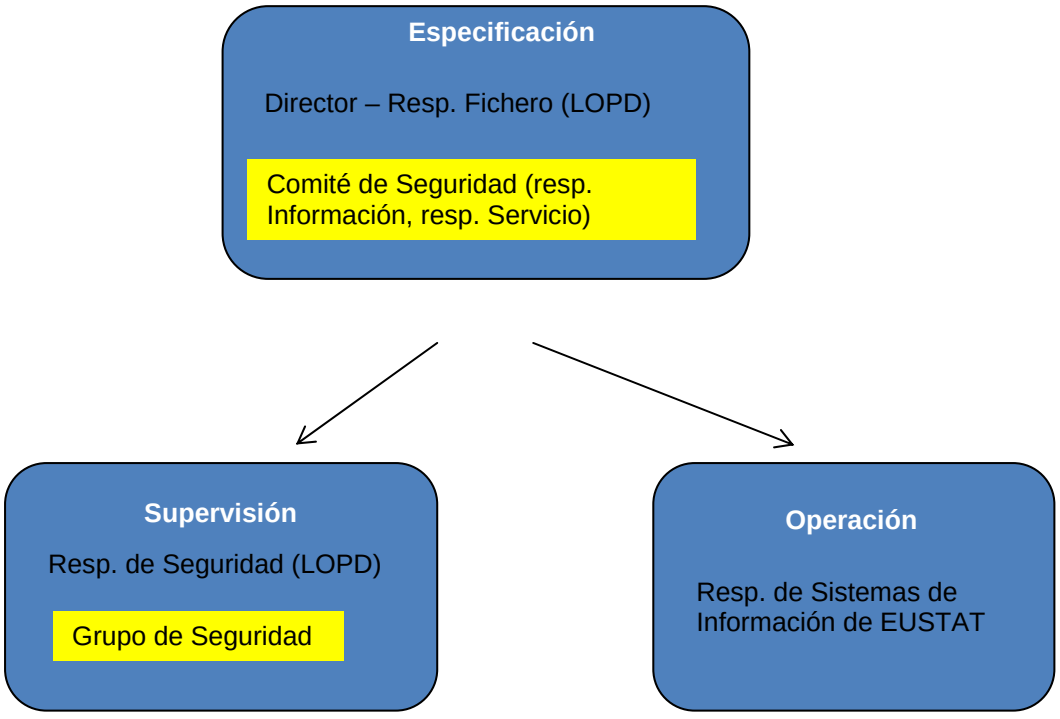
El art. 10 del ENS establece la **función diferenciada**. Se refiere a que se deben realizar unos nombramientos diferenciando las responsabilidades en materia de seguridad. En concreto, se deben diferenciar los siguientes puestos:

- Responsable de la Información.
- Responsable de Seguridad.
- Responsable del Servicio.

El Centro Criptológico Nacional, en su guía dedicada a las "Responsabilidades y Funciones", hace hincapié en que el **Responsable de la Seguridad debe ser independiente del Responsable del Sistema**, pero abre la puerta a que se unifiquen las **responsabilidades de la información y el servicio en una sola persona**.

La estructura que proponen desde el CCN es diferenciar en tres grandes bloques la responsabilidad: la **especificación** de las necesidades, la **operación** del sistema de información que se atiene a los requisitos, y la **supervisión** de acuerdo con el ENS.

Esquema aprobado en EUSTAT:



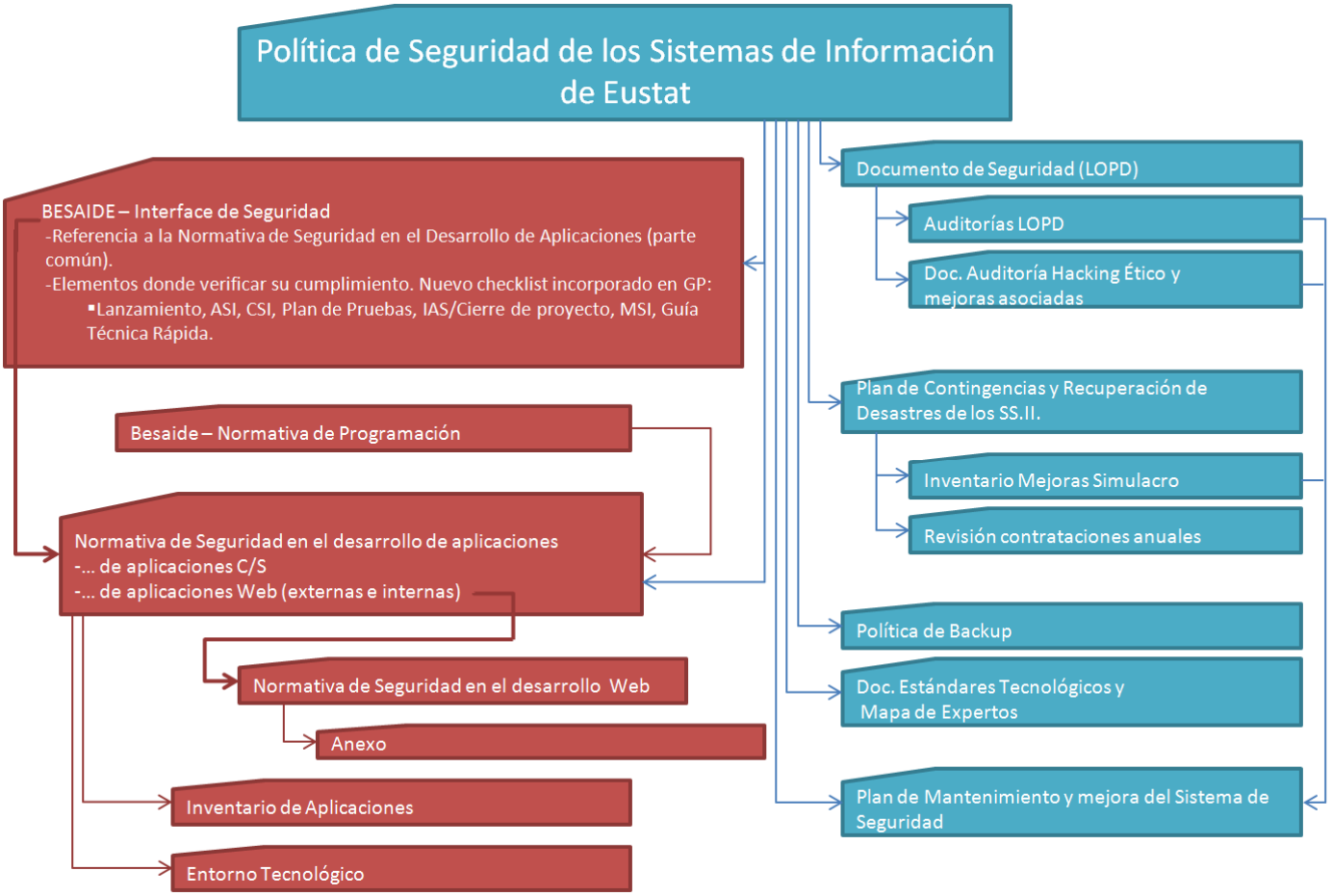
Estando el Comité de Seguridad formado por el Director, las dos Subdirectoras, el Responsable de Seguridad, el Responsable de área de Sistemas de Información y el Responsable del área jurídico-administrativa.

Y el Grupo de Seguridad compuesto por la Subdirectora de Coordinación Técnica y Difusión, el Responsable de Seguridad, y el Responsable de área de Sistemas de Información.

3.3 La ordenación del resto de documentos

Lógicamente, antes de la aprobación del ENS, existían en todas las organizaciones multitud de documentos, que directa o indirectamente, tienen que ver con los servicios ofrecidos, la información almacenada, los sistemas de información, el software adquirido, las metodologías de desarrollo, y la seguridad. Es conveniente describir todos estos documentos en la política de seguridad, añadiendo un anexo que contenga las ubicaciones de todos los documentos referenciados.

De esta forma, la política de seguridad de EUSTAT es un "documento marco" que sirve de guía para localizar el resto de documentos relevantes:



En color rojo aparecen los documentos relacionados con el desarrollo de aplicaciones (normativas de desarrollo, inventario de aplicaciones, entorno tecnológico, etc.), y en color azul, los que afectan al Centro de Proceso de Datos, y a la Seguridad del Sistema, destacando especialmente los siguientes:

- El documento de seguridad (LOPD).

- El Plan de contingencias y recuperación de desastres.
- La política de copias de seguridad.
- El documentos de estándares tecnológicos y mapa de expertos.
- El Plan de mantenimiento y mejora del sistema de seguridad.

3.4 La gestión de incidentes

El término “incidente” que se emplea en el ENS es más amplio que las “incidencias de seguridad” de la LOPD. Ya no se trata de registrar y gestionar únicamente las ocurrencias que ponen en peligro los **datos**, sino que de igual forma, tenemos que gestionar aquellas que afectan a los **servicios** que ofrecemos, tanto para el funcionamiento interno, como para los ofrecidos al exterior.

La certificación ISO9001 supone tener que habilitar registros entre los cuales tenemos los siguiente relacionados con los sistemas de seguridad:

- Registro de malware.
- Programación de copias de seguridad.
- Registro de recuperaciones incorrectas.
- Incidencias graves con parada de servicio.
- Listado de no conformidades.

Según se encuentra recogido en nuestro Documento de Seguridad, una de las principales obligaciones de todos los usuarios es la comunicación al Responsable de Seguridad de cualquier incidencia que tenga que ver con la seguridad. Los usuarios pueden abrir incidencias de seguridad por medio de una aplicación en la intranet. El Responsable de Seguridad se ocupa de que todos los usuarios hayan leído el Documento de Seguridad.

El Responsable de Seguridad registra los incidentes, valora la gravedad, intenta darles solución, y si no es posible aplica medidas correctivas en los sistemas. En función de la gravedad del incidente, convoca al Grupo de Seguridad, que a su vez puede decidir convocar al Comité de Seguridad.

Se ha implantado también un sistema de monitorización que continuamente está comprobando el funcionamiento todos los sistemas:

- Servidores.
- Elementos de comunicaciones y cortafuegos.
- Infraestructura VMWare.
- Bases de datos ORACLE.
- Web de EUSTAT.
- Aplicaciones Web (encuestas).
- Cabinas de disco.
- Temperatura de la sala de servidores.

En caso de que algún elemento no funcione, el sistema de monitorización envía correos electrónicos al Responsable de Seguridad y al Responsable del Sistema. Los dos responsables pueden, en todo momento, comprobar el estado de los sistemas por medio de una aplicación web.

El siguiente esquema representa de qué forma se detectan y tratan los incidentes de seguridad en EUSTAT:

3.5 El análisis y la gestión de riesgos

El análisis de riesgos se debe realizar y aprobar anualmente. Esta es una tarea fundamental, ya que nos permitirá saber dónde debemos dedicar el esfuerzo de mejora, para continuar reduciendo el riesgo del sistema.

Realizar un análisis de riesgos requiere utilizar un software específico, por una parte por el gran número de elementos que hay que valorar, y por otra, porque no se trata de hacer las valoraciones de una sola vez, sino que el proceso supone realizar valoraciones, corregirlas, asignar probabilidades, etc. Y todo ello, además de ser cambiante, varía cada vez que modifiquemos los sistemas, añadamos nuevos activos de información, servicios, etc.

Existen múltiples metodologías válidas. El art. 13 del ENS sólo impone que se emplee una metodología reconocida internacionalmente. También es posible optar por un estándar de gestión de riesgos determinado (ISO 31.000, ISO 27.005,…). Sin embargo, las Administraciones Públicas tenemos a nuestra disposición una metodología de análisis y gestión de riesgos, con un software gratuito (solo para Administraciones públicas) que nos va a facilitar el cumplimiento de la metodología:

- **Magerit** es la metodología elaborada por el Consejo Superior de Administración electrónica. Actualmente se encuentra en la versión 3.
- **Pilar** es el software desarrollado y financiado parcialmente por el Centro Criptográfico Nacional para facilitar el uso de la metodología Magerit para el análisis y la gestión de riesgos. Existen tres diferentes versiones de Pilar: la completa, la sencilla y la reducida. El formato de los ficheros es común, por lo que podemos empezar por una versión sencilla y pasar a la completa más adelante.

En la práctica es muy recomendable utilizar Pilar para el análisis de riesgos, ya que tiene un **perfil ENS** que permite medir el cumplimiento de las medidas de seguridad del anexo II del ENS.

3.6 Las medidas de seguridad

Los artículos 7, 8 y 9 se refieren a las medidas de seguridad. En el caso de un sistema de información totalmente nuevo, lo lógico sería estudiar las medidas después del análisis de riesgos, pero normalmente nos encontraremos en la situación contraria. Tenemos unas medidas previas y realizamos el análisis de riesgos para mejorarlas.

Art. 7: Prevención, Reacción y Recuperación:

- Medidas de prevención: Reducir la posibilidad de que las amenazas se materialicen. Se logra por disuasión y reducción de la exposición.
- Medidas de detección unidas a medidas de reacción. Se trata de atajar los incidentes a tiempo.
- Medidas de recuperación para restaurar la información y los servicios.

Art. 8: Líneas de defensa:

- Múltiples capas de seguridad.
- Constituida por medidas de naturaleza organizativa, física y lógica.

Art.º 9: Reevaluación periódica: “Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.”

Pero es en el anexo II cuando el ENS describe explícitamente 75 medidas de seguridad a aplicar dependiendo de la categorización que hagamos (anexo I). Son 4 medidas en el **marco organizativo**, la primera de las cuales es aprobar la política de seguridad. Hay 31 medidas en el **marco operacional,** y 40 **medidas de protección**. Emplear Pilar con el perfil ENS va a facilitar comprobar el cumplimiento de esas 75 medidas para las categorizaciones del nivel más alto.

3.7 La auditoría

De acuerdo con el art. 34 del ENS, tenemos que hacer una auditoría ordinaria que verifique el cumplimiento del ENS al menos cada dos años. Además tendríamos que hacer una auditoría extraordinaria cuando hubiera cambios sustanciales en el sistema de información.

El art. 34.5 establece que “El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del presente real decreto, identificar sus deficiencias y sugerir las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.”

Y por último el 34.5, que “Los informes de auditoría serán presentados al responsable del sistema y al responsable de seguridad competentes. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.”

4 Conclusión

La nuevas Leyes (Ley de Procedimiento Administrativo Común, y la Ley de Régimen Jurídico del Sector Público), que entran en vigor el próximo dos de Octubre, van a reclamar de las Administraciones Públicas un cumplimiento riguroso del Esquema Nacional de Seguridad. El organismo que todavía no haya aprobado una Política de Seguridad, debería hacerlo con la mayor urgencia, nombrando los responsables que deberán poner en marcha un análisis de riesgos lo antes posible. Es conveniente también, realizar la primera auditoría que nos indicará el grado de cumplimiento, y señalará las medidas correctoras que tendremos que poner en marcha.

Es probable que no podamos evitar al 100% todos los posibles incidentes de seguridad, pero tenemos que ser capaces de transmitir a la Dirección el estado real de la seguridad en nuestro organismo estadístico, junto con las recomendaciones adecuadas para destinar los recursos donde realmente sean provechosos.