UNIVERSIDAD POLITÉCNICA DE VALENCIA
ESCUELA TÉCNICA SUPERIOR DE INFORMÁTICA APLICADA

Integración de la herramienta SGSI Tracking con la norma ISO 27001 y el reglamento de la LOPD en un entorno virtualizado

PROYECTO FIN DE CARRERA

David Miguel Cutanda Mompó

Juan Carlos Ruiz García
Josep S. Cuñat Ferrando

22 de Septiembre de 2010

Agradecimientos

En un primer lugar compartido me gustaría agradecer por una parte a Juan Carlos Ruiz García, Profesor del grupo de Tolerancia a Fallos del ETSINF, por su paciencia y comprensión dada la dificultad de complementar el presente proyecto con mi trabajo; y por otra parte a Josep S. Cuñat Ferrando, Director de Consultoría IT de Setival SCV, tanto en calidad de alumno como de compañero, por todo el tiempo y paciencia dedicados a este proyecto, así como sus consejos y la confianza que siempre ha depositado en mí.

No me podría olvidar tampoco de mi gran amigo José Vila Montaner, el que es, por méritos propios el padre de esta criatura, sin la cual, es obvio, que no se podría haber realizado el presente proyecto.

También quiero agradecer a todos mis compañeros en Setival SCV por su apoyo, hayan o no hayan participado activamente de mis dudas, comentarios e inquietudes.

Quiero dedicarles este proyecto muy especialmente a mis padres, Benjamín y Manuela, a mis abuelas, María y Manuela y a mi pequeña Lluna, por compartir conmigo todos los momentos de mi vida, buenos o malos, y por estar siempre ahí. No me puedo olvidar de mis amigos, que sin ellos no habría conservado la cordura alcanzar mi meta, gracias a: Sergio, Javier, Diana, Govinda, Joan, Rodilla, José María, Civera y Pepe. Y a mis compañeros de carrera: Jorge, Jacob, Andrés, Pedro y Emilio.

Y a todos a los que no os he nombrado, y habéis formado parte de mi vida, gracias.

Tabla de contenidos

Tabla de Ilustraciones

1. Contexto y Motivación

La *Información* es un activo, que como cualquiera de los demás activos de una empresa, debe ser adecuadamente protegida. Se puede soportar en muchos formatos: puede ser impresa o escrita en papel, almacenada y transmitida electrónicamente, hablada en una conversación, etc. Sea cual sea la forma en la que se recoja, notifique o almacene, la información debe ser protegida.

La *Seguridad de la Información* consiste básicamente en proteger este activo con el fin de garantizar la continuidad de negocio, minimizar los riesgos, maximizar beneficio por inversión y las oportunidades de negocio. La seguridad de la información es, básicamente, un conjunto de controles, políticas, procesos, procedimientos y funciones hardware y software.

Las organizaciones y sus Sistemas de Información y redes se enfrentan a amenazas de muy distintos tipos como el fraude informático, espionaje, sabotaje, vandalismo, fuego o inundaciones. Ejemplos de cómo estas amenazas comprometen la seguridad son: códigos maliciosos, hacking informático, ataques de denegación de servicio, etc. Además de las amenazas intencionadas o maliciosas, también es necesario considerar las no intencionadas, relacionadas con mantenimiento y averías, que también comprometen la seguridad de la información. Como es lógico, no todos los Sistemas de Información se han concebido para ser seguros, pero se pueden alcanzar ciertos niveles de seguridad mediante un mantenimiento apropiado y procedimientos establecidos.

Un *Sistema de Gestión de la Seguridad de la Información* (en adelante SGSI), representa un conjunto de políticas, procedimientos, y salvaguardas definidos para poder atenuar, o en su caso eliminar, las amenazas sobre la información.

En este contexto aparece en 2005 la norma ISO/IEC 27001, que establece un estándar para la seguridad de la información por el cual se establece un conjunto de controles que permiten a una organización obtener un certificado que hace mención de que la organización ha implantado y mantiene un SGSI adecuado a sus necesidades. Esta certificación es consistente con la norma ISO/IEC 17799, que representa un código de buenas prácticas en seguridad de la información. La norma ISO/IEC 27001 se basa en el modelo Plan-Do-Check-Act (Figura 1) (en adelante PDCA).

El modelo PDCA se aplica para estructurar todos los procesos del SGSI. En la figura se muestra como el sistema recoge los requisitos y expectativas de seguridad de la información, y a través de él, se obtienen a la salida los elementos de seguridad que responden a dichas necesidades. Las fases del plan se describen a continuación:

- Planificar: Definir política, objetivos, procesos y procedimientos del SGSI, siempre de acuerdo con las políticas y objetivos de la organización.
- Desplegar: Implementar y operar la política, controles, procesos y procedimientos del SGSI.

- Verificar: Evaluar y medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, e informar los resultados a la Dirección para su revisión.
- Actuar: Adoptar medidas correctivas y preventivas, fruto de los resultados de la auditoría interna del SGSI, o de la revisión por la Dirección, o de otras fuentes relevantes, para lograr mejora continua del SGSI.

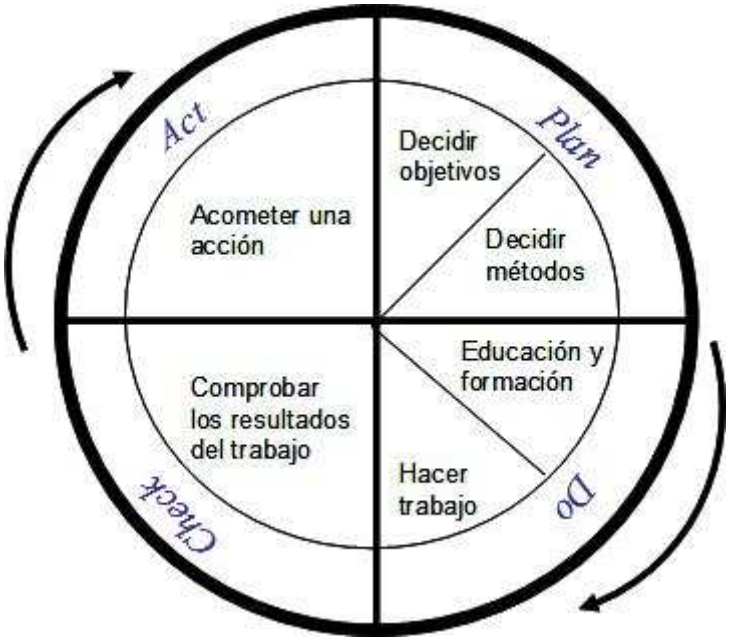


Ilustración 1 - Ciclo PDCA

A nivel nacional también se considera la seguridad de la información. En paralelo a la ISO/IEC 27001 surge en España la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (en adelante LOPD). Esta ley, aunque menos amplia que la norma ISO/IEC 27001, se fundamenta en el valor y la importancia de la información; aunque en este caso centrada en proteger los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, especialmente de su honor e intimidad personal. Bajo esta perspectiva la LOPD también establece medidas y salvaguardas, además de procedimientos y registros, orientados a proteger los datos de carácter personal. Generalizando se podría establecer, que aunque tienen una finalidad diferente, a nivel práctico la LOPD resulta ser un subconjunto de los controles de la ISO/IEC 27001, ya que ambos se centran en proteger los activos de información.

En base a estas necesidades se desarrolla en Setival SCV la plataforma SGSI Tracking, como una herramienta multifunción diseñada para facilitar la implantación y mantenimiento de un SGSI. SGSI Tracking integra diversos módulos de herramientas open source para monitorización de red, tales como inventario de red, gestión centralizada de eventos, gestión de incidencias, etc. Se trata pues de una aplicación que permite llevar un seguimiento exhaustivo de los sistemas de información.

2. Introducción

2.1. Autor

Este proyecto y su memoria han sido realizados por David Cutanda Mompó para obtener el título de Ingeniero en Informática (especialidad de Arquitectura de Computadores) en la Universidad Politécnica de Valencia.

El presente proyecto ha sido supervisado por Juan Carlos Ruiz García, profesor del grupo de investigación de Tolerancia a Fallos en la ETSinf de la Universidad Politécnica de Valencia, en calidad de tutor de proyecto. Además, este proyecto ha sido dirigido y supervisado por Josep S. Cunyat, Ingeniero en Telecomunicación y Director de Departamento de Consultoria IT de Setival SCV, en calidad de director de las prácticas en empresa que dan lugar al siguiente proyecto.

2.2. Objetivos

En el presente proyecto se aborda la última fase de desarrollo de dicha herramienta, concretamente la fase previa a su comercialización. Esta fase se compone de los siguientes objetivos:

- Integrar con la herramienta SGSI Tracking los principales objetivos de control de la norma ISO/IEC 27001 y los controles técnicos del Reglamento de la Ley Orgánica 15/1999 de Protección de Datos Personales.
- Creación de un entorno de pruebas implementado mediante virtualización, para en primer lugar, poner en marcha un entorno para la demostración efectiva, controlada y repetible de la herramienta SGSI Tracking para todos los potenciales clientes de Setival SCV.
- Implantación de la herramienta SGSI Tracking en Setival SCV, incluyendo la implantación, parametrización y generación de documentación técnica y de usuario final dentro del proceso de implantación y certificación de la norma ISO 27001 que se ha llevado a cabo en Setival SCV.

2.3. Contenido de la memoria

Para cumplir con los objetivos del proyecto se ha dividido la memoria en los siguientes puntos:

- Punto 3: Análisis de la norma ISO/IEC 27001 y el reglamento de la LOPD a fondo, para así extraer los controles de cada una que sean automatizables, para posteriormente ponerlos en comun y aplicarlos a cada uno de los módulos de SGSI Tracking. Dando como resultado alertas, métricas, estadísticas, etc. que faciliten el cumplimiento de las mismas.
- Punto 4: Descripción de la puesta en marcha del entorno de pruebas de SGSI Tracking y su puesta a punto para ser empleado como entorno de demostración.
- Punto 5: Descripción de la implantación de SGSI Tracking en Setival SCV, incluyendo la parametrización y generación de documentación, en el marco de la implantación de la ISO/IEC 27001 en Setival SCV.

3. Marco Legal y Controles de Seguridad, Integración con la Herramienta SGSI Tracking

3.1. Objetivo de la sección

Como se ha descrito con anterioridad, el presente proyecto final de carrera se engloba en dos normas fundamentales, a nivel nacional la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, y a nivel internacional la ISO/IEC 27001 sobre la Seguridad en la Información. En esta sección, en primer lugar se va a analizar por separado cada una, primero de forma global, y luego posteriormente de los puntos y controles aplicables a la aplicación SGSI Tracking (obviamente representarán los apartados más técnicos de ambas). Finalmente se expondrán los controles seleccionados y se mostrará su posible aplicación dentro de la herramienta SGSI Tracking.

3.2. Requisitos de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)

La Ley Orgánica de Protección de Datos regula el uso y explotación de datos de carácter personal. Su implantación está basada en dos fuentes diferenciadas:

- Ley Orgánica 15/1999 de 13 de diciembre, de *Protección de Datos de Carácter Personal*.
- Real Decreto 1720/2007, reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de *Protección de Datos de Carácter Personal*.

Estos dos textos se analizarán a continuación.

3.2.1. Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)

El presente texto, que consta de 49 artículos, constituye una ley orgánica que es de obligado cumplimiento en el territorio español.

La ley orgánica 15/1999 de Protección de Datos de Carácter Personal establece las obligaciones para el tratamiento de este tipo de datos, puesto que se trata de un documento legislativo, no establece medidas específicas ni técnicas para el cumplimiento de la misma, estas medidas vienen establecidas en el RD 1720/2007.

El texto está organizado en los siguientes apartados:

- TÍTULO I: Disposiciones generales
- TÍTULO II: Principios de Protección de Datos
- TÍTULO III: Derechos de las personas
- TÍTULO IV: Disposiciones sectoriales
    - CAPÍTULO I: Ficheros de Titularidad Pública
    - CAPÍTULO II: Ficheros de Titularidad Privada

- TÍTULO V: Movimiento internacional de datos
- TÍTULO VI: Agencia de Protección de Datos
- TÍTULO VII: Infracciones y sanciones

A continuación se hará una descripción breve del contenido de cada uno de los puntos de esta ley, acorde a su importancia respecto a la finalidad del presente proyecto. Con este repaso de busca entender la finalidad del texto y de revisar todos los requisitos que permitan posteriormente analizar su posible aplicación a la herramienta SGSI Tracking.

TÍTULO I: Disposiciones generales

En el presente título se describe, básicamente:

- **Objeto:** Define de forma clara y concisa que el objetivo de la presente ley es proteger el tratamiento de datos de carácter personal, las libertades públicas y los derechos de las personas físicas, especialmente su honor y su intimidad personal y familiar.

- **Ámbito de aplicación:** En el presente artículo se especifica concretamente, a que situaciones, y en nuestro caso, a que datos de carácter personal se aplica la presente ley; así como en qué casos se regirán por sus disposiciones específicas, y no por la ley 15/1999.

- **Definiciones:** Glosario acerca de la terminología que se emplea en la ley 15/1999, se dan las definiciones en el Anexo I – Definiciones LO 15/1999 de la presente memoria.

TÍTULO II: Principios de la Protección de Datos

En este conjunto de artículos se establecen los fundamentos del tratamiento de datos de carácter personal. Se repasan estos requisitos artículo por artículo:

- **Calidad de los datos:** Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, por lo que no podrán emplearse con finalidades distintas a las anteriormente mencionadas. Solo se podrán tratar datos que sean adecuados, pertinentes y no excesivos; también se determina el responsable tiene la obligación de poner al día los datos de carácter personal objeto de tratamiento, para que correspondan con veracidad a la situación actual del afectado, así como ser cancelados cuando no se requiera su utilización.

- **Derecho de información:** Antes de recabar los datos, se debe informar a los interesados expresa, precisa e inequívocamente de:
  - La existencia del fichero de datos de carácter personal y su finalidad.
  - Su obligación de responder a las preguntas que le sean planteadas.
  - La posibilidad de ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición (en adelante ARCO).
  - De la identidad y dirección del responsable del fichero.

Además se especifica cómo se debe informar dependiendo del medio empleado, y se detallan situaciones concretas en las que no se aplica el presente artículo.

- **Consentimiento del afectado:** Se requiere el consentimiento inequívoco del afectado en cualquier caso mientras la ley no especifique lo contrario, como por ejemplo:
    - Que se establezca un contrato por el cual sea necesario el tratamiento de los datos del interesado para poder llevar a cabo la relación contractual,
    - O cuando el tratamiento de los datos tenga una finalidad de preservar un interés vital del interesado.

- **Datos especialmente protegidos:** Este artículo especifica formalmente los datos de carácter personal más delicados, y que, por tanto son amparados por la ley. Concretamente estos datos son:
    - Ideología, religión o creencias.
    - Origen racial, salud o vida sexual.

  En ambos casos, el artículo establece que solo podrán ser tratados si, por una parte lo disponga una ley; o el afectado preste su consentimiento expresamente, y por escrito. Para estos tipos de datos, se especifican excepciones. Se contempla además la casuística de datos relativos a la comisión de infracciones penales o administrativas, que solo podrán ser tratados por las administraciones públicas.

- **Seguridad de los datos:** El responsable del fichero debe adoptar medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos, evitando su alteración, pérdida, tratamiento o acceso no autorizado. Evaluando los riesgos posibles, la tecnología empleada y la naturaleza de los datos almacenados.

- **Deber de secreto:** El responsable del fichero y cualquiera que participe en el tratamiento de datos de carácter personal está obligado a guardar secreto profesional y a guardarlos.

- **Comunicación de datos:** El responsable del fichero podrá comunicar datos de carácter personal a un tercero para el cumplimiento de fines relacionados con las funciones legítimas del cesionario y el cedente, con el previo consentimiento del interesado. A continuación se especifican excepciones en las cuales no se requerirá el consentimiento, como por ejemplo:

- **Acceso a los datos por cuenta de terceros:** No se considerará comunicación de datos al acceso de un tercero a datos de carácter personal cuando dicho acceso se realice durante la prestación de un servicio al responsable del tratamiento. En caso de que se del tratamiento de datos por cuenta de terceros, se debe realicar un contrato para regular dicha situación. El contrato debe contener:
    - Que el encargado de tratamiento solo debe tratar los datos de acuerdo con las instrucciones del responsable del fichero.
    - Se deben establecer las medidas de seguridad a aplicar a los datos.

- Que una vez cumplida la relación contractual, los datos de carácter personal deben ser destruidos o devueltos al responsable de tratamiento.
- Que en caso de que el responsable de tratamiento incumpla cualquiera de los puntos anteriores, se le considerará responsable de fichero, respondiendo de las infracciones correspondientes.

TÍTULO III: Derechos de las personas

En este fragmento del texto se describen básicamente los derechos de las personas de las que se tratan los datos de carácter personal. Se omiten tutela de derechos y derecho de indemnización, ya que no se considera determinante para la finalidad del presente proyecto.

- **Impugnación de valoraciones:** Los ciudadanos no pueden verse sometidos a una decisión con efectos jurídicos, si esta misma está basada en el tratamiento de datos de carácter personal destinados a evaluar determinados rasgos de su personalidad, así mismo tendrán derecho a impugnar actos administrativos que impliquen una evaluación de su comportamiento basada en el tratamiento de datos de carácter personal.

- **Derecho de Consulta al Registro General de Protección de Datos:** El interesado podrá consultar en el registro general de protección de datos la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable de tratamiento.

- **Derecho de acceso:** Los interesados tendrán derecho a solicitar y obtener gratuitamente información acerca de sus datos de carácter personal sometidos a tratamiento, así como el origen de los datos, sus finalidades y las transacciones o comunicaciones de datos que se realicen. El acceso a dichos datos solo se podrá ejercer una vez cada 12 meses, si el interesado no acredite un interés legítimo.

- **Derecho de rectificación y cancelación:** El interesado podrá solicitar la rectificación o cancelación de los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente ley y cuando dichos datos resulten incorrectos. Dicha cancelación dará lugar a un bloqueo de los mismos, conservándolos solo para la atención de las posibles responsabilidades de su tratamiento. El responsable de tratamiento tendrá la obligación de hacer efectivo dicho derecho en el plazo de diez días, así como de notificar la rectificación o cancelación efectuada al responsable del fichero en el caso de que los datos hayan sido previamente comunicados.

- **Procedimiento de oposición, acceso, rectificación y cancelación:** Estos derechos están establecidos reglamentariamente, por lo que no se debe exigir ninguna contraprestación por el ejercicio de los mismos.

TÍTULO IV: Disposiciones Sectoriales

El presente título contempla medidas específicas de diversos ámbitos separados, en lo concerniente a datos de carácter personal, tanto para entidades públicas como privadas.

- **Capítulo I - Ficheros de Titularidad Pública:** En el presente capítulo se establecen las medidas específicas a tomar para el tratamiento de datos de carácter personal en las administraciones públicas.

  Este tipo de entidades solo podrán crear, modificar, o suprimir ficheros de datos de carácter personal si se hace por medio de una disposición general publicada en un diario oficial, como por ejemplo el BOE. Además se especifica concretamente los datos que se deben especificar a la agencia de protección de datos en caso de la creación de un fichero, estos requerimientos se especifican en el Anexo II – Disposiciones para creación de ficheros de titularidad pública. En caso de supresión de fichero, se especifica que se debe establecer el destino de los datos, o en su caso las previsiones que se adopten para su destrucción.

  Del mismo modo, las administraciones públicas no podrán comunicar los datos a otras administraciones para el ejercicio de competencias diferentes o que se basen en competencias distintas a las del establecimiento del fichero, salvo que se establezca lo contrario.

  También se especifican excepciones acerca de los derechos de los afectados, a los que, por ejemplo, se les puede denegar el acceso, la rectificación o la cancelación de sus datos en función de los peligros que se pudieran derivar para la defensa del estado o la seguridad pública entre otras nociones; o en el caso de que sean ficheros responsabilidad de la hacienda pública y se obstaculice actuaciones administrativas que tengan como fin el cumplimiento de obligaciones tributarias.

- **Capítulo II - Ficheros de Titularidad Privada:** Al igual que en el caso de los ficheros de titularidad pública, se especifican en este capítulo las obligaciones concretas acerca de ficheros de titularidad privada.

  En primera instancia, se especifica que solo podrán crearse ficheros de titularidad privada cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que establece la presente ley.

  Para la notificación e inscripción de ficheros de titularidad privada se especifica que se deben notificar a la agencia:
  - El responsable del fichero
  - La finalidad del fichero
  - Ubicación del fichero
  - Tipo de datos de carácter personal que contiene el fichero
  - Las medidas de seguridad adoptadas, niveles básico, medio y alto

- Cesiones de datos de carácter personal
- Transferencias internacionales de datos de carácter personal

Así como los cambios, cuando procedan, que afecten a la finalidad del tratamiento de datos, la identidad de su responsable, o la ubicación de los mismos. Si transcurre un mes desde la notificación sin que la agencia de protección de datos sin que la agencia haya resuelto sobre el mismo, se considerará como inscrito a todos los efectos.

En el caso de que se realice una cesión de datos, se deberá informar a todos los afectados de la finalidad, la naturaleza de los datos cedidos y el nombre y dirección del cesionario.

En el resto del título se van estableciendo condiciones específicas acerca de datos:

- Incluidos en fuentes de acceso público
- Para prestación de servicios de información sobre solvencia patrimonial
- Para tratamientos con fines de publicidad y de prospección comercial
- Para censos promocionales

TÍTULO V: Movimiento internacional de datos

No se podrán realizar transferencias internacionales de datos de carácter personal a países que no puedan garantizar un nivel de protección equiparable al que presta la LO 15/1999; solo se podrán realizar estas transferencias cuando se obtenga una autorización previa del Director de la Agencia de Protección de Datos. En caso de cumplir estos requisitos, el nivel de protección que ofrece el país de destino será evaluado por la Agencia de Protección de Datos.

TÍTULO VI: Agencia de Protección de Datos

Especifica formalmente la naturaleza de la Agencia de Protección de Datos, así como los medios humanos y financieros para desempeñar su función. Establece las funciones concretas de la Agencia, como responsable del cumplimiento del presente texto; por ello, se le otorga además el poder de inspeccionar los ficheros a los que hace referencia la LO 15/1999.

También describe cómo se designará al Director del organismo, las condiciones de la ocupación de dicho cargo; y la designación de un Consejo Consultivo de apoyo al Director, del que se especifican los miembros integrantes del mismo, y su proceso de selección.

Finalmente describe las competencias asignadas a organismos de Protección de Datos correspondientes a las comunidades autónomas, así como la regulación central de los ficheros responsabilidad de cada uno de esos organismos autonómicos.

TÍTULO VII: Infracciones y Sanciones

Los responsables de los ficheros y los encargados de tratamiento son los que están sujetos al régimen sancionador de la presente ley. Se distingue entre el régimen sancionador para entidades privadas y administraciones públicas:

- **Entidades Privadas:** Básicamente se distingue entre tres tipos de infracciones, las leves, las graves y las muy graves. Y en base a esta separación se establecen niveles de sanciones, se muestran los tipos de infracción y sanción en el Anexo III – Infracciones y Sanciones.
- **Administraciones Públicas:** En este caso no se imponen medidas económicas, sino disciplinarias, por las cuales el director de la agencia podrá proponer el inicio de actuaciones de este tipo, de modo que será obligatorio informar a la agencia del resultado de las mismas.

Finalmente, se expone la prescripción de dichas sanciones, y en qué casos se producirán, así como la capacidad de la agencia para inmovilizar un fichero de datos de carácter personal en caso de una infracción muy grave, si se demuestra que se utilicen o cedan datos de carácter personal ilícitamente o que se impida el ejercicio de los derechos de los ciudadanos.

3.2.2. Real decreto 1720/2007 Por el que se aprueba el reglamento de desarrollo de la LO 15/1999

El presente texto, que consta de 158 artículos, constituye un reglamento que desarrolla los requerimientos de la Ley Orgánica 15/1999, que es de obligado cumplimiento en el territorio español.

El Real Decreto 1720/2007 desarrolla las medidas a implantar necesarias para el cumplimiento con la legislación. Es un documento eminentemente más aplicado, del cual se pueden sacar conclusiones de los requerimientos técnicos exigidos.

El texto está organizado en los siguientes apartados:

- TÍTULO I: Disposiciones generales
- TÍTULO II: Principios de Protección de Datos
- TÍTULO III: Derechos de acceso, rectificación, cancelación y oposición
- TÍTULO IV: Disposiciones aplicables a determinados ficheros de titularidad privada
- TÍTULO V: Obligaciones previas al tratamiento de los datos
- TÍTULO VI: Transferencias internacionales de datos
- TÍTULO VII: Códigos tipo
- TÍTULO VIII: De las medidas de seguridad en el tratamiento de datos de carácter personal
- TÍTULO IX: Procedimientos tramitados por la agencia española de protección de datos

A continuación se hará una descripción breve del contenido de cada uno de los puntos del reglamento, acorde a su importancia respecto a la finalidad del presente proyecto. Con

este repaso de busca entender la finalidad del texto y de revisar todos los requisitos que permitan posteriormente analizar su posible aplicación a la herramienta SGSI Tracking.

TÍTULO I: Disposiciones Generales

De forma semejante a la Ley Orgánica 15/1999, en este título se presenta:

- **Objeto:** Desarrollar la Ley Orgánica 15/1999, de 13 de Diciembre de Protección de datos de carácter personal.

- **Ámbito objetivo de aplicación:** Del mismo modo que la LO 15/1999, el ámbito de aplicación abarca los datos de carácter personal registrados en soporte físico susceptibles de tratamiento; el reglamento no alcanzará a los ficheros integrados por personas jurídicas, así como las agendas de contactos profesionales.

- **Ámbito territorial de aplicación:** Se aplicará el presente reglamento al tratamiento de ficheros en el establecimiento del encargado de tratamiento, siempre y cuando el establecimiento de encuentre en territorio español.

- **Ficheros o tratamientos excluidos:** No será de aplicación a los siguientes ficheros o tratamientos:
    a) Ficheros realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
    b) A los sometidos a la normativa sobre protección de materias clasificadas.
    c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

- **Definiciones:** Se detallan las definiciones incluidas en el reglamento en el Anexo IV – Definiciones RD 1720/2007.

- **Fuentes accesibles al público:** Se consideran fuentes accesibles al público:
    a) El censo promocional
    b) Guías de servicios de comunicaciones electrónicas
    c) Listas de personas que pertenecen a grupos profesionales (Colegios profesionales)
    d) Diarios y boletines oficiales
    e) Medios de comunicación social

TÍTULO II: Principios de Protección de Datos

En el presente título se presentan los principios fundamentales de protección de datos referentes al regalemento.

- **Calidad de los datos:** Los contenidos de este apartado, aunque ampliados, se encuentran descritos en el punto de calidad de los datos de la LO 15/1999.

- **Consentimiento para el tratamiento de los datos y el deber de información:** Como se mencionaba en el correspondiente artículo del RD 1720/2007, se debe obtener el consentimiento del interesado antes de comenzar el tratamiento de los datos, esta solicitud debe hacer referencia a un tratamiento o serie de tratamientos concretos y sus condiciones.

  En caso de que se quiera realizar tratamiento de datos de carácter personal de menores de edad, se consideran los siguientes casos:

  a) Mayores de 14 años: Podrán prestar su consentimiento, no será necesaria la aprobación de sus padres o tutores.
  b) Menores de 14 años: Será necesario el consentimiento de los padres o tutores en cualquier caso.

  No se podrán recoger datos de menores que permitan obtener información sobre los demás miembros del grupo familiar, o sus características. Corresponderá al responsable del fichero garantizar que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado.

  El consentimiento se podrá recabar siguiendo el siguiente procedimiento:

  a) Se debe informar en los términos previstos en Derecho de Información de la LO 15/1999, y se le debe de otorgar un plazo de treinta días para manifestar su negativa al tratamiento, avisándole de que en caso de no pronunciarse se entenderá que lo consiente.
  b) Será necesario que el responsable del fichero pueda conocer si la notificación ha sido devuelta. En ese caso no podrá proceder al tratamiento de los datos.
  c) Debe facilitarse al afectado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos.
  d) Una vez solicitado el consentimiento, no podrá volver a solicitarse hasta que transcurra un año a contar de la fecha de la anterior solicitud.

  El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ningún gasto. En el caso de que se produzca esta solicitud, el responsable de tratamiento cesará en el tratamiento de los datos en un plazo máximo de 10 días.

- **Encargado del tratamiento:** El acceso a los datos por parte de un encargado de tratamiento no se considerará comunicación de datos si se cumplen los requisitos establecidos en la LO 15/1999 y el RD 1720/2007. Cuando el responsable de tratamiento contrate una prestación de servicio que comporte un tratamiento de datos deberá comprobar que el encargado de tratamiento garantice el cumplimiento de lo establecido en el presente reglamento. En caso de que el encargado de tratamiento trate los datos a otra finalidad, o los utilice incumpliendo las estipulaciones del contrato establecido, será considerado responsable de tratamiento, respondiendo a las infracciones en las que haya incurrido personalmente. Finalmente cabe destacar que una vez finalizada dicha relación contractual el encargado de tratamiento debe destruir o devolver los datos de carácter personal correspondientes. El encargado de tratamiento deberá conservar, bloqueados, los datos de los que se pudieran derivar responsabilidades respecto a su relación con el encargado de tratamiento.

TÍTULO III – Derechos de acceso, rectificación, cancelación y oposición

En este título del reglamento se extiende lo establecido en la LO 15/1999 de datos de carácter personal, se mencionan, por tanto, requisitos y cuestiones añadidas a lo antes mencionado.

- **Disposiciones generales:** Los derechos ARCO son personalísimos y solo pueden ser ejercidos por el afectado o su representante legal o autorizado. Para ello, se deberá conceder un medio sencillo y gratuito al afectado para ejercerlos; así mismo, el responsable del fichero deberá atender la solicitud aunque el interesado no haya empleado el medio puesto a su disposición, siempre que permita acreditar el envío y recepción de la solicitud. Será necesario que dicha solicitud incluya:
    a) Nombre y Apellidos del Interesado
    b) Petición que se concreta en la solicitud
    c) Dirección a efectos de notificaciones, fecha y firma del solicitante
    d) Documentos acreditativos de la petición que formula, en su caso.

  El responsable de fichero responderá, se posean o no datos del interesado, a cualquier solicitud; así como requerirá los datos necesarios en caso de recibir una solicitud incompleta. En caso de ejercitar los derechos ante un encargado de tratamiento, deberá dar el traslado de la solicitud al responsable, para que resuelva la solicitud de derechos ARCO.

- **Derecho de acceso:** Es el derecho del afectado a obtener información de que si sus propios datos:
    a) Si sus datos de carácter personal están siendo objeto de tratamiento.
    b) La finalidad del tratamiento.
    c) Información disponible acerca del origen de dichos datos.
    d) Comunicaciones realizadas o previstas de los mismos.
    e) Datos personales almacenados, bien de un determinado fichero, bien su totalidad.

  Cuando se realice el derecho de acceso, el interesado podrá elegir entre recibir la información a través de uno de los siguientes medios:
    a) Visualización en pantalla
    b) Escrito
    c) Telecopia
    d) Correo electrónico
    e) Cualquier otro sistema adecuado a la configuración o implantación del fichero, o la naturaleza del tratamiento.

  Una vez recibida una solicitud adecuada, el responsable del fichero la deberá resolver en el plazo máximo de un mes a contar desde su recepción. Deberá responder de forma legible e ininteligible, sin emplear claves o códigos que requieran el uso de dispositivos mecánicos específicos. Finalmente, el responsable del tratamiento podrá denegar el ejercicio de los derechos de acceso si se ha ejercido en los doce meses

anteriores a la solicitud o si así lo establece una ley o norma; en este caso deberá informar al afectado de su derecho de solicitar la tutela de la Agencia de Protección de Datos.

- **Derechos de rectificación y cancelación:** Son, respectivamente, los derechos de modificar los datos inexactos o incorrectos, y de suprimir los datos que resulten ser inadecuados o excesivos. Ambas solicitudes deberán indicar a que datos se refiere y deberá ir acompañada de la documentación necesaria para su justificación. El responsable del fichero debe responder a la solicitud en un plazo máximo de diez días.
  El responsable de tratamiento podrá denegar la cancelación cuando los datos de carácter personal deban ser conservados de forma obligatoria o en relaciones contractuales entre la persona y la entidad responsable. Del mismo modo que en el derecho de acceso, el responsable informará al interesado de su derecho de recabar la tutela de la Agencia de Protección de Datos.

- **Derecho de oposición:** Derecho del afectado a que no se lleve a cabo el tratamiento de sus datos en los siguientes casos:
  a) Cuando no sea necesario su consentimiento para el tratamiento.
  b) Cuando se trate de ficheros que tengan como finalidad la realización de actividades de publicidad.
  c) Cuando el tratamiento tenga por finalidad de adoptar una decisión sobre el interesado solo tratando sus datos de carácter personal.

  Del mismo modo que en los apartados anteriores, el derecho de oposición se realizará mediante solicitud al responsable de tratamiento, que deberá responder en un plazo inferior a diez días. El responsable de tratamiento deberá excluir del tratamiento los datos del afectado o denegar motivadamente la solicitud.

TÍTULO IV: Disposiciones aplicables a determinados ficheros de titularidad privada

El presente título regula casos particulares en materia de ficheros de titularidad privada, atendiendo a casuísticas concretas que requieren una especial atención.

- **Ficheros de información sobre solvencia patrimonial y crédito:** El ejercicio de los derechos ARCO en el caso de estos ficheros se rige por el TÍTULO III del presente reglamento, con las siguientes consideraciones:
  a) Si la petición se dirige al responsable del fichero, está obligado a satisfacerla en cualquier caso.
  b) Si la petición se dirige a las personas o entidades a las que se presta el servicio, solo deberán comunicar al afectado los datos relativos al mismo, así como facilitar la identidad del responsable.
  c) Pueden tratarse datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor, o por quién actúe por su cuenta o interés.

Solo se podrá incluir en estos ficheros datos determinantes para enjuiciar la solvencia económica del afectado, cumpliendo lo siguientes requisitos:

a) Existencia previa de deuda cierta, vencida, exigible, que haya resultado impagada.
b) Que no hayan pasado seis años desde la fecha en que se debería haber realizado el pago.
c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

El responsable del fichero deberá informar a los interesados de los cuales se registren datos en el plazo de treinta días desde dicho registro. Se deberá realizar una notificación por cada deuda concreta mediante un medio fiable, auditable e independiente.

Solo podrán tratarse datos que correspondan con la deuda en cada momento concreto, el pago o cumplimiento de la misma implicará la cancelación de dichos datos, o se cancelarán cuando hayan transcurrido seis años de la fecha establecida para el pago. Los terceros podrán acceder a la información contenida en estos ficheros cuando:

a) El afectado mantenga con el tercero algún tipo de relación contractual no vencida.
b) El afectado pretenda celebrar un contrato con el tercero que implique el pago aplazado del precio.
c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

A continuación se detallan peculiaridades acerca del ejercicio de los derechos ARCO sobre este tipo de ficheros, esto no contradice lo enunciado en el TÍTULO III:

- Derechos de acceso:
  - Si la solicitud se dirige al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos del mismo.
  - Si la solicitud se realizara a cualquier otra entidad participante, deberá comunicar al mismo todos los datos relativos al mismo a los que pueda acceder, así como la identidad y dirección del titular del fichero común.
- Derechos de Rectificación y Cancelación:
  - Si la solicitud se dirige al titular del fichero común, éste tomará las medidas necesarias para trasladar dicha solicitud a la entidad que haya facilitado los datos.
  - Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación del fichero común y a notificarlo al titular del fichero común y al interesado en un plazo de diez días.
  - Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad

informará al afectado sobre este hecho en un plazo máximo de diez días.

- **Tratamientos para actividades de publicidad y prospección comercial:** Aquellos que se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, etc. Sólo podrán utilizar nombres y direcciones de los afectados solo cuando:
    a) Figuren en fuentes accesibles al público. En este caso se debe informar en cada comunicación el origen de los datos y la identidad del responsable de tratamiento, así como de los derechos que le asisten y ante quien se podrán ejercer.
    b) Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

  En caso de que la entidad contrate o encomiende a terceros la realización de una campaña publicitaria, debe cumplir las siguientes normas:
    a) Cuando los parámetros identificativos sean fijados por la entidad que contrate la campaña, será responsable del tratamiento de los datos.
    b) Cuando los parámetros identificativos sean fijados por la entidad contratada, será responsable del tratamiento de los datos.
    c) Cuando intervengan ambas entidades, ambas serán responsables del tratamiento.

  Se considerarán parámetros identificativos a las variables utilizadas para identificar el público objetivo de la campaña. Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán almacenar los mínimos datos posibles para identificarlo y así evitar el envío de publicidad.

TÍTULO V: Obligaciones previas al tratamiento de datos

Describe las obligaciones a seguir tanto por entidades públicas como privadas previas al tratamiento de datos de carácter personal.

- **Creación, modificación o supresión de ficheros de titularidad pública:** Debido a que la herramienta SGSI Tracking no está concebida para entidades públicas, se obvia el presente punto del reglamento.

- **Notificación e inscripción de los ficheros de titularidad pública o privada:** Los ficheros de titularidad pública serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. Dicha notificación deberá incluir:
    a) La identificación del responsable del fichero
    b) La identificación del fichero, sus finalidades y usos previstos
    c) Sistema de tratamiento empleado
    d) Colectivo de personas del que se obtienen los datos
    e) Procedimiento y procedencia de los datos

f) Categorías de datos
g) Indicación de nivel de seguridad exigible
h) Identificación del encargado de tratamiento, si procede
i) Destinatarios de cesiones o transferencias internacionales de datos

La notificación es independiente del sistema de tratamiento empleado en su organización y del soporte empleado para el tratamiento de los datos, cuando un fichero esté almacenado en soportes automatizados y no automatizados, solo será necesaria una notificación referida al fichero correspondiente. La inscripción del fichero debe encontrarse siempre correctamente actualizada, antes de realizar cualquier cambio que afecte al contenido de la inscripción o supresión de un fichero debe ser notificado a la agencia previamente.

En la parte final del título se mencionan las competencias de oficio de la Agencia de Protección de Datos acerca de la inscripción, cancelación y rectificación de ficheros a instancia de los interesados, con el fin de regular y proteger los datos de carácter personal.

TÍTULO VI: Transferencias internacionales de datos

El presente título establece las obligaciones en el caso de que se tengan que realizar transferencias internacionales de datos, así como la obligación del responsable del fichero de evaluar el nivel de protección que ofrece el país destino de la transferencia.

- **Disposiciones generales:** Para cualquier transferencia internacional de datos será necesaria la autorización del Director de la Agencia de Protección de Datos, que solo otorgará si el exportador de datos da las garantías necesarias. No será necesaria la autorización si:
  a) El estado del importador ofrece un nivel adecuado de protección
  b) Cuando la transferencia incurra en alguna de las excepciones contempladas en la LO 15/1999.

- **Transferencias a estados que proporcionen un nivel adecuado de protección:** En este caso no se precisará la autorización expresa del director de la agencia. Estos niveles deben ser estimados por la agencia, que publicará y mantendrá actualizada una lista de países cuyo nivel de protección se considere equiparable a lo requerido por el RD 1720/2007. En cualquier momento, el director de la Agencia Española de Protección de Datos, podrá suprimir la transferencia de datos cuando:
  a) Las autoridades del estado del importador de datos determinen que éste ha vulnerado las normas de protección de datos establecidas en su país.
  b) Si existen indicios razonables de que se están vulnerando las normas de protección de datos, y las autoridades del estado del importador no han adoptado ni adoptarán medidas para resolver la situación.

- **Transferencias a estados que no proporcionen un nivel adecuado de protección:** Se requerirá la autorización del director de la Agencia Española de Protección de Datos,

para su concesión, se requerirá un contrato escrito por el cual tanto importador como exportador asuman las responsabilidades para salvaguardar la vida privada de los afectados y sus derechos y libertades fundamentales. Se consideran también situaciones en las cuales, el director podrá revocar dicha transferencia de datos.

TÍTULO VII: Códigos tipo

Los códigos tipo básicamente consisten en acuerdos o convenios para regular y armonizar los tratamientos de datos correspondientes a distintos ámbitos. Estos códigos tipo deben establecer condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal. Estos códigos se considerarán de buena práctica profesional, y serán vinculantes para los que se adhieran a los mismos.

Los códigos tipo son de carácter voluntario, y podrán hacer referencia a la totalidad o una parte de los tratamientos realizados por entidades pertenecientes a un mismo sector; por lo que deberán ser formulados por entidades representativas de dicho sector. Los códigos tipo:

- Deben estar redactados en términos claros y accesibles
- Deben respetar la norma vigente e incluir:
    a) Ámbito de aplicación
    b) Previsiones para la aplicación de los principios de protección de datos
    c) Establecer estándares homogéneos para el cumplimiento de la LO 15/1999
    d) Establecer procedimientos para el ejercicio de derechos ARCO
    e) Establecer cesiones y transferencias internacionales que se prevean
    f) Formación en materia de protección de datos de quienes los traten
    g) Mecanismos de supervisión de cumplimiento de los adheridos al código tipo
    h) Cláusulas tipo para obtener el consentimiento de los afectados
    i) Cláusulas tipo para informar a los afectados
    j) Modelos para el ejercicio de los derechos ARCO
    k) Modelos de cláusulas de cumplimiento por parte de encargados de tratamiento

TÍTULO VIII: De las medidas de seguridad en el tratamiento de datos de carácter personal

El presente título representa la parte más técnica del reglamento, establece las medidas de seguridad para los datos, definiendo niveles de protección correspondientes a cada tipología de datos, ordenando respecto a la sensibilidad de los mismos; asignando finalmente las tipologías a unas medidas de seguridad adecuadas.

Disposiciones generales

Los responsables y encargados de tratamiento deben implantar las medidas de seguridad necesarias de acuerdo al presente título, sea cual sea el sistema de tratamiento. Para ello se establecen tres niveles en los tipos de datos:

- **Nivel Básico:** Todos los ficheros se consideran de nivel básico, por lo que todos los ficheros deben cumplir las medidas de seguridad de nivel básico.

- **Nivel Medio:** Aplican todas las medidas de nivel básico y medio, se consideran ficheros de nivel medio, los que incluyan:
    a) Datos de infracciones administrativas o penales
    b) Datos de solvencia patrimonial y crédito
    c) Datos tributarios y financieros
    d) Datos responsabilidad de entidades gestoras y servicios comunes de la seguridad social, así como datos responsabilidad de mutuas de accidentes laborales y enfermedades profesionales
    e) Datos que ofrezcan una definición de características o personalidad de los ciudadanos

- **Nivel Alto:** Aplican todas las medidas de nivel básico, medio y alto, se consideran ficheros de nivel alto aquellos que incluyan:
    a) Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual
    b) Datos recabados con fines policiales, sin el consentimiento del afectado
    c) Datos derivados de la violencia de género

Como excepciones destacables a mencionar, a los ficheros responsabilidad de operadores de comunicaciones electrónicas o que exploten redes públicas respecto de datos de tráfico, aplicarán, además de las medidas de nivel básico y medio, las correspondientes al registro de accesos de las medidas de seguridad de nivel alto; del mismo modo, se podrán implantar medidas de seguridad de nivel básico a ficheros que contengan datos de salud, referentes únicamente al grado de minusvalía o discapacidad, para el cumplimiento de deberes públicos.

Cuando se trata de las obligaciones técnicas a cumplir con terceros que, bien tratan los datos, bien acceden a ellos para realizar una función alternativa al tratamiento de los mismos, se debe tener en cuenta:

- **Encargado del tratamiento:** Cuando el responsable del fichero permita el acceso a datos de carácter personal y que preste servicio en los locales del responsable o de forma remota, este hecho deberá hacerse constar en el documento de seguridad, además de hacer cumplir al personal del encargado al cumplimiento de las medidas de seguridad previstas. En cambio, si el encargado presta servicio en sus propias instalaciones, deberá elaborar su pertinente documento de seguridad.

- **Prestadores de servicios sin acceso a datos personales:** El responsable del fichero tomará las medidas necesarias para evitar el acceso del personal del prestador de servicios a los datos de carácter personal. Se establecerá un contrato con el prestador que recoja expresamente la prohibición de acceder a los datos de carácter personal y la obligación de secreto respecto a los datos que se hayan podido conocer durante la prestación del servicio.

Se debe hacer constar en el documento de seguridad las delegaciones de autorizaciones que se realicen sobre las personas habilitadas a autorizar, así como las que son autorizadas. En ningún caso esta designación implica la delegación de las responsabilidades del responsable del fichero.

Se establece también que los accesos a datos de carácter personal a través de redes de comunicaciones deberán de garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Del mismo modo, cuando se realice el tratamiento de datos en dispositivos portátiles o fuera de las instalaciones del responsable o encargado, esta circunstancia se deberá hacer constar en el documento de seguridad, así como se deberán tomar las medidas de seguridad pertinentes.

Finalmente se establece que los ficheros temporales o copias de documentos creadas exclusivamente para realizar trabajos temporales deben cumplir los niveles de seguridad igualmente.

Del documento de seguridad

El responsable de fichero o encargado de tratamiento deberá elaborar un documento de seguridad que recoja las medidas de índole técnica y organizativa de obligatorio cumplimiento para el personal de la entidad. El documento de seguridad puede ser único, haciendo referencia a todos los ficheros registrados, aunque se permite elaborar diversos documentos de seguridad atendiendo a criterios organizativos.

El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por este reglamento
c) Funciones y obligaciones del personal respecto a datos de carácter personal
d) Estructura de los datos de carácter personal y descripción de los sistemas que los soportan
e) Procedimiento de gestión de incidencias
f) Procedimiento de copias de respaldo
g) Medidas a tomar para el transporte y destrucción de soportes o documentos

Si el documento de seguridad aplica medidas de nivel medio o alto, deberá contener, además:

a) Identificación del responsable de seguridad
b) Controles periódicos necesarios para cumplir lo citado en dicho documento

El documento de seguridad deberá mantenerse actualizado en todo momento, y será revisado cuando se realicen cambios sustanciales en el sistema de información de la entidad. Un cambio se considerará relevante siempre y cuando pueda desembocar en un incumplimiento de las medidas de seguridad.

Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Medidas de Seguridad de Nivel Básico

- **Funciones y obligaciones del personal:**
  - Se deben establecer las funciones y obligaciones de todos los usuarios o perfiles de usuario con acceso a datos de carácter personal, reflejándolas en el documento de seguridad.
  - El responsable del fichero se encargará de que el personal conozca las normas de seguridad respecto a datos de carácter personal, así como las responsabilidades de su incumplimiento.

- **Registro de incidencias:**
  - Debe existir un procedimiento de notificación y gestión de incidencias de datos de carácter personal, así como establecer un registro en el que figure:
    - Tipo de incidencia
    - Momento en el que se ha producido
    - Persona que realiza la notificación
    - Persona que gestiona la incidencia
    - Efectos derivados de la incidencia
    - Medidas aplicadas

- **Control de acceso:**
  - Los usuarios solo tendrán acceso a los recursos necesarios para desempeñar su función.
  - Se debe crear y mantener un listado actualizado de usuarios y perfiles, así como los accesos autorizados para cada uno.
  - Se establecerán medidas para que los usuarios no puedan acceder a recursos distintos de los autorizados.
  - Solo el personal especificado en el documento de seguridad estará capacitado para otorgar autorización de acceso a los recursos.
  - En caso de haber personal externo con acceso a los recursos deberá estar sometido a las mismas obligaciones de seguridad que el personal propio.

- **Gestión de soportes y documentos:**
  - Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, estar inventariados y que solo sean accesibles por el personal autorizado en el documento de seguridad. En caso de contener información sensible se podrán etiquetar de forma que sean fáciles de identificar por el personal autorizado a su acceso, y que dificulte la identificación en el resto de los casos.
  - Cualquier salida de soportes y documentos, incluidos los anexos de correo electrónico, deberán ser autorizados por el responsable de fichero o encontrarse autorizada en el documento de seguridad.
  - Cuando se traslade documentación se adoptarán medidas dirigidas a evitar su sustracción, pérdida y acceso no autorizado.

  - Cuando se desechen soportes que contengan datos de carácter personal deben ser debidamente destruidos, evitando el acceso a la información contenida en el mismo, o su recuperación.

- **Identificación y autentificación:**
  - Se deben implantar medidas que garanticen la correcta identificación y autentificación de los usuarios.
  - Se establecerá un mecanismo que permita la identificación inequívoca de los usuarios que intenten acceder al sistema de información.
  - Si el mecanismo de identificación está basado en contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento de contraseñas, para garantizar su confidencialidad e integridad.
  - Se establecerá en el documento de seguridad la periodicidad del cambio de contraseñas, que en ningún caso debe ser superior a un año.

- **Copias de respaldo y recuperación:**
  - Deben existir procedimientos de actuación para la realización de copias de seguridad con una periodicidad, como mínimo, semanal.
  - Deben existir procedimientos para la recuperación de los datos, garantizando en todo momento su reconstrucción.
  - Se deberán verificar cada seis meses los procedimientos anteriores.
  - Las pruebas anteriores a la implantación de sistemas de información no se realizarán con datos reales, salvo que sea imprescindible; en tal caso, se realizan copias de seguridad antes de las pruebas.

Medidas de Seguridad de Nivel Medio

- **Responsable de Seguridad:**
  - Se deberán designar en el documento de seguridad uno o varios responsables de seguridad, esta designación no supone que el responsable asuma las responsabilidades que corresponden al responsable del fichero, o al encargado de tratamiento, en su caso.

- **Auditoría:**
  - Los sistemas de información deberán someterse, de forma obligatoria, a una auditoría interna que verifique el cumplimiento del RD 1720/2007 cada dos años.
  - De forma extraordinaria se realizará una auditoria siempre que se produzcan cambios sustanciales en el sistema de información, y esto pueda revertir en el incumplimiento de las medidas de seguridad implementadas.

- **Gestión de soportes y documentos:**
  - Mantener un registro de entrada y salida de soportes, que permita conocer:
    - Tipo de documento
    - Fecha y hora

        - Emisor (entrada)
        - Receptor (salida)
        - Número de documentos o soportes
        - Tipo de información que contienen
        - Forma de envío
        - Responsable del envío/recepción, debidamente autorizado

- **Identificación y autentificación:**
    - El responsable deberá implementar un sistema que limite el número de intentos de acceso al sistema de información. Si el método de identificación está basado en contraseñas se fijará un bloqueo de cuenta tras cierto número de intentos en un periodo de tiempo.

- **Control de acceso físico:**
    - Solo el personal autorizado en el documento de seguridad tendrá acceso a los lugares donde se encuentren físicamente los sistemas de información.

- **Registro de Incidencias:**
    - A los registros de incidencias establecidos en las medidas de seguridad de nivel básico, hay que añadir los procedimientos empleados para realizar una recuperación de datos, así como la persona que realizó la tarea. Se requerirá para ello, una autorización del Responsable de Seguridad.

Medidas de Seguridad de Nivel Alto

- **Gestión y distribución de soportes:**
    - Se deben etiquetar los soportes de forma que sean fáciles de identificar por el personal autorizado a su acceso, y que dificulte la identificación en el resto de los casos.
    - La distribución de soportes que contengan datos de carácter personal de nivel alto se realizarán cifrando su contenido, o empleando otro mecanismo que garantice que dicha información no sea accesible en su traslado.

- **Copias de respaldo y recuperación:**
    - Se deberá mantener una copia de seguridad de los datos y los procedimientos en una ubicación alternativa a la que se realiza el tratamiento.

- **Registro de Accesos:**
    - De cada intento de acceso a los sistemas de información se registrará, como mínimo:
        - Identificación de usuario
        - Fecha y hora
        - Fichero accedido
        - Tipo de acceso
        - Autorizado o denegado

        - Registro accedido (en caso de ser autorizado)
    - Este registro deberá mantenerse como mínimo un periodo de dos años
    - El Responsable de Seguridad se encargará de revisar al menos una vez al mes el registro de acceso, para elaborar un informe de las revisiones realizadas y los problemas detectados.
    - No será necesario el registro de acceso en las siguientes condiciones:
        - Si el responsable del fichero es una persona física
        - Si el responsable del fichero o tratamiento garantiza que únicamente él tiene acceso al fichero.

- **Telecomunicaciones:**
    - Cuando se realice transmisión de datos de carácter personal de nivel alto a través de redes públicas, se realizarán cifrando los datos.

Medidas de seguridad aplicables a ficheros y tratamientos no automatizados

Medidas de seguridad de nivel básico

- **Obligaciones comunes:**
    - A los ficheros no automatizados se les aplicará lo dispuesto en el presente título en:
        - Disposiciones Generales:
            - Alcance
            - Niveles de seguridad
            - Encargado de tratamiento
            - Prestaciones de servicios sin acceso a datos personales
            - Delegación de autorizaciones
            - Régimen de trabajo fuera de los locales del responsable del fichero o encargado de tratamiento
        - Del Documento de Seguridad
        - Medidas de seguridad aplicables a ficheros y tratamientos automatizados:
            - Funciones y obligaciones del personal
            - Registro de incidencias
            - Control de acceso
            - Gestión de soportes

- **Criterios de archivo:**
    - Se archivará la documentación de acuerdo a la legislación respectiva, éstos criterios deben garantizar la conservación, la localización y acceso, para poder posibilitar el ejercicio de los derechos ARCO.
- **Dispositivos de almacenamiento:**
    - Los dispositivos que almacenen documentación que contenga datos de carácter personal deberán poseer un mecanismo de cierre. Si no es posible, el

responsable de seguridad establecerá medidas para impedir el acceso al personal no autorizado.

- **Custodia de soportes:**
  - En el periodo de tiempo en el que la documentación no se encuentre archivada, estando al uso, la persona que esté al cargo de dicha documentación debe custodiarla y evitar accesos no autorizados a la misma.

Medidas de seguridad de nivel medio

- Responsable de seguridad: Correspondiente a las medidas de seguridad de nivel medio para ficheros automatizados.

- Auditoría: Correspondiente a las medidas de seguridad de nivel medio para ficheros automatizados.

Medidas de seguridad de nivel alto

- **Almacenamiento de la información:**
  - Los dispositivos de almacenamiento de documentación se deberán encontrar en áreas de acceso restringido, mediante llave o cualquier mecanismo equivalente. Deberán permanecer cerradas mientras no sea necesario el acceso a los documentos.
  - Si no fuera posible cumplir con lo solicitado previamente, de deberán tomar medidas alternativas, que deberán figurar en el documento de seguridad.

- **Copia o reproducción:**
  - Solo podrán realizar copias de documentos el personal debidamente autorizado en el documento de seguridad.
  - Una vez finalizado el periodo de empleo de las mismas, se destruirán para evitar el acceso a la información contenida en la misma, o su recuperación posterior.

- **Acceso a la documentación:**
  - El acceso a la documentación se limitará al personal autorizado.
  - Se establecerán mecanismos que permitan registrar el acceso a la documentación en el caso de que pueda ser accedida por múltiples usuarios.
  - El acceso a personas no autorizadas en el documento de seguridad deberá registrarse de acuerdo al documento de seguridad.

- **Traslado de documentación:**
  - Cuando se traslade documentación se deberán adoptar medidas para evitar el acceso o sustracción de la misma.

TÍTULO IX: Procedimientos tramitados por la agencia española de protección de datos

El presente título establece el procedimiento de actuación de la agencia de protección de datos en referencia a las competencias asignadas a la misma. Concretamente se describen procedimientos para:

- Procedimientos relativos al ejercicio de la potestad sancionadora
- Procedimientos relacionados con la inscripción o cancelación de ficheros
- Procedimientos relacionados con las transferencias internacionales de datos
- Procedimiento de inscripción de códigos tipo
- Otros procedimientos:
    - Procedimiento de exención del deber de información al interesado
    - Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos

Los procedimientos no se describen en profundidad ya que no se los considera de vital importancia para la consecución del presente proyecto.

3.3.Requisitos de la norma ISO/IEC 27001:2005

Como se describió en la introducción, la norma ISO/IEC 27001:2005 es un estándar para la implantación de un Sistema de Gestión de Seguridad de la Información (en adelante SGSI). Para desarrollar el análisis de los requisitos de la misma nos basaremos fundamentalmente en dos textos:

- Norma ISO/IEC 27001, norma certificable que establece los requisitos y controles aplicables de un SGSI.
- Norma ISO/IEC 17799 (también conocida como ISO/IEC 27002), norma no certificable que constituye un código de buenas prácticas, sobre el que se establecieron los controles del anexo A de ISO/IEC 27001.

A continuación se analiza la norma ISO/IEC 27001, basándonos en las recomendaciones establecidas en la ISO/IEC 17799.

3.3.1. Norma ISO/IEC 27001

La norma ISO/IEC 27001 es un documento organizado en 8 capítulos y 3 anexos. Supone, como se ha dicho con anterioridad una norma certificable en materias de seguridad en las tecnologías de la información.

El texto se encuentra organizado en los siguientes apartados:

0. Introducción
1. Objeto y campo de aplicación
2. Normas para consulta
3. Términos y definiciones
4. Sistema de Gestión de Seguridad de la Información
5. Responsabilidad de dirección
6. Auditorías internas del SGSI
7. Revisión del SGSI por dirección
8. Mejora del SGSI

A. Anexo A: Objetivos de control y controles
B. Anexo B: Los principios de la OCDE y esta norma internacional
C. Anexo C: Correspondencia entre las normas ISO 9001:2000, ISO 14001:2004 y esta norma internacional.

A continuación se realizará un análisis completo de los requisitos de la norma, para al final, poder evaluar su aplicación a la herramienta SGSI Tracking, se sigue la numeración de la norma ISO/IEC 27001 para facilitar su referencia.

0. Introducción

La norma ISO 27001 implementa un proceso para la creación, implementación operación, supervisión, revisión mantenimiento y mejora de un SGSI. Este proceso dependerá

de las necesidades, objetivos, medios, requisitos de seguridad, procesos, tamaño y estructura de la organización.

En la norma se propone un enfoque por proceso para el establecimiento completo del SGSI en la organización. Para que una organización funcione adecuadamente se deben definir y gestionar numerosas actividades, cualquier actividad que gestione unas entradas y produzca unas salidas se puede entender como un proceso. La identificación y aplicación de un conjunto de procesos a una organización, así como la identificación de sus interacciones, se puede considerar enfoque a proceso. De este modo, en materia de seguridad de la información se establecen las siguientes directivas:

a) Comprender los requisitos de seguridad de la información de la organización, así como la necesidad de establecer una política de seguridad de la información
b) Implementar y operar controles para administrar los riesgos de seguridad de la información
c) Supervisar y revisar el rendimiento y la eficacia del SGSI
d) Asegurar la mejora continua sobre la base de la medición objetiva

Como se mencionó en la introducción, esta norma sigue el modelo PDCA, aplicándolo sobre todos los procesos del SGSI. Además, proporciona un estándar robusto para establecer las directrices que rigen la evaluación de riesgos de seguridad de la información, así como el diseño, implementación, gestión y reevaluación de la seguridad.

Finalmente, cabe destacar que ISO/IEC 27001:2005 es compatible con las normas:

- ISO 9001:2000
- ISO 14001:2004

Asegurando una implementación integrada y consistente de todos los sistemas. En la norma se referencia a una tabla de relación entre capítulos de las 3 normas con el fin de facilitar la integración, puesto que no se considera relevante para el objeto del presente proyecto, no se incluye en la memoria.

1. *Objeto y campo de aplicación*

La norma ISO 27001 establece los requisitos para crear, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI.

Se puede aplicar a todo tipo de organizaciones, al ser una norma adaptable a los requisitos empresariales concretos; pudiendo realizar una selección de controles de seguridad seleccionados en base a un análisis de riesgos empresariales. Es importante destacar que los requisitos definidos en los puntos 4, 5, 6, 7 y 8 no se podrán excluir de ninguna organización.

Toda exclusión de controles necesarios para cumplir con los criterios de aceptación del riesgo debe ser justificada mediante la aceptación de los riesgos por parte de las personas responsables. Sin embargo, la certificación solo se entregará si se considera que dichas exclusiones no afecten a la capacidad de asegurar la seguridad de la información en la entidad.

2. *Normas para consulta*

Se cita la norma ISO 17799 como indispensable para la aplicación de la presente norma.

3. *Términos y definiciones*

Se citan los términos y definiciones correspondientes al presente punto en el Anexo V – Términos y definiciones ISO/IEC 27001:2005.

4. *Sistema de Gestión de Seguridad de la Información*

En el presente punto se fijan las acciones necesarias que ha de realizar la organización en la creación y el arranque y mantenimiento de un SGSI en cada una de las fases del ciclo PDCA. Se citan a continuación las fases con sus requerimientos más relevantes para la consecución de la presente memoria.

Creación y gestión del SGSI

Creación del SGSI

- Definir el **alcance y los límites del SGSI**, siempre basándose en la actividad empresarial. Se deben aportar detalles y justificación de cualquier exclusión del alcance.
- Definir una **política del SGSI** acorde a los requisitos empresariales, que:
  - Provea mecanismos para fijar objetivos y establezca unos principios de actuación en materia de seguridad de la información.
  - Tenga en cuenta todos los requisitos empresariales, legales, reglamentarios y derivados de relaciones contractuales.
  - Comprenda la estrategia de gestión de riesgos.
  - Establezca criterios para evaluar los riesgos.
  - Sea aprobada por dirección.
- Definir el **enfoque de evaluación de riesgos**:
  - Especificar una metodología de evaluación de riesgos adecuada.
  - Desarrollar los criterios de aceptación del riesgo y los niveles de riesgo asumibles.

- **Identificar los riesgos**:
  - Identificar los activos y sus propietarios dentro del SGSI y del alcance.
  - Identificar las amenazas que afectan a dichos activos.
  - Identificar las vulnerabilidades bajo las que podrían actuar dichas amenazas
  - Identificar el impacto que tendría sobre los activos una pérdida de:
    - Confidencialidad
    - Integridad
    - Disponibilidad
- **Analizar y valorar los riesgos**:
  - Evaluar los efectos de fallos de seguridad en la actividad empresarial.
  - Evaluar la probabilidad de que se provoquen los fallos de seguridad.
  - Estimar los niveles de riesgo.
  - Determinar si los riesgos son aceptables o requieren un tratamiento en función del criterio de aceptación de riesgo.
- Identificar y evaluar las **opciones para el tratamiento de riesgos**, las posibles acciones a realizar son:
  - Aplicar los controles adecuados.

  - Asumir los riesgos de manera consciente y objetiva, de acuerdo a la política de seguridad de la información.
  - Evitar los riesgos.
  - Transferir los riesgos a otras partes, como proveedores de servicios.
- **Seleccionar objetivos de control y controles** para el tratamiento de riesgos, para cumplir los requisitos identificados en la evaluación y el tratamiento de riesgos. Los objetivos de control y controles del Anexo A deben seleccionarse en la medida que sirvan para satisfacer los objetivos seleccionados.
- Obtener la **aprobación por dirección de los riesgos residuales** propuestos.
- Obtener la **aprobación por dirección para implementar y operar el SGSI**.
- Elaborar una declaración de aplicabilidad (SOA) que incluya:
  - Objetivos de control y controles seleccionados
  - Objetivos de control y controles implementados actualmente.
  - Exclusión de cualquier objetivo de control o control, acompañado de su debida justificación.

Implementación y operación del SGSI:

La organización debe:

- **Formular un plan de tratamiento de riesgos** para gestionar los riesgos de seguridad de la información.
- **Implementar el plan de tratamiento de riesgos** para obtener los objetivos de control identificados.
- **Implementar los controles seleccionados** para cumplir los objetivos de control.
- **Definir una metodología para medir la eficacia de los controles seleccionados**.
- **Implementar programas de formación**.
- **Gestionar la operación del SGSI**.
- **Gestionar los recursos del SGSI**.
- **Implementar procedimientos** que permitan la detección temprana de problemas de seguridad y una respuesta ante cualquiera de ellos.

Supervisión y revisión del SGSI

La organización debe:

- **Ejecutar procedimientos de supervisión y revisión** para:
  - Detectar lo antes posible los errores en los resultados.
  - Identificar lo antes posible las debilidades del sistema y los incidentes.
  - Permitir a dirección evaluar si las actividades de seguridad delegadas dan los resultados esperados.
  - Ayudar a detectar eventos de seguridad y prevenir incidentes mediante indicadores.
  - Determinar si las medidas tomadas ante cualquier incidente han sido adecuadas.
- **Realizar revisiones periódicas de la eficacia del SGSI** teniendo en cuenta todos los mecanismos implantados para la supervisión. Se debe incluir el cumplimiento de la política, de los objetivos y la revisión de los controles de seguridad.

- **Medir la eficacia de los controles** que verifican el cumplimiento de los requisitos de seguridad.
- **Revisar las evaluaciones de riesgos** a intervalos planificados, revisando riesgos residuales y niveles de riesgo aceptables.
- **Realizar auditorías internas del SGSI** a intervalos planificados.
- **Realizar una revisión global del SGSI**, verificando que el ámbito de aplicación es adecuado y que se identifican puntos de mejora en los procedimientos del SGSI.
- **Actualizar los planes de seguridad** teniendo en cuenta las conclusiones obtenidas en las actividades de supervisión y revisión.
- **Registrar las acciones e incidencias** que puedan afectar al funcionamiento del SGSI.

Mantenimiento y mejora del SGSI

Se deben de realizar de forma regular las siguientes acciones:

- **Implementar en el SGSI las mejoras identificadas**.
- **Llevar a cabo acciones preventivas y correctivas**.
- **Comunicar las acciones y mejoras a las partes interesadas** con un nivel de detalle acorde a las necesidades del informado.
- **Asegurar que las mejoras alcancen los objetivos previstos**.

Requisitos de documentación

Debe incluir las decisiones de dirección y los registros y procedimientos necesarios para cumplir con los objetivos de seguridad. La documentación debe incluir:

- Declaraciones de la política y de los objetivos del SGSI.
- Alcance del SGSI.
- Procedimientos y mecanismos de control.
- Descripción de la metodología de evaluación de riesgos.
- Informe de evaluación de riesgos.
- Procedimientos documentados necesarios para asegurar un adecuado funcionamiento de sus procesos de seguridad de la información y para describir cómo medir la eficacia de los controles.
- Registros requeridos por la norma.
- Declaración de aplicabilidad (SOA).

Control de documentos

Los documentos del SGSI requeridos por la norma deben ser protegidos y controlados, por lo que se debe de establecer un procedimiento documentado para definir las acciones necesarias para:

- Aprobar en forma los documentos previamente a su distribución.
- Revisa y actualizar los documentos, así como identificar los cambios y el último estado del documento que contiene la última versión.
- Asegurar que están disponibles las versiones correspondientes de los documentos.
- Asegurar la disponibilidad adecuada de los documentos, y que se almacenan, se transfieren y se destruyen siguiendo los procedimientos adecuados.

- Asegurar que se identifican los documentos externos.
- Asegurar que la distribución de documentos está controlada.
- Prevenir el uso no intencionado de documentos obsoletos.

Control de registros

Se deben crear y mantener registros que proporcionen evidencias de la conformidad de los requisitos y de la eficacia del SGSI. Deben permanecer legibles, fácilmente identificables y recuperables; así como protegidos y deben de poderse recuperar. Todos los procedimientos deberán estar documentados e implementados.

5. Responsabilidad de la dirección

Compromiso de la dirección

La dirección debe suministrar evidencias de su compromiso a través de las siguientes acciones:

- Formular la política del SGSI.
- Velar porque se establezcan los objetivos y planes del SGSI.
- Establecer roles y responsabilidades.
- Comunicando a la organización la importancia de cumplir los objetivos y la política de seguridad de la información, las necesidades legales y la necesidad de mejora continua.
- Proporcionar recursos suficientes para el SGSI.
- Decidir los criterios de evaluación de riesgos y los niveles aceptables de riesgo.
- Velar porque se realicen auditorías internas del SGSI.
- Dirigir las revisiones del SGSI.

Gestión de recursos

Provisión de recursos

La organización debe proveer los recursos necesarios para:

- Establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.
- Asegurar que los procedimientos responden a los requisitos empresariales.
- Identificar y cumplir los requisitos legales, así como las obligaciones contractuales.
- Mantener la seguridad adecuada mediante la aplicación de los controles implantados.
- Llevar a cabo revisiones cuando sean necesarias, y responder cuando sea necesario de los resultados de las mismas
- Mejorar la eficiencia del SGSI

Concienciación, formación y capacitación

La dirección debe asegurar que el personal designado con obligaciones sobre el SGSI esté correctamente capacitado para desarrollar sus funciones, para ello puede emplear:

- Determinar las competencias necesarias para el personal encargado del SGSI.
- Impartir formación.
- Evaluar la eficacia de las acciones realizadas.
- Mantener registros de formación.

Del mismo modo dirección se debe de encargar de informar al personal de la trascendencia de las actividades de seguridad de la información.

6. *Auditorías Internas del SGSI*

Se deben realizar auditorías del SGSI a intervalos planificados para comprobar si el SGSI:

- Cumple con los requisitos de ISO/IEC 27001, de la legislación y norma aplicables.
- Cumple con los requisitos de seguridad de la información identificados.
- Se implanta y mantiene de forma efectiva.
- Da el resultado esperado.

Se debe realizar un programa de auditorías, en los que se debe especificar los criterios, el alcance, la frecuencia y los métodos de auditoría. La selección de los auditores y la dirección de las auditorías deben garantizar objetividad e imparcialidad durante todo el proceso.

Se requiere un procedimiento documentado para regular la planificación, realización, información de los resultados y el mantenimiento de registros relacionados con auditorías internas.

7. *Revisión del SGSI por la dirección*

Se deben de realizar revisiones del SGSI por la dirección al menos una vez al año. La revsión debe contemplar las oportunidades de mejora y la necesidad de cambios en el SGSI, incluyendo la política y objetivos de seguridad de la información. Se debe documentar y mantener un registro de las mismas

Datos iniciales de la revisión

- Resultados de auditorías y revisiones del SGSI.
- Comentarios de las partes interesadas.
- Técnicas, productos o procedimientos que se podrían utilizar para mejorar el comportamiento y la eficacia del SGSI.
- Estado de las acciones preventivas o correctivas.
- Vulnerabilidades o amenazas no abordadas con la evaluación de riesgos previa.
- Resultados de las mediciones de eficacia.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.

Resultados de la revisión

Los resultados de la revisión deben incluir cualquier decisión y acción relativas a:

- La mejora de la eficacia del SGSI.
- Actualización de evaluación de riesgos.
- Modificaciones de los procedimientos y controles que afectan a la seguridad de la información.
- Las necesidades de recursos.
- La mejora en el modo de medir la eficacia de los controles.

8. Mejora del SGSI

Mejora continua

Se debe mejorar de forma continua la eficacia del SGSI, empleando la política y los objetivos de seguridad de la información, los resultados de las auditorías, análisis de eventos de seguridad, revisión de las acciones correctivas y preventivas, así como las revisiones por dirección.

Acción correctiva

Son acciones creadas para eliminar la causa de las no conformidades con los requisitos del SGSI para evitar que se vuelvan a repetir, el procedimiento documentado de acciones correctivas debe incluir requisitos para:

- Identificar no conformidades.
- Determinar sus causas.
- Evaluar la necesidad de adoptar acciones para prevenir la ocurrencia de no conformidades.
- Determinar e implantar las acciones correctivas necesarias.
- Registrar el resultado de las acciones realizadas.
- Revisar las acciones realizadas.

Acción Preventiva

La organización también debe determinar acciones necesarias para eliminar la causa de posibles no conformidades con los requisitos del SGSI. Deben ser apropiadas en relación a los problemas potenciales. El procedimiento documentado de acciones preventivas debe definir requisitos para:

- Identificar las posibles no conformidades y sus causas.
- Evaluar la necesidad de emprender acciones preventivas.
- Determinar e implementar las acciones preventivas necesarias.
- Registrar los resultados de las acciones adoptadas.
- Registrar las acciones preventivas adoptadas.

A. Anexo A – Objetivos de control y controles

Los objetivos de control y controles contenidos en el Anexo VI – Objetivos de control y controles de ISO/IEC 27001. Como se mencionó anteriormente, el anexo de objetivos de control y controles establece un conjunto de requisitos para el cumplimiento de la norma ISO 27001. Estos requisitos son seleccionables, y como también se mencionó con anterioridad, su selección en base a las necesidades, objetivos y medios de la organización debe reflejarse en la declaración de aplicabilidad de la entidad.

B. Anexo B – Principios de la OCDE y esta norma internacional

Detalla la relación y puntos de enlace entre las directrices de la OCDE para la seguridad de los sistemas y redes de información. Instaurando unas directrices y principios para la creación e implementación de un sistema de gestión de la seguridad de la información en base a algunos de sus principios, empleando para ello el modelo PDCA y los procesos descritos en los capítulos 4, 5, 6 y 8 de la presente norma.

Para más información se pone a la disposición del lector un enlace hacia dichas directrices:

http://www.csi.map.es/csi/pdf/ocde_directrices_esp.pdf

C. *Anexo C – Correspondencia entre las normas ISO 9001:2000, ISO 14001:2004 y esta norma internacional*

En el presente anexo se muestra una tabla de correspondencia entre las normas ISO 9001:2000, ISO 14001:2004 y la norma ISO 27001:2005. Se realiza este enlace para facilitar la integración de las mismas, en caso de entidades que implementen dos o más de ellas con el fin de facilitar la integración y unión de requisitos de las mismas; siempre con el fin de facilitar la gestión de los sistemas a la entidad.

3.4.Selección y aplicación de los requisitos de la LOPD e ISO/IEC 27001 a SGSI Tracking

A continuación, y para cerrar el primer punto del presente proyecto, se procede a seleccionar y detallar la implementación de los requisitos aplicables a la herramienta SGSI Tracking. Es importante destacar que estos criterios se emplearon para seleccionar e integrar cada uno de los módulos de la herramienta. Para cumplir con este fin, se considera lo más adecuado, para mejorar la legibilidad de la memoria, centrarnos en cada uno de los módulos de SGSI Tracking, y así relacionar los requisitos aplicables a cada uno de los módulos de la herramienta. Para ello se va a seguir la siguiente estructura:

- Planificar
  - Procesos de etiquetado
  - Inventario de red
  - Inventario de Activos
- Desplegar
- Verificar
  - Monitorización de equipos
  - Correlador de eventos
  - Marcadores
- Actuar
  - Documentación de incidencias
  - Gestión de incidencias
- Control
  - Pasarelas de correo
  - Gestión de usuarios
  - Alertas periódicas
- Documentación

Como se puede observar, la herramienta se fundamenta en el Ciclo PDCA, dividiendo su funcionalidad en cada una de las herramientas aplicables a sus fases. Además destaca el apartado de documentación, no contenido en el ciclo, que cuenta con un pequeño gestor documental, aprovechable para el cumplimiento de todos los requisitos.

Se pasa a continuación al análisis de cada uno de los módulos de la herramienta, acorde a la LO 15/1999, el RD 1720/2007 y la ISO 27001, esta última apoyada en la ISO 17799.

3.4.1. Planificar

Fase del ciclo PDCA en la que se definen la política, objetivos, procesos y procedimientos del SGSI. En la herramienta se incluyen dos módulos y un pequeño repositorio de documentación referente a los mismos. Está formado por los módulos:

- Proceso de Etiquetado
- Inventario de Red
- Inventario de activos

Se muestra a continuación una captura de la pantalla introductora a esta sección:

Ilustración 2 – SGSI Tracking - Planificar

Procesos de Etiquetado

En el siguiente repositorio se almacena la documentación del SGSI referente a inventario de activos. Se ha considerado incluir los procesos para el etiquetado relacionados con ISO 27001, con el fin de servir de referencia para la realización del inventario de activos de información necesario para realizar el análisis de riesgos del SGSI. Se muestra una captura de pantalla:

Ilustración 3 – SGSI Tracking - Etiquetado de Activos

Integración:

Requisitos RD 1720/2007:

Se consideran, en primer lugar, las necesidades de etiquetado requeridas por el RD 1720/2007, en su Título VIII:

Gestión de Soportes y Documentos (Nivel básico):

- Identificación de soportes que contengan datos de carácter personal (automatizados y no automatizados): Estas medidas están incluidas en el procedimiento de inventario de activos y de análisis de riesgos del SGSI; de tal modo que se definen la metodología para etiquetar los activos, que debe incluir los datos de carácter personal de la entidad.

Gestión y distribución de soportes (Nivel Alto):

- Se deben etiquetar los soportes de forma que sean fáciles de identificar por el personal autorizado y difícil de identificar en cualquier otro caso. Este requerimiento está apoyado igualmente por el procedimiento de Inventario y Etiquetado de Activos del SGSI.

Requisitos ISO/IEC 27001:

Del mismo modo, se consideran los siguientes puntosde ayuda al cumplimiento de los siguientes controles de ISO/IEC 27001:

- En el punto 4.2.1.d de análisis y valoración de riesgos de la creación del SGSI especifica que, para realizar una adecuada identificación de riesgos se deben de identificar los activos de información que están dentro del ámbito de aplicación del SGSI y a los propietarios o responsables de los mismos.
- En el punto 4.3.1 de generalidades en los requisitos de documentación se requiere por una parte, que se documenten los procedimientos que soportan al SGSI, y más específicamente que se describa la metodología de evaluación de riesgos; por otra parte, en el punto 4.3.2 de control de documentos en los requisitos de documentación afirma que se debe de asegurar que los documentos están disponibles para todo aquel que los necesita para desempeñar sus funciones.

Del análisis de los requisitos se puede concluir, que dados los mecanismos de control de acceso a la herramienta y cada uno de los módulos que los forman, y la disponibilidad proporcionada por la herramienta SGSI Tracking como herramienta online; facilitan el conocimiento y aplicación de la metodología a seguir especificada por ambas normas, así como su fácil acceso por el personal debidamente autorizado.

Es importante destacar que se puede sustituir la documentación con facilidad, bien como administrador desde la misma interfaz de SGSI Tracking, bien desde la interfaz del servidor Joomla que lo soporta.

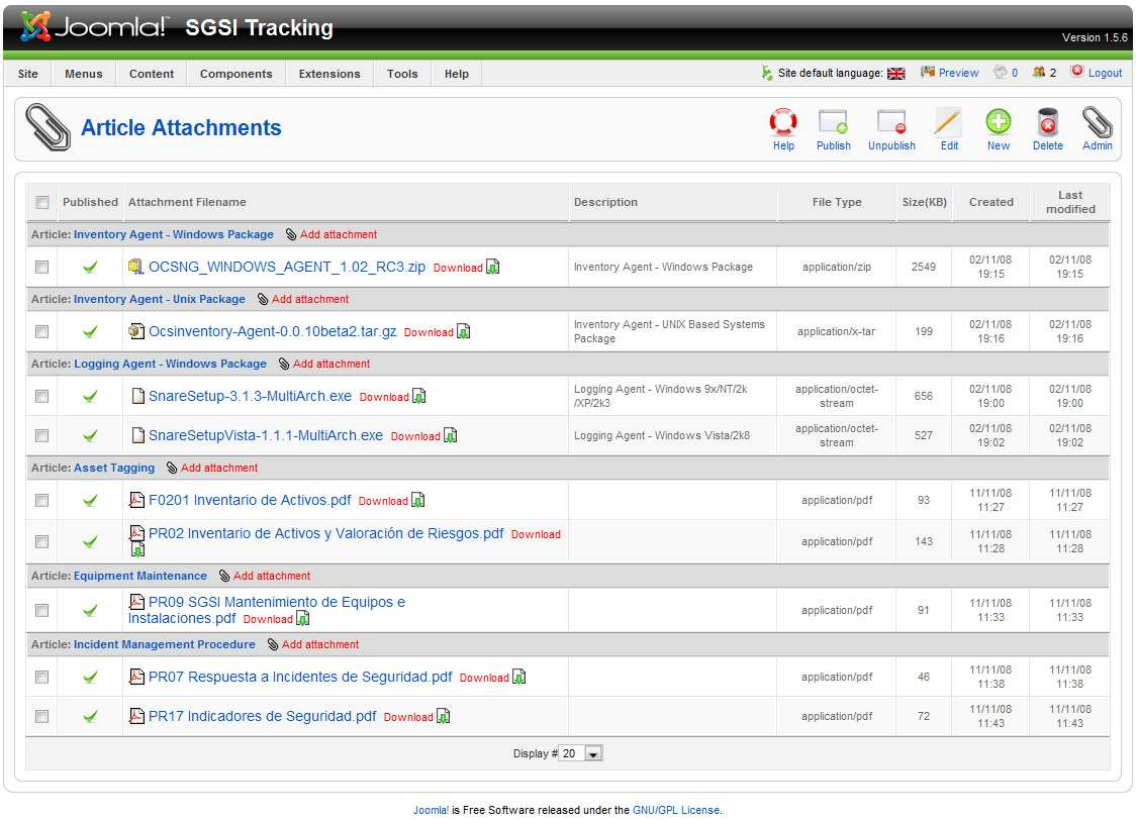


Ilustración 4 – SGSI Tracking – Adjuntos Joomla

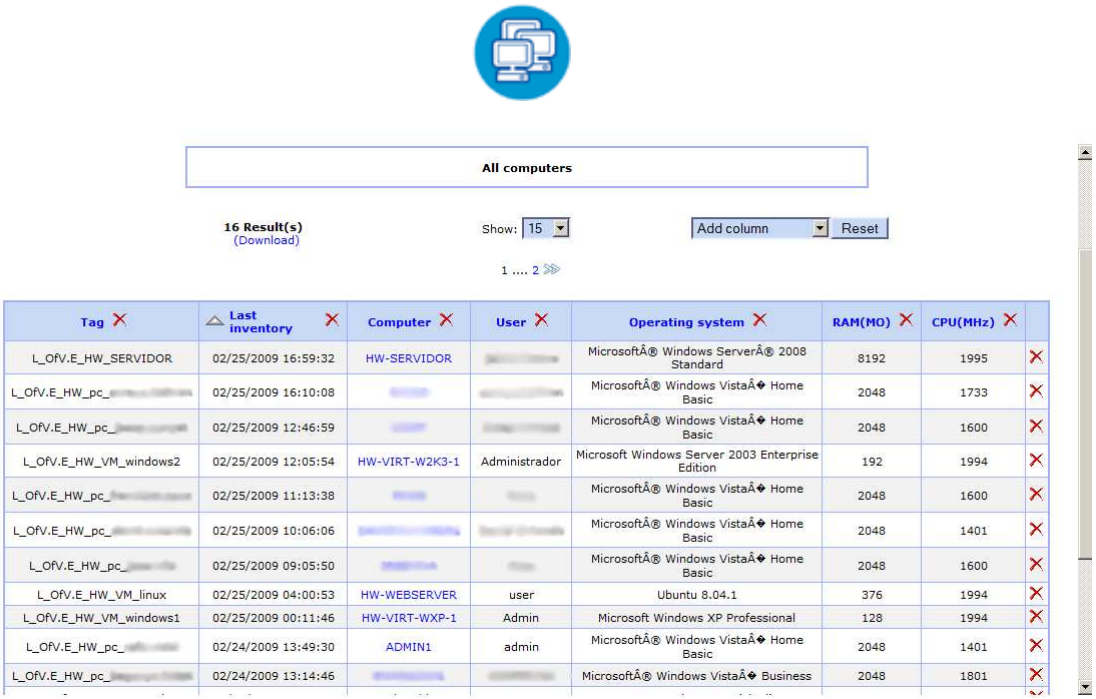
Inventario de red

El siguiente módulo integra la herramienta OCS Inventory, que es básicamente una herramienta de inventario automatizado de red, además de una herramienta habilitada para realizar despliegues software. Mediante la instalación de un software cliente en todos los equipos de la entidad, se mantiene actualizado el inventario.

Ilustración 5 – SGSI Tracking - Inventario de Red

Integración

Para el repaso de la herramienta se procede a repasar las partes de la misma relevantes para la finalidad de este análisis de integración de la herramienta con la normativa a considerar. Se muestra una captura de pantalla del apartado *All Computers*:



All computers

16 Result(s) (Download)

Show: 15 Add column Reset

1 2

Tag	Last inventory	Computer	User	Operating system	RAM(MO)	CPU(MHz)	
L_OfV.E_HW_SERVIDOR	02/25/2009 16:59:32	HW-SERVIDOR	[redacted]	MicrosoftÂ® Windows ServerÂ® 2008 Standard	8192	1995	
L_OfV.E_HW_pc_[redacted]	02/25/2009 16:10:08	[redacted]	[redacted]	MicrosoftÂ® Windows VistaÂ♦ Home Basic	2048	1733	
L_OfV.E_HW_pc_[redacted]	02/25/2009 12:46:59	[redacted]	[redacted]	MicrosoftÂ® Windows VistaÂ♦ Home Basic	2048	1600	
L_OfV.E_HW_VM_windows2	02/25/2009 12:05:54	HW-VIRT-W2K3-1	Administrador	Microsoft Windows Server 2003 Enterprise Edition	192	1994	
L_OfV.E_HW_pc_[redacted]	02/25/2009 11:13:38	[redacted]	[redacted]	MicrosoftÂ® Windows VistaÂ♦ Home Basic	2048	1600	
L_OfV.E_HW_pc_[redacted]	02/25/2009 10:06:06	[redacted]	[redacted]	MicrosoftÂ® Windows VistaÂ♦ Home Basic	2048	1401	
L_OfV.E_HW_pc_[redacted]	02/25/2009 09:05:50	[redacted]	[redacted]	MicrosoftÂ® Windows VistaÂ♦ Home Basic	2048	1600	
L_OfV.E_HW_VM_linux	02/25/2009 04:00:53	HW-WEBSERVER	user	Ubuntu 8.04.1	376	1994	
L_OfV.E_HW_VM_windows1	02/25/2009 00:11:46	HW-VIRT-WXP-1	Admin	Microsoft Windows XP Professional	128	1994	
L_OfV.E_HW_pc_[redacted]	02/24/2009 13:49:30	ADMIN1	admin	MicrosoftÂ® Windows VistaÂ♦ Home Basic	2048	1401	
L_OfV.E_HW_pc_[redacted]	02/24/2009 13:14:46	[redacted]	[redacted]	MicrosoftÂ® Windows VistaÂ♦ Business	2048	1801	

Ilustración 6 - Inventario de red – All Computers

En esta pantalla de la aplicación SGSI Tracking muestra el inventario de equipos de red actualizado de la entidad.

Requisitos ISO/IEC 27001

En el dominio de control A.7.1 Responsabilidad sobre los activos se especifica que la organización debe identificar con claridad todos sus activos de información y debe crear y mantener actualizado un inventario de sus activos más importantes. Del mismo modo se especifica que toda la información y los activos asociados a la información deben tener como propietario a una parte designada de la organización.

Con este módulo, y posteriormente en el bloque de Inventario de Activos, se cumplen los requisitos de este punto de la norma. Como se puede observar en el módulo *All computers* se muestra un inventario de activos actualizado de todos los equipos informáticos de la entidad, con multitud de campos. Cabe destacar para el cumplimiento concreto de la asignación de propietario los campos Nombre Usuario y Propietario, que asignan propiedad a dicho activo. Se pueden seleccionar campos como:

Ilustración 7 – Inventario de Red – Campos All computers

El siguiente punto a repasar es el apartado de *All Softwares*:

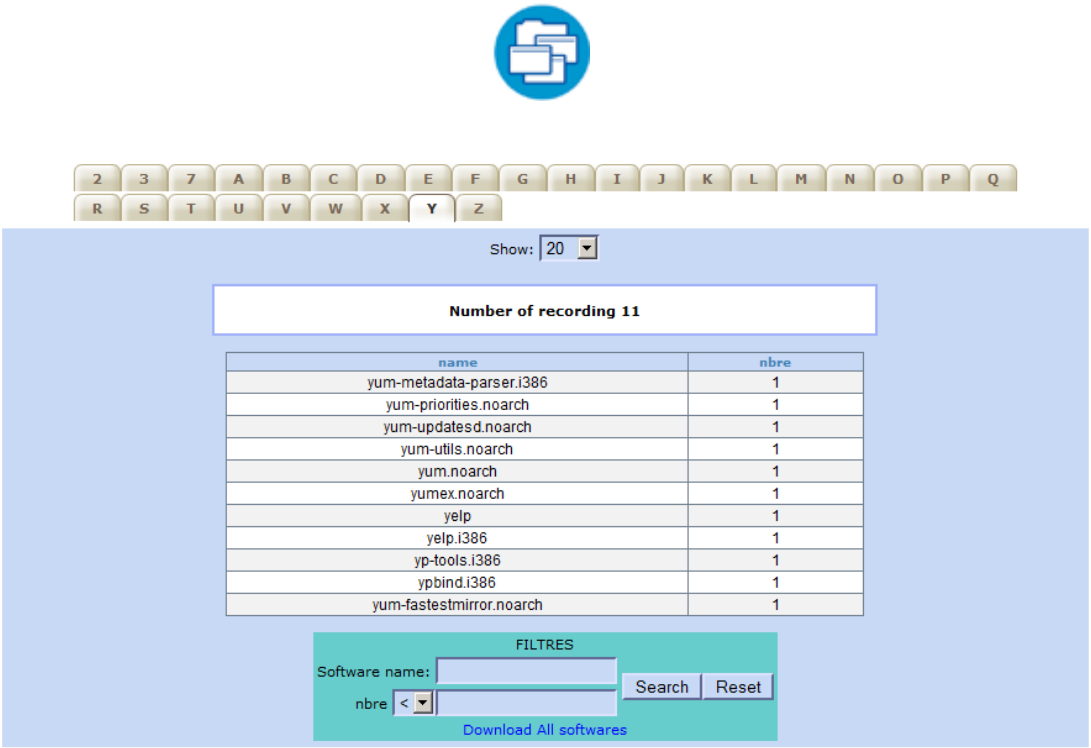


Ilustración 8 – Inventario de Red – All Softwares

Este apartado es básicamente un inventario de aplicaciones, que recoge todas las aplicaciones instaladas en todos los equipos de los que se realiza el inventario.

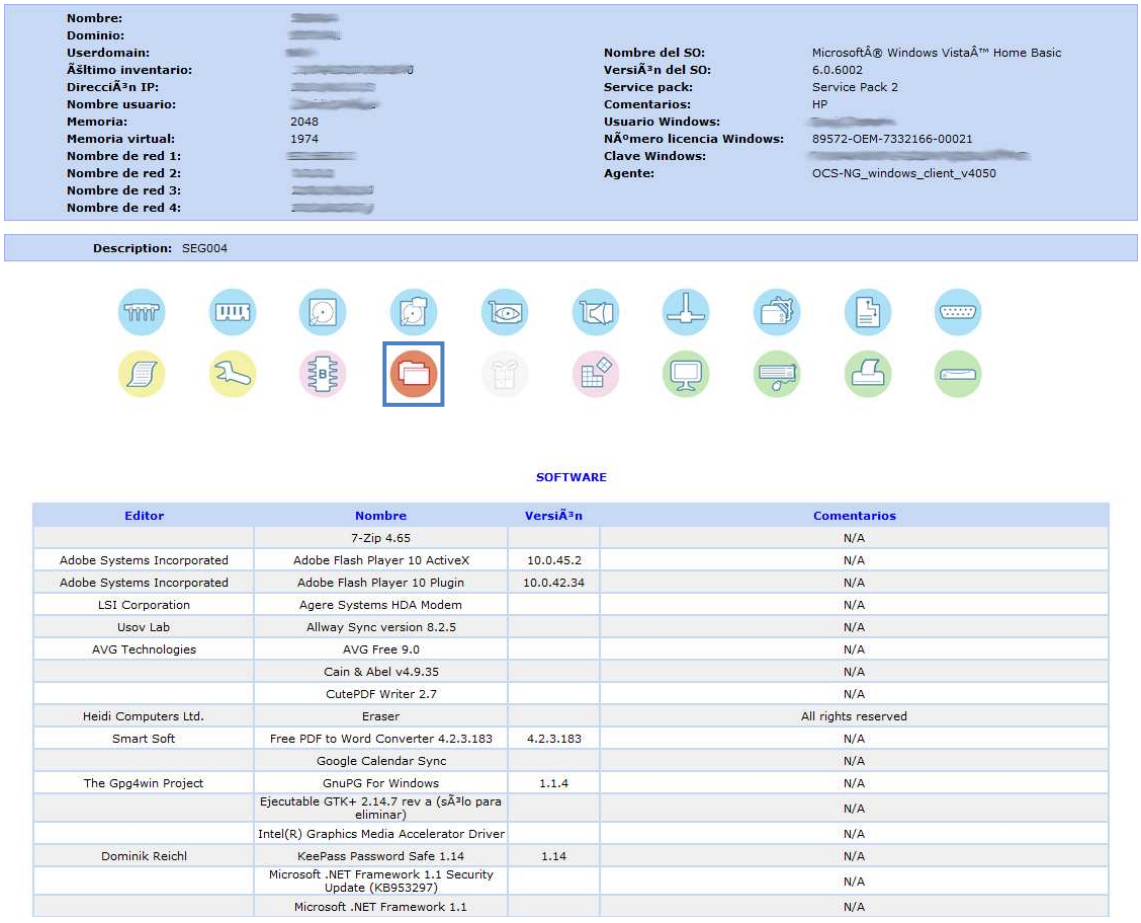
Requisitos RD 1720/2007

TÍTULO VIII – Medidas de Seguridad de Nivel Básico – Funciones y Obligaciones del Personal:

Se deben establecer las funciones y obligaciones de todos los usuarios o perfiles de usuario con acceso a datos de carácter personal, reflejándolas en el documento de seguridad. El responsable del fichero se encargará de que el personal conozca las normas de seguridad respecto a datos de carácter personal, así como las responsabilidades de su incumplimiento.

En las funciones y obligaciones del personal, es un requisito frecuente el buen uso de los sistemas de información, limitándose sólo a las finalidades establecidas. Además usualmente, se especifica un listado de aplicaciones cuyo uso está prohibido en la entidad,

como por ejemplo las bien conocidas herramientas P2P tales como eMule, Ares, Bittorrent, etc.; las cuales suponen una grave amenaza a la confidencialidad de la información. Con este inventario se puede verificar fácilmente la existencia de las mismas, y después mediante la vista propia de cada equipo se pueden ver a su vez, las aplicaciones instaladas en cada uno de ellos, con el fin de poder asignar responsabilidades; se muestra a continuación una captura que lo muestra:



Nombre:	[redacted]		
Dominio:	[redacted]		
Userdomain:	[redacted]	**Nombre del SO:**	MicrosoftÂ® Windows VistaÂ™ Home Basic
Ãšltimo inventario:	[redacted]	**VersiÃ³n del SO:**	6.0.6002
DirecciÃ³n IP:	[redacted]	**Service pack:**	Service Pack 2
Nombre usuario:	[redacted]	**Comentarios:**	HP
Memoria:	2048	**Usuario Windows:**	[redacted]
Memoria virtual:	1974	**NÃºmero licencia Windows:**	89572-OEM-7332166-00021
Nombre de red 1:	[redacted]	**Clave Windows:**	[redacted]
Nombre de red 2:	[redacted]	**Agente:**	OCS-NG_windows_client_v4050
Nombre de red 3:	[redacted]		
Nombre de red 4:	[redacted]		

Description: SEG004

SOFTWARE

Editor	Nombre	VersiÃ³n	Comentarios
	7-Zip 4.65		N/A
Adobe Systems Incorporated	Adobe Flash Player 10 ActiveX	10.0.45.2	N/A
Adobe Systems Incorporated	Adobe Flash Player 10 Plugin	10.0.42.34	N/A
LSI Corporation	Agere Systems HDA Modem		N/A
Usov Lab	Allway Sync version 8.2.5		N/A
AVG Technologies	AVG Free 9.0		N/A
	Cain & Abel v4.9.35		N/A
	CutePDF Writer 2.7		N/A
Heidi Computers Ltd.	Eraser		All rights reserved
Smart Soft	Free PDF to Word Converter 4.2.3.183	4.2.3.183	N/A
	Google Calendar Sync		N/A
The Gpg4win Project	GnuPG For Windows	1.1.4	N/A
	Ejecutable GTK+ 2.14.7 rev a (sÃ³lo para eliminar)		N/A
	Intel(R) Graphics Media Accelerator Driver		N/A
Dominik Reichl	KeePass Password Safe 1.14	1.14	N/A
	Microsoft .NET Framework 1.1 Security Update (KB953297)		N/A
	Microsoft .NET Framework 1.1		N/A

Ilustración 9 – Inventario de Red – Vista personalizada por equipo

A este apartado se puede acceder mediante la sección *All Computers*, haciendo clic sobre el nombre del equipo que se quiere auditar y después accediendo al inventario de software de la máquina mediante el icono marcado en la ilustración 8.

Finalmente otro mecanismo que facilita la búsqueda es emplear *Search with various criteria*, que nos permite buscar software y recibir un listado de equipos que lo instalan:

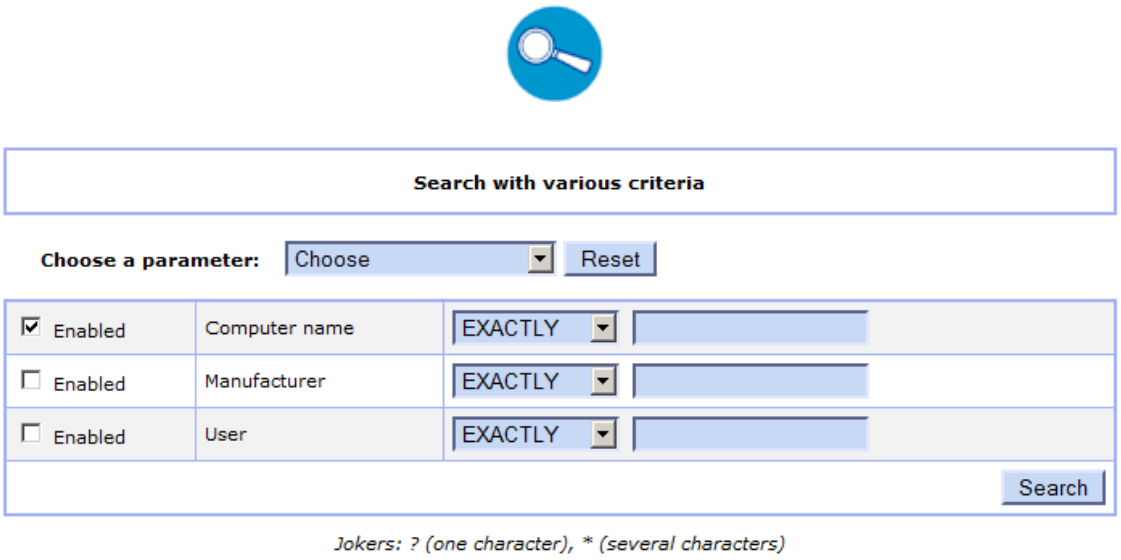


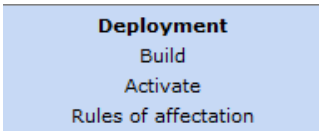
Ilustración 10 – Inventario de Red – Search with various criteria

Requisitos ISO/IEC 27001

En el objetivo de control A.7.1.3 de Uso aceptable de los activos, afirma que se deben identificar, documentar e implantar reglas para un uso aceptable de los activos asociados con el tratamiento de información. Estas reglas, deben estar dirigidas a todos los empleados y terceras partes, debiendo estar sustentadas por acuerdos formales, tales como contratos.

Más allá que en los requisitos anteriores, un uso aceptable de los activos se considera en ISO/IEC 27001 no solo no comprometer la seguridad de los datos, sino que además se realice un uso racional de los activos. Por lo que, no solo encontraremos medidas destinadadas a eliminar software peligroso ante la seguridad de la información, sino que además se seleccionarán aplicaciones y herramientas prohibidas, ya que no son necesarias para desarrollar las funciones de cada puesto en la entidad. Del mismo modo, *All softwares* permite auditar estos requisitos.

Centrándonos en otro módulo importante a los ojos de la normativa, nos centramos en *Deployment*, que es una parte del inventario de red que se encarga del despliegue de paquetes en las máquinas del inventario, mediante la construcción de paquetes que posteriormente se podrán descargar e instalar mediante el agente de inventario en cualquier equipo.



Consta principalmente de 3 bloques que se explican brevemente a continuación:

- ***Build*:** Esta parte del módulo se emplea para construir el paquete para hacer el despliegue, de modo que se puede seleccionar las características del mismo, su uso en el equipo cliente, avisar al usuario, etc.

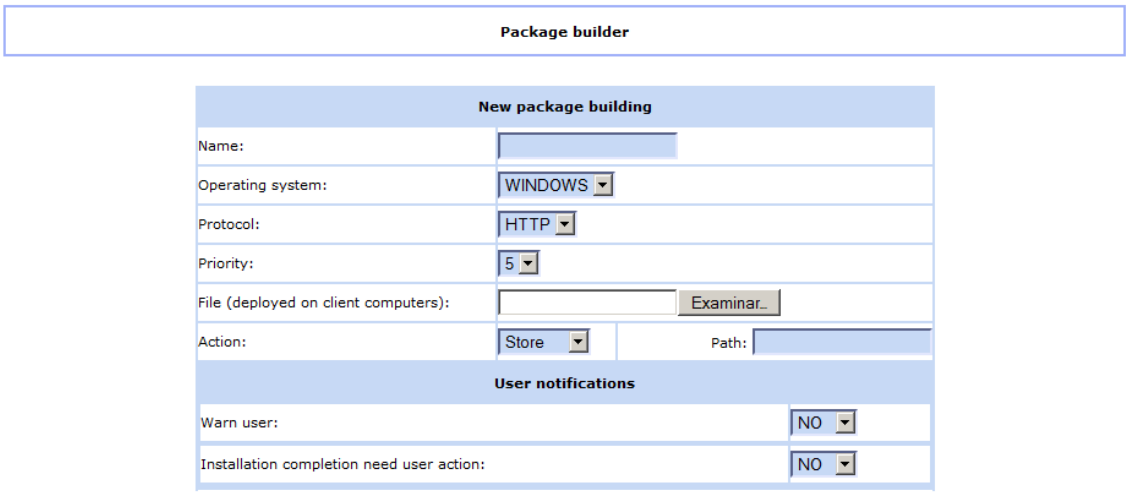


Ilustración 11 – Inventario de Red – Package builder

- ***Activate*:** Con este formulario se pueden activar los paquetes previamente creados, que aparecen en un listado. Los paquetes solo están a disposición de los clientes si están activados.

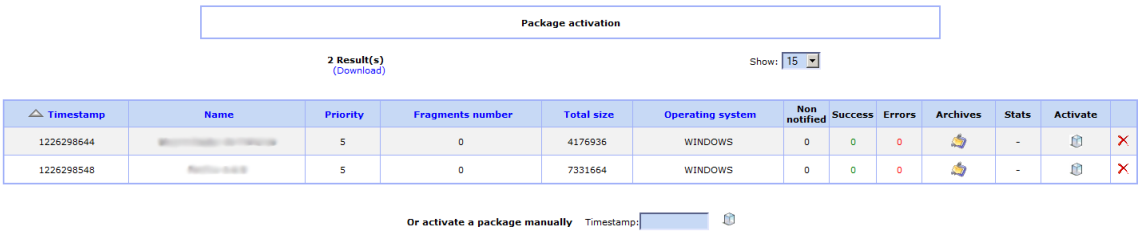


Ilustración 12 – Inventario de Red – Package activation

- ***Rules of affectation*:** En este menú se puede seleccionar a que conjunto de dispositivos afecta el despliegue. Esto es útil si por ejemplo se necesita desplegar una herramienta en los servidores y no en los clientes, o viceversa.

Requisitos ISO/IEC 27001

El control A.12.4.1 de Control de software en explotación establece que se deben desarrollar procedimientos para controlar la instalación del software en los sistemas. Concretamente para este caso se seleccionan las siguientes pautas de ISO/IEC 17799:

- Las actualizaciones de los programas en producción se deben realizar por el administrador de sistemas previa autorización de gerencia.
- Cualquier programa que se vaya a instalar debe haber pasado pruebas de uso, aceptación de los usuarios y estar correctamente actualizado. Todas estas pruebas deben ser realizadas en un sistema independiente.
- Utilizar un sistema de control de software, para mantener un listado del software instalado, y la documentación del sistema.

Como se ha podido observar, cumple con dos primeros requisitos que se han especificado. El mecanismo de control que implementa facilita la gestión de actualizaciones o software, centralizando la capacidad de distribución sobre el Administrador de Sistemas de la entidad.

Pasando a comentar la creación de un listado de software, se cuenta con el modulo *All Softwares*, antes comentado, que constituye en sí mismo un listado de software automatizado.

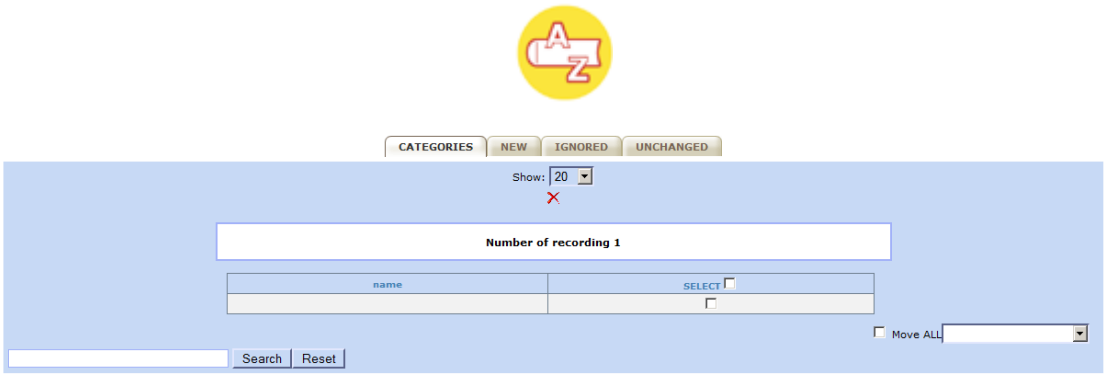


Ilustración 13 – Inventario de Red - Dictionary

El módulo *Dictionary*, basado en el inventario de software automatizado de *All Softwares*, añade una funcionalidad extra al mismo. Concretamente con este módulo podremos establecer categorías de software con fines de auditoría; creando grupos de aplicaciones sensibles o prohibidas y monitorizar de forma sencilla las instalaciones.

Nos permite realizar las siguientes acciones en cada pestaña:

- *Categories*: En esta pestaña se muestra el listado de todas las categorías de software de que se dispone.
- *New*: Es un listado del software no clasificado en ninguna categoría.
- *Ignored*: Listado de software que no se desea auditar.
- *Unchanged*: Listado de software auditado y que no ha sufrido ningún cambio.

Requisitos ISO 27001:

Esto también ayuda a cumplir con los requisitos comentados anteriormente y establecidos en la norma sobre el control A.12.4.1 de Control de software en explotación. Manteniendo un

Del mismo modo, a continuación se pasa a describir el módulo *Registry*. El módulo se emplea para seleccionar concretamente qué entradas del registro de sistema de cada uno de los equipos inventariados se van a almacenar en el servidor con el fin de realizar una auditoría personalizada del mismo. En el registro del sistema se puede encontrar los datos de configuración de todos los programas del sistema, incluido Windows. Esto aún mejora la capacidad de auditoría de software del módulo, ya que, de este modo no solo se puede conocer la instalación o cambio de versión de la aplicación; sino también los aspectos más determinantes de la configuración del mismo. En el caso de Windows por ejemplo podríamos auditar los programas que se ejecutan al iniciar sesión en Windows, y en caso de otro software se podría controlar por ejemplo la configuración de SNARE, que es el programa cliente del Registro de eventos de SGSI Tracking. Ambos se muestran a continuación:

Registry requests

2 Result(s)
(Download)

Show: 15

name	regtree	regkey	regvalue
Programas al Inicio	2	SOFTWARE\Microsoft\Windows\CurrentVersion\Run	*
Objetivos SNARE	2	SOFTWARE\InterSect Alliance\AuditService\Objective	*

Ilustración 14 – Inventario de Red - Registry

Requisitos ISO/IEC 27001

Tal y como sucedía en el caso anterior, esto también ayuda a cumplir con los requisitos comentados anteriormente y establecidos en la norma ISO/IEC 27001, sobre el control A.12.4.1 de Control de software en explotación.

Inventario de Activos

El siguiente módulo integra la herramienta GLPI, esta herramienta es un inventario de activos centralizado. Destaca por tomar los datos del módulo anterior, ampliando sus posibilidades con mayor capacidad de clasificación y nuevas funciones administrativas.

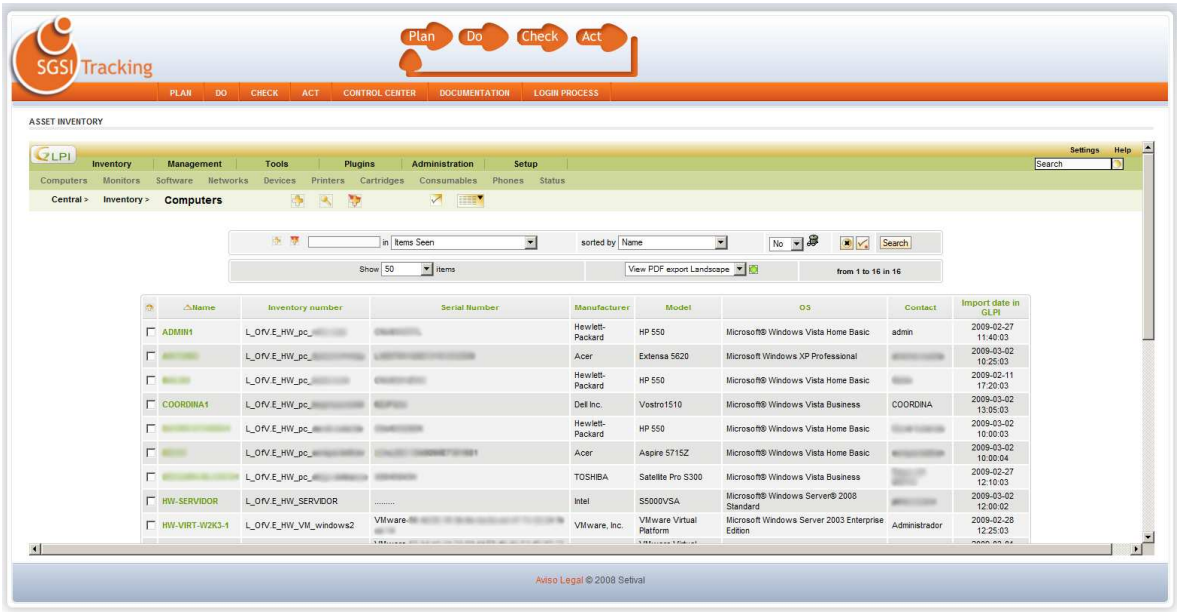


Ilustración 15 –SGSI Tracking - Inventario de Activos

Integración

El primer punto a repasar es *Iventory*:

Ilustración 16 - Inventario de Activos - Inventory (Tipos)

Esta sección supone propiamente el inventario de GLPI. Como se puede observar en este caso se encuentra dividido en las siguientes secciones, con el fin de facilitar el acceso y modificación al mismo:

- *Computers (*Ordenadores)
- *Monitors (Monitores)*
- *Software*
- *Networks (Redes)*
- *Devices (Dispositivos)*
- *Printers (Impresoras)*

- *Cartidges (Cartuchos)*
- *Consumables (Consumibles)*
- *Phones (Teléfonos)*
- *Status (Estados)*

Para mostrar hasta qué punto se puede almacenar información en GLPI, se repasarán las partes del inventario que puedan cumplir con los requisitos de la legislación analizada. Comenzaremos con el inventario de ordenadores. Esta es la ficha tipo se muestran todos los campos identificativos que se pueden almacenar.

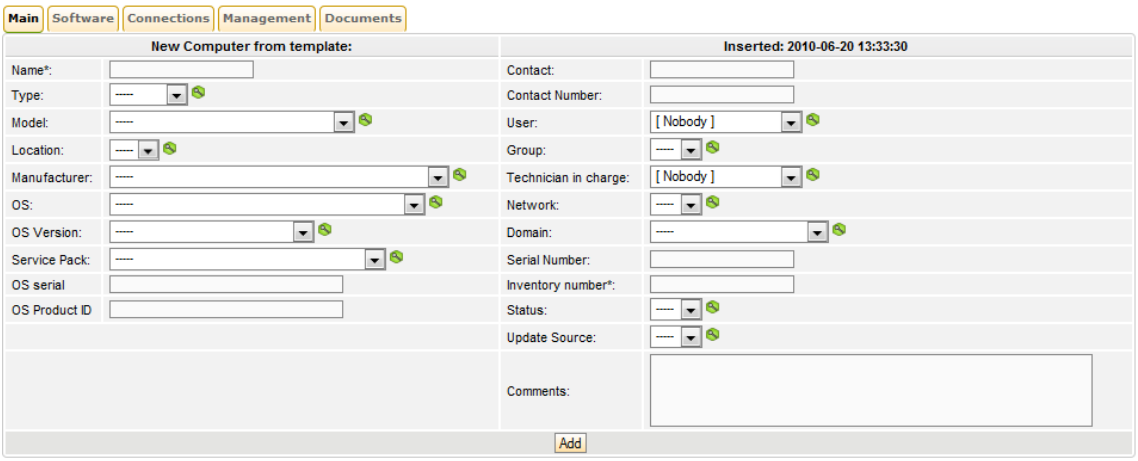
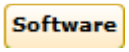


Ilustración 17 - Inventario de Activos – Computers

Como se puede observar se pueden almacenar valores como nombre, modelo, sistema operativo, *contact* (responsable), usuario, red, etc. Es importante destacar que el inventario se actualiza automáticamente mediante sincronización con la herramienta OCS Inventory, por lo que en la mayoría de los campos aparecen valores fruto de esa sincronización, aunque se pueden añadir nuevos manualmente.



Esta parte del inventario de activos también se sincroniza con OCS Inventory automáticamente, aunque en este caso nos resulta más sencillo hacer un repaso del software instalado en cada una de las máquinas inventariadas, pudiéndose acceder a la ficha completa de información de cada programa. Como se puede observar en la ilustración 18, primero se ofrece una identificación del software, con valores como nombre, plataforma, fabricante, etc. que nos facilitan la identificación del mismo. Cabe destacar el campo actualización (*update)*, el cual almacena la versión actual del *software*. También se dispone de un inventario de software completo en la selección del inventario de *software*.

Ilustración 18 - Inventario de Activos - Inventario Software/Máquina

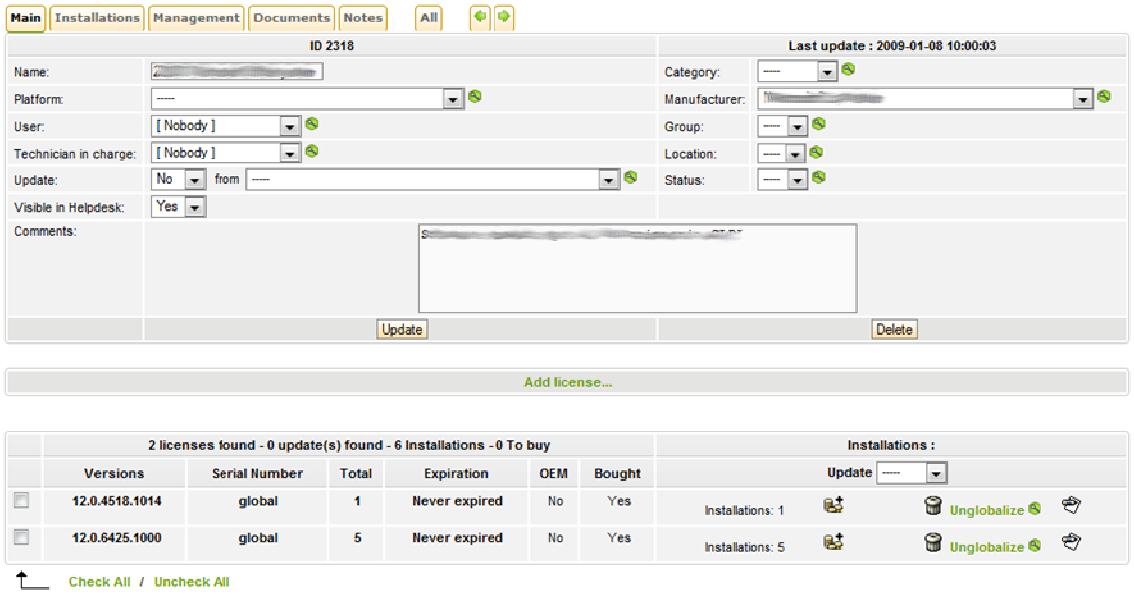


Ilustración 19 - Inventario de Activos - Software

A continuación de los datos identificativos, también podemos observar que se mantiene una relación de las licencias instaladas en todos los equipos por dicho software, así como el número de instalaciones y en que equipos se encuentran.

Requisitos ISO/IEC 27001

En primer lugar, en *computers*, se proporcionan mecanismos para ayudar a cumplir con todos los requisitos del objetivo de control A.7.1 Responsabilidad sobre los activos, que contiene los controles:

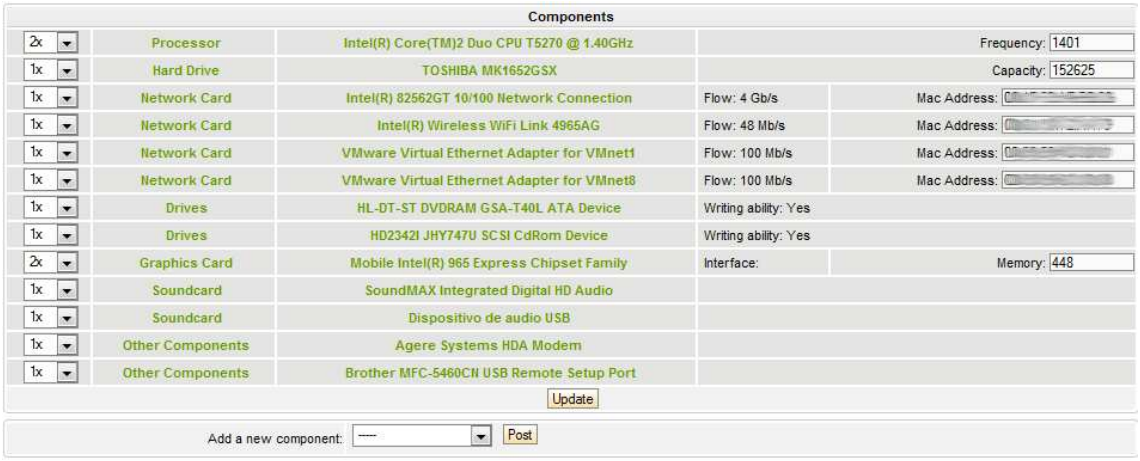
- A.7.1.1 Inventario de activos:
  - La organización debe identificar con claridad todos sus activos y debe crear y mantener actualizado un inventario de sus activos más importantes.
  - El inventario de activos debería contener para cada activo la siguiente información:
    - Propietario del activo.
    - Clasificación de la información.
    - Información necesaria para recuperarse de un desastre, incluyendo tipo de activo, formato, información de *back up*, información de licencias y de valor para el negocio.
- A.7.1.2 Propiedad de los activos: Toda la información y los activos asociados a la información deben tener como propietario a una parte designada de la organización. El termino propietario también se puede aplicar a sobre procesos, aplicaciones o un conjunto de datos, etc. En ningún caso implica propiedad o derecho sobre el activo.
- A.7.1.3 Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para un uso aceptable de los activos asociados con información.

En segundo lugar, la ficha software, (en especial el campo *update)*, facilita el cumplimiento del control A.12.4.1 de Control de Software en Explotación, antes mencionado, ya que se mantiene un listado de software actualizado y se regulan las actualizaciones del mismo.

Por último, la gestión de licencias software, monitoriza el control A.15.1.2 – Derechos de propiedad intelectual (DPI), que indica que:

- Se deberían implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladoras y contractuales sobre el uso del material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario.
- Los derechos de la propiedad intelectual incluyen al software o copyright de documentos, derechos de diseño, marcas registradas, patentes y fuentes de licencia de código.
- Los productos de software propietario son suministrados usualmente bajo un acuerdo de licencia que especifica los términos y condiciones, por ejemplo limitar el uso de productos para maquinas especificas o limitar el copiado solamente en la creación de las copias de respaldo.

Además en la parte inferior de la ficha Computers, en la pestaña Main, se detalla el siguiente listado de componentes físicos que construyen la máquina inventariada:



Requisitos ISO/IEC 27001

Tener un listado de hardware instalado facilita identificar cada hardware instalado con datos de interés, de este modo facilitando la realización de las recomendaciones requeridas por el control A10.3.1 de Gestión de la Capacidad:

- El uso de recursos debe monitorizarse y deben realizarse proyecciones de requisitos de capacidades futuras para asegurar funcionamiento adecuado de los el sistemas. Para ello hay que contemplar los siguientes aspectos:
  - Para cada actividad que se esté llevando a cabo o para una actividad nueva, los requisitos de capacidad deben ser identificados.
  - Se deben monitorizar los sistemas con el fin de asegurar y mejorar la disponibilidad y la eficiencia de los mismos.
  - Implementar controles detectivos para detectar problemas con rapidez
  - Realizar proyecciones de capacidad
- Se requiere poner particular atención sobre los recursos clave (costo elevado o baja disponibilidad, etc.). Se deberían identificar tendencias relativas a aplicaciones del negocio o herramientas de administración.
- Los administradores deberían usar esta información para identificar y evitar los posibles cuellos de botella.

Otro punto importante en el inventario de ordenadores que nos proporciona GLPI es Connections, que muestra todas las conexiones directas como indirectas que posee cada equipo; por ejemplo contempla monitores, impresoras, red, etc.

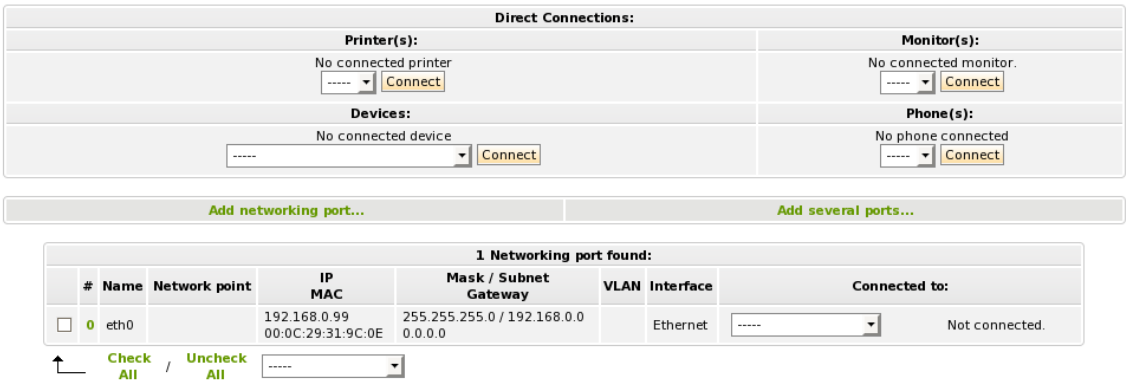


Ilustración 20 - Inventario de Activos – Connections

Continuando con el inventario nos detenemos en esta ocasión en Networks, el inventario de redes. Mostramos a continuación su vista principal.

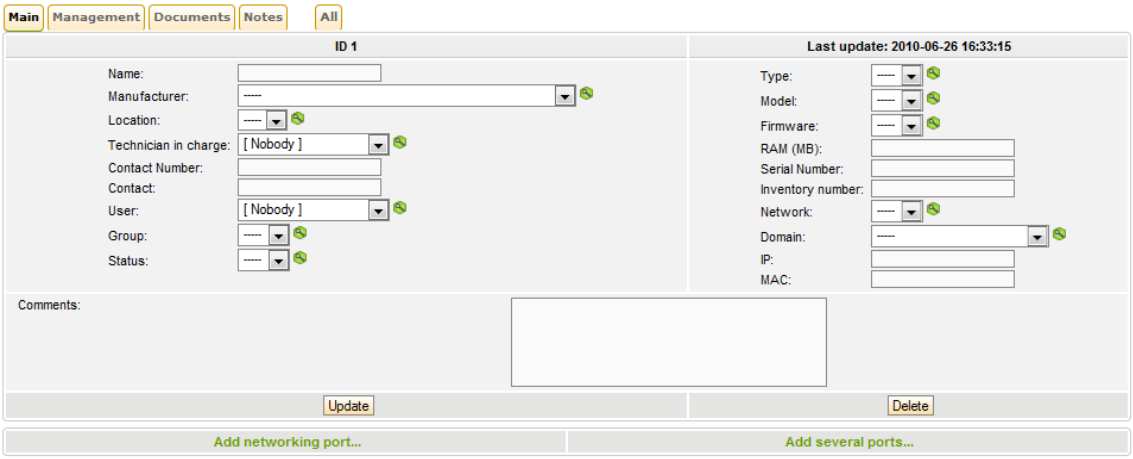


Ilustración 21 - Inventario de Activos – Networks

Requisitos ISO/IEC 27001

Mediante la revisión del inventario de conexiones indirectas y redes, se facilita el cumplimiento del control A.10.6.1 de Controles de red, controlando las redes a las que se encuentra conectado cada uno de los equipos de la entidad. Concretamente el control afirma que se debe prevenir el acceso no autorizado a los servicios de red, tanto para las redes internas como externas y que el acceso de los usuarios a la red no comprometa la seguridad de la misma, para ello:

- Las redes y la información en tránsito en las mismas deben gestionarse y protegerse de manera adecuada.
- Los gestores y administradores de red deben implementar controles para garantizar la seguridad de los datos en la misma, y la protección de los servicios conectados contra el acceso no autorizado. En particular, no se deben descuidar los siguientes aspectos:

- Si se considera necesario, establecer una segregación de tareas que separe la responsabilidad operativa de las gestión de redes de la gestión de operaciones de sistemas.
- Se deben establecer los procedimientos y responsabilidades para la administración de equipamiento remoto, incluyendo los equipos en las áreas de usuarios.
- Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas.
- También pueden requerirse controles especiales para para proteger los sistemas conectados a las redes y mantener la disponibilidad de los servicios de red.
- Debe establecerse un registro y monitorización para permitir la grabación de las acciones relevantes respecto a seguridad que afecten a las redes.
- La gerencia de la entidad debe asegurarse para optimizar el servicio a la actividad de la empresa que los controles se aplican uniformemente a toda la infraestructura de procesamiento de información en todos los departamentos de la empresa.

Finalmente, es importante destacar el inventario *Devices*, que constituye un inventario automatizado de dispositivos (con dispositivos incluimos soportes que sean sensibles de contener información como lápices USB, discos externos, DVD, etc. Esta es la vista principal de la ficha de un dispositivo:

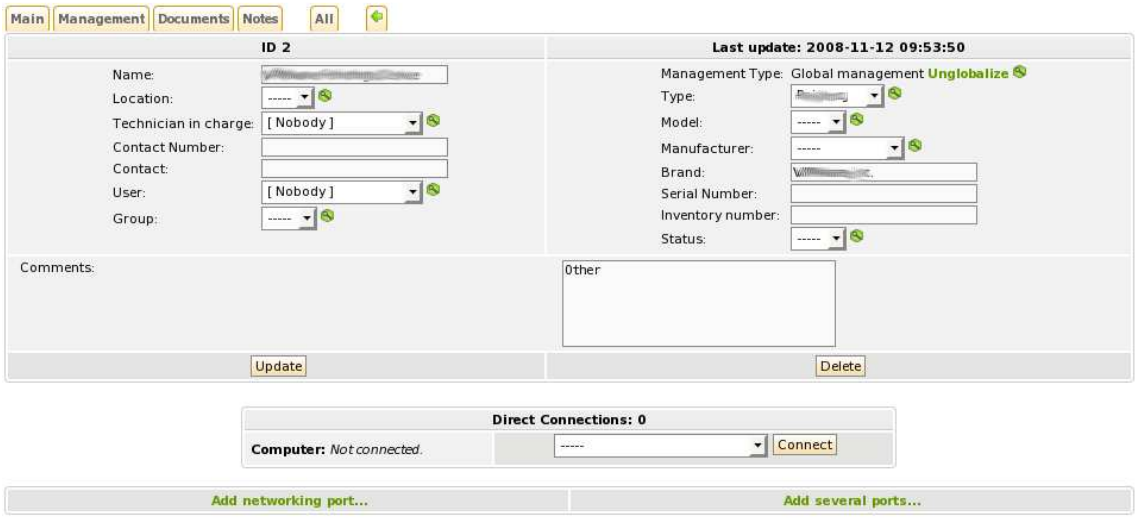


Ilustración 22 - Inventario de Activos – Devices

Como se puede observar contiene campos como nombre, localización, contacto, número de inventario, comentarios (que pueden ser empleados para dar detalles acerca del tipo de información que contiene), etc.

Requisitos RD 1720/2007:

Del mismo modo que los procesos de etiquetado facilitaban un método de etiquetado de soportes, con el inventario de soportes también se ofrecen mecanismos para cumplir con los requisitos LOPD de Gestión de Soportes y Documentos (Nivel básico) y Gestión y distribución de soportes (Nivel Alto).

Pasamos a continuación al apartado *Management*:

El primer punto de este apartado sobre el que nos centraremos es *Suppliers* (Proveedores):

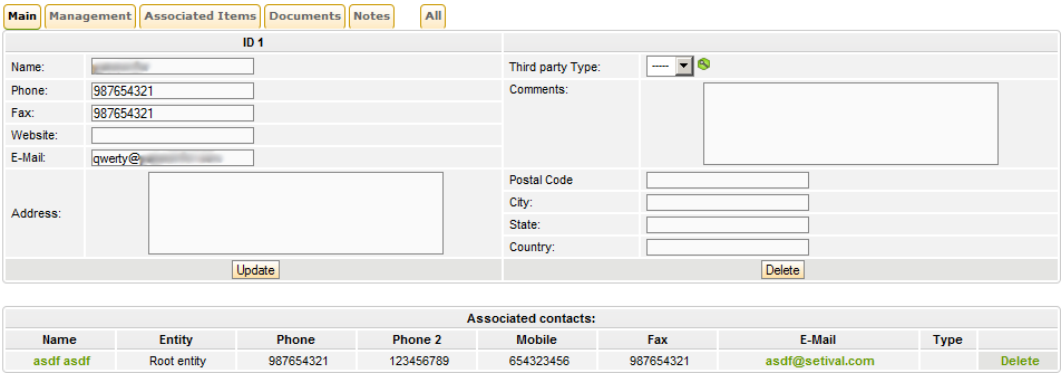


Ilustración 23 - Inventario de Activos – Suppliers

Esta es una ficha tipo de proveedores, en la cual se mantienen campos de contacto y un apartado para el tipo de proveedor, y su descripción. Es importante destacar que también se asocian a cada uno de los proveedores referencias a sus contratos asociados, cuyo inventario puede contener el mismo documento anexado a él. Facilitando la gestión de los mismos. La ficha de *Contracts* es la siguiente:

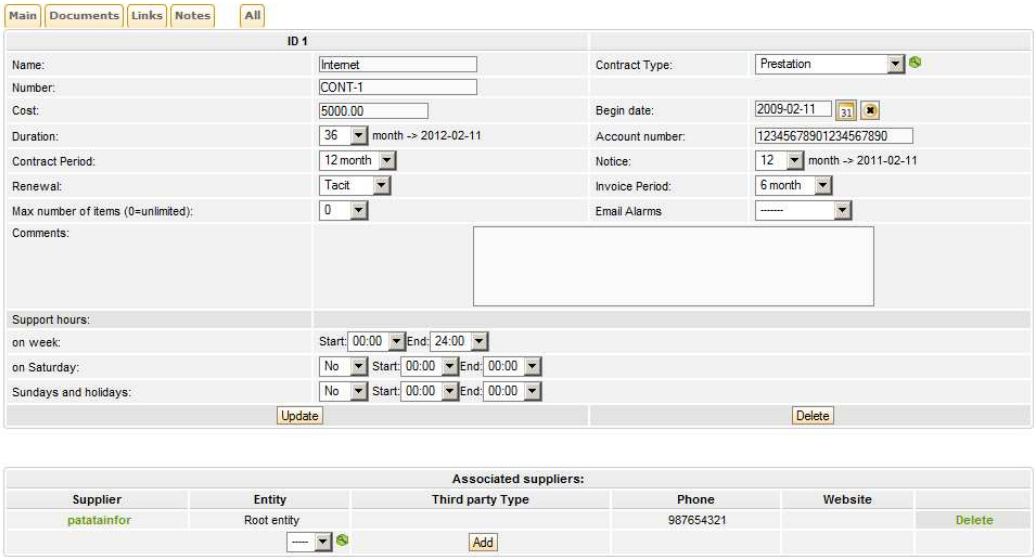


Ilustración 24 - Inventario de Activos – Contracts

Requisitos ISO/IEC 27001

En primer lugar, mediante la gestión e inventario de proveedores proporcionada por la herramienta se facilita el cumplimiento del control A.6.1.4 de Proceso de autorización de recursos para el procesado de la información, que especifica que para cada nuevo recurso de procesado de la información, debe definirse e implantarse un proceso de autorización por parte de la Dirección; considerándose una buena práctica mantener un inventario de proveedores, así como descripción de la eficacia de su servicio, y un control de la satisfacción por el mismo.

En segundo lugar, al mantener un inventario de contratos, proporciona un mecanismo para el cumplimiento del control A.6.2.3 de Tratamiento de la seguridad en contratos con terceros, que requiere permitiendo con el inventario, anotar detalles de los acuerdos, así como anexarlos y tener control centralizado de su expiración.

Para finalizar con el repaso de Inventario de Activos, se va a repasar el apartado Reports (Informes) proporcionado por la herramienta, seleccionando los informes relevantes en las normas y legislación que nos ocupa:

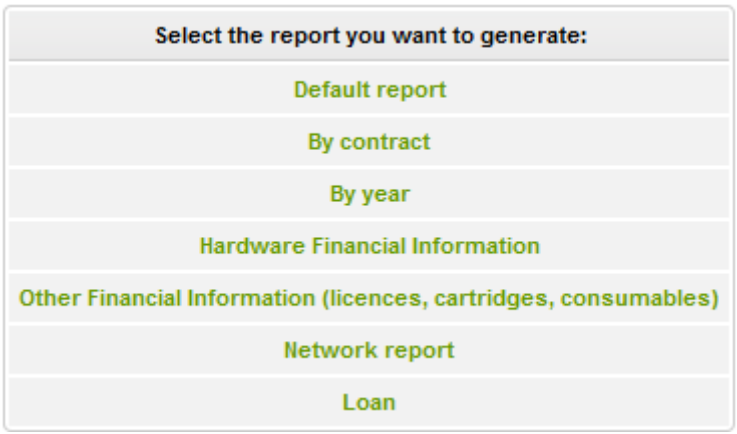


Ilustración 25 – Inventario de Activos – Reports

- *Default Report*: Da un listado tipos de objetos inventariasdos, como *Computers*, *Software*, *Networks*, etc. Indicando el número de objetos inventariados de cada tipo, además lista los sistemas operativos instalados, indicando el número de instalaciones también.
- *By contract*: Devuelve un listado de los activos afectado por un determinado contrato.
- *Network Report*: Devuelve un listado de activos asociados a una determinada red.

Requisitos ISO/IEC 27001

Se ofrece un listado de los controles de ISO/IEC 27001 apoyados por estos informes, respectivamente, ya mencionados con anterioridad:

- A.7.1 Responsabilidad sobre los activos
- A.6.2.3 de Tratamiento de la seguridad en contratos con terceros
- A.10.6.1 de Controles de red

3.4.2. Desplegar

Segunda fase del ciclo PDCA, en ella, se implementa y opera la política, controles, procesos y procedimientos del SGSI. Este módulo está formado por un repositorio con las aplicaciones cliente de los módulos de SGSI Tracking y un repositorio documental.

Ilustración 26 – SGSI Tracking - Desplegar

Como se puede observar, en primer y segundo lugar aparece una selección para la instalación de las herramientas cliente de SGSI Tracking, tanto para plataformas Windows como para plataformas basadas en UNIX.

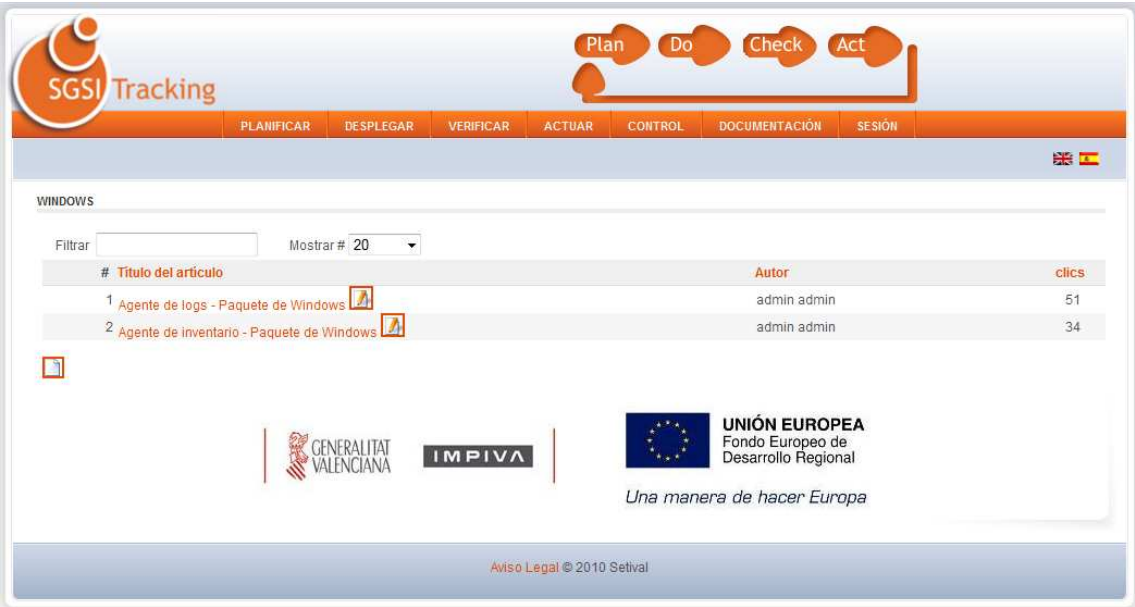


Ilustración 27 - Desplegar – Windows

En la selección de cualquiera que sea el sistema operativo que seleccionamos, nos aparecen:

- Agente de logs: Herramienta cliente del módulo correlador de eventos de SGSI Tracking.
- Agente de inventario: Herramienta cliente del módulo inventario de red de la herramienta SGSI Tracking.

No se especifican requisitos de las herramientas cliente ya que cumplen los mismos que los módulos servidores de los mismos. Por tanto se deja la descripción a los apartados correspondientes.

Solo nos queda por mencionar el apartado de Plantillas de Etiquetado, que es básicamente un pequeño gestor documental, regulado por privilegios. Es una potente herramienta que permite soportar y centralizar de forma sencilla documentación necesaria para la implantación y despliegue del SGSI de la entidad. Se propone un ejemplo para demostrar la utilidad del apartado:

Ilustración 28 - Desplegar - Plantillas de Etiquetado

Comenzaremos con los documentos públicos:

Política de Seguridad del SGSI: Documento cuyo objetivo principal es garantizar a los usuarios el acceso a la información con la cantidad y calidad que se requiere para el desempeño de sus funciones, así como evitar serias pérdidas de información y accesos no autorizados a la misma. Los principios que debe respetarse son los siguientes:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad

La definición de los conceptos se encuentra en el Anexo VII – Conceptos básicos de Seguridad de la Información. También menciona el compromiso de la Dirección y del Responsable de seguridad de apoyar y promover el establecimiento de las medidas necesarias para seguir las directrices de seguridad mencionadas.

Programa de formación en materias de Seguridad de la Información: Calendario de acciones formativas respecto a seguridad de la información de la entidad.

Requisitos ISO/IEC 27001

Los requisitos y controles de la norma ISO/IEC 27001 que se cumplen con estos documentos son para el primero:

- Requisito 4.2.1 de Creación del SGSI.
- Requisito 4.3.1 de Generalidades de Requisitos de la documentación.
- Control A.5.1.1 de Documento de Política de Seguridad de la información, que requiere que:
    - La política de seguridad establece el compromiso de la dirección y el enfoque de la organización para gestionar la seguridad de la información.
    - La política de seguridad debe ser comunicada a todos los empleados.
    - Esta política debe ser comunicada a todos los usuarios de la organización de manera pertinente, accesible y comprensible.

Y para el segundo:

- Control A.8.2.2 de Concienciación, formación y capacitación en seguridad de la información, especificando que todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.

Documentos privados:

Procedimiento de alta y baja de usuarios: El objeto del presente documento es describir las medidas de control de acceso lógico aplicadas a los sistemas de la entidad así como controlar y restringir el acceso y uso de los sistemas de información de la entidad.

Etiquetado de equipos: Establece las directrices para realizar un marcado y uso de la información de la entidad de manera correcta.

Mantenimiento de equipamiento: Instrucción técnica que describe los procedimientos y tareas periódicas a realizar por los administradores para mantener adecuadamente el equipamiento relacionado con el SGSI.

Requisitos ISO/IEC 27001 y RD 1720/2007

Del mismo modo, se pasa a describir los requisitos satisfechos por los documentos privados:

Para el Procedimiento de alta y baja de usuarios:

- Requisitos de Control de acceso de las medidas técnicas del RD 1720/2007.

- Control A.8.3.3.de Retirada de los derechos de acceso, que requiere que los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.
- Control A.11.2.1 de Registro de usuario, que establece que se deben establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios. Estos procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el alta inicial de los nuevos hasta la baja de los usuarios que ya no requieran dicho acceso a los sistemas y servicios.

Para el etiquetado de equipos:

- Requisitos de Gestión de soportes y documentos de las medidas técnicas del RD 1720/2007.

Para el mantenimiento de equipamiento:

- Control A.9.2.4 de Mantenimiento de los equipos por el cual el equipamiento debe mantenerse correctamente para asegurar su disponibilidad continuada e integridad Además, el equipamiento deberá mantenerse conforme a las recomendaciones e intervalos especificados por el fabricante. Sólo el personal de mantenimiento autorizado debe realizar las tareas de mantenimiento y reparación del equipo.

En cualquier caso se insiste en que esto es un pequeño ejemplo, se podría integrar en este gestor gran parte de la documentación tanto del SGSI como requerida por la LOPD.

3.4.3. Verificar

Tercera fase del ciclo PDCA, en ella, se debe evaluar y medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, e informar los resultados a la Dirección para su revisión. Está formado por dos módulos:

- Monitorización de equipos
- Correlador de Eventos
- Marcadores

Se muestra a continuación una captura inicial de la fase:

Ilustración 29 – SGSI Tracking - Verificar

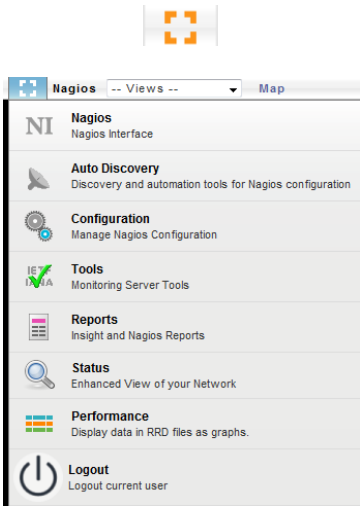
Monitorización de Equipos

El siguiente módulo integra la herramienta Nagios, que es una aplicación de monitorización activa de la red, que permite llevar a cabo el control de las máquinas conectadas a la red, y los servicios que estas máquinas proveen.

Ilustración 30 – SGSI Tracking - Monitorización de Equipos

Integración

Se considera interesante para la descripción de este módulo centrarnos, en primer lugar, en la forma de añadir equipos a la monitorización, y finalmente se estudiarán las vistas e informes de Nagios más adecuadas a las necesidades de la reglamentación. Comencemos por *Auto discovery* (Detección Automática).



Auto discovery pone a nuestra disposición realizar búsqueda de rangos de IP que nos permitirá descubrir que equipos se monitorizarán, así como las características de cada uno. Se muestra una ventana de resultado de búsqueda.

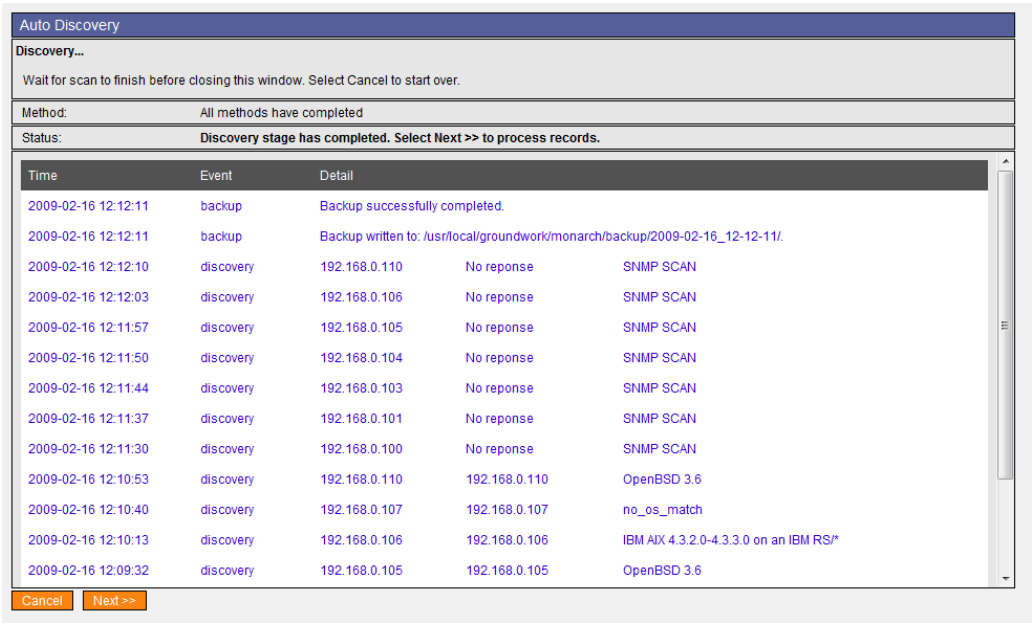


Ilustración 31 - Monitorización de Equipos - Autodiscovery

Muestra un listado de las IP encontradas, lo que nos lleva directamente a configurar los elementos encontrados por dicho proceso.

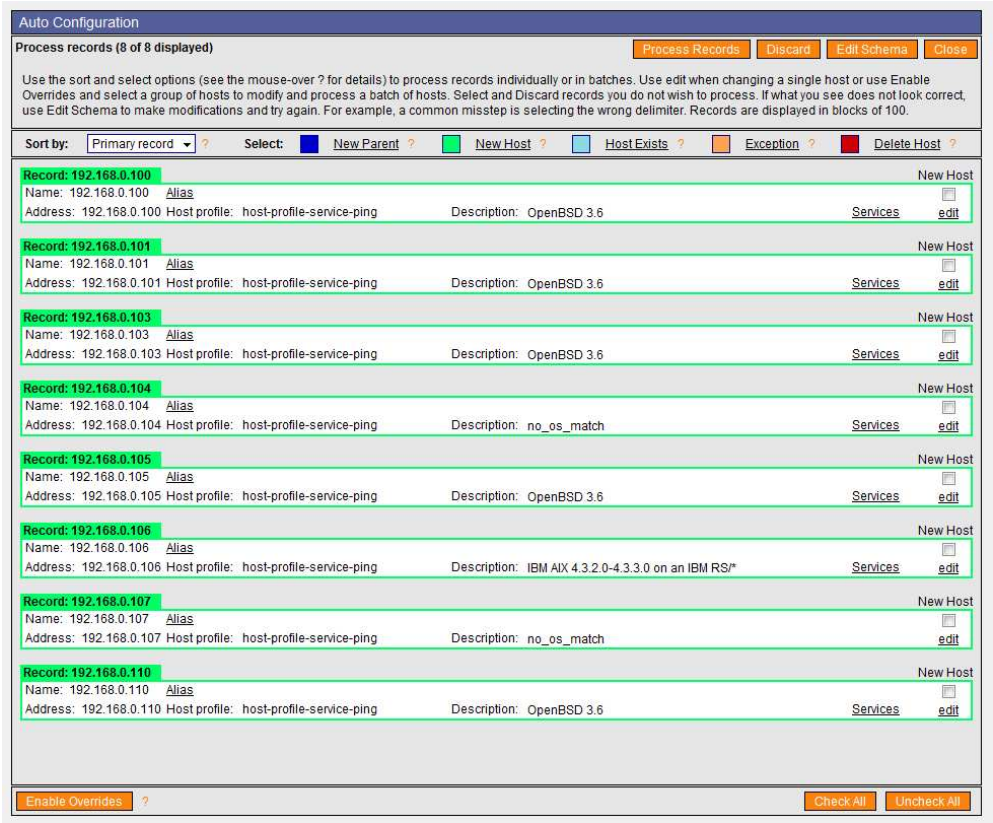


Ilustración 32 - Monitorización de Equipos - Aunto Configuration

En este paso se nos muestran dos atributos principales de cada uno de los *hosts* encontrados:

- *Alias*: Nombre del equipo en la red.
- *Services*: Servicios detectados por la aplicación.

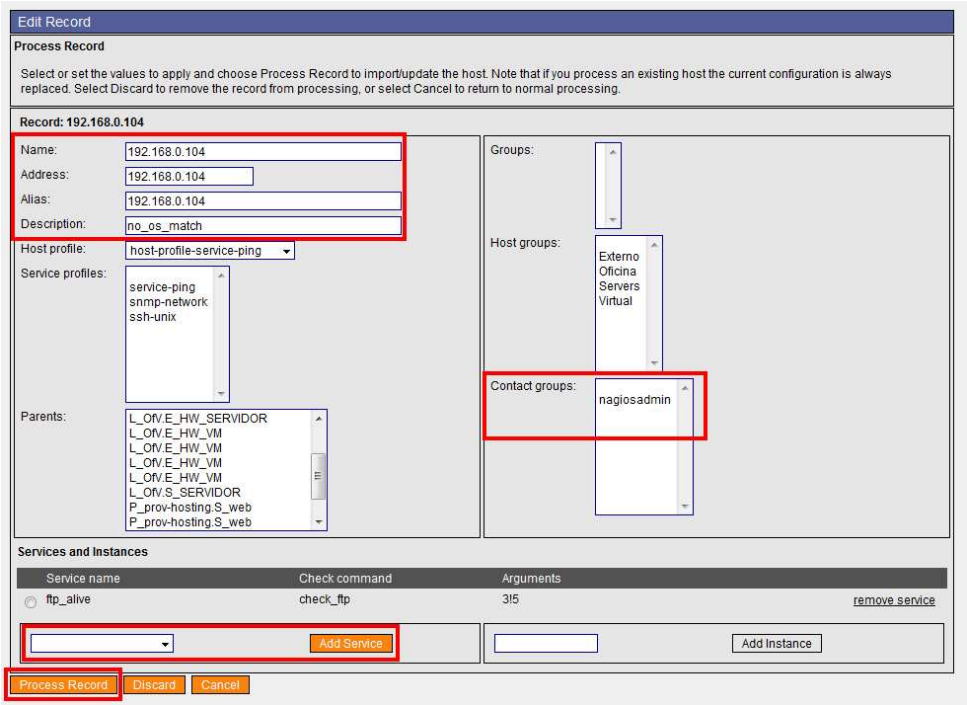


Ilustración 33 - Monitorización de Equipos - Edit Record

Por último cabe comentar que se puede añadir información extra a la ficha de cada *Host* en Nagios. Se resaltan en la ilustración los campos alias, descripción y grupos a los que pertenece, entre otros.

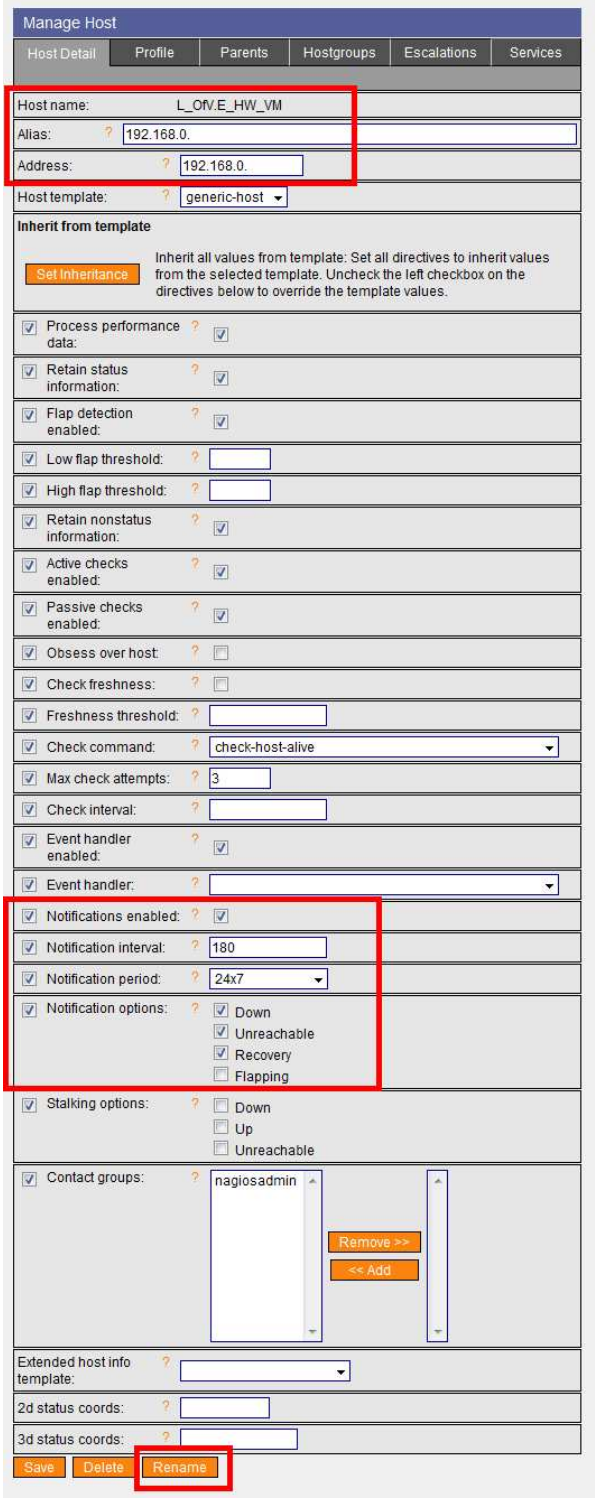


Ilustración 35 - Monitorización de Equipos - Manage Host - Host Details

El siguiente punto a repasar es *Configuration*, en el cual se pueden añadir más opciones y avisos a los Host cuando ya están inventariados. En la ilustración 35, se muestran de nuevo los campos básicos, y en la parte inferior los tipos de alerta que queremos recibir de este host. Se ofrecen diversas posibilidades de alerta:

- *Down*: Si se cae el *Host*.
- *Unreachable: Host* inalcanzable.
- *Recovery: Host* alcanzado de nuevo.
- *Flapping:* El Host aparece y desaparece varias veces en un corto periodo de tiempo.

En la ilustración 34, se muestran las opciones de cada servicio que soporta la máquina. Permitiendo seleccionar y añadir servicios a monitorizar. De este modo también se recibirán alertas cuando el servicio haya caído. Estas alertas se mandan automáticamente al módulo Gestión de Incidencias de SGSI Tracking.

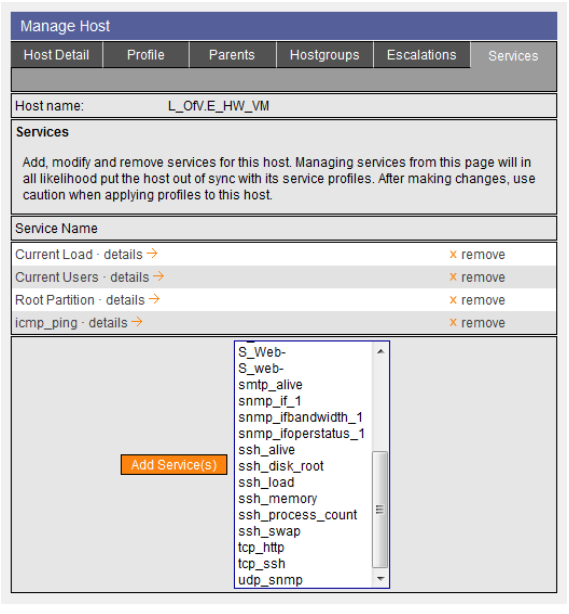


Ilustración 34 - Monitorización de Equipos - Manage Host - Services

Requisitos ISO/IEC 27001

Mediante las capacidades de la herramienta Nagios, se facilita el cumplimiento de los siguientes controles de la norma ISO 27001:

Primero, el control A.10.6.1 de Controles de red, antes mencionado en el apartado de Inventario de Activos.

El control A.10.6.2 de Seguridad de los servicios de red, que recomienda:

- Que los requisitos de seguridad, niveles del servicio, y requisitos de la administración de todos servicios de red deberían identificarse y ser incluidos en cualquier acuerdo de servicios de red. Esto debe hacerse con independencia de si estos servicios se proporcionan entre departamentos de la compañía o se subcontratan a terceros.
- Los servicios pueden ir del uso de ancho de banda sin control alguno a servicios de valor añadido. Algunos ejemplos de ítems que proporcionan seguridad a nivel de red:
    - Tecnologías aplicadas a la seguridad de servicios de la red, como autenticación, encriptación y control de conexiones de red.
    - Parámetros técnicos requeridos para efectuar la conexión de forma segura.
    - Procedimientos para el restringir uso de servicios de red.

El control A.11.4.3 de Identificación de equipos en las redes, que especifica que:

- El uso de identificación automática en los equipos debe ser considerada para autenticar conexiones desde equipos y localizaciones específicas.
- Puede utilizarse un identificador en los equipos que indique si este equipo se puede conectar a la red.
- Puede ser necesario considerar protección física del equipo para mantener la seguridad del identificador de equipo.
- La identificación de equipo puede aplicarse adicionalmente a la autenticación del usuario en equipos o conexiones que requieran una seguridad más elevada.

Por último el control A. 10.3.1 de Gestión de la Capacidad, ya mencionado en el Inventario de activos, mediante la monitorización de disponibilidad y eficiencia de los equipos.

El siguiente paso es volver a la vista principal de Nagios, y repasar la vista principal que Nagios que nos ofrece.

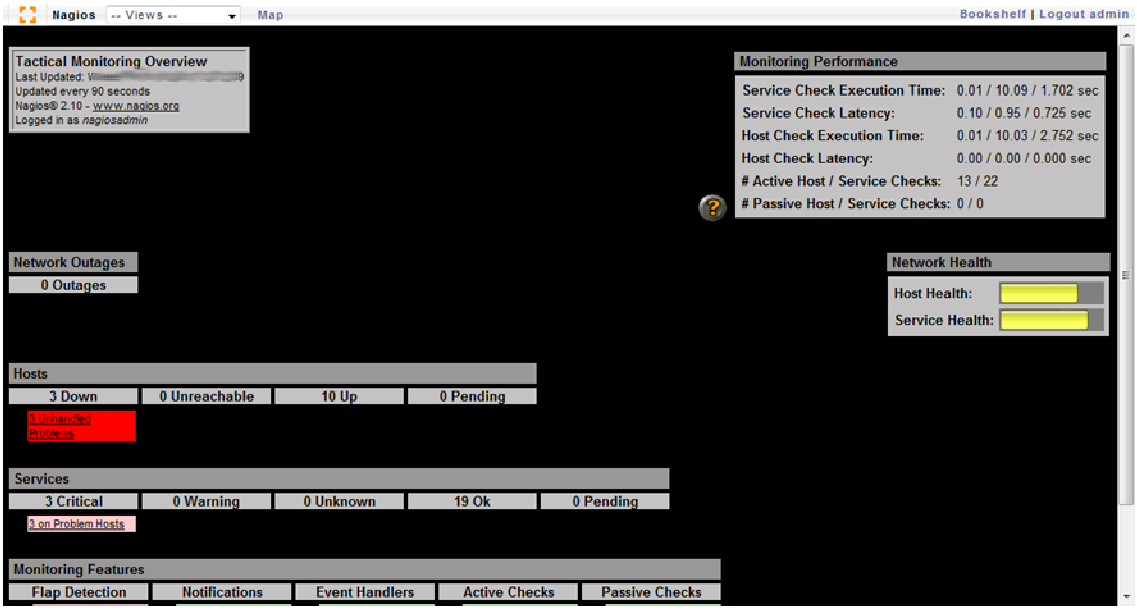


Ilustración 36 - Monitorización de Equipos - Vista principal

La vista principal contiene los equipos y servicios monitorizados. Los apartados *Hosts* y *Services* ofrecen un resumen del número de cada uno de ellos que están caídos, inalcanzables o desconectados. Pulsando sobre cada uno se muestra un listado de los equipos o servicios que se encuentran en ese estado.

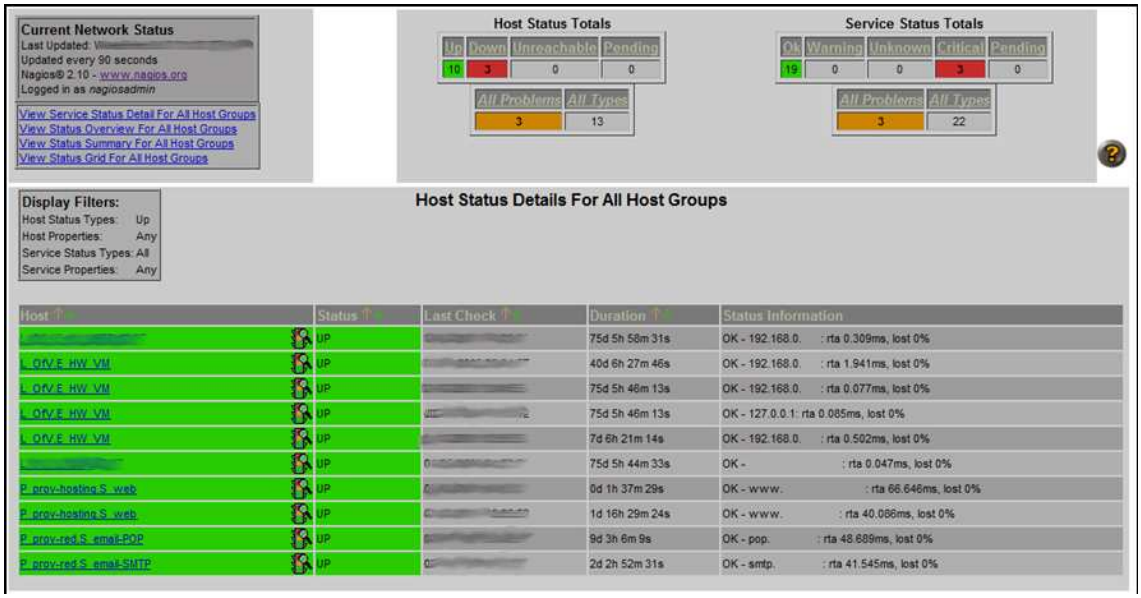


Ilustración 37 - Monitorización de Equipos - Host up

En esta tabla informa de la última vez visto en otro estado, la duración del estado actual, así como el porcentaje de paquetes perdidos en la última comunicación con los equipos. Si pulsamos sobre alguno de los Hosts, obtenemos una vista detallada de su estado.

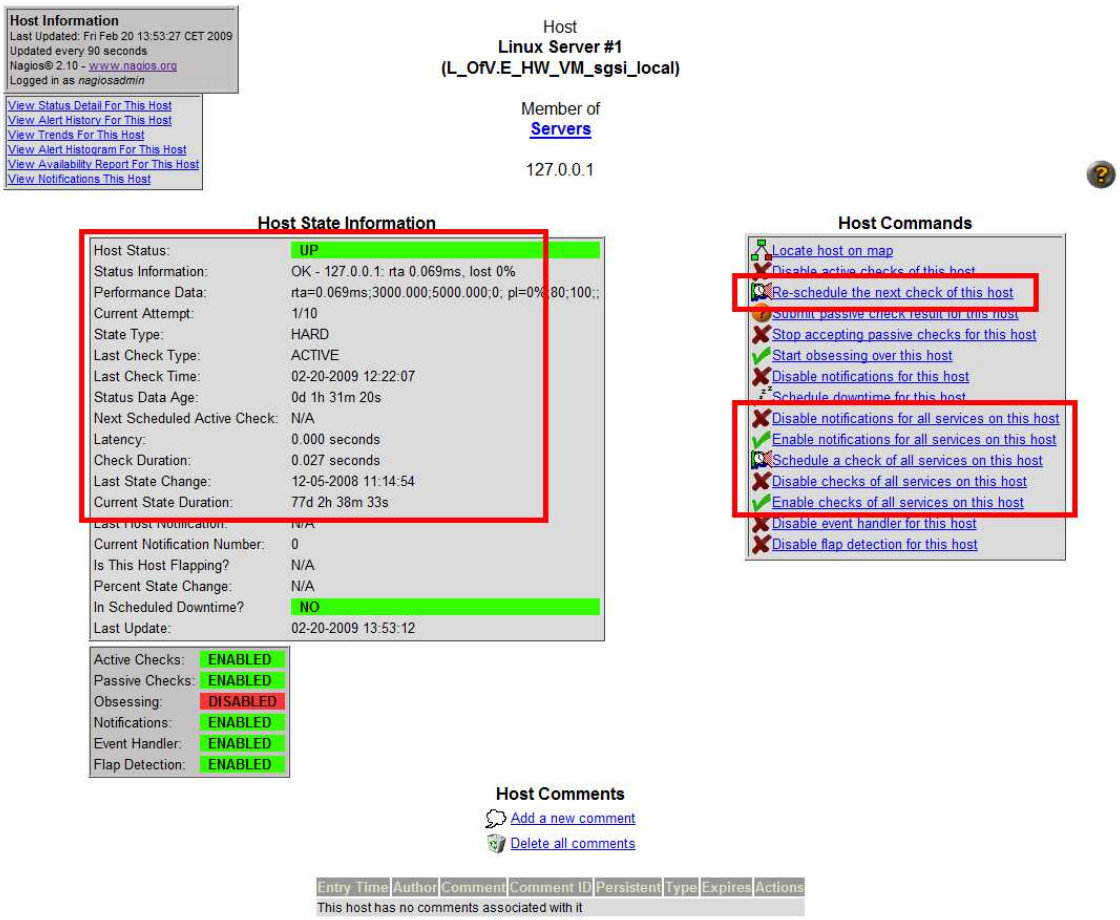


Ilustración 38 - Monitorización de Equipos - Ficha de Host

En la ilustración 38 se remarcan diversos aspectos de la ficha de Host ofrecida por Nagios, en primer lugar, destacamos los datos informativos del host, concretamente campos como estado actual (*Host Status*), el resultado detallado del servicio chequeado (*Status Information*), tiempos del último/siguiente chequeo (*Last Check Time, Next Scheduled Active Check*) y el último cambio de estado (*Last State Change*), entre otros. Despues se han marcado también comandos a ejecutar para la configuración de la monitorización de la máquina, se detallan a continuación:

- *Re-scheudle the next check of this host*: Fuerza la sincronización del *Host* al momento.
- *Scheudle a check of all services on this host:* Fuerza la sincronización de los servicios asociados al *Host*.
- *Disable/enable notifications for all services on this host*: Habilita/deshabilita el envoi de notificaciones ante cambios en los servicios del *Host* actual.
- *Disable/Enable checks of all services on this host*: Habilita/deshabilita las sincronizaciones automáticas de los servicios del *Host* actual.

Requisitos ISO/IEC 27001

Con las capacidades descritas se cumple, del mismo modo, los requisitos correspondientes al control A.10.6.2 de Seguridad de los servicios de red, mostrado anteriormente.

Es importante destacar que Nagios dispone de diferentes vistas de menú que nos permiten ver el estado de Host y servicios presentados atendiendo a resúmenes o a problemáticas concretas de cada tipo. No se muestran en detalle ya que cumplen los mismos requisitos mencionados con anterioridad.

Ilustración 39 - Monitorización de Equipos - Vistas de Nagios

Por último, comentar es el apartado *Reports* (informes), que nos proporciona mecanismos para generar informes personalizados sobre los datos que maneja la aplicación.

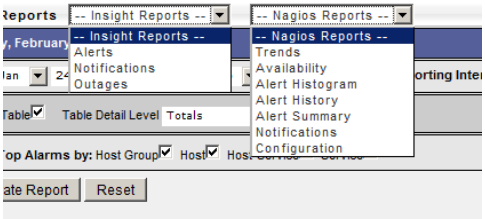


Ilustración 40 - Monitorización de Equipos

Se pueden observar claramente dos menús que se corresponden con dos tipos distintos de informe:

- *Insight Reports*: Son informes personalizables, destinados a la comprensión del sistema completo, ya que son informes que nos muestran informes globales de alarmas, avisos y notificaciones de la red global. Todo esto acompañado por gráficas representativas de periodos de tiempo, y de valores tan representativos como clasificaciones por *host*, por grupos de *host*, por *host* y servicio, etc. Se muestra un ejemplo en la ilustración 41.

- *Nagios Reports*: Son básicamente informes, en los que, tras seleccionar un *host* o un servicio, obtenemos resultados temporales de tendencias, disponibilidad, histogramas de alertas y notificaciones enviadas por la aplicación, entre otros. Se puede observar un ejemplo de los resultados en la ilustración 42.

Ilustración 41 - Monitorización de Equipos - Insight Records

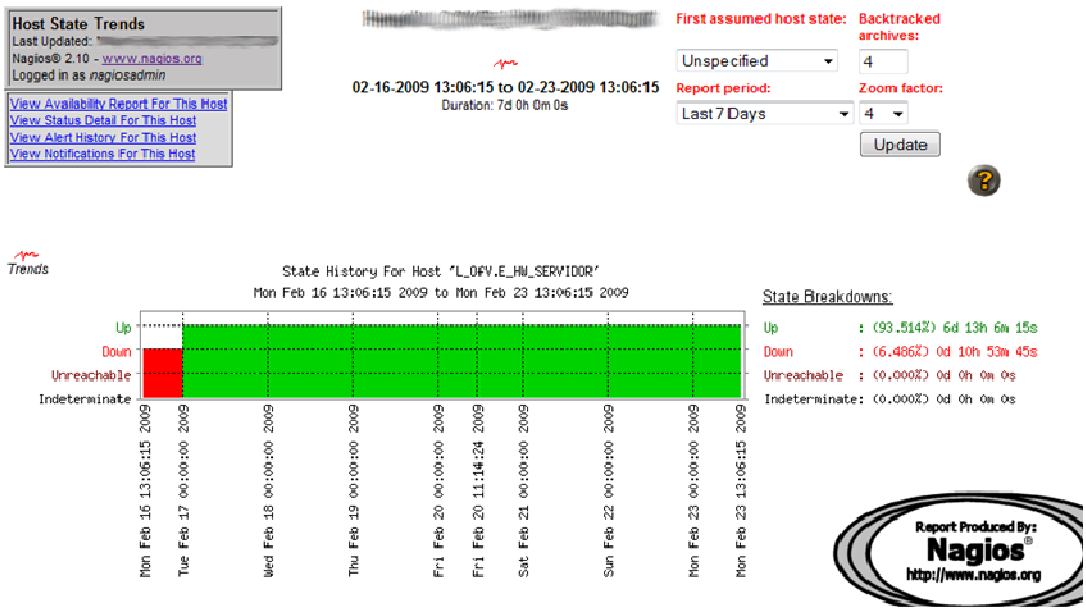


Ilustración 42 - Monitorización de Equipos - Nagios Reports

Requisitos ISO/IEC 27001

Mediante lageneración de estos informes de rendimiento de Host y servicios, así como controlando hasta el mínimo detalle la disponibilidad de los mismos, se facilita el cumplimiento de los siguientes controles de la norma ISO 27001, mencionados anteriormente:

El control A.10.6.1 de Controles de red, antes mencionado en el apartado de Inventario de Activos.

El control A.10.6.2 de Seguridad de los servicios de red, mostrado anteriormente.

Correlador de Eventos

El siguiente módulo del apartado verificar de SGSI Tracking es el Correlador de eventos, que integra la herramienta Splunk. Consiste básicamente en un log de eventos de sistema centralizado, facilitando la revisión de logs de seguridad de clientes y servidores.

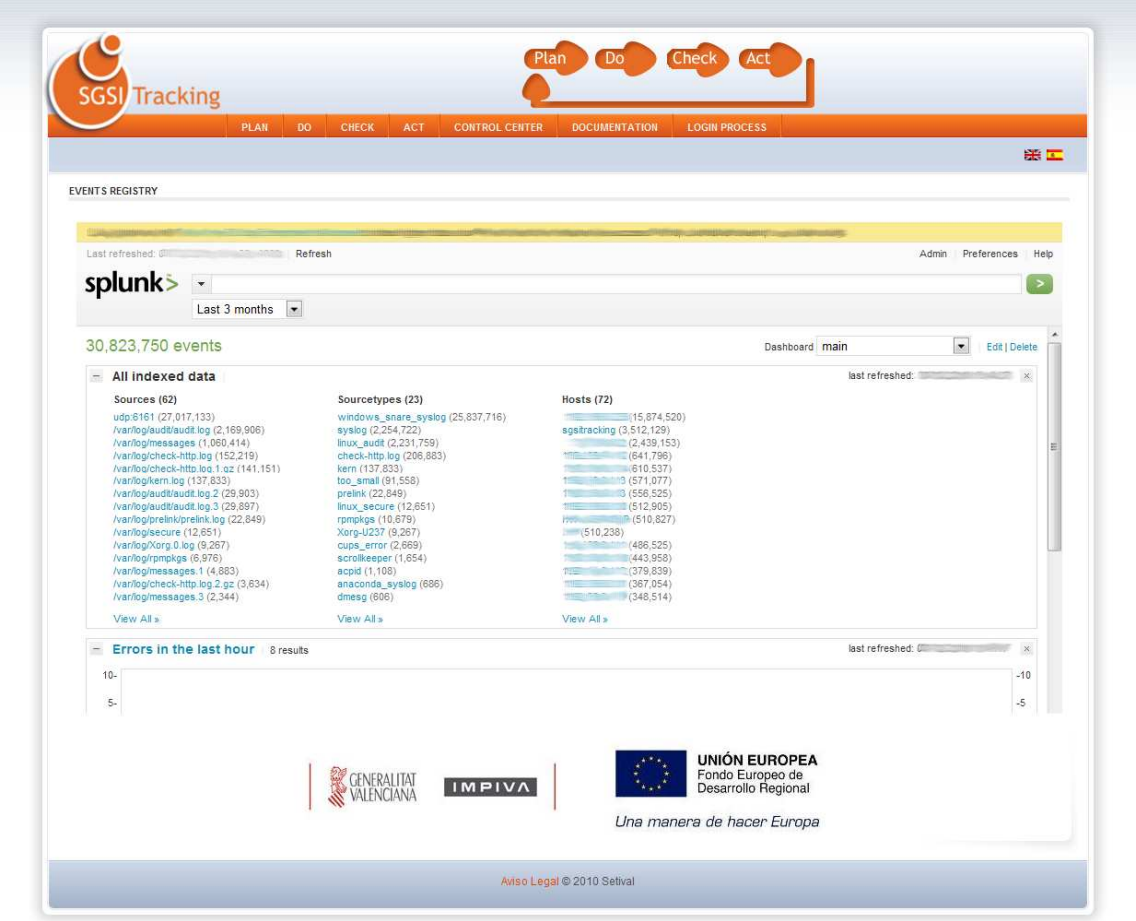


Ilustración 43 - SGSI Tracking - Correlador de Eventos

Integración

Para comenzar, se van a describir las posibilidades de Splunk para la búsqueda de eventos, obteniendo así informes y gráficos personalizados.

Ilustración 44 - Correlador de Eventos - Barra de búsqueda

En la ilustración 44 se muestra la barra de búsqueda de Splunk, en ella se pueden introducir búsquedas de acuerdo a patrones que se le introduzcan. Estos patrones se pueden establecer de acuerdo a cualquier parte del contenido de los eventos recogidos por la herramienta, por ejemplo se puede buscar por número de evento, por *host*, etc. Es importante

destacar que además se pueden emplear periodos de tiempo bien establecidos por la herramienta o perfectamente personalizados.

Ilustración 45 - Correlador de Eventos - Selección de periodo temporal

Una vez realizada la búsqueda se muestran los resultados mediante el *Dashboard* correspondiente.

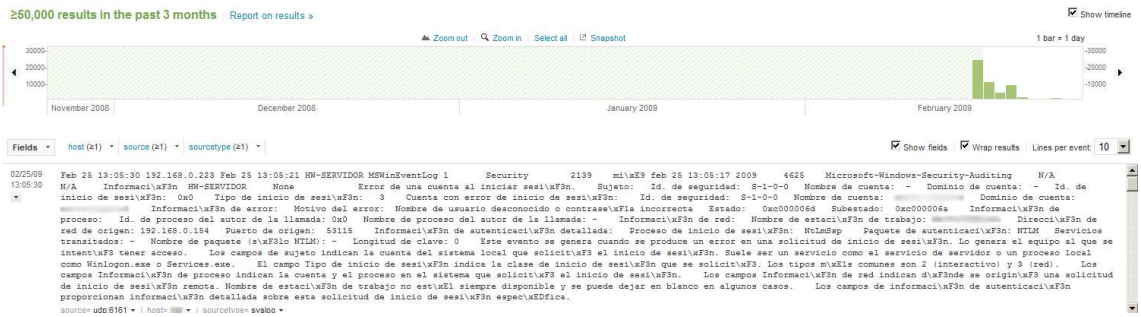


Ilustración 46 - Correlador de Eventos - Dashboard de búsqueda

El Dashboard está formado básicamente por gráficas temporales que indican el número de evento por periodo de tiempo (dependiendo de los criterios empleados para la búsqueda) y por el listado de los eventos generados por la misma.

Es importante destacar, a su vez, que se pueden programar búsquedas, de modo que se facilita mantener un conjunto de ellas que faciliten la auditoría del log de sistemas.

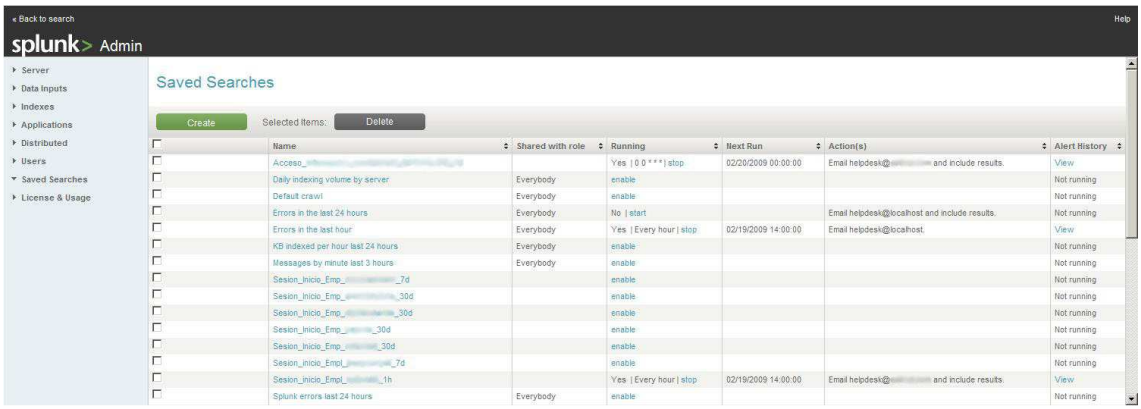


Ilustración 47 - Correlador de Eventos - Saved searches

El proceso de creación de búsquedas se realiza mediante el siguiente formulario.

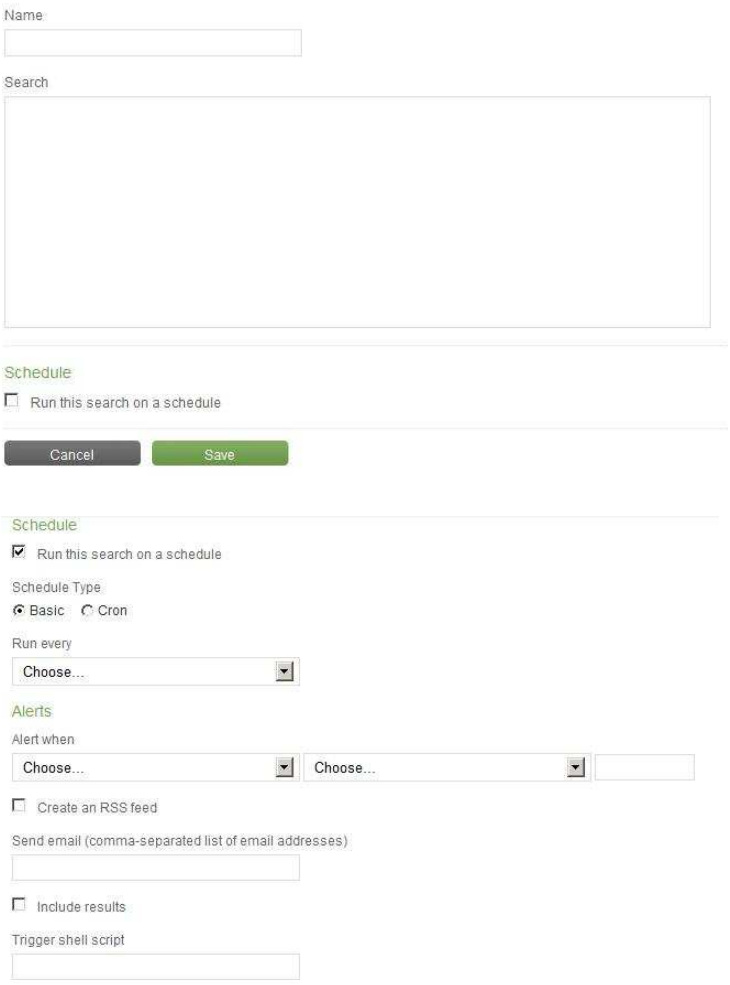


Ilustración 48 - Correlador de Eventos - Create Saved Search

Como se puede observar, en su forma más elemental, la creación de una búsqueda guardada nos permite darle un nombre y el comando de búsqueda. Aunque aparece el

comando *Scheudle* (Planificar), el cual cuando lo habilitamos nos da la posibilidad de realizar búsquedas automatizadas planificadas. Entre sus opciones cabe destacar la posibilidad de que cada vez que se ejecute la búsqueda se envíe un log via *email*.

Es importante destacar que tan importante es la configuración del servidor Splunk como del cliente Snare, que será el encargado de seleccionar los registros del sistema operativo local y enviarlos al puerto de recepción de eventos del servidor Splunk. Se muestra a continuación una captura del menú de selección de eventos a auditar de Snare.

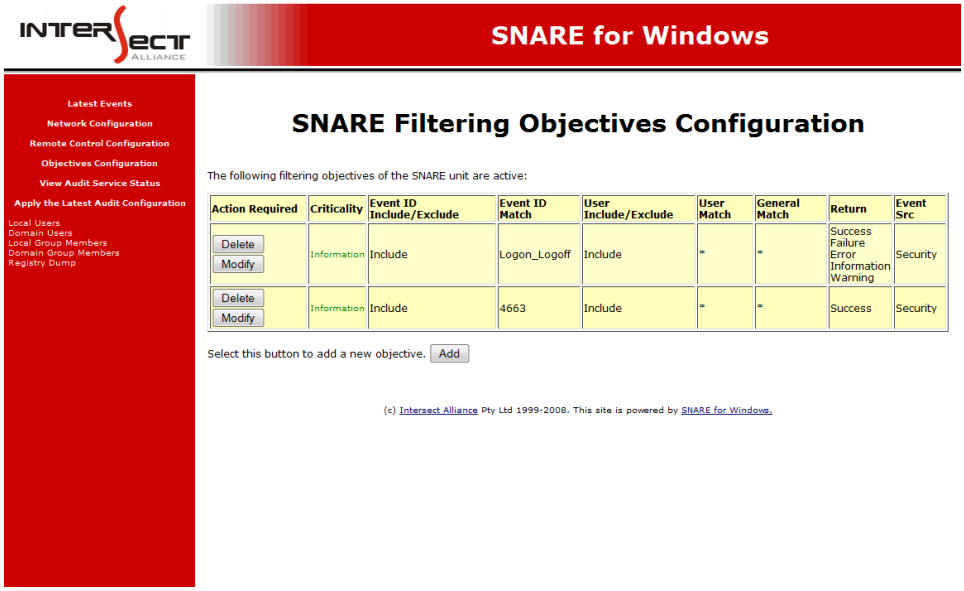


Ilustración 49 - Correlador de Eventos - Snare – Objectives

Del mismo modo se muestra la pantalla de creación de una entrada en el listado de eventos auditados.

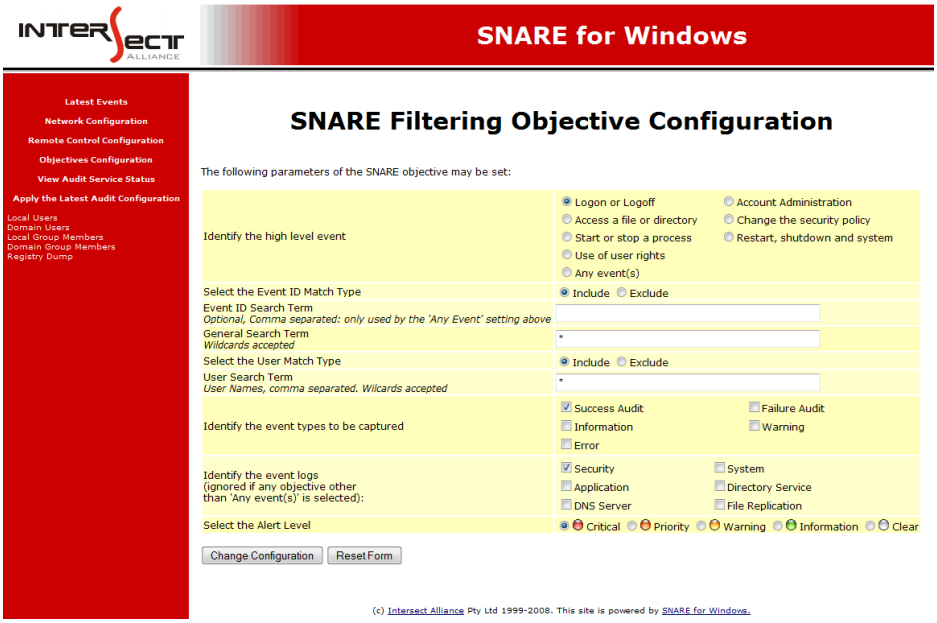


Ilustración 50 - Correlador de Eventos - Snare - Objective Configuration

Como se puede observar, el menú nos permite seleccionar el grupo de eventos de alto nivel de forma pre configurado con la herramienta. Aunque también se nos permite realizar una selección personalizada por número de eventos, términos de búsqueda, tipo de evento (auditoría satisfactoria, fallo de auditoría, informativo, alerta o error), log de eventos del sistema del que se extrae y criticidad asignada por el usuario. Facilitando la preselección de eventos importantes para auditoría y evitando saturar la red con envío de *logs* completos.

Como se ha podido observar, aún no se ha especificado ningún tipo de requisitos de la normativa objeto del siguiente proyecto, esto es debido a que la información que nos otorga el Correlador de eventos proviene de los *log* de los sistemas operativos que soporten cada uno de los equipos que integren la red y se deseen monitorizar, por lo que los requisitos cumplidos dependerán de la capacidad de cada sistema y de la selección de los eventos adecuados. De este modo, y con el fin de ilustrar la capacidad de este módulo se procede a seleccionar eventos a auditar de un sistema ejemplo. Para ello se empleará la librería de eventos de Windows Vista/7/Server 2008.

Se muestra a continuación una tabla con los eventos seleccionados más relevantes para auditoría de la legislación objeto de estudio, a continuación se mencionarán los requisitos que se cumplen mediante la monitorización de dichos eventos. Se seguirá la organización propia del mismo registro de Seguridad de Windows.

Eventos seleccionados del log de Seguridad de Windows Vista/7/Server 2008

Evento	**Descripción**	**Información relevante**
	Account Logon	
4678	Solicitud de ticket de autentificación de Kerberos	Nombre de Cuenta que reclama el ticket Identificador del servicio destino Dirección IP y puerto del cliente
4679	Solicitud de ticket de servicio de Kerberos	La misma que 4678
4772	Fallo en solicitud de ticket de autentificación de Kerberos	La misma que 4678
4773	Fallo en solicitud de ticket de servicio de Kerberos	La misma que 4678
4776	El controlador de domino intenta validar credenciales para una cuenta	Nombre de la cuenta Nombre del terminal desde el que accede Código de error que detecta: - Nombre de usuario incorrecto - Usuario bloqueado - Usuario que intenta loguear fuera de sus periodos temporales establecidos - Cuenta o contraseña caducados
4777	El controlador de domino falla al validar credenciales para una cuenta	La misma que 4776

Account Management

4720	Una cuenta de usuario nueva ha sido creada	Nombre y dominio de la cuenta administración Nombre y dominio de la nueva cuenta Nombre del usuario de la cuenta nueva Indicadores de la nueva cuenta: - Indicador de si la cuenta requiere contraseña - Caducidad de la cuenta y de la clave introducida - Cuenta deshabilitada - Periodos autorizados de acceso de la cuenta - Privilegios (Administrador o no)
4720	Una cuenta de usuario ha sido habilitada	Nombre y dominio de la cuenta administración Nombre y dominio de la cuenta habilitada
4723	Se ha realizado un intento de modificación de la contraseña de una cuenta	La misma que 4720
4724	Se ha realizado un intento de reiniciar la contraseña de una cuenta	La misma que 4720
4725	Se ha deshabilitado una cuenta de usuario	La misma que 4720
4726	Se ha eliminado una cuenta de usuario	La misma que 4720
4738	Se ha realizado un cambio en una cuenta de usuario	La misma que 4776
4739	Se ha realizado un cambio en la política del dominio	Detalla cual es el cambio concreto en la política: - Caducidad de contraseñas - Umbral de bloqueo de cuentas - Duración del bloqueo - Requisitos de longitud y complejidad de contraseñas - Histórico de contraseñas
4740	Se ha bloqueado una cuenta de usuario	Nombre y dominio de la cuenta que bloquea Nombre de la cuenta bloqueada
4741	Se ha dado de alta un equipo en el dominio	Nombre y dominio de la cuenta administración Nombre y dominio de la nueva cuenta

4742	Se ha modificado una cuenta de equipio del dominio	La misma que 4741
4743	Se ha eliminado una cuenta de equipo del dominio	La misma que 4741
4764	Se ha modificado el tipo de un grupo	Nombre y dominio del grupo Privilegios modificados
4767	Se ha desbloqueado una cuenta de usuario	
	Logon/Logoff	
4624	La cuenta se ha autentificado adecuadamente	Identificación de la cuenta que autentifica Identificación y tipo de autentificación Red desde la que se realiza la autentificación
4625	Una cuenta ha fallado en la autentificación	Los mismos que 4624, solo que se añade un código para averiguar el contexto del fallo
4634	Una cuenta se ha desconectado	La misma que 4624
4650	Se ha establecido una conexión IPSec (conexión remota segura)	Datos del nodo local y remoto
4652	Ha fallado la negociación de una conexión IPSec	La misma que 4650
4655	Ha finalizado una conexión IPSec	La misma que 4650
	Non Audit (Event Log)	
1100	El servicio del registro de eventos se ha caido	N/A
1102	El registro de eventos se ha borrado	N/A
1104	El registro de eventos está lleno	N/A
1105	Copia de seguridad autmática del registro de eventos	N/A
1108	El servicio del registro de eventos ha generado un error	N/A
	Object Access	
4656	Se ha solicitado un manejador para un objeto (Se solicita antes de cualquier operación sobre un fichero o carpeta auditado)	Nombre y dominio de la cuenta que realiza el acceso Tipo y nombre del objeto que se accede (Ruta de fichero incluida) Enlace con el siguiente evento sobre el objeto

4657	Un valor del registro de sistema se ha modificado	Nombre y dominio de la cuenta que realiza el acceso Datos identificativos de la entrada de registro modificada Valores anterior y posterior del registro
4658	Se ha cerrado el manejador para un objeto	La misma que 4656
4660	Un objeto ha sido eliminado	La misma que 4656
4663	Se ha accedido a un objeto	La misma que 4656
4670	Se han modificado los permisos sobre un objeto	La misma que 4656
4698	Se ha creado una tarea programada	Nombre y dominio de la cuenta que realiza la acción Nombre de la tarea programada Contenido de la tarea (XML con las propiedades de la tarea)
4699	Una tarea programada ya sido eliminada	La misma que 4698
4700	Una tarea programada ha sido habilitada	La misma que 4698
4701	Una tarea programada ha sido deshabilitada	La misma que 4698
4702	Una tarea programada ha sido actualizada	La misma que 4698
4868	El administrador de certificados ha denegado una solicitud pendiente de un certificado	N/A
4870	El servicio de certificados ha revocado un certificado	Número de serie del certificado Razón
4876	Copia de seguridad del servicio de certificado iniciada	Tipo de Backup
4877	Copia de seguridad del servicio de certificado finalizada	N/A
4880	Se ha iniciado el servicio de certificado	N/A
4881	Se ha detenido el servicio de certificados	N/A
4887	El servicio de certificado aprobó un certificado y expidió un certificado	Estado de la petición Nombre y clave del sujeto del certificado
5140	Se ha accedido a un objeto de red	Nombre y dominio de la cuenta que realiza la operación Dirección IP y puerto del origen de la creación Nombre del objeto compartido en red
5142	Un objeto de red ha sido añadido	La misma que 5140

5143	Un objeto de red ha sido modificado	La misma que 5140
5144	Un objeto de red ha sido eliminado	La misma que 5140
5150	La plataforma de filtro de Windows ha bloqueado un paquete	Origen y destino del paquete Tipo de paquete
5154	La plataforma de filtro de Windows ha permitido a una aplicación recibir por un puerto conexiones entrantes	Nombre de la aplicación Dirección, puerto, y protocolo de la comunicación Características del filtro
5155	La plataforma de filtro de Windows ha bloqueado a una aplicación recibir por un puerto conexiones entrantes	La misma que 5154
5156	La plataforma de filtro de Windows ha permitido una conexión	La misma que 5154
5157	La plataforma de filtro de Windows ha bloqueado una conexión	La misma que 5154
	Policy Change	
4704	Se ha asignado un derecho de usuario	Nombre y dominio de la cuenta que realiza la modificación Nombre y dominio de la cuenta objeto de la modificación Derecho modificado
4705	Se ha eliminado un derecho de usuario	La misma que 4704
4706	Una regla para un dominio se ha creado	Nombre y dominio de la cuenta que realiza la modificación Dominio objeto de la modificación Regla
4707	Una regla para un dominio se ha eliminado	La misma que 4705
4709	El servicio IPSec se ha iniciado	N/A
4710	El servicio IPSec se ha detenido	N/A
4713	Ha cambiado la política de Kerberos	Nombre y dominio de la cuenta que realiza la modificación Cambios realizados
4715	La política de acceso de un objeto ha cambiado	Nombre y dominio de la cuenta que realiza la modificación Objeto modificado Descriptores de seguridad original y modificado
4717	Se ha dado acceso de seguridad al sistema a una cuenta	Nombre de la cuenta objeto de la modificación Accesos que se han modificado

4718	Se ha denegado acceso de seguridad al sistema a una cuenta	La misma que 4718
4817	La política de auditoría a un objeto ha cambiado	Nombre y dominio de la cuenta que realiza la modificación Objeto modificado Descriptor de seguridad original y modificado
4946	Se ha añadido una excepción al cortafuegos de Windows	Nombre de la regla objeto de la modificación
4947	Se ha modificado una excepción del cortafuegos de Windows	La misma que 4946
4948	Se ha eliminado una excepción del cortafuegos de Windows	La misma que 4946
4950	Se ha cambiado la configuración del cortafuegos de Windows	Nombre y dominio de la cuenta querealiza la modificación Nueva configuración
	System	
4608	Windows se está iniciando	N/A
4609	Windows se está apagando	N/A
4616	La hora del sistema ha cambiado	Nombre y dominio de la cuenta que realiza el cambio Identificación del proceso que realiza el cambio Hora original y modificada
5024	El servicio de cortafuegos de Windows se ha indicado satisfactoriamente	N/A
5025	El servicio del cortafuegos de Windows se ha detenido	N/A
5030	El servicio del cortafuegos de Windows ha fallado al iniciar	N/A

Tabla 1 - Eventos de Seguridad de Windows Vista/7/Server 2008

Una vez mostradas las posibilidades, se muestra una pequeña selección de los controles que se pueden satisfacer con las capacidades del módulo Splunk y los contenidos del registro de Windows Vista/7/Server 2008.

Requisitos ISO/IEC 27001

Mediante la monitorización exhaustiva o automatizada del registro de Windows que permite realizar la herramienta SGSI Tracking se pueden satisfacer los siguientes requisitos de la norma:

- A.10.10.1 de Registro de auditorías: Mediante la revisión de los eventos del sistema se pueden registrar las actividades de los usuarios, por ejemplo, Mediante eventos de Account Management, Logon/Logoff y Object Access. Con esto, se supervisa la creación, modificación y accesos de cuentas. Además de el acceso a objetos auditados por el sistema. Pudiendo mantenerse dichos registros como prueba, o para supervisar el control de acceso a los sistemas.
- A.10.10.2 de Supervisión del uso de sistema: Del mismo modo, mediante el control de Login/Logoff de los usuarios en los sistemas (eventos 4624, 4625, 4634, etc.), se puede supervisar que cuenta de usuario ha accedido a los sistemas, del mismo modo que cuando ha desconectado de cada uno de ellos.
- A.10.10.4 de Registros de Administración y Operación: Mediante los eventos mencionados anteriormente, también, aplicando filtros a la búsqueda, monitorizar concretamente los accesos de administradores a los sistemas. Además, se pueden supervisar las siguientes tareas:
    - *Account Management*: Se puede supervisar la creación, modificación, bloqueo, cambio de contraseña y grupos de usuario; tanto en grupo de trabajo como en un dominio.
    - *Non Audit (event log)*: Se puede verificar el estado de los log del sistema, así como comprobar si se ha eliminado el mismo, o si genera un error.
    - *Object Access*: Se puede verificar si se han modificado los permisos de un objeto, el estado y funcionamiento completo de las tareas programadas del sistema, el estado del servicio de certificados, etc.
    - *Policy change*: Permite monitorizar todos los cambios de reglas y de políticas que afecten a:
        - Derechos de Usuario
        - Políticas de dominio
        - Kerberos
        - Acceso y seguridad de objetos
        - Funcionamiento del cortafuegos de Windows
- A.10.10.5 de Registro de Fallos: Se pueden registrar fallos de accesos, aplicaciones, inicio de servicios, etc.
- A.10.10.6 se Sincronización de Reloj: Mediante el evento 4609, ubicado en la clasificación *System*, que permite registrar los cambios en la hora del sistema.
- A.11.2.1 de Registro de Usuario: Al poder controlarse los accesos satisfactorios o erróneos a todos los sistemas, así como acceso a recursos de red, esta funcionalidad ayuda a cumplir los requisitos de este control.

- A.11.2.2 de Gestión de Privilegios: Del mismo modo que en A.10.10.4 y A.10.10.5, se cumple.
- A.11.4.2 de Autentificación de usuario para conexiones externas: Del mismo modo que las locales, también se registran las conexiones VPN a la red.
- A.11.4.4 de Diagnóstico remoto y protección de los puertos de configuración: Mediante el uso de los eventos 5150, 5154, 5156 y 5157, de Object Access; además la revisión del firewall de Windows, también sería aplicable en este caso.
- A.13.2.3 de Recopilación de Evidencias: Todos los eventos registrados pueden suponer evidencias en caso de que se tengan que emprender acciones disciplinarias tras un incidente de seguridad. Prestando la posibilidad de seguir la trazabilidad de los sucesos.

Requisitos RD 1720/2007

Mediante la monitorización del control de acceso a objetos antes mencionada. Si se habilita la directiva de auditoría sobre los datos de nivel alto. Se cumple perfectamente los requisitos del artículo de Registro de Accesos, correspondiente a las medidas de nivel alto del Título VIII.

Marcadores

Por último, se procede a revisar el módulo Marcadores, que constituye un conjunto de métricas, que se pueden sacar de los módulos anteriores. Estas métricas se establecen para verificar el correcto estado del SGSI, así como para valorar su eficiencia. Se muestra a continuación una captura de pantalla de su vista principal.

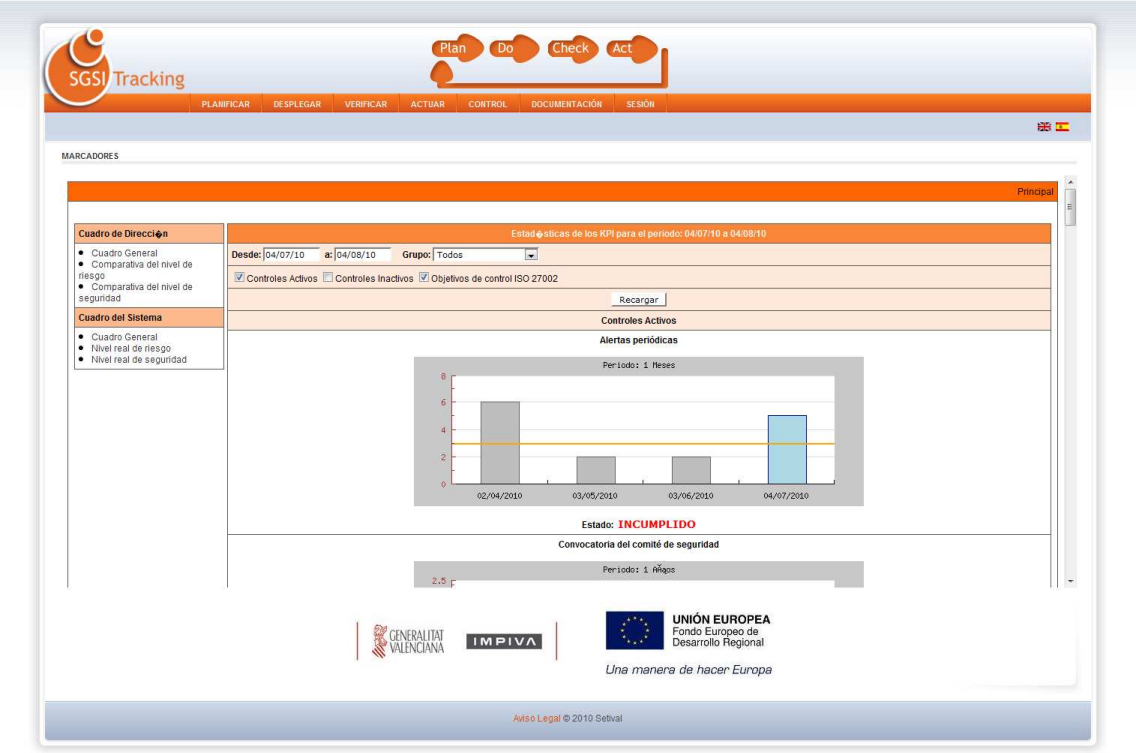


Ilustración 51- SGSI Tracking – Marcadores

Se pueden crear estadísticas y registros de acuerdo a las necesidades de cada organización. Estas gráficas se pueden seleccionar de todos los datos almacenados de la herramienta SGSI Tracking, y suponen una selección de resultados adecuados para la revisión del cumplimiento de la norma ISO 27001, basada en las recomendaciones de ISO 27002.

Requisitos ISO/IEC 27001

Básicamente, esta herramienta de recopilación y síntesis de información, supone un mecanismo útil para el cumplimiento del punto 4.2.3 de Supervisión y revisión del SGSI, ya que nos proporciona un mecanismo para:

- Ejecutar procedimientos de supervisión y revisión.
- Realizar revisiones periódicas de la eficacia del SGSI teniendo en cuenta los resultados de estas mediciones de eficacia.

Del mismo modo, y en directa relación, también proporciona un mecanismo para el cumplimiento del punto 7.2 de Datos iniciales de la revisión (En el punto 7 de Revisión del SGSI por la dirección), concretamente porque representa un resumen rápido de los resultados de las mediciones de eficacia del SGSI.

3.4.4. Actuar

Última fase del ciclo PDCA, el principal objetivo de esta fase es adoptar medidas correctivas y preventivas, fruto de los resultados de la auditoría interna del SGSI, o de la revisión por la Dirección, o de otras fuentes relevantes, para lograr mejora continua del SGSI.

Está formada por los siguientes módulos:

- Documentación de incidencias
- Gestión de Incidencias

Se muestra a continuación una captura de pantalla de su vista principal.

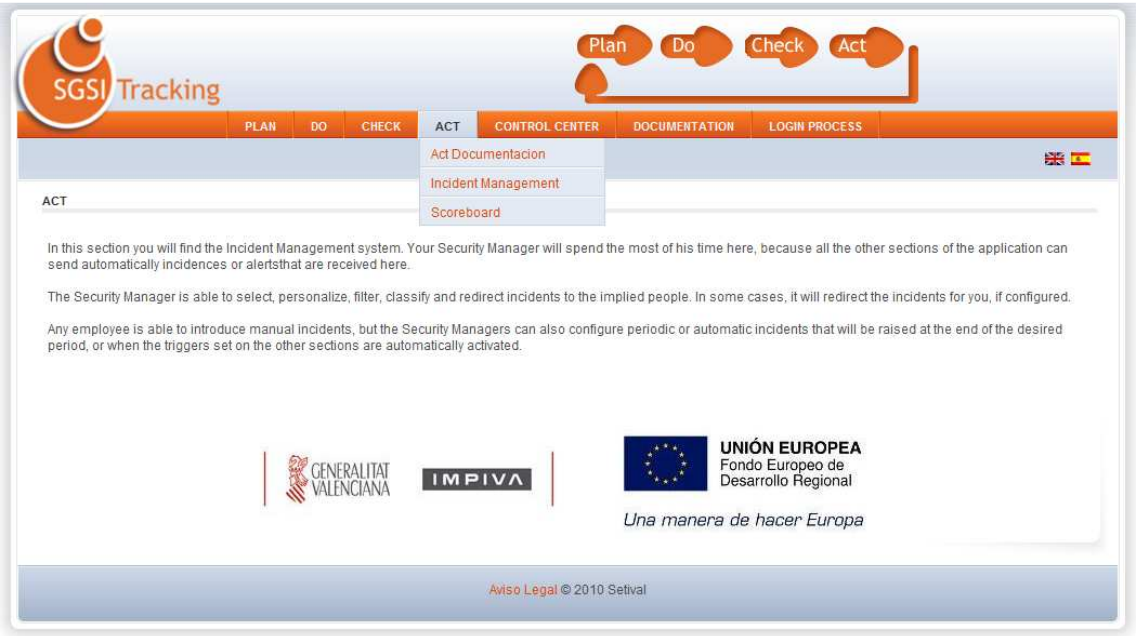


Ilustración 52 - SGSI Tracking – Actuar

Documentación de incidencias

El presente módulo constituye un pequeño repositorio documental, del mismo modo que el punto Desplegar, abordado anteriormente. En este caso la finalidad del módulo es mantener documentación relacionada con la fase Actuar del Ciclo PDCA. Como ejemplo se ha incluido el procedimiento de gestión de incidencias, que es útil para el manejo del módulo de Gestión de incidencias.

Ilustración 53 - SGSI Tracking - Documentación de Incidencias

Es importante anotar, antes de pasar a describir el módulo de gestión de incidentes, que las incidencias en sí suponen un control de la ejecución de todos los procedimientos, ya que estos mismos, sus resultados, o sus fallos suelen dar lugar a una incidencia. De ahí a la elección del módulo como centro de la fase Actuar, a la que representa. Como cierre de de la descripción de esta parte documental, se muestra un ejemplo de tipología de incidencias en el Anexo VIII – Tipología de Incidencias.

Gestión de incidencias

El siguiente módulo constituye la herramienta de red de gestión de incidencias de SGSI Tracking. Para su integración se ha empleado la herramienta One or Zero. Se muestra a continuación una captura de la pantalla inicial del módulo.

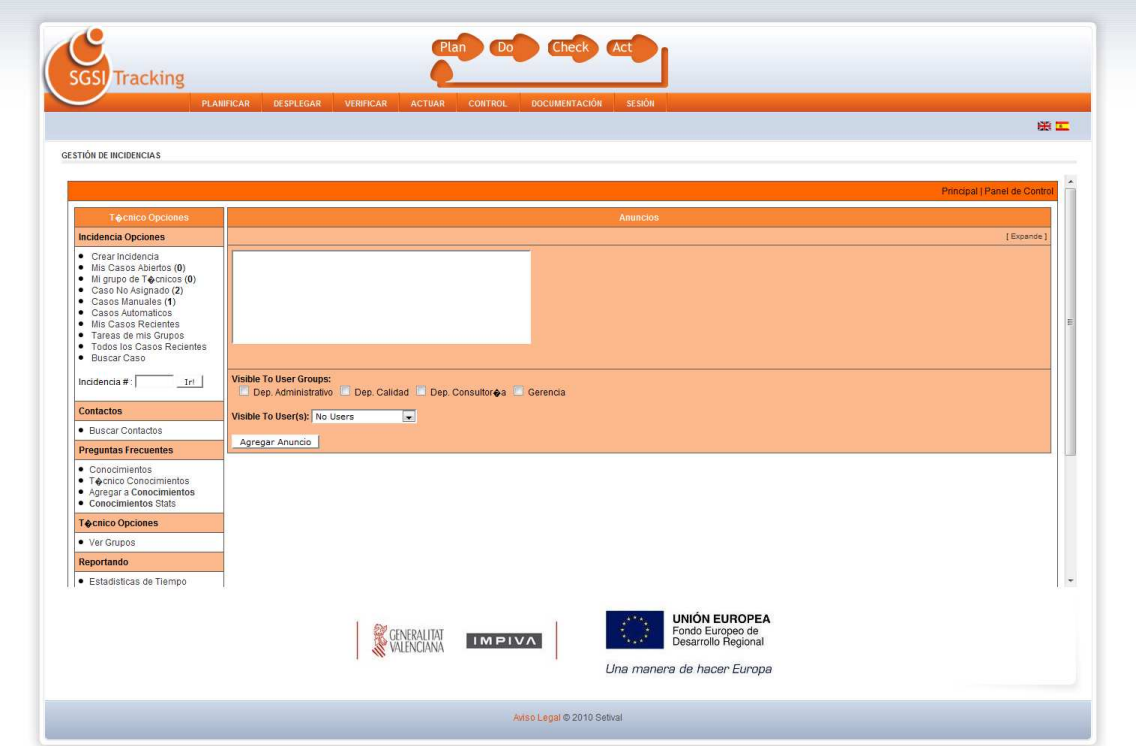


Ilustración 54 - SGSI Tracking - Documentación de Incidencias

Integración

Lo primero a destacar de esta herramienta, es que, del mismo modo que el conjunto de herramientas de SGSI Tracking, esta también regula el acceso a la misma a través de usuarios, que pueden disponer de distintos privilegios. Esto establece perfiles de privilegios, los cuales nos permitirán realizar distintas acciones y acceder a distintas informaciones en la aplicación. Los perfiles establecidos son los siguientes:

- *Administrator*: Posee permisos para dar de alta, modificar y crear cualquier incidencia.
- *Task Manager*: Aparece en el listado de encargados de resolución de incidencias, y puede ser asignado a la resolución de las mismas, las cuales puede modificar. También puede dar de alta incidencias.
- *User*: Puede crear incidencias.
- *Viewer*: Solo puede ver las incidencias.

En base a estos perfiles establecidos, se gestiona la apertura, asignación, resolución y cierre de las incidencias de este módulo. Para comenzar a ilustrar el funcionamiento del mismo se pasa a mostrar un ejemplo de un alta de incidencia de usuario del tipo *User*.

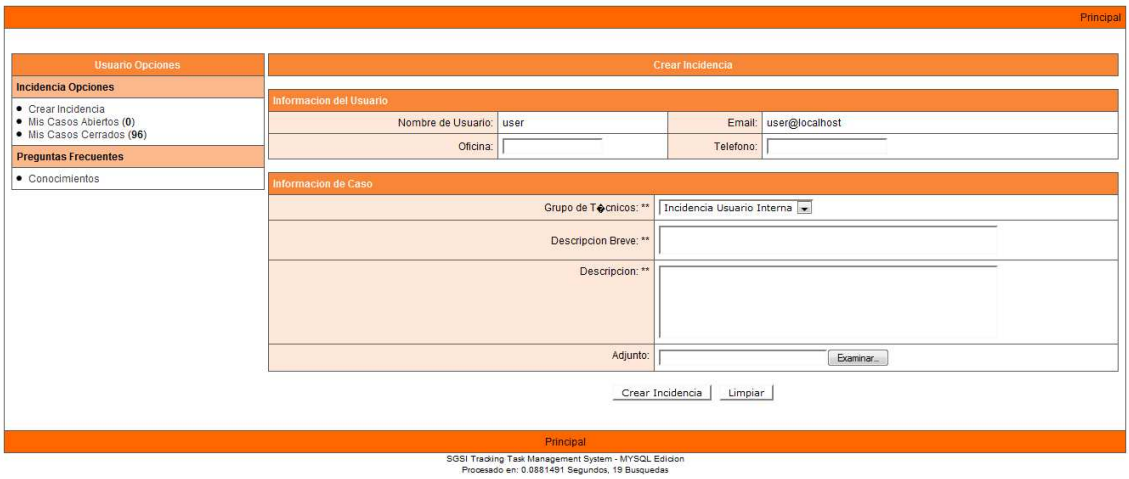


Ilustración 55 - Gestor de Incidencias - Alta incidencia (*User*)

En esta vista aparece sólo un subconjunto de los campos que realmente se almacenan para gestionar una incidencia, concretamente solo son campos que permiten crear una incidencia, la cual posteriormente será clasificada y asignada por el personal cualificado para tal fin. Los campos destacables de este formulario son:

- Nombre de usuario que da de alta la incidencia
- Email
- Oficina
- Teléfono
- Grupo de técnicos: Clasificación de la incidencia dependiendo de que sean peticiones de cambio o incidencias de seguridad, tanto interna como externa.
- Descripción breve
- Descripción
- Adjunto: Da la posibilidad de adjuntar un archivo a la creación de la incidencia.

En contraposición, y con el fin de ilustrar al completo el proceso de gestión de incidencias que lleva a cabo la herramienta, se muestra a continuación una captura de pantalla de una creación de incidencia de un usuario del tipo *Administrator*, el cual tiene permisos para asignar o resolver incidencias.

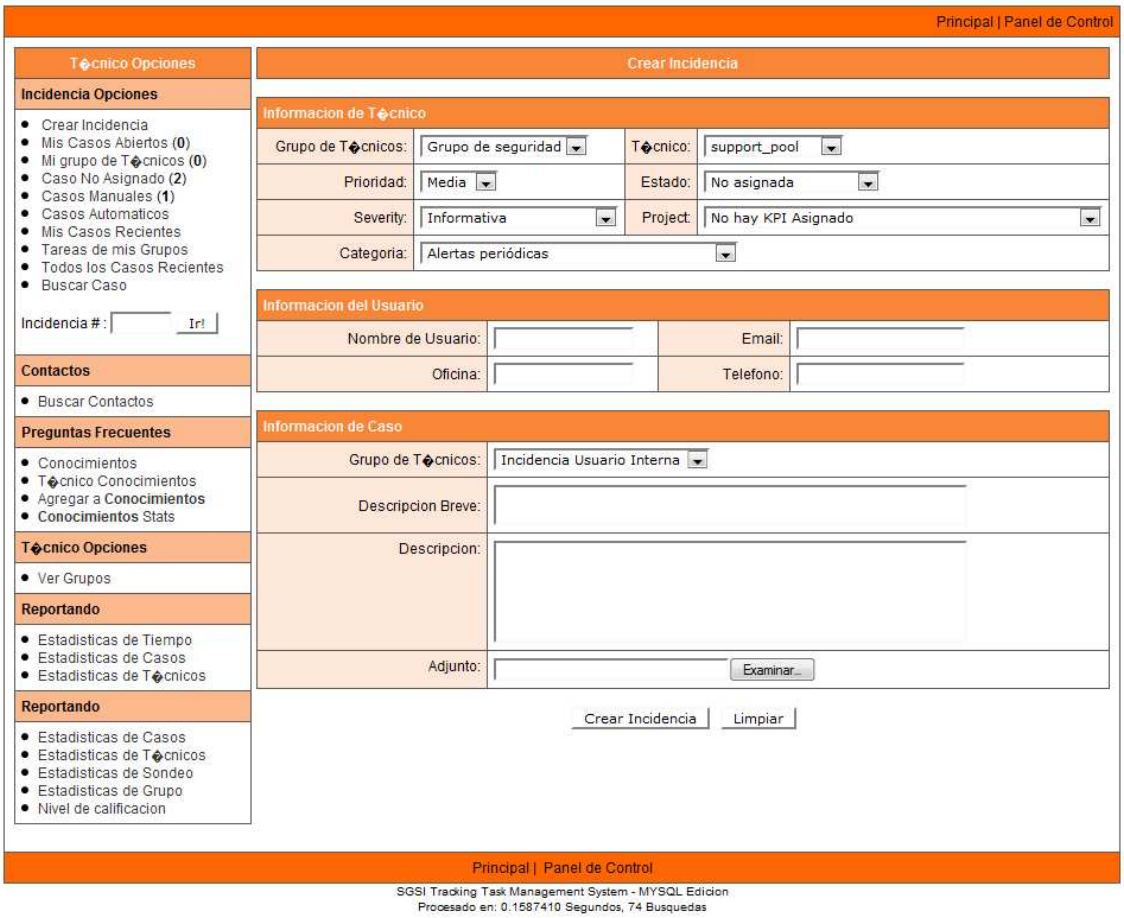


Ilustración 56 - Gestor de Incidencias - Crear incidencia (*Administrator*)

A los campos que incluia el caso anterior, en esta ocasión se añaden los siguientes, directamente relacionado con la gestión de la misma:

- Grupo de técnicos: Grupo asignado a la resolución de la incidencia.
- Técnico: Usuario del tipo *Task Manager* que pertenece al grupo anterior, y que se asigna a la resolución de la incidencia.
- Prioridad: Prioridad temporal asignada a la resolución de la incidencia, está graduada en niveles, que se muestran a continuación:
    - Baja
    - Media
    - Alta
    - Crítica

  Se muestra a continuación una captura de la configuración de este parámetro.

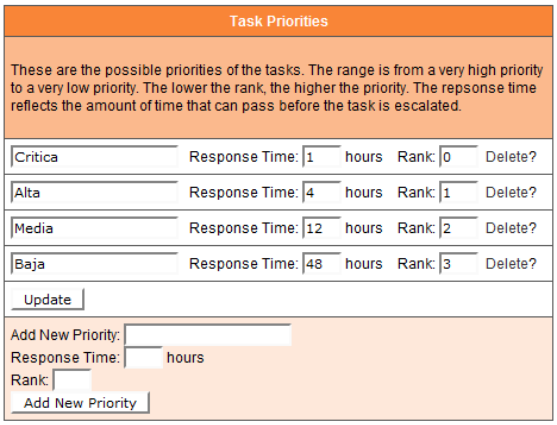


Ilustración 57 - Gestor de Incidencias - Prioridad de resolución

Esta graduación se establece de acuerdo a las necesidades de resolución de cada entidad, estos periodos temporales vienen establecidos en el procedimiento de gestión de incidencias.

- Estado: Permite establecer el estado actual de la incidencia. Se establece mediante los siguientes valores:
  - No asignada
  - En progreso
  - Esperando respuesta
  - Reabierta
  - Cerrada
- *Severity*: Severidad de la incidencia, en este caso también, se establecen estados acorde a la misma:
  - Informativa
  - Convocatoria
  - Cambio
  - Vulnerabilidad
  - Incidencia de Seguridad
  - Contingencia
  - Desastre
  - No conformidad
- Project: Supone una especialización superior a *Severity*, permitiendo seleccionar campos completamente seleccionados por la entidad, con el fin de realizar una categorización más exhaustiva de la incidencia.

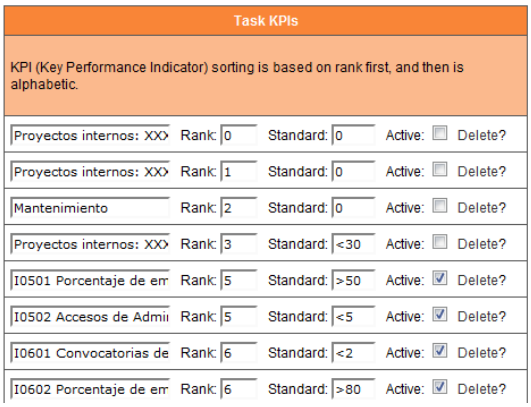


Ilustración 58 - Gestor de Incidencias - Configuración campo project (KPI)

- Categoría: Dominio de control de ISO 27001 al que afecta. Hay que añadir la clase Alertas periódicas, la cual es una incidencia generada en base a requisitos periódicos tanto de ISO 27001 como relacionadas con la LOPD. Este tipo de incidencias se pueden programar para que se den de alta de forma automática, sirviendo de recordatorio de la resolución de las mismas.

Para completar este recorrido sobre la gestión de las incidencias, pasamos a la vista para actualizar una incidencia ya creada por un usuario *Administrator*.

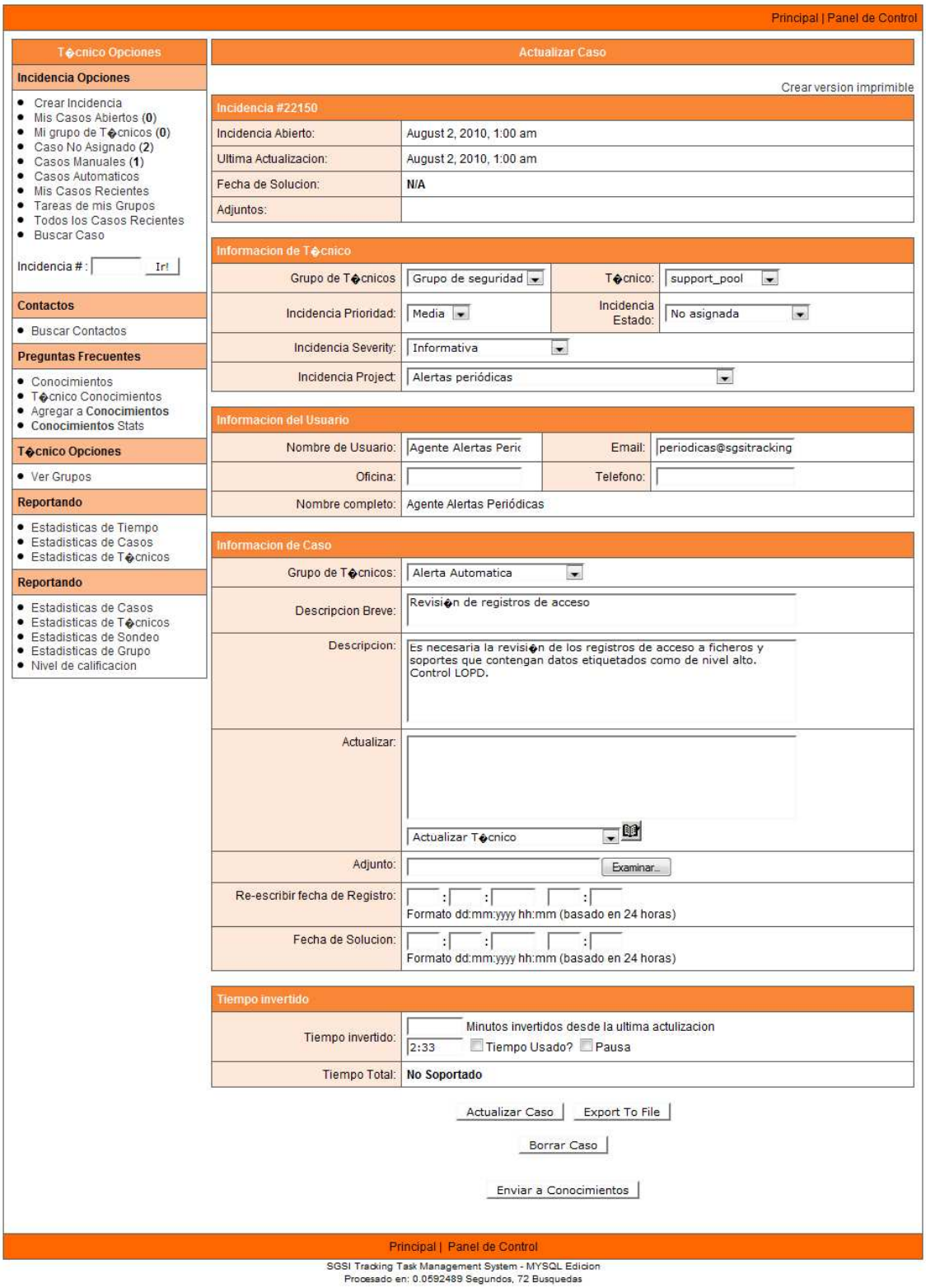


Ilustración 59 - Gestor de Incidencias - Actualizar incidencia

Sobre los campos mencionados en el anterior formulario añadimos los siguientes, que hacen referencia directa a la documentación de la gestión de la incidencia. Dando campos para registrar todos los pasos y tiempo empleado para la resolución de la misma. Los campos nuevos a destacar son los siguientes:

- Información del caso:
  - Actualizar: Campo para anotaciones de solución de la incidencia.
  - Fecha resolución: Campo para añadir fecha/hora exacta de la resolución de la misma.
- Tiempo invertido: Supone un contador de tiempo desde el comienzo del tratamiento de la incidencia, hasta su cierre, con motivos de monitorización de uso de recursos humanos.

Por último es importante destacar que en esta vista se pueden actualizar todos los campos vistos con anterioridad, dado que en ciertos casos, por ejemplo, puede ser necesario un cambio en el personal asignado a la resolución por un fallo de planificación inicial, o necesidades que se den a lo largo de la resolución de la incidencia.

Como mecanismo adicional a este sistema, es importante destacar que la herramienta se encarga de avisar por email tanto a usuarios afectados, como a técnicos o grupos asignados a su resolución por email. Agilizando la gestión de las mismas, y evitando accesos innecesarios a la herramienta por parte de los técnicos. Que solo accederán en caso de que se les asigne una resolución.

Se comentan las posibilidades listados de incidencias que se dan a los usuarios técnicos que son los encargados de gestionarlas:

- Mis casos abiertos: Ofrece una vista de las tareas abiertas asignadas (creadas o con resolución asignada) al usuario actual.
- Mi grupo de técnicos: Ofrece una vista de las tareas (tanto abiertas como finalizadas) por el grupo al que pertenece el usuario actual.
- Casos no asignados: Permite ver las tareas que todavía están pendientes de asignación.
- Mis casos recientes: Muestra tareas completadas o cerradas recientemente por el usuario actual.
- Tareas de mis grupos: Muestra las tareas completadas o cerradas recientemente por los grupos a los que pertenece el usuario actual.

Pasando a la supervisión de la gestión de incidencias, la herramienta nos ofrece diferentes mecanismos, que se pasa a comentar a continuación:

- Todos los casos recientes: Todos las tareas completadas o cerradas recientemente por cualquier grupo.
- Buscar Caso: Búsqueda por campos de un evento o conjunto de eventos. Se muestra una captura de pantalla a continuación para mostrar los mismos.

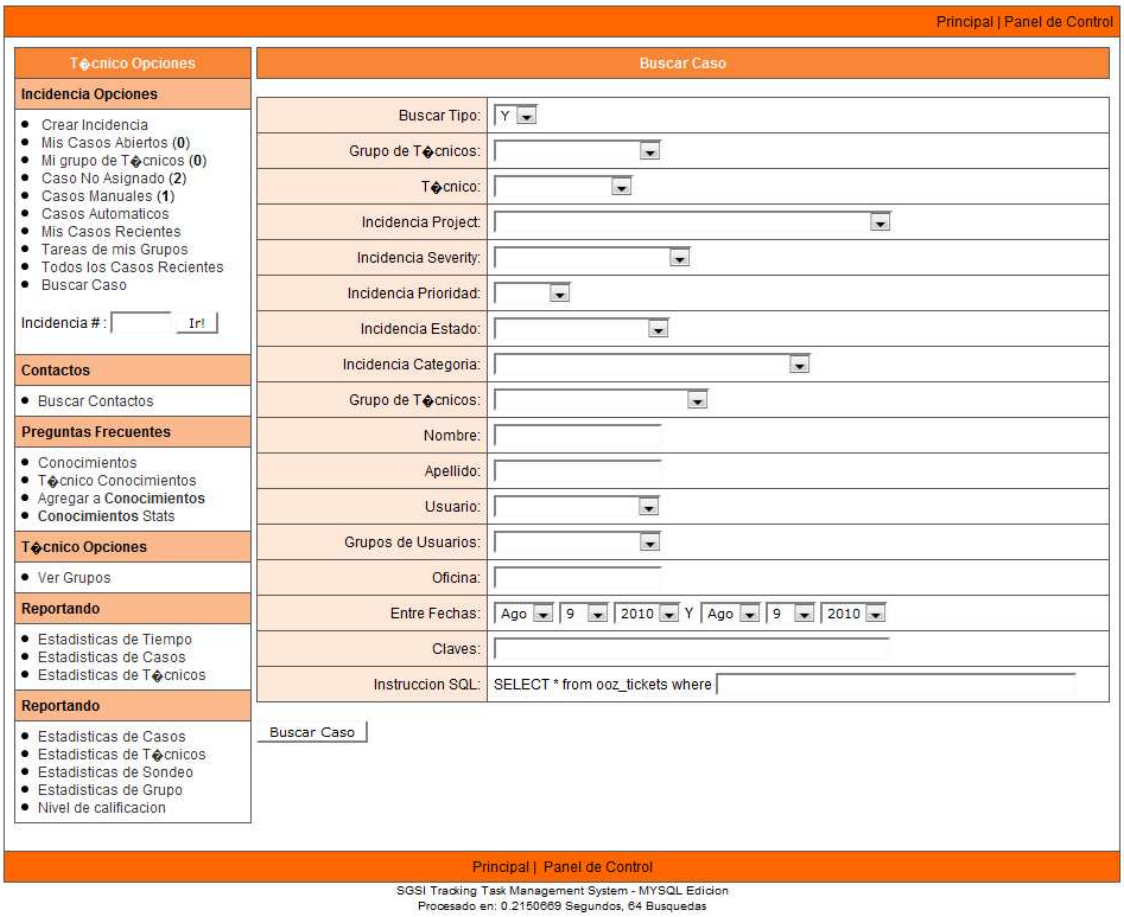


Ilustración 60 - Gestor de Incidencias - Buscar caso

- Estadísticas de Tiempo: Da gráficas y datos acerca de los tiempos de tratamiento y resolución de incidencias. Nos permite seleccionar el rango de muestreo, y nos otorga los resultados que se muestran a continuación.

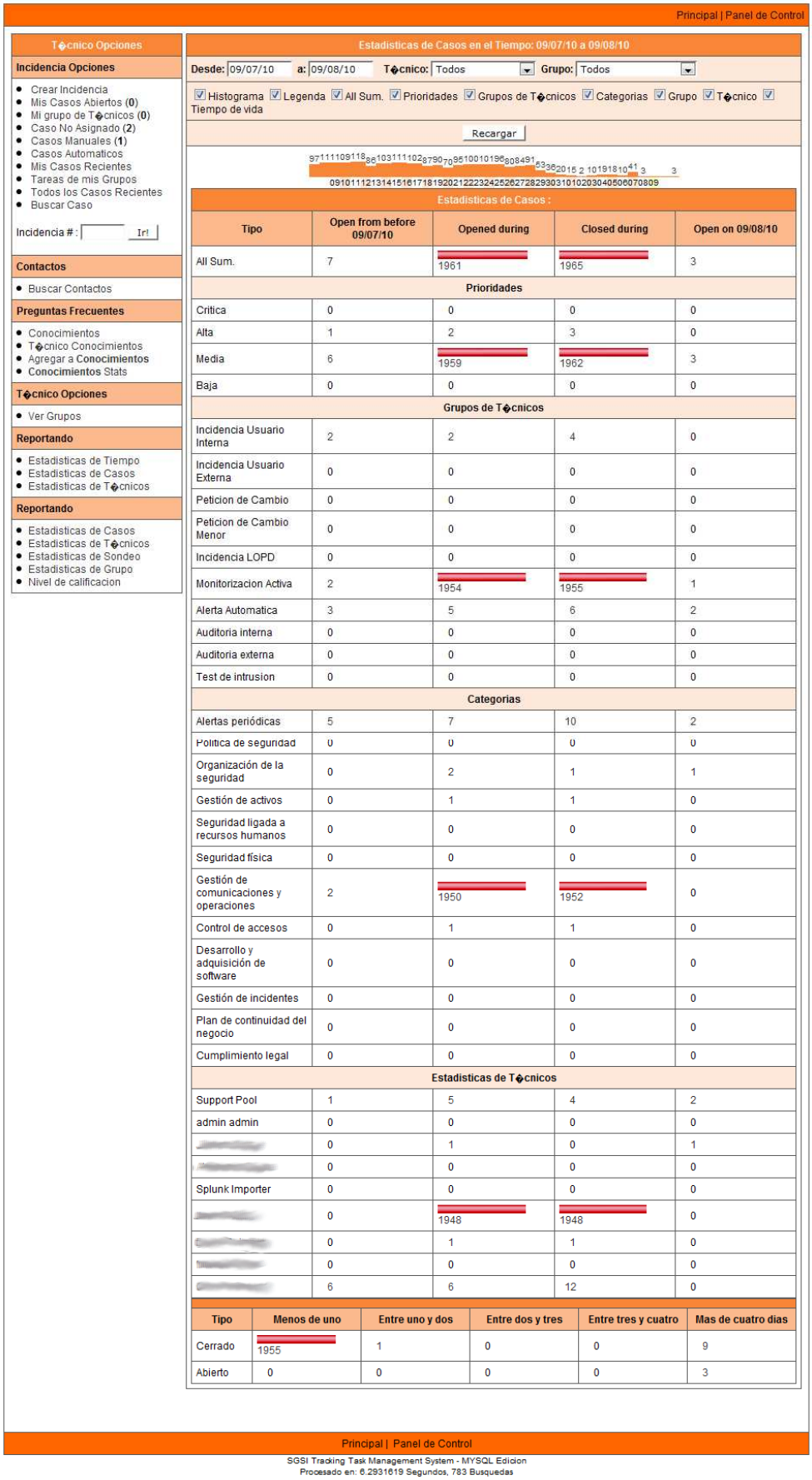


Ilustración 61 - Gestor de incidencias - Estadisticas de tiempo

- Estadísticas de Casos: Muestra una visión global del estado de las tareas abiertas, lo que supone un buen mecanismo para supervisar en global, la eficiencia de la gestión de incidencias.

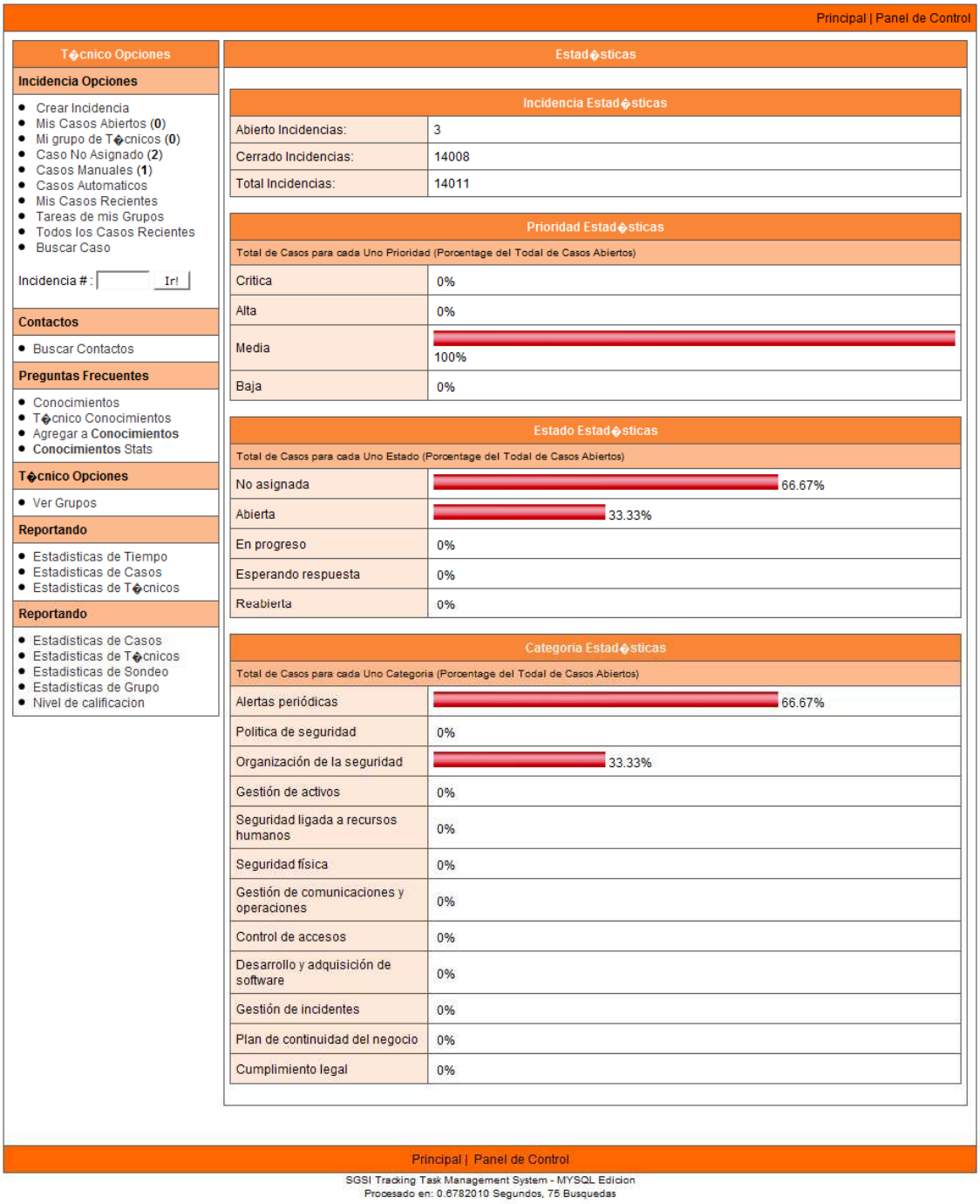


Ilustración 62 - Gestor de incidencias - Estadisticas de casos

A continuación repasamos el cumplimiento de las normas y reglamentos en base a la gestión de incidencias proporcionada por el siguiente módulo.

Requisitos ISO/IEC 27001

Con el uso del presente módulo de la herramienta SGSI Tracking, se cumple, o se facilita el cumplimiento, de los siguientes requisitos de la norma:

A.13.1.1 de Notificación de los eventos de seguridad de la información: Los eventos relacionados con la seguridad de la información deben ser comunicados mediante un procedimiento adecuado de la forma más rápida posible. Para ello se aconseja:

- Establecer un procedimiento formal de gestión de eventos, establecer los canales de comunicación para soportarlo, así como un destinatario fiable, conocido y disponible para las mismas.
- Todos los empleados, contratistas y terceros deben ser informados de sus responsabilidades en referencia a la gestión de eventos.
- Se deben implementar procesos de retroalimentación para asegurar que los eventos de seguridad de la información reportados han llegado a su destino y han sido tratadas adecuadamente.

Además, se deben considerar los siguientes Aspectos a considerar en cualquier proceso de gestión de incidentes:

- Clasificación: según ámbito, categoría o actividad a al que corresponden.
- Priorización: según criterios de impacto, urgencia, tiempo o esfuerzo de resolución.
- Escalado: se establecen niveles de comunicación y escalado en función del nivel de conocimiento de la materia, del tiempo, del poder de decisión /autorización, plazos, etc.

Mediante el establecimiento de un procedimiento, publicado en la herramienta, y el empleo del módulo de gestión de incidencias, se cumplen los requisitos.

A.13.1.2 de Notificación de los puntos débiles de la seguridad: En este requerimiento se establece que:

- Todos los empleados, contratistas y terceras partes son usuarios de los sistemas de información deben anotar y reportar cualquier vulnerabilidad detectada en estos sistemas.
- Deben notificar estos hechos a sus gerencias o a su proveedor de servicios tan pronto como sea posible para prevenir eventos de seguridad de la información. El medio empleado para la notificación debe ser sencillo y debe estar disponible y ser accesible por toda la organización.
- Los usuarios deben estar informados de que una vez identificada una posible vulnerabilidad no la deben “probar” por su cuenta, esto puede ser considerado como un mal uso del sistema, y puede dar lugar a daños en el mismo y resultar en responsabilidad legal para dicho empleado.

El módulo de gestión de incidencias también recoge los datos de vulnerabilidades detectadas, mediante una tipología de las incidencias.

A.13.2.1 de Responsabilidades y procedimientos: Se deben establecer procedimientos y responsabilidades para asegurar una respuesta rápida y efectiva a las incidencias de seguridad de la información. Para ello se aconseja seguir las siguientes directivas:

- Los procedimientos deben ser establecidos para manejar distintos tipos de incidencias como fallos en los sistemas de información o pérdida de servicio, códigos maliciosos, denegación de servicio, errores resultantes de datos incompletos o desactualizados, vulnerabilidades en la confidencialidad e integridad, mal uso de los sistemas de información, etc.
- Como extra a los planes de contingencia establecidos también deben incluir campos como análisis e identificación de la causa de la incidencia, contención, planteamiento e implementación de acciones correctivas para evitar su recurrencia, comunicaciones con los afectados o implicados tras la recuperación de la incidencia, etc.
- Se deben redactar registros de auditoría y registrar evidencias para analizar problemas internos o emplearlas como pruebas forenses en problemas con contratos, requisitos regulados, procedimientos civiles o reclamaciones a proveedores de servicios.
- Finalmente también deben incluir acciones para recuperarse de vulnerabilidades de seguridad para así poder controlar formalmente las que hayan sido corregidas. Para ello los procedimientos deben asegurar que solo el personal autorizado puede acceder a los sistemas y datos vivos, que todas las acciones de emergencia que se realicen queden correctamente documentadas, que se notifiquen y revisen dichas acciones por gerencia y que la integridad de los sistemas afectados se verifique lo antes posible.

A.13.2.2 de Aprendizaje de los incidentes de seguridad de la información: En este requisito se especifica:

- Deben existir mecanismos para monitorizar y cuantificar los tipos, volúmenes y costes de las incidencias de seguridad de la información.
- La información obtenida de la monitorización y revisión de las incidencias debe emplearse para identificar aquellas que más se repiten y las que suponen un mayor coste para la organización.
- La evaluación de los incidentes pasados y sus tendencias puede indicar la necesidad de implementar nuevos controles o mejorar los existentes para limitar la frecuencia, coste y daños provocados por ocurrencias futuras de las mismas o para ser tomado en cuenta en el proceso de revisión de la política de seguridad.

Estos dos últimos requisitos vienen cubiertos por el sistema de gestión de incidencias implementado por el módulo, así como por las herramientas de supervisión mencionadas con anterioridad.

Requisitos RD 1720/2007

Se muestran a continuación los requisitos satisfechos mediante el presente módulo, en materia de protección de datos de carácter personal:

- Registro de Incidencias (Nivel Básico): Debe existir un procedimiento de notificación y gestión de incidencias de datos de carácter personal, así como establecer un registro en el que figure:
    - Tipo de incidencia
    - Momento en el que se ha producido
    - Persona que realiza la notificación
    - Persona que gestiona la incidencia
    - Efectos derivados de la incidencia
    - Medidas aplicadas
- Registro de Incidencias (Nivel Medio): A los registros de incidencias establecidos en las medidas de seguridad de nivel básico, hay que añadir los procedimientos empleados para realizar una recuperación de datos, así como la persona que realizó la tarea. Se requerirá para ello, una autorización del Responsable de Seguridad.

Del mismo modo, con el desarrollo y publicación de un procedimiento de gestión de incidencias, y con la consideración de incidencias tipo LOPD y de restauración de datos; se cumple con los requisitos establecidos.

3.4.5. Control

El siguiente apartado de la herramienta SGSI Tracking, representa las opciones del administrador de la misma, se muestra a continuación una captura inicial de la misma.

Ilustración 63 - SGSI Tracking - Control

Está formada por los siguientes módulos:

- Pasarelas de Correo
- Gestión de Usuarios
- Alertas Periódicas

Pasarelas de Correo

En módulo se permite configurar destinos personalizados para el punto de entrada de correo electrónico al gestor de incidencias. Por ejemplo se podrá asignar unas características concretas a todas las incidencias que vienen de otra parte de SGSI Tracking (por ejemplo, del módulo de Monitorización de Red). También podemos definir puntos de entrada personalizados. Este sistema discrimina únicamente por la dirección de correo electrónico fuente.

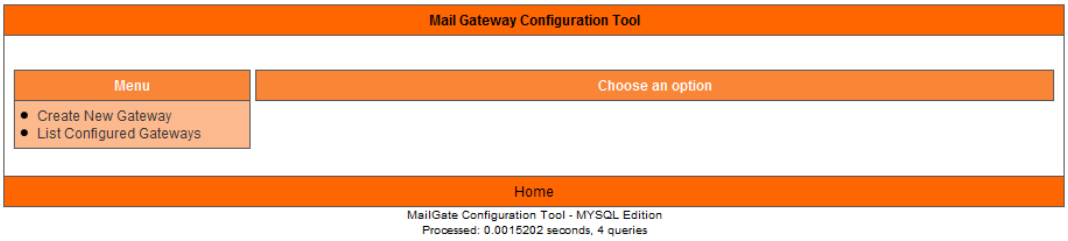


Ilustración 64 - SGSI Tracking - Pasarelas de correo

Como se ha podido observar en la captura inicial, se nos muestran dos opciones. Podemos crear una nueva pasarela de correo, o listar las pasarelas existentes.

En el proceso de creación, se selecciona cada una de las características que tendrán nuestras puertas de acceso de entre las que tiene configuradas en ese momento la aplicación de gestión de incidencias (Prioridad, estado, responsable de resolución, etc.). También podemos hacer que la pasarela reescriba la dirección de correo y el nombre de usuario desde los que se nos ha enviado el correo, mostrando otros datos distintos en la aplicación de gestión de incidencias.

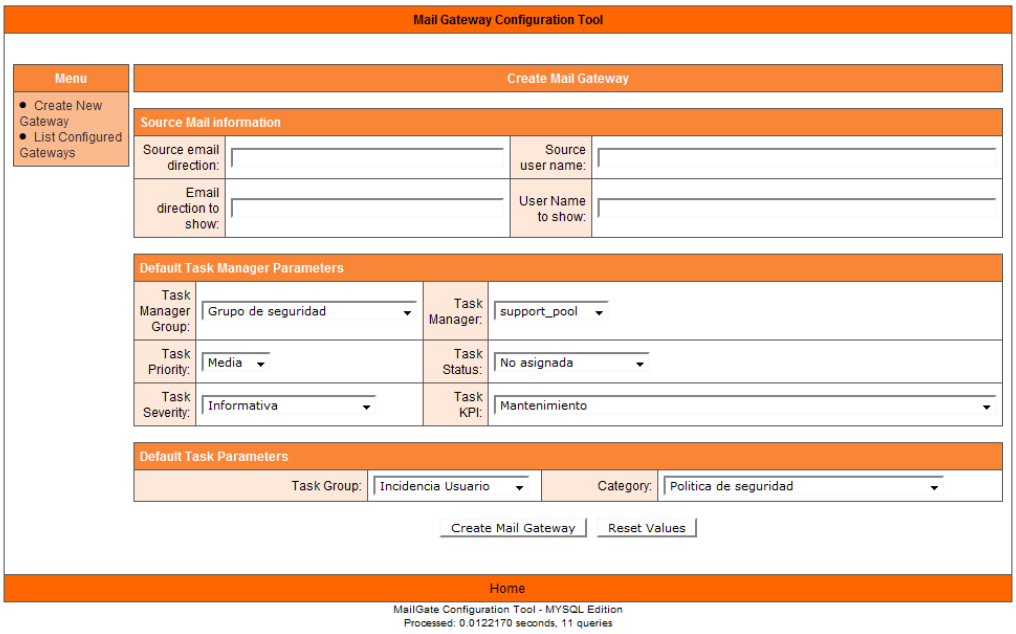
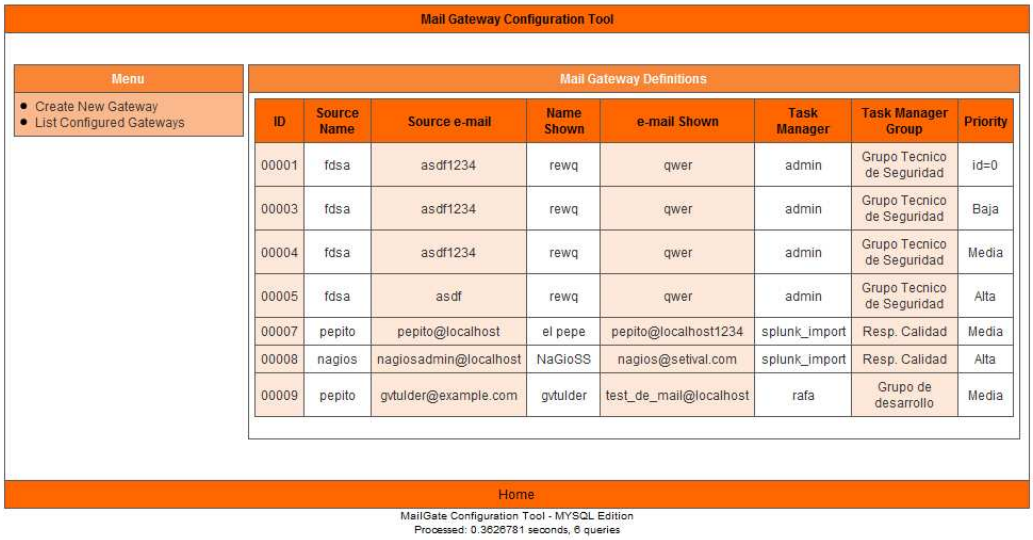


Ilustración 65 - Pasarelas de Correo - Crear una pasarela

Podemos ver en cada momento las pasarelas que tenemos definidas, y modificar su comportamiento mediante la opción *List Configured Gateways*. Nos aparece un listado en el que podemos ver, de un solo vistazo, las características principales de las pasarelas de correo que tengamos configuradas. A continuación se muestra una captura de la vista de listado. Al pulsar sobre cualquiera de los elementos de una de las pasarelas, pasamos a la pantalla de edición, en la que podemos modificar todas sus características, del mismo modo que en el proceso de creación.



ID	Source Name	Source e-mail	Name Shown	e-mail Shown	Task Manager	Task Manager Group	Priority
00001	fdsa	asdf1234	rewq	qwer	admin	Grupo Tecnico de Seguridad	id=0
00003	fdsa	asdf1234	rewq	qwer	admin	Grupo Tecnico de Seguridad	Baja
00004	fdsa	asdf1234	rewq	qwer	admin	Grupo Tecnico de Seguridad	Media
00005	fdsa	asdf	rewq	qwer	admin	Grupo Tecnico de Seguridad	Alta
00007	pepito	pepito@localhost	el pepe	pepito@localhost1234	splunk_import	Resp. Calidad	Media
00008	nagios	nagiosadmin@localhost	NaGioSS	nagios@setival.com	splunk_import	Resp. Calidad	Alta
00009	pepito	gvtulder@example.com	gvtulder	test_de_mail@localhost	rafa	Grupo de desarrollo	Media

Ilustración 66 - Pasarelas de correo - Listado de pasarelas

Mediante el uso de estas pasarelas se configura la comunicación entre cualquier módulo y el de gestión de incidencias, el cual, nos permite el envío de correos de aviso a los administradores del sistema y del SGSI.

Gestión de Usuarios

El módulo de gestión de usuarios nos permite crear, editar o eliminar usuarios con acceso al conjunto de la herramienta SGSI Tracking. Se muestra una captura inicial a continuación.

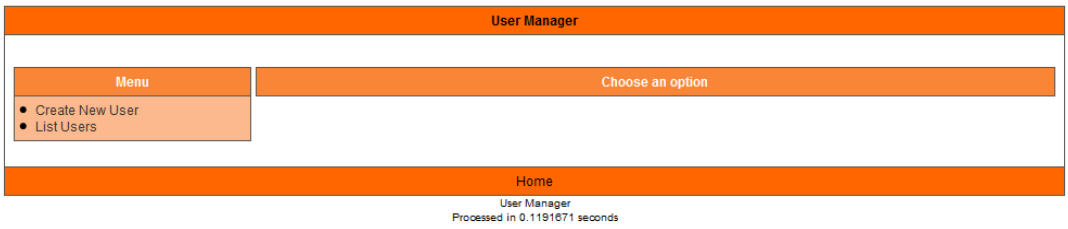


Ilustración 67 - SGSI Tracking - Gestión de usuarios

Integración

Este panel ha sido diseñado para controlar de forma centralizada los usuarios y sus privilegios, y ayudar a mantener una estructura uniforme de usuarios en cada una de las aplicaciones integradas, y evitar además nombres duplicados y otros problemas derivados de la modificación en cada aplicación de los usuarios.

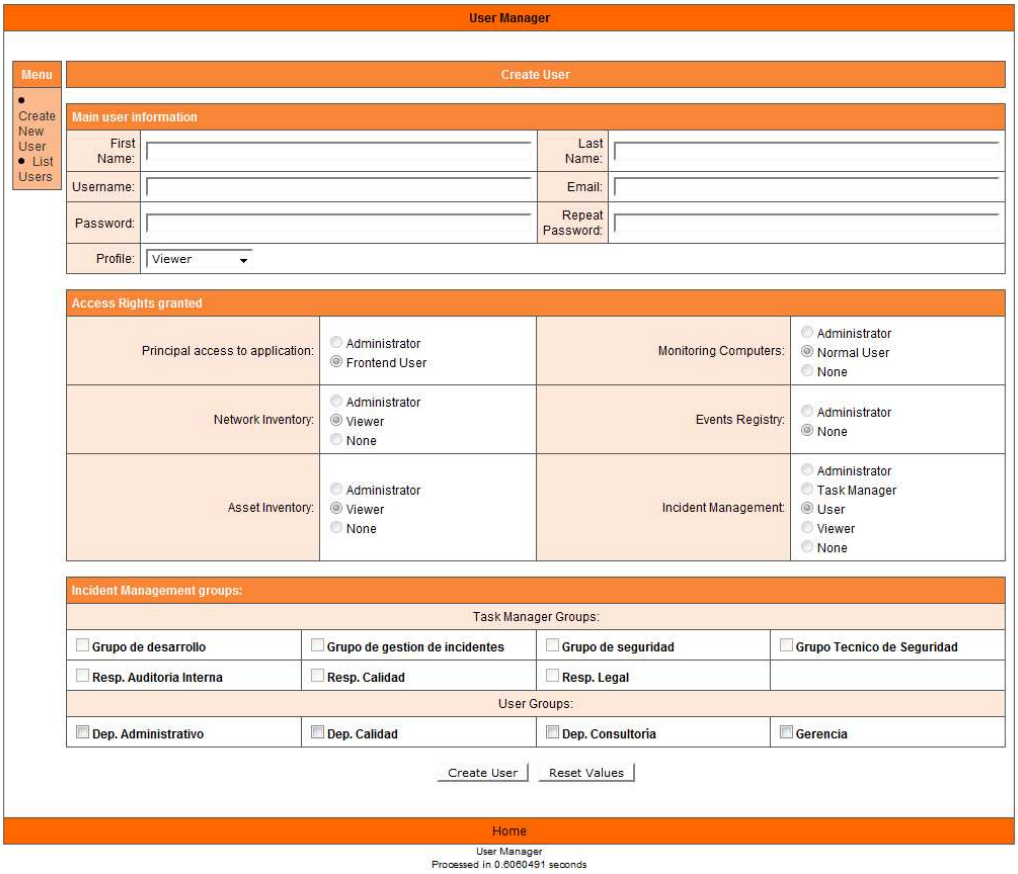


Ilustración 68 - Gestión de Usuarios - Creación de usuario

En el apartado de creación de usuarios se nos permite asignar unos datos comunes al usuario (nombre completo, usuario, contraseña y dirección de correo), asignarle el nivel de privilegios que le corresponde en cada aplicación y los grupos de gestión de incidencias a los que pertenece.

Tenemos tres opciones para la gestión de los privilegios: Administrador, Visor y Personalizado. Los dos primeros tienen unos parámetros predefinidos, mientras que el tercero nos permite cambiar a voluntad los privilegios disponibles en cada una de las aplicaciones existentes. Se muestra a continuación los privilegios asignados en cada caso.

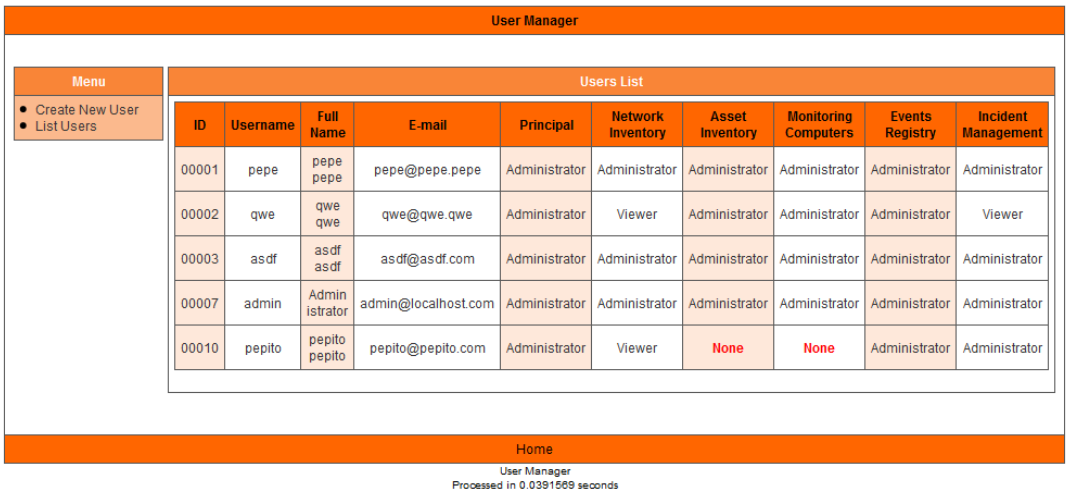
- *Principal Access:* Controla el acceso a la aplicación. Sin este acceso no tiene sentido ningún otro.
    - *Administrator*: Se permite acceso total tanto al portal (página principal de SGSI Tracking) como a su panel de administración, que permite cambiar parámetros visuales y de funcionamiento del portal.
    - *Frontend User*: Sólo permite acceso al portal (página principal de SGSI Tracking).

Los siguientes elementos se refieren a ítems del menú que desembocan en aplicaciones embebidas dentro de SGSI Tracking.

- *Network Inventory / Asset Inventory:*
    - *Administrator*: Permite el acceso a la configuración personalizada de la aplicación, así como a diferentes ventanas que permiten gestionar el inventario y realizar cambios sobre él.
    - *Viewer*: Permite el acceso a la aplicación en modo solo lectura, ocultando las opciones de modificación de parámetros de la aplicación y gestión avanzada de inventario.
    - *None*: Prohíbe el acceso a esta la aplicación.
- *Monitoring Computers:*
    - *Administrator*: Permite el acceso a la configuración personalizada de la aplicación, así como a diferentes ventanas que permiten gestionar la red y los servicios dependientes de ella. También permite la generación de informes y estadísticas avanzadas de rendimiento de las máquinas y la red.
    - *Normal User*: Permite el acceso a la aplicación en modo solo lectura, ocultando las opciones de modificación de parámetros de la aplicación y gestión de red. Solo permite la generación de estadísticas simples.
    - *None*: Prohíbe el acceso a esta la aplicación.
- *Events Registry:*
    - *Administrator:* Permite el acceso total a la aplicación, así como a las opciones de configuración avanzadas.
    - *None:* Prohibe el acceso a la aplicación.
- *Incident Management:*
    - *Administrator:* Perfil dedicado al administrador, que además puede ser uno de los encargados de resolver incidencias. Puede realizar cualquier operación sobre las incidencias, y además también puede modificar parámetros de la misma, cómo las opciones de los diferentes campos de las incidencias.
    - *Task Manager:* Perfil dedicado al técnico encargado de resolver incidencias. Además de introducir nuevas incidencias, puede modificar (actualizar, tratar y cerrar) incidencias creadas por otros usuarios en los grupos de su competencia (definidos por los *Task Manager Group*), pero no puede modificar parámetros de configuración de la aplicación.
    - *User:* Permite al usuario introducir nuevas incidencias y ver los elementos publicados en la aplicación. Para este nivel y los inferiores solo están disponibles los grupos de usuarios.
    - *Viewer:* Sólo permite la visión de los elementos publicados en la aplicación, sin posibilidad de modificar nada.
    - *None:* Prohibe el acceso a la aplicación.

Finalmente, tenemos los *Incident Management Groups* (grupos del gestor de incidencias), que permiten agrupar los usuarios dependiendo de su rol en la entidad. Estos grupos solo estarán activados para ser seleccionados en el caso de que los privilegios de acceso a la aplicación de gestión de incidencias sean los adecuados. Para activar los *Task Manager Groups* es necesario como mínimo tener privilegios de *Task Manager*, y para los *User Groups* es suficiente con tener acceso a la aplicación.

Para visualizar los usuarios existentes en el sistema debemos pulsar el ítem *List Users*.



ID	Username	Full Name	E-mail	Principal	Network Inventory	Asset Inventory	Monitoring Computers	Events Registry	Incident Management
00001	pepe	pepe pepe	pepe@pepe.pepe	Administrator	Administrator	Administrator	Administrator	Administrator	Administrator
00002	qwe	qwe qwe	qwe@qwe.qwe	Administrator	Viewer	Administrator	Administrator	Administrator	Viewer
00003	asdf	asdf asdf	asdf@asdf.com	Administrator	Administrator	Administrator	Administrator	Administrator	Administrator
00007	admin	Administrator	admin@localhost.com	Administrator	Administrator	Administrator	Administrator	Administrator	Administrator
00010	pepito	pepito pepito	pepito@pepito.com	Administrator	Viewer	None	None	Administrator	Administrator

Ilustración 69 - Gestión de Usuarios - Listado de usuarios

Si pulsamos en cualquiera de los campos de un usuario podemos acceder a la pantalla de edición, en la que podemos cambiar los niveles de acceso, los datos del usuario, y los grupos a los que dicho usuario pertenece. El funcionamiento de la ventana de edición es el mismo que la pantalla de introducción de usuario.

Requisitos ISO/IEC 27001

Con el uso del presente módulo de la herramienta SGSI Tracking, se cumple, o se facilita el cumplimiento del control:

A.11.2.2 de Gestión de privilegios: Antes mencionado en el módulo Correlador de eventos. En esta ocasión no se menciona con fines de revisión, sino con fines de control. Como se ha observado se ha tenido especial cuidado al limitar el uso de privilegios en la aplicación, que permite ajustar los privilegios para cada una de las aplicaciones a un nivel sobresaliente para la norma ISO 27001.

A.15.3.2 de Protección de herramientas de auditoría de los sistemas de información: Que establece que:

- Los accesos a las herramientas de auditoría de sistemas deben ser protegidos con el fin de prever cualquier posible mal uso o daño.
- Las herramientas de auditoría de sistemas, software o archivos de datos, deben estar separadas de los sistemas de desarrollo y de producción y no se mantendrán en librerías o en áreas de los usuarios, salvo que se les proporcione un nivel apropiado de protección adicional.
- Si el personal experto está implicado en la auditoria, puede existir un riesgo de mal uso de las herramientas de auditoría y de la información a la que acceden. Los controles para determinar los riesgos y para restringir el acceso físico pueden ser considerados para tratar estos riesgos y se debe tomar consecuencia como el cambio inmediato de contraseñas divulgadas a los auditores.

Todos estos requisitos se cumplen mediante estos controles de acceso, además la herramienta SGSI Tracking funciona en una máquina virtual, lo que aísla completamente la herramienta.

Alertas Periódicas

El último módulo del apartado Control, establece alertas periódicas relacionadas con las dos normas objetivo del estudio del presente proyecto, se muestra una captura inicial a continuación.

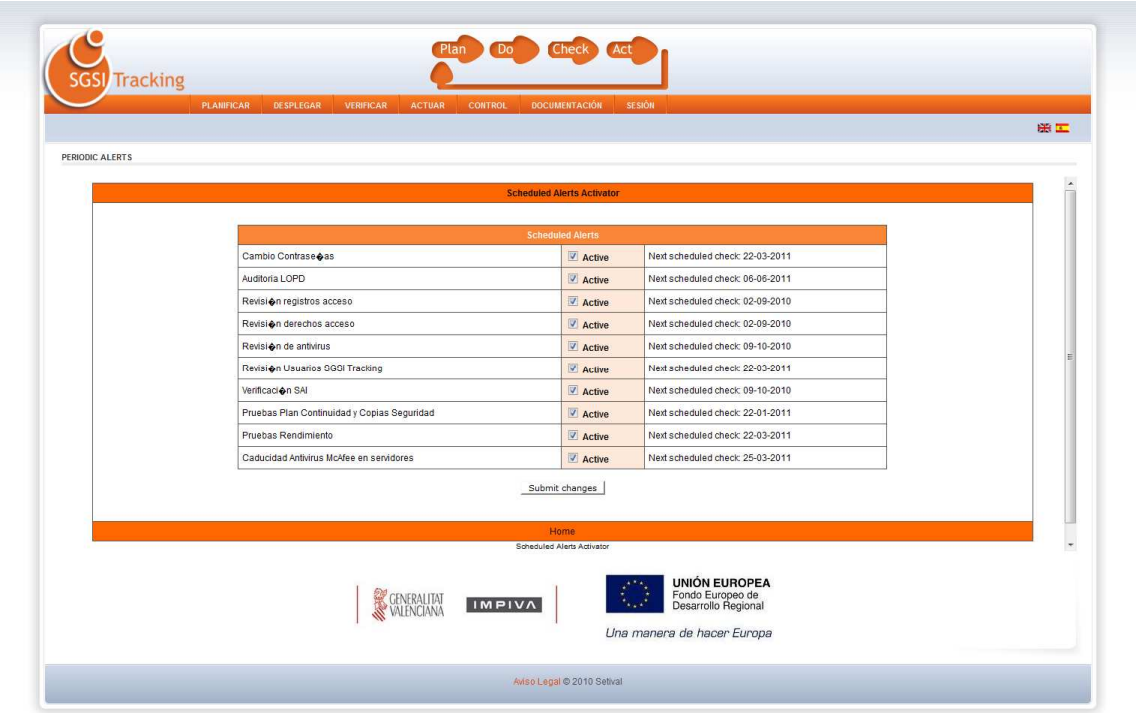


Ilustración 70 - SGSI Tracking - Alertas periódicas

Integración

Es importante destacar que este conjunto de alertas periódicas es perfectamente personalizable por el cliente, ya que se podrán añadir directamente a su demanda. Se muestra un listado del paquete seleccionado por defecto para la aplicación:

- Cambio de Contraseñas: Aviso de cambio periódico de contraseñas de usuario y administradores,

Requisitos ISO/IEC 27001

Control A.11.2.1 de Registro de Usuario, para su cumplimiento se deben fijar cambios periódicos en las contraseñas, con el fin de evitar accesos no autorizados.

- Auditoría LOPD: Aviso para realizar la próxima auditoría LOPD.

Requisitos RD 1720/2007

De acuerdo con el requisito de Auditoría, contenido en el Título VIII de Medidas de Seguridad en el tratamiento de datos de carácter personal en el nivel Medio, los sistemas de información deberán someterse, de forma obligatoria, a una auditoría interna que verifique el cumplimiento del RD 1720/2007 cada dos años.

- Revisión de registros de acceso: Se deben revisar los registros de acceso de los usuarios, tanto usuarios estándar como administradores.

Requisitos ISO/IEC 27001

Control A.10.10.1 de Registro de Auditorías, que establece que se debe revisar registros de auditorías de acceso a los usuarios a intervalos regulares.

- Revisión de derechos de acceso y usuarios SGSI Tracking:

Requisitos ISO/IEC 27001

Control A.11.2.4 de Revisión de los derechos de acceso a usuario, que establece que se debe revisar los derechos de acceso a los usuarios a intervalos regulares.

- Revisión antivirus: Se debe revisar el estado del antivirus de una muestra de equipos en intervalos establecidos.

Requisitos ISO/IEC 27001

Control A.10.4.1 de Controles contra código malicioso, menciona la necesidad de revisar el software antivirus a intervalos de tiempo establecidos.

- Verificación SAI: Recomendación de verificación, mediante pruebas, del estado del equipo de seguridad contra corte de suministro eléctrico, con el fin de tener la seguridad de su adecuado funcionamiento.

- Pruebas plan de Continuidad y Copias de Seguridad: Se deben realizar pruebas del plan de continuidad de negocio, así como de las copias de seguridad.

Requisitos ISO/IEC 27001

Control A.14.1.5 de Pruebas, mantenimiento y reevaluación de los planes de continuidad de negocio establece que se tendrán que realizar pruebas del plan de continuidad de negocio de forma periódica, para asegurar su efectividad.

Por otra parte, el control A.10.5.1 de Copias de seguridad de la información, menciona que se deben probar periódicamente las copias de seguridad, de acuerdo a la política de copias de seguridad establecida.

Requisitos RD 1720/2007

De acuerdo con el requisito de Auditoría, contenido en el Título VIII de Medidas de Seguridad en el tratamiento de datos de carácter personal en el nivel Básico, se establece que se deben realizar copias de seguridad, y que éstas, como mínimo, se deben probar una vez cada 6 meses.

- Pruebas Rendimiento: Se deben realizar pruebas de rendimiento de los sistemas de forma periódica.

Requisitos ISO/IEC 27001

Control A.10.3.1 de Gestión de capacidades, menciona la necesidad de realizar pruebas de rendimiento de los equipos, con el fin de minimizar el riesgo de fallos de los mismos.

3.4.6. Documentación

Repositorio documental de la herramienta SGSI Tracking. En el mismo se puede ubicar cualquier documentación relacionada con el uso de la herramienta SGSI Tracking, documentación de ISO 27001, documentación LOPD y cualquier documentación de uso común o instrucción técnica pertinente. Se muestra una captura inicial a continuación.

Ilustración 71 - SGSI Tracking – Documentación

No se pasa a enumerar los requisitos cumplidos con el siguiente apartado, ya que dada la flexibilidad que ofrece una herramienta de gestión documental, se podrían cubrir prácticamente todos los controles y requisitos documentales de la normativa estudiada. En cualquier caso, se citan los ejemplos mostrados anteriormente en el módulo Desplegar – Plantillas de etiquetado, el cual tiene una funcionalidad semejante al actual.

4. Implementación de un entorno de pruebas virtualizado para la herramienta SGSI Tracking

4.1.Planteamiento inicial y elección de la tecnología

Tanto en la fase final del desarrollo de la herramienta SGSI Tracking (Alfa), como en las pruebas de cualquier herramienta previa a su comercialización (Beta); es necesario implementar entornos de prueba separados y seguros.

La virtualización consiste básicamente en la creación de una capa de abstracción entre el hardware de la máquina física y el software del sistema operativo; de este modo, se pueden mantener diversas máquinas virtuales sobre un mismo sistema físico. Entre las ventajas y principales usos de la misma destacan:

- Ejecutar una o más aplicaciones que no son soportadas por el sistema operativo del *Host*.
- Pruebas de un sistema operativo o aplicaciones alternativas.
- Virtualización de servidores
- Duplicado de entornos específicos
- Creación de un entorno protegido

Vistas las ventajas, se va a justificar porque desde el principio del desarrollo se pensó en la virtualización. El principal motivo es que, dados los requisitos herramienta, es necesario que se sitúe en un entorno aislado, además, debe ser modular y reproducible en cualquier sistema que se precie.

También son importantes los requisitos legales o normativos. La norma ISO 27001 establece requisitos para la adecuada gestión de entornos de pruebas, concretamente en el objetivo de control A.10.1.4 de Separación de los recursos de desarrollo, prueba, y operación. La separación de los entornos para desarrollo, prueba y producción es importante para reducir los riesgos de un acceso o de cambios no autorizados del entorno productivo. Son consideraciones sobre buenas prácticas al respecto:

- El proceso de entrega a producción del software desde un estado de desarrollo debe ser definirse y documentarse.
- El software de desarrollo y el de producción deberían funcionar en entornos diferentes (P. ej. en otra máquina, dominio, etc.).
- Los compiladores, editores y otros servicios del sistema no deberían ser accesibles desde los sistemas de producción, cuando no se necesiten.
- Los usuarios deben utilizar diferentes perfiles de usuario para los sistemas en prueba y en producción y los sistemas deben exhibir mensajes de identificación apropiados para reducir el riesgo de error.
- Los datos sensibles no deberían ser copiados en el entorno del sistema de prueba (P. ej. Datos de Carácter Personal).

Pasando a la fase de producción de la herramienta, implantación y uso de la misma en los clientes; se ha tenido en cuenta el siguiente requisito de ISO 27001. El control A.15.3.2 de Protección de las herramientas de auditoría de los sistemas de información se establece que:

- Los accesos a las herramientas de auditoría de sistemas deben ser protegidos con el fin de prever cualquier posible mal uso o daño.
- Las herramientas de auditoría de sistemas, software o archivos de datos, deben estar separadas de los sistemas de desarrollo y de producción y no se mantendrán en librerías o en áreas de los usuarios, salvo que se les proporcione un nivel apropiado de protección adicional.
- Si el personal experto está implicado en la auditoria, puede existir un riesgo de mal uso de las herramientas de auditoría y de la información a la que acceden. Los controles para determinar los riesgos y para restringir el acceso físico pueden ser considerados para tratar estos riesgos y se debe tomar consecuencia como el cambio inmediato de contraseñas divulgadas a los auditores.

Se han tenido en cuenta también los costes de implantación, siempre con el fin de ofrecer un precio competitivo, ahorrando tanto en recursos humanos de Setival, como en la inversión económica del cliente. Antes de la aparición de la virtualización, para poder mantener una separación de entornos como esta, era necesario realizar una inversión considerable dado que equipos y redes separados requerirían de toda una replicación de la infraestructura física de sistemas de información de la entidad.

Para finalizar con los motivos de selección de la tecnología, es importante destacar que las máquinas virtuales son altamente portables, permitiendo apagarla en un equipo, copiarla en otro, y ejecutarla sin ningún tipo de problema o configuración adicional (lo que facilita la instalación y traslado de la herramienta SGSI Tracking). Además, existen sistemas de máquinas virtuales preparados para sistemas de alta disponibilidad, los cuales, permiten su copia en caliente de un sistema a otro, incluso moverla entre servidores sin apagar la máquina.

La solución elegida tanto para la implementación de un entorno de pruebas, como para implantar la herramienta en los clientes es VMWare Server 2, dado que aprovechando cualquier servidor de la entidad se puede poner un pequeño servidor de máquinas virtuales.

4.2. Creación y configuración de la red de pruebas de SGSI Tracking bajo VMWare Server 2

El presente punto de la memoria realiza una pequeña memoria descriptiva de los pasos seguidos tanto en la selección de máquinas virtuales de la misma, como de la configuración de la herramienta VMWare Server 2 para establecer un entorno de demostración separado y seguro.

Se plantea un entorno de pruebas sencillo, en el cual situaremos dos máquinas clientes de SGSI Tracking, una Windows y otra Linux, con el fin de probar ambos sistemas y su interacción. Es importante destacar que en todos los casos, las máquinas virtuales se han configurado adecuadamente, por una parte, la máquina de SGSI Tracking se ha configurado de

acuerdo al manual de instalación de la misma, configurando los puertos y la dirección IP de su servidor; por otra parte, en las máquinas cliente se ha instalado los aplicaciones cliente de la herramienta SGSI Tracking; así como se ha realizado una configuración acorde a los requisitos de la norma y a las recomendaciones establecidas en la presente memoria. No se describen estos pasos porque se considera que están fuera del alcance del propósito del presente proyecto.

Para la redacción de la siguiente memoria se ha procedido a instalar VMWare Server 2 en un equipo de sobremesa estándar, además se dispone de las siguientes máquinas virtuales:

- Debian Demo: Cliente Linux
- XP-pruebas: Cliente Windows
- SGSI Demo: Máquina de SGSI Tracking que se empleará en la demo

Para comenzar, se muestra una captura inicial de la interfaz de acceso web de VMWare Server.

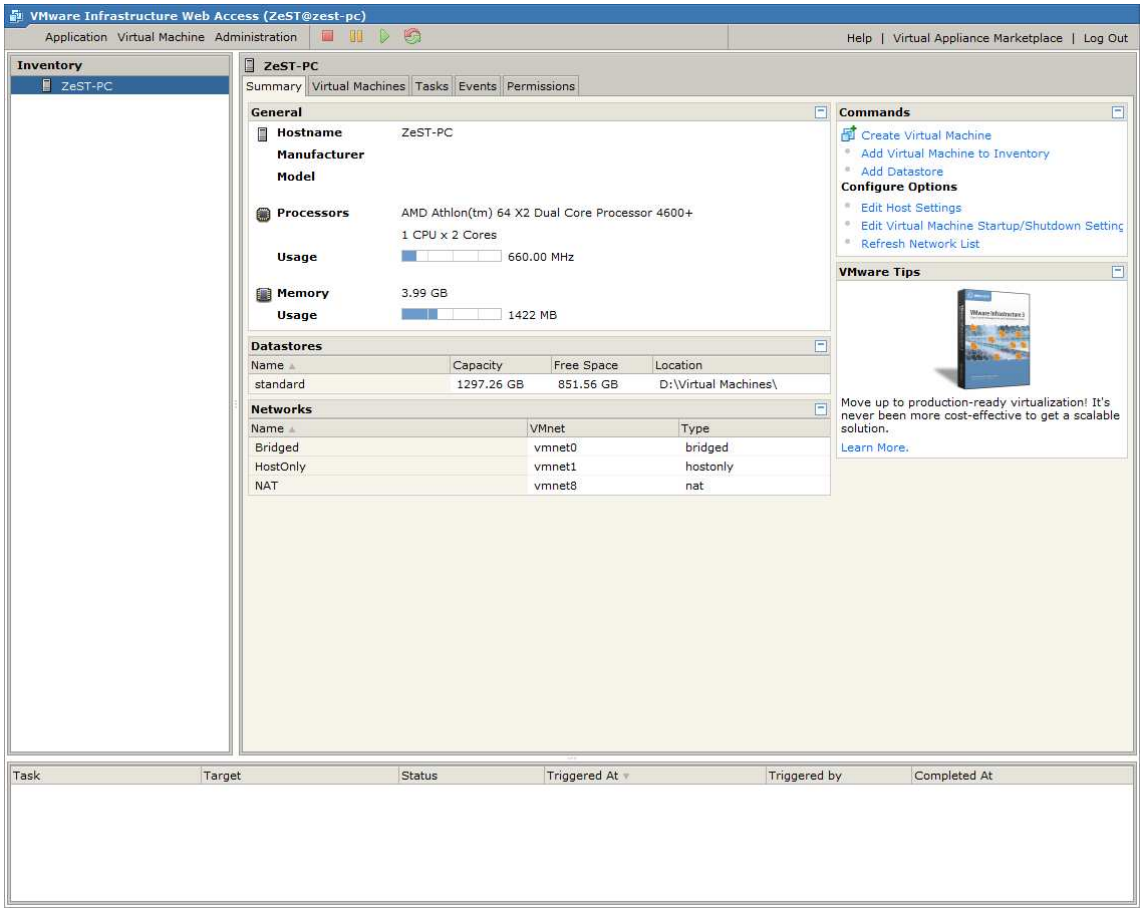


Ilustración 72 - Red Pruebas - VMWare Server 2

La pantalla inicial nos muestra los datos de la máquina *Host*, como los recursos de que dispone (procesadores, memoria, redes, etc.). Además nos ofrece comandos para crear, añadir, y manipular las máquinas virtuales, así como la configuración global de *Host*.

El primer paso es incluir las máquinas virtuales mencionadas en el listado de máquinas de la aplicación, para ello se emplea el asistente del que dispone la misma. De este modo ya nos aparecerán en el listado *Inventory*.

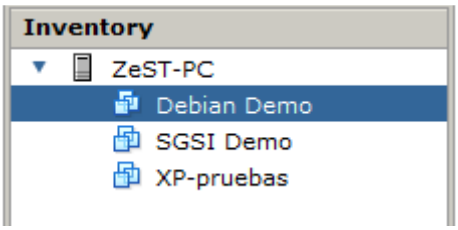


Ilustración 73 - VMWare Server – Inventory

A continuación se muestra configuración global de la máquina SGSI Demo. Repasaremos los apartados y se especificará en los que se requiera una configuración especial.

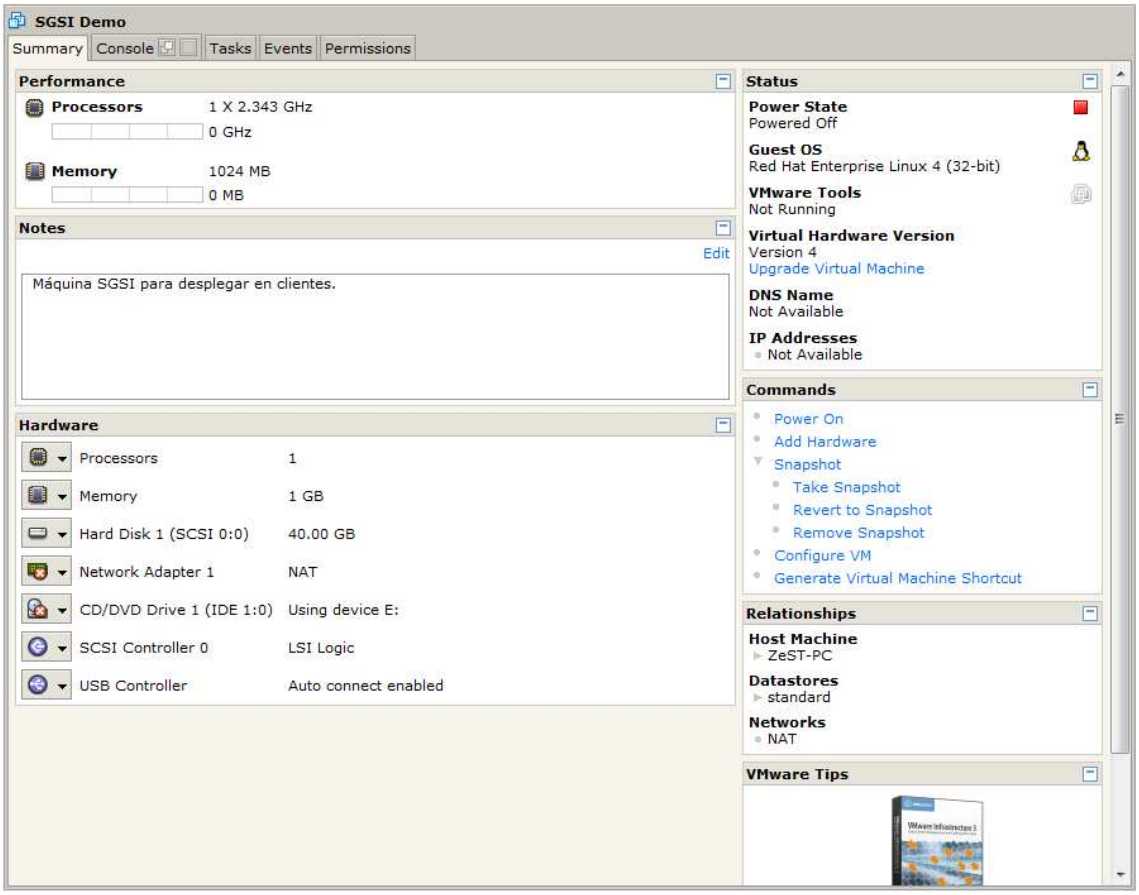


Ilustración 74 - VMWare Server - Vista máquina virtual

Campos que aparecen en la ilustración:

- *Performance*: Rendimiento de la máquina virtual, en términos porcentaje de ocupación de procesadores y memoria de la misma.

- *Notes*: Notas acerca de la máquina virtual, es interesante para administradores que gestionan un gran número de máquinas virtuales.
- *Hardware*: Establece el hardware que integra la máquina virtual, permitiendo realizar una configuración específica de cada uno de los dispositivos, se describen a continuación, centrándonos en los cuales requieren atención para establecer el entorno de pruebas:
    - *Processors:* Permite seleccionar el número de procesadores que empleará la máquina virtual.
    - *Memory:* Permite asignar la cantidad de memoria en MB que se asigna a la máquina. Incluye recomendaciones de acuerdo al sistema operativo a instalar.
    - *Hard disk:* En nuestro caso permite especificar el tipo de disco, así como su puerto de conexión. En el caso de la creación de una máquina virtual o un disco nos permite seleccionar el tamaño en GB.
    - *Network Adapter:* Adaptador de red, nos permite ajustar la MAC del dispositivo, y además nos permite especificar a la subred a la que conectamos la máquina virtual. Este campo se debe rectificar, para ajustar todos los host de la red de pruebas para que se conecten a la misma subred, aislada en su caso de las redes de producción de Setival.

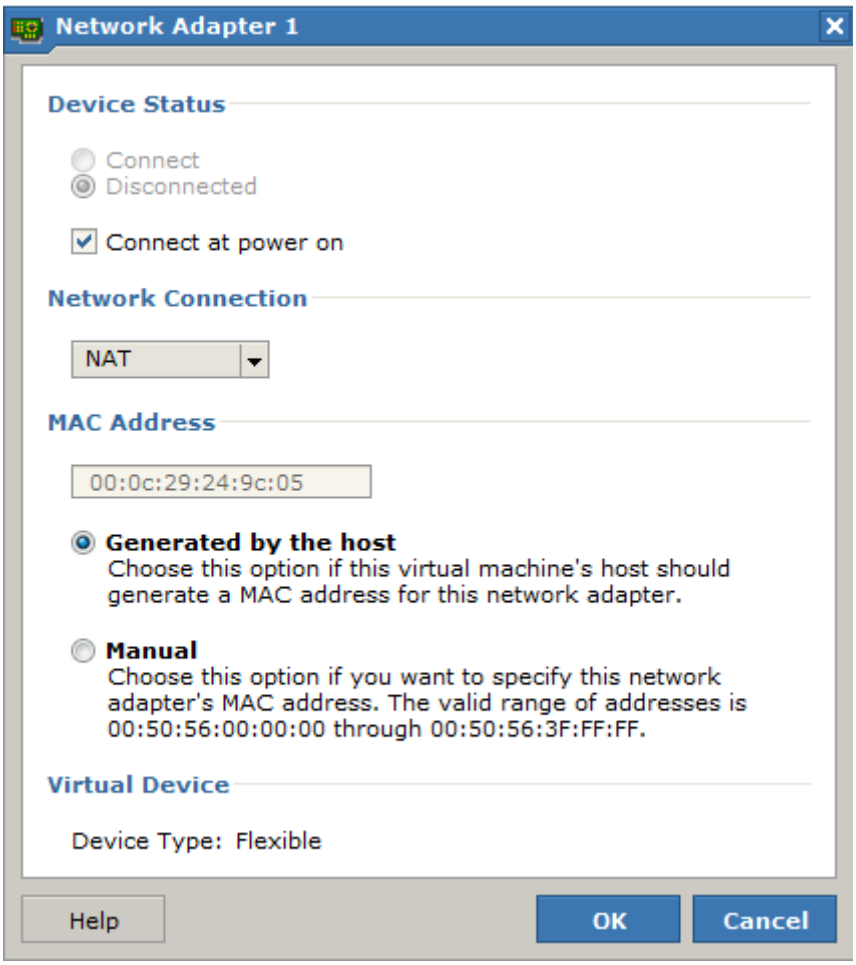


Ilustración 75 - VMWare Server - Network Adapter

Se ha seleccionado NAT, porque es un segmento de red en el que solo se ven las máquinas que están en el mismo (exclusivamente dentro del *Host*). De forma predeterminada las máquinas de uso de producción de Setival están en el segmento bridged, el cual conecta la máquina virtual a la red tal cual lo está la máquina *Host*.

  - *SCSI Controller*: Habilita y deshabilita la controladora SCSI.
  - *USB Controller*: Habilita y deshabilita la controladora USB.
- *Status*: Nos da varios datos importantes acerca del estado de la máquina virtual, destacan:
  - *Power State*: Encendida, suspendida o apagada.
  - *DNS Name*: Nombre del DNS.
  - *IP Adresses*: Direcciones IP de la máquina virtual.
- *Commands*: Ofrece comandos (acciones) que se pueden realizar sobre una máquina virtual:
  - *Power On/Off*: Encender/Apagar.
  - *Add hardware*: Añadir hardware.
  - *Snapshot*: Herramientas para capturar estados de la máquina virtual.
  - *Configure VM*: Configuración de la máquina virtual (Sistema Operativo, configuración de BIOS, ejecución de script, etc.).
- *Relationships*: Muestra el nombre, *datastore* y red asignados a la máquina.

Con esta sencilla implementación se puede disponer de una subred propia, donde se encuentran las máquinas de demostración o prueba, completamente aislada de la red de producción. Además es completamente modulable, por lo que se ha podido instalar en un portátil de Setival para hacer demostraciones *on site* para los clientes.

5. Implantación de la Norma ISO 27001 y SGSI Tracking en Setival SCV

5.1. Necesidades, personal e inicio de la implantación

Desde los comienzos de Setival SCV se pensó en obtener un certificado de ISO 27001. Existen diversos motivos para tomar esta decisión:

- El principal activo de la empresa es la información, dado que se trata de una empresa de servicios, con prácticamente pocos productos (y estos productos son bienes intangibles, en esencia, información).
- Setival SCV dispone de información privilegiada de los clientes en sus sistemas, ya que es imprescindible para poder realizar proyectos de consultoría.
- Puesto que se realiza consultoría de seguridad informática, incluyendo servicios de implantación de ISO 27001, se considera imprescindible disponer de esta certificación.

En Abril de 2009, se tomó la decisión de implantar la norma en la entidad. Desde un principio la responsabilidad y organización de la implantación recayó en Josep Cuñat Ferrando, en calidad de Consultor Jefe, quien delegó la implantación e controles técnicos en David Cutanda Mompó, en calidad de Administrador de Sistemas. El comienzo de la implantación de la norma coincidió con la fase final del desarrollo de la herramienta SGSI Tracking, por lo que, con el fin de facilitar y agilizar la implantación de ISO 27001, se decidió instaurarla.

5.2. Descripción de la implantación

En el presente punto se describen las acciones y configuración de SGSI Tracking y los equipos de Setival SCV desde el punto de vista de Administrador de Sistemas, siempre alineado con las recomendaciones y consejos del Consultor Jefe al cargo de la implantación.

Tras la realización del Análisis de Riesgos y la Declaración de Aplicabilidad, los requisitos, a grandes rasgos, que se presentaron al Administrador de Sistemas fueron los siguientes:

- Identificar y mantener un inventario de activos, establecer un propietario para cada activo.
- Adquirir e instalar un SAI.
- Controlar el acceso al CPD.
- Incluir medidas de seguridad en los equipos portátiles, tales como cifrado, borrado seguro de información, etc. Y formar a los usuarios en su manejo.
- Formalizar y mejorar el proceso de copias de seguridad de la información de acuerdo a los requisitos normativos.
- Realizar un proceso de alta y baja de usuarios adecuado y formalizarlo en un procedimiento. Además proceder a realizar revisiones de usuarios y perfiles de forma periódica.

- Como primer responsable en la recepción de incidencias y peticiones de cambio, instaurar un sistema para su gestión, asignación y resolución. Así como ser la persona encargada de preparar instrucciones y formar a los usuarios en su manejo.
- Revisar y ajustar la configuración de seguridad de Routers, Servidores y todos los equipos de la entidad (incluyendo directivas de seguridad en el control de acceso a todos los sistemas, estableciendo complejidad, caducidad y bloqueo de las cuentas de usuario). Así como instalar y gestionar todo el software relacionado con auditoría y seguridad de la información.
- Gestionar la capacidad de los sistemas, intentado prevenir caídas de sistemas por agotamiento de recursos.
- Realizar un control y gestión de la salida de soportes de información, así como aplicar medidas de seguridad cuando sea necesario.
- Controlar la instalación de aplicaciones no permitidas en la política de seguridad (tales como mensajería instantánea, descargas P2P, etc.).
- Implantar registros de auditorías, eventos y errores en los sistemas, así como configurar los sistemas y aplicaciones para obtener resultados seleccionados y centralizados en la herramienta SGSI Tracking.
- Monitorizar el uso y disponibilidad de servicios de red, tanto internos como externos.
- Registrar las actividades de administración de sistemas, así como las de supervisión.

Se va a pasar a describir cada uno de estos puntos, haciendo especial hincapié en los relacionados con el uso de la herramienta SGSI Tracking y los que se considere oportuno para la consecución del presente proyecto.

- **Creación y mantenimiento del inventario de activos**

Para este fin se empleó los módulos de inventario de red e inventario de activos de SGSI Tracking. De forma previa a su puesta en marcha se instalo la herramienta cliente de OCS Inventory en todos los equipos de Setival SCV. Se siguieron las mismas directivas que se describen en la adecuación de la herramienta, por lo que:

- Se empleó el inventario de red para detectar todos los activos de información conectados a la misma.
- Tras la sincronización entre el inventario de red y el de activos se procedió a completar los datos relevantes de cada activo, principalmente el propietario. Así como los activos que no estaban incluidos en el inventario de red.

No se incluyen capturas de pantalla puesto que son semejantes a las que se incluyeron en el punto 3.4.1 Planificar de la presente memoria.

- **Adquirir e instalar un SAI**

Se repasaron los requisitos de negocio, así como la cantidad de equipo que debería estar conectado. Del mismo modo se consideró necesario que el mismo pudiera realizar apagados seguros de los equipos, así como arrancarlos cuando se restablezca el suministro. Dado que es muy importante para la entidad mantener la conectividad externa por VPN, así

como los servicios ofrecidos al exterior de cara a los clientes. Se adquirió e instaló un SAI capacitado para ello.

- **Controlar el acceso al CPD**

Se estableció un registro de acceso a personal no autorizado al CPD, del mismo modo se colocó una llave a dicha sala, la cual está cerrada por defecto. Se informó a todos los empleados de la necesidad de escoltar las visitas.

- **Medidas de seguridad para equipos que salen de las instalaciones**

Ante la inminente salida de los equipos portátiles por parte de la entidad (todos los equipos cliente de Setival SCV son portátiles), es un requisito de la norma ISO 27001 proteger la información almacenada en este tipo de soportes. La justificación es sencilla, dado que salen de la entidad, existe un riesgo potencialmente alto de que se produzcan robos o accesos no autorizados a esos equipos, por lo que es necesario aplicar medidas de seguridad adicionales sobre los mismos.

Para el cumplimiento de estas medidas se procedió a instalar dos aplicaciones, las cuales se describe brevemente a continuación:

o Truecrypt: Se trata básicamente de una herramienta para el cifrado de datos. Entre sus principales capacidades destacan la capacidad de cifrar volúmenes enteros (unidades lógicas o discos físicos), o crear particiones de datos cifradas. Ésta última es la que se seleccionó dados los requerimientos y el coste de la otra opción.

Otro de los motivos de decidir Truecrypt como herramienta de cifrado es que monta, de forma automática, las unidades cifradas en el arranque del sistema, solicitando la clave de forma automático al inicio de sesión.

Ilustración 76 - Truecrypt - Autentificación

Pasando ya a especificar las medidas de seguridad implantadas, para las particiones cifradas de los portátiles se seleccionó el algoritmo de cifrado AES con un hash RIPEMD-160, que se consideró la solución óptima a los requerimientos de complejidad y rendimiento requeridos por las actividades desarrolladas.

Ilustración 77 - Truecrypt - Algoritmo de Cifrado

También se implantaron medidas destinadas a poder recuperar la información de una partición cifrada en caso de que el empleado (el conocedor único de su clave de cifrado) no colaborara al finalizar la relación contractual. El método es el siguiente:

1. Se crea la partición cifrada con una clave maestra, la cual es común a todos los equipos, y únicamente conocida por el administrador de sistemas y el responsable de seguridad.
2. Se hace una copia de seguridad de la cabecera de la partición, con el fin de restaurarla en caso de la no colaboración del empleado. Esto nos permite acceder a la partición con la clave maestra.
3. Cambiar la clave de la partición con el empleado, para que la pueda acceder en su uso normal.

Tras estos pasos, configurando tanto el arranque automático de la partición, lo único que cabe es recordar al empleado que toda información de negocio que transporte en su portátil deberá ser almacenada en esta partición.

Mediante la aplicación de esta medida se protege la información contenida en los portátiles contra amenazas relacionadas con la confidencialidad de la misma. Se muestra la ventana de Truecrypt y el explorador de archivos con la unidad cifrada montada.

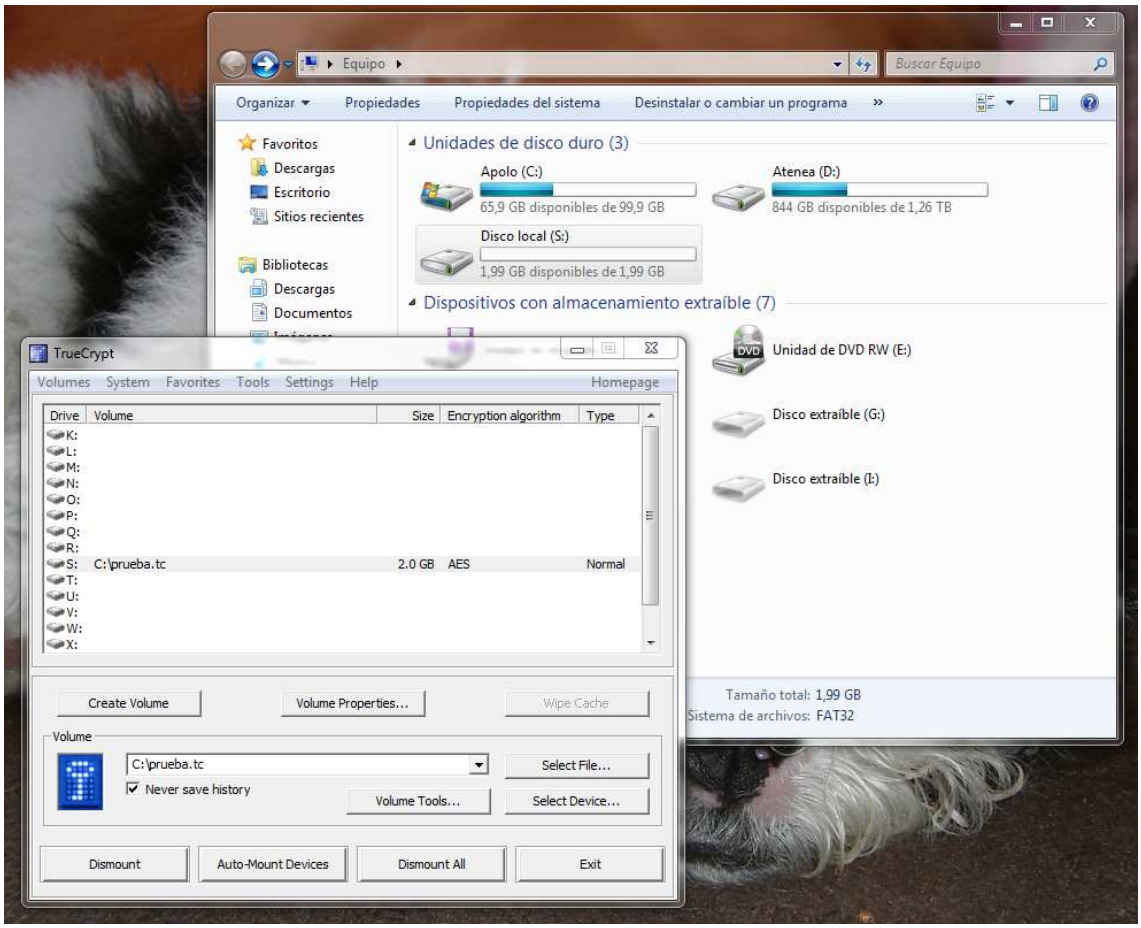


Ilustración 78 - Truecrypt - Unidad cifrada

- Eraser: Se trata en su base, de una herramienta para el borrado seguro de información.

  Es bien conocido el funcionamiento de los sistemas de archivos FAT 32 y NTFS, ambos disponen de unas tablas de asignación de archivos (cada una designada de acuerdo a su arquitectura), cuando Windows realiza un borrado de un archivo lo único que hace es establecer como liberado el espacio ocupado por los datos en la tabla de asignación de archivos. Lo que directamente deja los datos en el disco hasta que se realice su sobre escritura (lo cual no tenemos certeza de cuándo será).

  La herramienta Eraser ofrece la posibilidad de realizar borrados seguros por medio de sobre escritura reiterada. El funcionamiento de la herramienta es el siguiente, cuando se ordena un borrado sobre escribe el espacio ocupado por el archivo un número determinado de veces (para Setival SCV se seleccionó un borrado de 7 pasadas, lo que garantiza que no de podrán recuperar los datos). Después de realizar la sobre escritura se elimina de forma normal la tabla de asignación de archivos.

  Esta medida se toma pensando en copias de datos de negocio no alojados en la partición cifrada, que se quieran eliminar de forma definitiva e irrecuperable.

- **Formalizar y mejorar el proceso de copias de seguridad**

Para llevar a cabo este punto, lo primero fue redactar el procedimiento de copias de seguridad a implementar, y a continuación seleccionar y configurar la herramienta de copias adecuada a estos requisitos.

En primer lugar, se consideraron los siguientes conjuntos de datos a realizar copias, así como la periodicidad requerida o considerada:

DATOS	PERIODICIDAD	TIPO DE COPIA	HISTORIAL DE COPIAS
Datos de Consultoría y Nuevas Tecnologías	Diaria	Incremental	2 Semanas, 1 completa semanal
Datos de Servicios y Aplicaciones	Diaria	Incremental	1 Semana, 1 completa semanal
Máquinas Virtuales	Semanal	Completa	2 Semanas

Ilustración 79 - Copias Seguridad- Tabla

Es importante destacar, además, que se consideró realizar una copia de seguridad externalizada, ya que en caso de un desastre mayor, como un incendio, se destruiría la copia de seguridad. Como solución final se plantea alojar las copias de seguridad en dos discos externos, los cuales se irán cambiando de la vivienda del responsable de seguridad a la oficina con una periodicidad semanal. Esta periodicidad se estableció estudiando los requisitos de negocio, concretamente cual sería el límite de información que la organización podía asumir la pérdida de datos.

Esta externalización supone que la copia de seguridad tendrá que salir de las instalaciones, por lo que se ha considerado, además, el cifrado de las copias para evitar problemas con la confidencialidad.

En segundo lugar, la herramienta seleccionada fue Cobian Backup, un conocido software gratuito de copias de seguridad que permite:

- Ejecutarse como servicio y programar las copias de forma automática.
- Respaldos completos, diferenciales e incrementales.
- Cifrado y compresión de las copias de seguridad.
- Ejecución de eventos pre y post respaldo (esto era necesario para ejecutar un script que detuviera las máquinas virtuales para la copia, y una vez finalizada, las volviera a encender.

No se muestra en detalle el funcionamiento de la herramienta, ya que no se considera relevante, al contrario que la selección de requisitos y su justificación.

- **Realizar un proceso de altas/bajas de usuario adecuado**

En esta fase se revisó el procedimiento de altas y bajas de usuario, por una parte, para adaptarlo a las necesidades de sistemas de la entidad, y por otra, para adaptar los sistemas a sus necesidades, como por ejemplo:

- Formato de nombres de usuario
- Uso de Grupos de usuarios para facilitar la gestión de privilegios
- Revisión de equipos de la entidad cedidos, para la firma de cláusulas de aceptación y buen uso de los activos
- Establecer periodos de revisión de perfiles y usuarios autorizados en el sistema
- Etc.

- **Instaurar un gestor de incidencias**

Para la implementación de esta cuestión, se empleó SGSI Tracking, concretamente su módulo Gestor de Incidentes. El primer paso fue la creación de un manual de usuario para la herramienta en su conjunto, con el fin de realizar su difusión, apoyada de pequeñas sesiones formativas.

Se establecieron usuarios para la herramienta, mediante el gestor de usuarios de SGSI Tracking, para lo cual se establecieron separaciones de usuario y administrador. Para cualquier referencia repasar el punto Gestión de usuarios correspondiente a 3.4.5 Control.

Actualmente el sistema sigue en uso sin ningún tipo de problemas. Es importante recordar que el gestor de incidencias recibe las alertas generadas por el Monitorizador de red de la herramienta.

- **Revisión de la configuración de seguridad de routers, servidores y clientes. Instalación de herramientas de auditoría.**

Dada la infraestructura sencilla de los sistemas de información de la entidad, la revisión de la configuración del router se redujo a estos requerimientos:

- Comprobar que el firewall físico que incluye el router está habilitado y revisión de puertos abiertos al exterior, para evitar tener puertos abiertos sin ningún tipo de necesidad. Evitando vulnerabilidades de intrusión.
- Verificar la robustez de las claves de acceso a la configuración del router en remoto. Se seleccionó una clave con complejidad.
- Verificar la robustez de, por una parte el algoritmo de cifrado de la red inalámbrica (se seleccionó WPA 2), y por otra parte la robustez de la clave de acceso a la red wifi (se seleccionó una clave con la complejidad adecuada).

Pasando a la configuración de servidores y equipos, es importante destacar que no se dispone de un controlador de dominio, por lo que se tuvieron que emplear métodos alternativos a la configuración de seguridad del dominio. Estos métodos se basan en la creación de una plantilla de seguridad mediante la MMC (Microsoft Management Console), de

modo que, mediante una sencilla línea de comandos estas directivas podrán ser instauradas en cada uno de los equipos de la entidad. Se muestra a continuación una captura de la MMC, concretamente mediante la directiva de seguridad local.

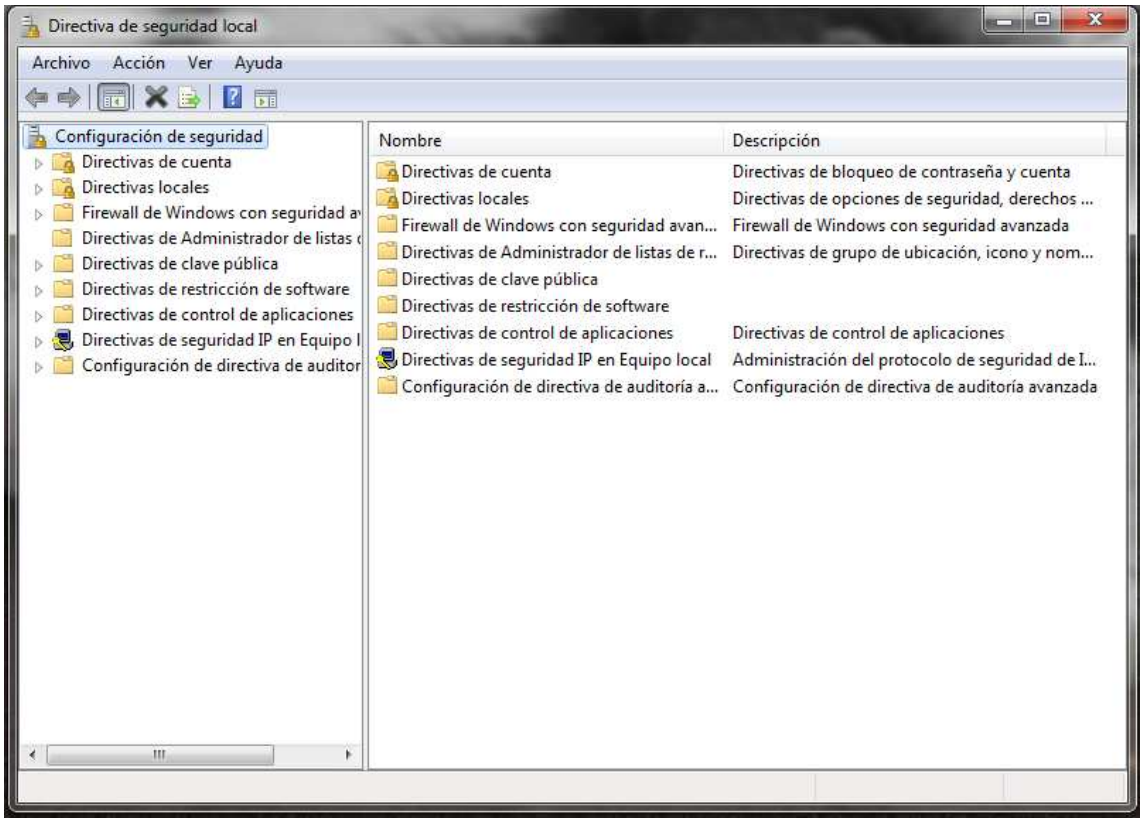


Ilustración 80 - MMC - Directiva de Seguridad Local

Concretamente se configura en esta directiva:

- Complejidad de contraseñas
- Longitud máxima y mínima de contraseñas (7 caracteres)
- Caducidad de contraseñas (3 meses)
- Configuración del bloqueo de cuenta (Bloqueo indefinido tras 30 intentos fallidos en 60 minutos)
- Directiva de auditoría (se configura de acuerdo a los eventos que se quieran monitorizar, se especificará más adelante, en la monitorización de eventos.

Una vez configurada la directiva de seguridad local, se puede exportar la misma mediante MMC, de modo que lo único que hay que hacer en cada equipo es volcarla para su funcionamiento. Los usuarios no deben ser administradores de sus equipos, por lo que, dado que no se dispone de un controlador de dominio, se procedió a crear un usuario normal nominal para el usuario, y un usuario administrador, con el cual se podrán realizar los cambios pertinentes sobre el equipo cliente.

Además, se debe verificó el estado del antivirus de todos los equipos (habilitado, actualizado, etc.), y la configuración del cortafuegos de Windows. Por último, se instalaron los clientes de la herramienta SGSI Tracking, tanto el cliente del Inventario de red como el del Correlador de eventos.

- **Gestionar la capacidad de los sistemas**

Esta gestión se basó, de forma inicial para la implantación, en ver el ritmo de crecimiento de la información, estimando cuanto tiempo podríamos estar sin ampliar los sistemas manteniendo el ritmo actual de crecimiento. Se procedió del mismo modo con el uso de CPU, memoria y uso de red. Se redactó un informe para dar constancia de ello.

- **Control y gestión de entrada y salida de soportes**

Se redactó un procedimiento de entrada y salida de soportes, en el cual se incluyeron registros para sus entradas y sus salidas, de acuerdo a la LOPD y la ISO 27001. Como Administrador es necesario estar al tanto de la entrada y la salida de los mismos, así como asegurarse de registrar dichos movimientos.

Se planteó también como medida alternativa el cifrado de dichos soportes cuando se considerara necesario, lo que es una decisión del Responsable de Seguridad. Para ello también se empleó la herramienta Truecrypt, la cual, dispone de un sistema para cifrado de soportes extraíbles, posibilitando incluso el montado del mismo en un equipo que no tenga instalada la herramienta, mediante una versión portable que incluye en el soporte. Se muestra a continuación una captura de pantalla de la configuración del soporte.

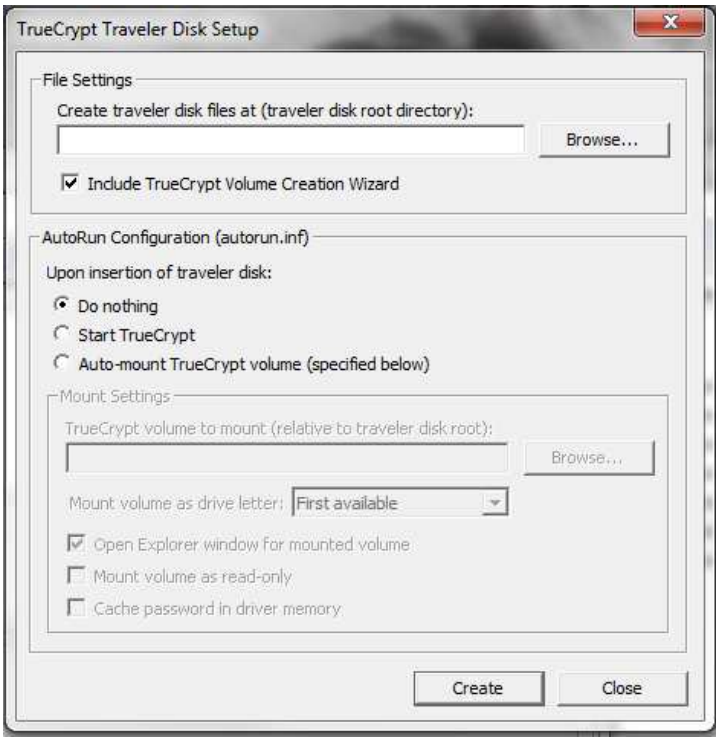


Ilustración 81 - Truecrypt - Traveler Disk Setup

- **Control de aplicaciones no permitidas**

En la política de seguridad de la información se especifica que hay cierto software prohibido. Para controlar la instalación de software no autorizado se empleó la herramienta Inventario de Red de SGSI Tracking, concretamente su Inventario de Software. Mediante la búsqueda de estos programas se pudo estipular que equipos tenían una copia instalada, y se procedió a solicitar su desinstalación al usuario. Se muestra una captura de pantalla ejemplo a continuación.

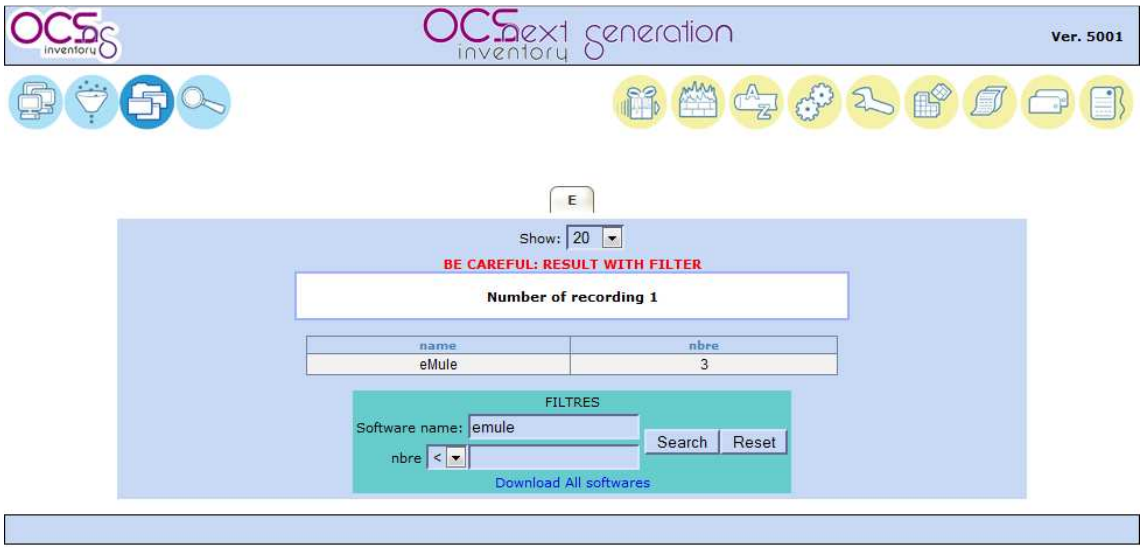


Ilustración 82 - Inventario de Red - Software no autorizado

- **Implantar registros de auditorías, eventos y errores en los sistemas**

Para el cumplimiento de los siguientes requisitos se empleó el módulo Correlador de Eventos, de la herramienta SGSI Tracking. Como se comentó, la herramienta centraliza los log de eventos de los sistemas que tienen instalado y configurado su cliente. Una vez instalada la herramienta se seleccionaron los siguientes conjuntos de eventos:

- Eventos de login/logout de los usuarios en los sistemas.
- Cambios en la directiva de seguridad, con el fin de detectar cambios en las mismas que puedan derivar en lagunas de control de algún equipo.
- Auditoría de acceso a objetos.

No se seleccionaron eventos adicionales, dadas las necesidades de la entidad. Estos eventos se encuentran referenciados en la Tabla 1 - Eventos de Seguridad de Windows Vista/7/Server 2008, clasificados por los grupos de auditoría que después se pueden seleccionar mediante la MMC en la directiva de seguridad local.

De este modo, se puede acceder de forma centralizada a estos eventos mediante la herramienta Splunk.

- **Monitorizar el uso y disponibilidad de los servicios de red.**

Para ello se empleó el módulo Monitorización de Equipos, de la herramienta SGSI Tracking. El proceso de implantación consistió en seleccionar que puertos y sistemas había que monitorizar, con el fin de después, generar incidencias automáticas asociadas a su actividad. Se seleccionaron los siguientes equipos:

- SGSI Tracking de Setival
- Máquinas virtuales de desarrollo de GeConsulting
- Máquinas virtuales de desarrollo de SGSI Tracking
- ERP
- Servidor de datos de Setival SCV
- Router
- Servicios de Correo electrónico y hosting
- Impresoras de red

Para referencia a la configuración del módulo, ver apartado de Monitorización de Equipos, correspondiente al punto 4 de la presente memoria.

- **Registrar las actividades de administración de sistemas**

Se registran de forma sencilla dada la configuración de auditoría existente. Para ello se seleccionaron los accesos de administrador a los servidores mediante el módulo Correlador de Eventos de la herramienta SGSI Tracking. Luego, se programó una búsqueda automática que envía sus resultados diariamente al Responsable de Seguridad. De modo que aparecen los login y logout de los administradores de sistemas diariamente. Para una referencia a su implementación se debe revisar el punto de cómo programar búsquedas de eventos en SGSI Tracking.

Con esto se finaliza el repaso a las medidas a implementar, hay que destacar que se han omitido datos en esta descripción con el fin de salvaguardar la información restringida y confidencial de Setival SCV. También es importante destacar que no se ha ofrecido un listado completo de las mismas, se han obviado los que no aportaban nada al presente proyecto fin de carrera.

Por último destacar que este conjunto de medidas no es en absoluto extrapolables a cualquier empresa, ya que son fruto de un trabajo personalizado de consultoría. Se muestran como ejemplo de medidas de implantación, así como justificación de la labor realizada en Setival SCV.

6. Conclusiones

Desde que se inició el desarrollo de la herramienta SGSI Tracking, su objetivo siempre ha sido no solo alinearse con la norma ISO/IEC 27001:2007, sino servir de medio para facilitar su cumplimiento. Quizás para otro tipo de normas más documentales, como por ejemplo la ISO 9001:2008, o la ISO 14001:2004; no se podría plantear una solución informática que pasara de ser un gestor documental para albergar los procedimientos. Sin embargo, la naturaleza técnica de ISO 27001, no solo permite, sino que requiere, una serie de controles y salvaguardas a aplicar sobre los sistemas de información. Este hecho condujo al equipo de Setival a diseñar una herramienta modular, seleccionando los módulos que inicialmente ofrecían capacidades adecuadas para tal fin, y se decidió integrarlas.

Hoy, y tras la consecución, por una parte de la implementación y por otra, la implantación de la herramienta en Setival SCV; es necesario que volvamos a plantearnos el objetivo de la herramienta, de ahí que se haya propuesto el siguiente proyecto, por una parte como muestra del camino que ha completado, y por otra como evidencia del camino que queda por completar.

Desde el punto de vista del autor, tras prácticamente dos años trabajando en Setival SCV, este proyecto, además de concluir sus estudios de ingeniería informática, supone un paso adelante en su formación como Consultor IT. Sin más, se pasan a repasar los puntos y conclusiones obtenidas del proyecto.

Se ha evaluado la herramienta SGSI Tracking en relación a su apoyo al cumplimiento de las siguientes normas:

- ISO/IEC 27001:2007 (Bajo las recomendaciones de implantación de ISO/IEC 17799:2002)
- Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, junto con el Reglamento 1720/2007 para la misma.

En general se ha observado un buen nivel de integración con los requisitos de la norma ISO 27001, centrada básicamente en los controles más técnicos. Se han detectado los siguientes puntos fuertes en base a los objetivos de control:

- A.7 – Gestión de Activos: SGSI Tracking mediante el bloque Planificar, facilita el cumplimiento de la mayoría de los requisitos , ofreciendo por una parte un inventario automatizado de red, de perfil completamente técnico, y por otra un inventario de activos completo, con multitud de campos, y que además recoge datos del inventario de red, facilitando mucho, la tarea de inventariar. Además se han situado en un pequeño repositorio documental los procedimientos de etiquetado y clasificación de la información.
- A.10 – Gestión de comunicaciones y operaciones: Se ayuda a obtener un muy alto grado de cumplimiento en este punto, mediante las herramientas del bloque Verificar, tanto el Correlador de Eventos como la Monitorización de equipos. Es importante

destacar también las capacidades que da el Inventario de Activos respecto al manejo de soportes.

- A.11 – Control de Accesos: La herramienta SGSI Tracking, por una parte como parte del sistema, cumple con los requisitos de acceso de ISO 27001, establece perfiles adecuados, otorgando la posibilidad de seleccionar privilegios separados para cada una de las aplicaciones. Pasando a considerarla una herramienta de auditoría, facilita la verificación de accesos de usuarios, administradores y acceso a objetos sensibles del sistema de información.
- A.13 – Gestión de Incidentes de seguridad de la información: El módulo gestor de Incidentes de la herramienta SGSI Tracking supone una solución completa, óptima y eficiente de gestión de incidencias, que recoge los mensajes de todos los módulos de la herramienta. Permite un acceso selectivo dependiendo de los privilegios de cada usuario y automatiza la notificación de cierre de incidencias.
- A.15 – Cumplimiento: Se ha obtenido un muy buen resultado en el presente objetivo. En primer lugar, la herramienta SGSI Tracking está correctamente adecuada a los requisitos LOPD; en segundo, mediante el uso del módulo Inventario de Activos se puede realizar una gestión sobresaliente de las licencias y contratos relacionados con los Derechos de Propiedad Intelectual; y por último, SGSI Tracking supone una herramienta de auditoría para el control del uso de los sistemas de información, y que ayuda a protegerlos y monitorizarlos.

Pasando a comentar los puntos débiles es necesario hacer una generalización, la herramienta dispone de un pequeño repositorio documental, pero no cumple los requisitos mínimos de lo que se requiere de un verdadero gestor documental (control de versiones, control de acceso a usuarios, etc.). Con la inclusión de un buen gestor documental la herramienta aumentará con creces el cumplimiento en prácticamente todos los objetivos de control. Repasamos ahora sí, punto por punto:

- A.5 – Política de Seguridad: Es un objetivo de control completamente documental, se recomienda incluir un módulo de gestión documental. Esta mejora facilitaría la distribución de la política de seguridad y centralizaría la gestión global del SGSI alrededor de la herramienta.
- A.6 – Aspectos organizativos de la seguridad de la información: Como su nombre indica, se trata de medidas organizativas como establecer un comité de seguridad de la información, acuerdos de confidencialidad o el trato con terceros. Del mismo modo, dadas las limitaciones, sería incluir un gestor documental que incluyera todos los formatos y procedimientos relacionados con este objetivo de control.
- A.8 – Gestión de los recursos humanos: Este objetivo de control se centra en la relación con los empleados, desde antes de ser contratados, hasta las medidas a tomar posteriores a su contratación. La herramienta SGSI tracking, a su favor, supone una herramienta de auditoría en caso de que den procesos disciplinarios. Sin embargo, este objetivo de control queda parcialmente descubierto, y se observa que en la herramienta cabe mejorar, dado que se emplea a lo largo de la relación contractual con el empleado, la inclusión de mecanismos de comunicación entre los responsables del SGSI y los empleados con fines formadores. Sería una buena solución la inclusión

de un pequeño foro, o blog, que avisara e informara a los usuarios de situaciones y recomendaciones relacionadas con la seguridad de la información. También sería útil incluir un gestor documental para mantener, por ejemplo, el procedimiento de alta y baja de empleados.

- A.9 – Seguridad física y ambiental: Dada la naturaleza del siguiente objetivo de control, lo único que sería destacable recomendar es la inclusión de un gestor documental, que soporte todos los procedimientos y formatos relacionados con el mismo.
- A.12 – Adquisición, desarrollo y mantenimiento de los sistemas de información: Se basa completamente en establecimiento de requisitos de seguridad de los equipos, controles criptográficos, seguridad de los archivos de sistema, etc. A pesar de que la herramienta SGSI Tracking supone un mecanismo de control del software en los equipos mediante su módulo Inventario de Red, quedan muchos puntos descubiertos, sobre todo a nivel procedimental, por lo que se recomienda de nuevo en este caso la inclusión de un gestor documental para el control y distribución adecuada y centralizada de los mismos.
- A.14 – Gestión de la continuidad de negocio: A pesar de que SGSI Tracking tiene configurada una alerta que avisa de la prueba del plan de continuidad, se puede considerar incluir un gestor documental que apoye la documentación referente a este punto.

Como conclusión final al análisis de cumplimiento de ISO 27001, cabe destacar que se ha obtenido un cumplimiento muy alto, pero que con alguna pequeña modificación se podría mejorar con creces.

Pasando a los requisitos LOPD, dada la naturaleza de la herramienta eminentemente técnica, solo se analizará el TÍTULO VIII del RD 1720/2007 en su apartado de medidas de seguridad para tratamientos de datos automatizados, que hace referencia a las medidas de seguridad en el tratamiento de datos de carácter personal, dado que el resto del texto menciona requisitos legales y normativos, que al no estar soportados en un sistema de información, escapan a las capacidades de la herramienta. Solo destacar que se recomienda, del mismo modo que en ISO 27001 la inclusión de un gestor documental, que pueda recoger toda la documentación asociada al cumplimiento de la ley.

Una vez hecha la aclaración, en este caso, se destacan los puntos fuertes de la herramienta en relación a la LOPD:

- Registro de incidencias (Art. 90 y 100): Se dispone del módulo Gestor de Incidencias adecuado completamente a los requisitos LOPD, como se ha mencionado con anterioridad.
- Control de acceso (Art. 91): SGSI Tracking ofrece mecanismos para el control y supervisión de los accesos a los sistemas que soporten datos de carácter personal.
- Gestión de Soportes y documentos (Art. 92 y 97): Mediante la herramienta Inventario de Activos de SGSI Tracking se puede mantener un inventario actualizado y anotado de los soportes que se poseen, así como marcar si están en tránsito y su responsable.
- Identificación y autentificación (Art. 93 y 98): SGSI Tracking incluye alertas para cambios de contraseñas programados, de acuerdo a la LOPD.

- Copias de respaldo y recuperación (Art. 94 y 102): SGSI Tracking incluye una alerta para el aviso de la prueba de restauración de la copia de seguridad.
- Auditoría (Art. 96): Se ha incluido una alerta en SGSI Tracking que avisa de la fecha de auditoría obligatoria.
- Gestión y distribución de soportes (Art. 101): La herramienta pone a disposición del usuario los procedimientos de etiquetado de información.
- Registro de Accesos (Art. 103): Mediante el Correlador de Eventos de SGSI Tracking y una adecuada configuración se puede cumplir el requisito de control de acceso sobre datos de nivel alto.

Realmente no se considera que existan puntos débiles a esta adecuación quitando el gestor documental, ya que la Ley Orgánica de Protección de Datos no supone, en la mayoría de su texto, requisitos a implantar sobre sistemas de información automatizados, dado que ese es el alcance de la herramienta. Como conclusión final se le otorga una integración sobresaliente.

Pasando al punto de implementación de un entorno de pruebas virtualizado, hay que destacar que se obtuvo con creces el objetivo planteado, resultó una solución, rápida, modulable y barata de poder mantener un entorno de pruebas seguro y reproducible.

Por último, respecto a la implantación de SGSI Tracking en Setival SCV, junto con la implantación de ISO 27001, hay que destacar que la organización pasó limpiamente el proceso de certificación, junto con una mención notoria por parte del auditor de la herramienta SGSI Tracking, por la cual estuvo muy interesado durante todo el proceso de auditoría. También es importante destacar la evidente utilidad que se le encontró a la herramienta, a la cual los empleados se adaptaron rápidamente, y la que además, ha reducido con creces el tiempo dedicado a la supervisión y gestión del SGSI.

Como conclusión final, SGSI Tracking es una herramienta poderosa, pero con muchas vías de mejora y optimización. Se considera que si se continúa trabajando en ella puede ser una herramienta referente en el mercado, además de ser comercializable por medio del servicio de consultoría de Setival SCV, y como complemento al mismo.

7. Bibliografía

1. UNE-ISO/IEC 27001:2007
2. UNE-ISO/IEC 17799:2005
3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
4. REAL DECRETO 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
5. Manual de Usuario de SGSI Tracking
6. Documentación de formación de Setival SCV respecto a ISO 27001 y LOPD.

Anexos

Anexo I – Definiciones LO 15/1999

Se muestran a continuación las definiciones correspondientes a la LO 15/1999 del 26 de Diciembre de Protección de Datos Personales, artículo 3:

a) **Datos de carácter personal:** cualquier información concerniente a personas físicas identificadas o identificables.

b) **Fichero:** todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) **Tratamiento de datos:** operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) **Responsable del fichero o tratamiento:** persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) **Afectado o interesado:** persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) **Procedimiento de disociación:** todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) **Consentimiento del interesado:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) **Cesión o comunicación de datos:** toda revelación de datos realizada a una persona distinta del interesado.

j) **Fuentes accesibles al público:** aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

Anexo II - Disposiciones para creación de ficheros de titularidad pública

Se muestran a continuación los campos necesarios a notificar a la agencia de protección de datos dada la creación de un fichero de titularidad pública:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

Anexo III – Infracciones y Sanciones LO 15/1999

Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.
e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente.
b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.
d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.
g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.
k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.
l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.
b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.
d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.
e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.
f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Las sanciones correspondientes a las citadas infracciones son:

- Las infracciones **leves** serán sancionadas con multa de 600 a 60.000 euros.
- Las infracciones **graves** serán sancionadas con multa de 60.000 a 300.000 euros.
- Las infracciones **muy graves** serán sancionadas con multa de 300.000 a 600.000 euros.

La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

Anexo IV – Definiciones RD 1720/2007

A los efectos previstos en este reglamento, se entenderá por:

a) **Afectado o interesado:** Persona física titular de los datos que sean objeto del tratamiento.
b) **Cancelación:** Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.
c) **Cesión o comunicación de datos:** Tratamiento de datos que supone su revelación a una persona distinta del interesado.
d) **Consentimiento del interesado:** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
e) **Dato disociado:** aquél que no permite la identificación de un afectado o interesado.
f) **Datos de carácter personal:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
g) **Datos de carácter personal relacionados con la salud:** las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.
h) **Destinatario o cesionario:** la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
i) **Encargado del tratamiento:** La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
j) **Exportador de datos personales:** la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.
k) **Fichero:** Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
l) **Ficheros de titularidad privada:** los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los

ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

o) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

p) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

q) Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

r) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

t) Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

u) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

En particular, en relación con lo dispuesto en el TÍTULO VIII de este reglamento se entenderá por:

a) **Accesos autorizados:** autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.
b) **Autenticación:** procedimiento de comprobación de la identidad de un usuario.
c) **Contraseña:** información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.
d) **Control de acceso:** mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
e) **Copia de respaldo:** copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
f) **Documento:** todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.
g) **Ficheros temporales:** ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.
h) **Identificación:** procedimiento de reconocimiento de la identidad de un usuario.
i) **Incidencia:** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
j) **Perfil de usuario:** accesos autorizados a un grupo de usuarios.
k) **Recurso:** cualquier parte componente de un sistema de información.
l) **Responsable de seguridad:** persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
m) **Sistema de información:** conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
n) **Sistema de tratamiento:** modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.
o) **Soporte:** objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.
p) **Transmisión de documentos:** cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.
q) **Usuario:** sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Anexo V – Términos y definiciones ISO/IEC 27001:2005

1. **Activo:** Cualquier bien que tiene valor para la organización.
2. **Disponibilidad:** La propiedad de ser accesible y utilizable por una entidad autorizada.
3. **Confidencialidad:** La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
4. **Seguridad de la información:** La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.
5. **Evento de seguridad de la información:** La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.
6. **Incidente de seguridad de la información:** Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.
7. **Sistema de Gestión de la Seguridad de la Información (SGSI)** ***[Information Security Management System (ISMS)]*****:** La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

   NOTA: El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, losprocedimientos, los procesos y los recursos.

8. **Integridad:** La propiedad de salvaguardar la exactitud y completitud de los activos.
9. **Riesgo residual:** Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.
10. **Aceptación del riesgo:** La decisión de aceptar un riesgo.
11. **Análisis de riesgos:** Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
12. **Evaluación de riesgos:** El proceso general de análisis y estimación de los riesgos.
13. **Estimación de riesgos:** El proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar la importancia del riesgo.
14. **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
15. **Tratamiento de riesgos:** El proceso de selección e implementación de las medidas encaminadas a modificar los riesgos.
16. **Declaración de aplicabilidad:** Declaración documentada que describe los objetivos de control y los controles que son relevantes para el SGSI de la organización y aplicables al mismo.

    NOTA: Los objetivos de control y los controles se basan en los resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, en los requisitos legales o reglamentarios, en las obligaciones contractuales y en las necesidades empresariales de la organización en materia de seguridad de la información.

Anexo VI - Objetivos de control y controles de ISO/IEC 27001

A.5 Política de seguridad

A.5.1 Política de seguridad de la información

***Objetivo*:** Proporcionar indicaciones para la gestión y soporte de la seguridad de la información de acuerdo con los requisitos empresariales y con la legislación y las normativas aplicables.

A.5.1.1 Documento de política de seguridad de la información

Control: La Dirección debe aprobar un documento de política de seguridad de la información, publicarlo y distribuirlo a todos los empleados y terceros afectados.

A.5.1.2 Revisión de la política de seguridad e la información

Control: La política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

A.6 Aspectos organizativos de la seguridad de la información

A.6.1 Organización interna

Objetivo: Gestionar la seguridad de la información dentro de la organización.

A.6.1.1 Comité de gestión de seguridad de la información.

Control: La Dirección debe prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explícitas y el reconocimiento de las responsabilidades de seguridad de la información.

A.6.1.2 Coordinación de la seguridad de la información

Control: Las actividades relativas a la seguridad de la información deben ser coordinadas entre los representantes de las diferentes partes de la organización con sus correspondientes roles y funciones de trabajo.

A.6.1.3 Asignación de responsabilidades relativas a la seguridad de la información

Control: Deben definirse claramente todas las responsabilidades relativas a la seguridad de la información.

A.6.1.4 Proceso de autorización de recursos para el procesado de la información

Control Para cada nuevo recurso de procesado de la información, debe definirse e implantarse un proceso de autorización por parte de la Dirección.

A.6.1.5 Acuerdos de confidencialidad

Control: Debe determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información.

A.6.1.6 Contacto con las autoridades

Control: Deben mantenerse los contactos adecuados con las autoridades competentes.

A.6.1.7 Contacto con grupos de especial interés

Control: Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros, y asociaciones profesionales especializados en seguridad.

A.6.1.8 Revisión independiente de la seguridad de la información

Control: El enfoque de la organización para la gestión de la seguridad de la información y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.

A.6.2 Terceros

Objetivo: Mantener la seguridad de la información de la organización y de los dispositivos de procesado de la

información que son objeto de acceso, tratamiento, comunicación o gestión por terceros.

A.6.2.1 Identificación de los riesgos derivados del acceso de terceros

Control: Deben identificarse los riesgos para la información y para los dispositivos de procesado de la información de la organización derivados de los procesos de negocio que requieran de terceros, e implantar los controles apropiados antes de otorgar el acceso.

A.6.2.2 Tratamiento de la seguridad en la relación con los clientes

Control: Antes de otorgar acceso a los clientes a los activos o a la información de la organización, deben tratarse todos los requisitos de seguridad identificados.

A.6.2.3 Tratamiento de la seguridad en contratos con terceros

Control: Los acuerdos con terceros que conlleven acceso, tratamiento, comunicación o gestión, bien de la información de la organización, o de los recursos de tratamiento de la información, o bien la incorporación de productos o servicios a los recursos de tratamiento de la información, deben cubrir todos los requisitos de seguridad pertinentes.

A.7 Gestión de activos

A.7.1 Responsabilidad sobre los activos

Objetivo: Conseguir y mantener una protección adecuada de los activos de la organización.

A.7.1.1 Inventario de activos

Control: Todos los activos deben estar claramente identificados y debe elaborarse y mantenerse un inventario de todos los activos importantes.

A.7.1.2 Propiedad de los activos

Control: Toda la información y activos asociados con los recursos para el tratamiento de la información deben tener un propietario[3)] que forme parte de la organización y haya sido designado como propietario

A.7.1.3 Uso aceptable de los activos

Control: Se deben identificar, documentar e implantar las reglas para el uso aceptable de la información y los activos asociados con los recursos para el procesado de la información.

A.7.2 Clasificación de la información

Objetivo: Asegurar que la información recibe un nivel adecuado de protección.

A.7.2.1 Directrices de clasificación

Control: La información debe ser clasificada según su valor, los requisitos legales, la sensibilidad y la criticidad para la organización.

A.7.2.2 Etiquetado y manipulado de la información

Control: Se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

A.8 Seguridad ligada a los recursos humanos

A.8.1 Antes del empleo

Objetivo: Asegurar que los empleados, los contratistas y los terceros entienden sus responsabilidades, y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos.

A.8.1.1 Funciones y responsabilidades

Control: Las funciones y responsabilidades de seguridad de los empleados, contratistas y terceros se deben definir y documentar de acuerdo con la política de seguridad de la información de la organización.

A.8.1.2 Investigación de antecedentes

Control: La comprobación de los antecedentes de todos los candidatos al puesto de trabajo, de los contratistas o de los terceros, se debe llevar a cabo de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación y de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos considerados.

A.8.1.3 Términos y condiciones de contratación

Control: Como parte de sus obligaciones contractuales, los empleados, los contratistas y los terceros deben aceptar y firmar los términos y condiciones de su contrato de trabajo, que debe establecer sus responsabilidades y las de la organización en lo relativo a seguridad de la información.

A.8.2 Durante el empleo

Objetivo: Asegurar que todos los empleados, contratistas y terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización, en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano.

A.8.2.1 Responsabilidades de la Dirección

Control: La Dirección debe exigir a los empleados, con tratistas y terceros, que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización.

A.8.2.2 Concienciación, formación y capacitación en seguridad de la información

Control: Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deben recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.

A.8.2.3 Proceso disciplinario

Control Debe existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad.

A.8.3 Cese del empleo o cambio de puesto de trabajo

Objetivo: Asegurar que los empleados, contratistas y terceros abandonan la organización o cambian de puesto de trabajo de una manera ordenada.

A.8.3.1 Responsabilidad del cese o cambio

Control: Las responsabilidades para proceder al cese en el empleo o al cambio de puesto de trabajo deben estar claramente definidas y asignadas.

A.8.3.2 Devolución de activos

Control: Todos los empleados, contratistas y terceros deben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

A.8.3.3 Retirada de los derechos de acceso

Control: Los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los empleados, contratistas y terceros deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o bien deben ser adaptados a los cambios producidos.

A.9 Seguridad física y ambiental

A.9.1 Áreas seguras

Objetivo: Prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la organización.

A.9.1.1 Perímetro de seguridad física

Control: Se deben utilizar perímetros de seguridad (barreras, muros, puertas de entrada con control a través de tarjeta, o puestos de control) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.

A.9.1.2 Controles físicos de entrada

Control: Las áreas seguras deben estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

A.9.1.3 Seguridad de oficinas, despachos e instalaciones

Control: Se deben diseñar y aplicar las medidas de seguridad física para las oficinas, despachos e instalaciones.

A.9.1.4 Protección contra las amenazas externas y de origen ambiental

Control: Se debe diseñar y aplicar una protección física contra el daño causado por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre.

A.9.1.5 Trabajo en áreas seguras

Control Se deben diseñar e implantar una protección física y una serie de directrices para trabajar en las áreas seguras.

A.9.1.6 Áreas de acceso público y de carga y descarga

Control: Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, a través de los que personal no autorizado puede acceder a las instalaciones, y si es posible, dichos puntos se deben aislar de los recursos de tratamiento de la información para evitar los accesos no autorizados.

A.9.2 Seguridad de los equipos

Objetivo: Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización.

A.9.2.1 Emplazamiento y protección de equipos

Control: Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental así como las ocasiones de que se produzcan accesos no autorizados.

A.9.2.2 Instalaciones de suministro

Control: Los equipos deben estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro.

A.9.2.3 Seguridad del cableado

Control: El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debe estar protegido frente a interceptaciones o daños.

A.9.2.4 Mantenimiento de los equipos

Control: Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad.

A.9.2.5 Seguridad de los equipos fuera de las instalaciones

Control: Teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización, deben aplicarse medidas de seguridad a los equipos situados fuera dichas instalaciones.

A.9.2.6 Reutilización o retirada segura de equipos

Control: Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado o bien se han recargado de manera segura, antes de su retirada.

A.9.2.7 Retirada de materiales propiedad de la empresa

Control: Los equipos, la información o el software no deben sacarse de las instalaciones, sin una autorización previa.

A.10 Gestión de comunicaciones y operaciones

A.10.1 Responsabilidades y procedimientos de operación

Objetivo: Asegurar el funcionamiento correcto y seguro de los recursos de procesamiento de la información.

A.10.1.1 Documentación de los procedimientos de operación

Control: Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.

A.10.1.2 Gestión de cambios

Control: Deben controlarse los cambios en los recursos y los sistemas de tratamiento de la información.

A.10.1.3 Segregación de tareas

Control: Las tareas y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

A.10.1.4 Separación de los recursos de desarrollo, prueba y operación

Control: Deben separarse los recursos de desarrollo, de pruebas y de operación, para reducir los riesgos de acceso no autorizado o los cambios en el sistema operativo.

A.10.2 Gestión de la provisión de servicios por terceros

Objetivo: Implantar y mantener el nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros.

A.10.2.1 Provisión de servicios

Control: Se debe comprobar que los controles de seguridad, las definiciones de los servicios y los niveles de provisión, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero.

A.10.2.2 Supervisión y revisión de los servicios prestados por terceros

Control: Los servicios, informes y registros proporcionados por un tercero deben ser objeto de supervisión y revisión periódicas, y también deben llevarse a cabo auditorias periódicas.

A.10.2.3 Gestión de cambios en los servicios prestados por terceros

Control: Se deben gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos.

A.10.3 Planificación y aceptación del sistema

Objetivo: Minimizar el riesgo de fallos de los sistemas.

A.10.3.1 Gestión de capacidades

Control: La utilización de los recursos se debe supervisar y ajustar así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el comportamiento requerido del sistema.

A.10.3.2 Aceptación del sistema

Control: Se deben establecer los criterios para la aceptación de nuevos sistemas de información, de las actualizaciones y de nuevas versiones de los mismos, y se deben llevar a cabo pruebas adecuadas de los sistemas durante el desarrollo y previamente a la aceptación.

A.10.4 Protección contra código malicioso y descargable

Objetivo: Proteger la integridad del software y de la información.

A.10.4.1 Controles contra el código malicioso

Control: Se deben implantar los controles de detección, prevención y recuperación que sirvan como protección contra código malicioso y se deben implantar procedimientos adecuados de concienciación del usuario.

A.10.4.2 Controles contra el código descargado en el cliente

Control: Cuando se autorice el uso de código descargado en el cliente, (Java Script, VBScript, applets de Java applets, controles ActiveX, etc.), la configuración debe garantizar que dicho código autorizado funciona de acuerdo con una política de seguridad claramente definida, y se debe evitar que se ejecute el código no autorizado.

A.10.5 Copias de seguridad

Objetivo: Mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información.

A.10.5.1 Copias de seguridad de la información

Control Se deben realizar copias de seguridad de la información y del software, y se deben probar periódicamente con conforme a la política de copias de seguridad acordada.

A.10.6 Gestión de la seguridad de las redes

Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

A.10.6.1 Controles de red

Control: Las redes deben estar adecuadamente gestionadas y controladas, para que estén protegidas frente a posibles amenazas y para mantener la seguridad de los sistemas y de las aplicaciones que utilizan estas redes, incluyendo la información en tránsito.

A.10.6.2 Seguridad de los servicios de red

Control: Se deben identificar las características de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en todo acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.

A.10.7 Manipulación de los soportes

Objetivo: Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización.

A.10.7.1 Gestión de soportes extraíbles

Control: Se deben establecer procedimientos para la gestión de los soportes extraíbles.

A.10.7.2 Retirada de soportes

Control: Los soportes deben ser retirados de forma segura cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos.

A.10.7.3 Procedimientos de manipulación de la información

Control: Deben establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido.

A.10.7.4 Seguridad de la documentación del sistema

Control: La documentación del sistema debe estar protegida contra accesos no autorizados.

A.10.8 Intercambio de información

Objetivo: Mantener la seguridad de la información y del software intercambiados dentro de una organización y con un tercero.

A.10.8.1 Políticas y procedimientos de intercambio de información

Control: Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

A.10.8.2 Acuerdos de intercambio

Control: Deben establecerse acuerdos para el intercambio de información y del software entre la organización y los terceros.

A.10.8.3 Soportes físicos en tránsito

Control: Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.

A.10.8.4 Mensajería electrónica

Control: La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.

A.10.8.5 Sistemas de información empresariales

Control: Deben formularse e implantarse políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información empresariales

A.10.9 Servicios de comercio electrónico

Objetivo: Garantizar la seguridad de los servicios de comercio electrónico, y el uso seguro de los mismos.

A.10.9.1 Comercio electrónico

Control: La información incluida en el comercio electrónico que se transmita a través de redes públicas debe protegerse contra las actividades fraudulentas, las disputas contractuales, y la revelación o modificación no autorizada de dicha información.

A.10.9.2 Transacciones en línea

Control: La información contenida en las transacciones en línea debe estar protegida para evitar transmisiones incompletas, errores de direccionamiento, alteraciones no autorizadas de los mensajes, la revelación, la duplicación o la reproducción no autorizadas del mensaje.

A.10.9.3 Información puesta a disposición pública

Control: La integridad de la información puesta a disposición pública se debe proteger para evitar modificaciones no autorizadas.

A.10.10 Supervisión

Objetivo: Detectar las actividades de procesamiento de la información no autorizadas.

A.10.10.1 Registro de auditorias

Control: Se deben realizar registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deben mantener estos registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso.

A.10.10.2 Supervisión del uso del sistema

Control: Se deben establecer procedimientos para supervisar el uso de los recursos de procesamiento de la información y se deben revisar periódicamente los resultados de las actividades de supervisión.

A.10.10.3 Protección de la información de los registros

Control: Los dispositivos de registro y la información de los registros deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.

A.10.10.4 Registros de administración y operación

Control: Se deben registrar las actividades del administrador del sistema y de la operación del sistema.

A.10.10.5 Registro de fallos

Control: Los fallos deben ser registrados y analizados y se deben tomar las correspondientes acciones.

A.10.10.6 Sincronización del reloj

Control: Los relojes de todos los sistemas de procesamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una precisión de tiempo acordada.

A.11 Control de acceso

A.11.1 Requisitos de negocio para el control de acceso

Objetivo: Controlar el acceso a la información.

A.11.1.1 Política de control de acceso

Control: Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos empresariales y de seguridad para el acceso.

A.11.2 Gestión de acceso de usuario

Objetivo: Asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas de información.

A.11.2.1 Registro de usuario

Control: Debe establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.

A.11.2.2 Gestión de privilegios

Control: La asignación y el uso de privilegios deben estar restringidos y controlados.

A.11.2.3 Gestión de contraseñas de usuario

Control: La asignación de contraseñas debe ser controlada a través de un proceso de gestión formal.

A.11.2.4 Revisión de los derechos de acceso de usuario

Control: La Dirección debe revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.

A.11.3 Responsabilidades de usuario

Objetivo: Prevenir el acceso de usuarios no autorizados, así como evitar el que se comprometa o se produzca el robo de la información o de los recursos de procesamiento de la información.

A.11.3.1 Uso de contraseña

Control: Se debe requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y el uso de las contraseñas.

A.11.3.2 Equipo de usuario desatendido

Control: Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.

A.11.3.3 Política de puesto de trabajo despejado y pantalla limpia

Control: Debe adoptarse una política de puesto de trabajo despejado de papeles y de soportes de almacenamiento extraíbles junto con una política de pantalla limpia para los recursos de procesamiento de la información.

A.11.4 Control de acceso a la red

Objetivo: Prevenir el acceso no autorizado a los servicios en red.

A.11.4.1 Política de uso de los servicios en red

Control: Se debe proporcionar a los usuarios únicamente el acceso a los servicios para que los que hayan sido específicamente autorizados.

A.11.4.2 Autenticación de usuario para conexiones externas

Control: Se deben utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos.

A.11.4.3 Identificación de los equipos en las redes

Control: La identificación automática de los equipos se debe considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos.

A.11.4.4 Diagnóstico remoto y protección de los puertos de configuración

Control: Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración.

A.11.4.5 Segregación de las redes

Control: Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en redes.

A.11.4.6 Control de la conexión a la red

Control: En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debe restringirse la capacidad de los usuarios para conectarse a la red, esto debe hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones del negocio (véase 11.1).

A.11.4.7 Control de encaminamiento (*routing)* de red

Control: Se deben implantar controles de encaminamiento (*routing*) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones empresariales.

A.11.5 Control de acceso al sistema operativo

Objetivo: Prevenir el acceso no autorizado a los sistemas operativos.

A.11.5.1 Procedimientos seguros de inicio de sesión

Control: El acceso a los sistemas operativos se debe controlar por medio de un procedimiento seguro de inicio de sesión.

A.11.5.2 Identificación y autenticación de usuario

Control: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal y exclusivo, y se debe elegir una técnica adecuada de autenticación para confirmar la identidad solicitada del usuario.

A.11.5.3 Sistema de gestión de contraseñas

Control: Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.

A.11.5.4 Uso de los recursos del sistema

Control: Se debe restringir y controlar rigurosamente el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

A.11.5.5 Desconexión automática de sesión.

Control: Las sesiones inactivas deben cerrarse después de un periodo de inactividad definido.

A.11.5.6 Limitación del tiempo de conexión

Control Para proporcionar seguridad adicional a las aplicaciones de alto riesgo, se deben utilizar restricciones en los tiempos de conexión.

A.11.6 Control de acceso a las aplicaciones y a la información

Objetivo: Prevenir el acceso no autorizado a la información que contienen las aplicaciones.

A.11.6.1 Restricción del acceso a la información

Control: Se debe restringir el acceso a la información y a las aplicaciones a los usuarios y al personal de soporte, de acuerdo con la política de control de acceso definida.

A.11.6.2 Aislamiento de sistemas sensibles

Control: Los sistemas sensibles deben tener un entorno de ordenadores dedicados (aislados).

A.11.7 Ordenadores portátiles y teletrabajo

Objetivo: Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y servicios de teletrabajo.

A.11.7.1 Ordenadores portátiles y comunicaciones móviles

Control: Se debe implantar una política formal y se deben adoptar las medidas de seguridad adecuadas de protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles.

A.11.7.2 Teletrabajo

Control Se debe redactar e implantar, una política de actividades de teletrabajo, así como los planes y procedimientos de operación correspondientes.

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información

A.12.1 Requisitos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad está integrada en los sistemas de información.

A.12.1.1 Análisis y especificación de los requisitos de seguridad

Control: En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deben especificar los requisitos de los controles de seguridad.

A.12.2 Tratamiento correcto de las aplicaciones

Objetivo: Evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones.

A.12.2.1 Validación de los datos de entrada

Control: La introducción de datos en las aplicaciones debe validarse para garantizar que dichos datos son correctos y adecuados.

A.12.2.2 Control del procesamiento interno

Control: Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deben incorporar comprobaciones de validación en las aplicaciones.

A.12.2.3 Integridad de los mensajes

Control: Se deben identificar los requisitos para garantizar la autenticidad y para proteger la integridad de los mensajes en las aplicaciones y se deben identificar e implantar los controles adecuados.

A.12.2.4 Validación de los datos de salida

Control: Los datos de salida de una aplicación se deben validar para garantizar que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias.

A.12.3 Controles criptográficos

Objetivo: Proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos.

A.12.3.1 Política de uso de los controles criptográficos

Control: Se debe formular e implantar una política para el uso de los controles criptográficos para proteger la información.

A.12.3.2 Gestión de claves

Control: Debe implantarse un sistema de gestión de claves para dar soporte al uso de técnicas criptográficas por parte de la organización.

A.12.4 Seguridad de los archivos de sistema

Objetivo: Garantizar la seguridad de los archivos de sistema.

A.12.4.1 Control del software en explotación

Control: Deben estar implantados procedimientos para controlar la instalación de software en los sistemas operativos.

A.12.4.2 Protección de los datos de prueba del sistema

Control: Los datos de prueba se deben seleccionar con cuidado y deben estar protegidos y controlados.

A.12.4.3 Control de acceso al código fuente de los programas

Control: Se debe restringir el acceso al código fuente de los programas.

A.12.5 Seguridad en los procesos de desarrollo y soporte

Objetivo: Mantener la seguridad del software y de la información de las aplicaciones.

A.12.5.1 Procedimientos de control de cambios

Control: La implantación de cambios debe controlarse mediante el uso de procedimientos formales de control de cambios.

A.12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Control: Cuando se modifiquen los sistemas operativos, las aplicaciones empresariales críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o en la seguridad de la organización.

A.12.5.3 Restricciones a los cambios en los paquetes de software

Control: Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.

A.12.5.4 Fugas de información

Control: Deben evitarse las situaciones que permitan que se produzcan fugas de información.

A.12.5.5 Externalización del desarrollo de software

Control: La externalización del desarrollo de software debe ser supervisada y controlada por la organización.

A.12.6 Gestión de la vulnerabilidad técnica

Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

A.12.6.1 Control de las vulnerabilidades técnicas

Control: Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar lasmedidas adecuadas para afrontar el riesgo asociado.

A.13 Gestión de incidentes de seguridad de la información

A.13.1 Notificación de eventos y puntos débiles de la seguridad de la información

Objetivo: Asegurarse de que los eventos y las vulnerabilidades de la seguridad de la información, asociados con los sistemas de información, se comunican de manera que sea posible emprender las acciones correctivas oportunas.

A.13.1.1 Notificación de los eventos de seguridad de la información

Control: Los eventos de seguridad de la información se deben notificar a través de los canales adecuados de gestión lo antes posible.

A.13.1.2 Notificación de los puntos débiles de la seguridad

Control: Todos los empleados, contratistas, y terceros que sean usuarios de los sistemas y servicios de información deben estar obligados a anotar y notificar cualquier punto débil que observen o que sospechen exista, en dichos sistemas o servicios.

A.13.2 Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Garantizar que se aplica un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información.

A.13.2.1 Responsabilidades y procedimientos

Control: Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

A.13.2.2 Aprendizaje de los incidentes de seguridad de la información

Control: Deben existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información.

A.13.2.3 Recopilación de evidencias

Control: Cuando se emprenda una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique acciones legales (tanto civiles como penales), deben recopilarse las evidencias, conservarse y presentarse conforme a las normas establecidas en la jurisdicción correspondiente.

A.14 Gestión de la continuidad del negocio

A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Objetivo: Contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación.

A.14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Control: Debe desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio.

A.14.1.2 Continuidad del negocio y evaluación de riesgos

Control: Deben identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información.

A.14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

Control: Deben desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requeridos, después de una interrupción o un fallo de los procesos de negocio críticos.

A.14.1.4 Marco de referencia para la planificación de la continuidad del negocio

Control: Debe mantenerse un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes sean coherentes, para cumplir los requisitos de seguridad de la información de manera consistente y para identificar las prioridades de realización de pruebas y de mantenimiento.

A.14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio

Control: Los planes de continuidad del negocio deben probarse y actualizarse periódicamente para asegurar que están al día y que son efectivos.

A.15 Cumplimiento

A.15.1 Cumplimiento de los requisitos legales

Objetivo: Evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad.

A.15.1.1 Identificación de la legislación aplicable

Control: Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplir dichos requisitos, deben estar definidos, documentados y mantenerse actualizados de forma explícito para cada sistema de información de la organización.

A.15.1.2 Derechos de propiedad intelectual (DPI) [*Intellectual Property Rights* (IPR)]

Control: Deben implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software/propietario.

A.15.1.3 Protección de los documentos[3] de la organización

Control: Los documentos importantes deben estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, regulatorios, contractuales y empresariales.

A.15.1.4 Protección de datos y privacidad de la información personal

Control: Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y las regulaciones y, en su caso, en las cláusulas contractuales pertinentes.

A.15.1.5 Prevención del uso indebido de los recursos de tratamiento de la información

Control: Se debe impedir que los usuarios utilicen los recursos de tratamiento de la información para fines no autorizados.

A.15.1.6 Regulación de los controles criptográficos

Control: Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.

A.15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

Objetivo: Asegurar que los sistemas cumplen las políticas y normas de seguridad de la organización.

A.15.2.1 Cumplimiento de las políticas y normas de seguridad

Control: Los directores deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad.

A.15.2.2 Comprobación del cumplimiento técnico

Control: Debe comprobarse periódicamente que los sistemas de información cumplen las normas de aplicación de la seguridad.

A.15.3 Consideraciones sobre la auditoría de los sistemas de información

Objetivo: Lograr que el proceso de auditoría de los sistemas de información alcance la máxima eficacia con las mínimas interferencias.

A.15.3.1 Controles de auditoría de los sistemas de información

Control: Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de empresariales.

A.15.3.2 Protección de las herramientas de auditoría de los sistemas de información

Control: El acceso a las herramientas de auditoría de los sistemas de información debe estar protegido para evitar cualquier posible peligro o uso indebido.

Anexo VII – Conceptos básicos de Seguridad de la Información

- **Confidencialidad:** La información perteneciente a la entidad debe ser conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.

- **Integridad:** La información de la entidad debe de ser completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.

- **Disponibilidad:** La información de la entidad está accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.

- **Autenticidad:** La información de la entidad es generada por un autor identificado que es imposible de suplantar, lo que incluye el no repudio de la información introducida pues se garantiza que el emisor de la información es quien dice ser.

Anexo VIII – Tipología de Incidencias

Incidencias de seguridad lógica

Las incidencias de de seguridad lógica se refirieren a incidencias en el uso del software y los sistemas, la protección de los datos, procesos y programas, así como las de los accesos autorizados de los usuarios a la información.

Incidencias de Sistemas

Suponen incidencias detectadas en los procesos de operación de los sistemas y que no tienen impacto directo sobre la seguridad de la información. Algunos ejemplos de incidencias de estos tipos son:

- Mal funcionamiento de programas.
- Ficheros erróneos.
- Ficheros inexistentes.
- Problemas de tamaño de base de datos, cuotas de disco de servidor de ficheros, etc.
- Problemas de comunicación con empresas externes.
- Problemas de salvaguarda/restauración de base de datos y ficheros.
- Caídas y bloqueos de sistemas.

Incidencias de Seguridad Gestionada

Se refieren principalmente a incidencias de seguridad detectadas en el proceso de Monitorización de los sistemas así como incidencias de seguridad detectadas por los usuarios de los sistemas de la compañía.

También se incluyen en este tipos las incidencias que detecta operación de los sistema y que, al contrario de lo que se comentaba en el anterior apartado sí comportan algún impacto sobre la seguridad de la información. Algunos ejemplos de este tipo de incidencias son:

- Intentos de conexión como usuario administrador genérico de un sistema.
- Problemas en el funcionamiento de hardware o software.
- Acceso no autorizado.
- Incumplimiento de normativas.
- Phishing, virus, spam.
- IDS
- Peticiones especiales.

Incidencias de seguridad física

Suponen incidencias en les barreras físicas y mecanismos de control implementados para proteger los sistemas, ubicaciones y soportes donde se trate información. Algunos ejemplos de estos tipos de incidencias son:

- Deficiencias en el control físico de acceso a les zonas de tratamiento de información o en el perímetro de seguridad.
- Accesos no autorizados a salas restringidas o por personal no identificado.
- Encontrar información confidencial o restringida abandonada en impresoras, sobre las mesas fuera de horario laboral o fuera de las instalaciones
- Encontrar incorrecciones en general en las instalaciones de medidas de seguridad física.

- Observar posibles amenazas de ’exposición de los equipos frente a robo, incendio, inundación, corrupción, etc.

Listado de posibles incidencias en los sistemas de información

Incidencias que afectan a la disponibilidad de los datos

- Imposibilidad o limitación del uso de las instalaciones
  - Fuego
  - Accidente industrial en las instalaciones
  - Fenómenos meteorológicos
  - Huelgas, manifestaciones
  - Otras
- Indisponibilidad de los sistemas
  - Avería del sistema informático
  - Anomalías en la disponibilidad de recursos propios
  - Anomalías en el funcionamiento de los sistemas propios
  - Saturación o caída de red
  - Denegación del servicio
  - Indisponibilidad del proveedor o tercero que presta servicios
- Pérdida de soportes informáticos
  - Por parte del personal de la organización
  - Por parte del servicio subcontratado
- Robo de soportes o equipos
- Desaparición de información de los sistemas de información
  - Por borrado accidental
  - Por pérdida dentro del sistema de información

Incidencias que afectan a la confidencialidad de los datos

- Lectura no autorizada de la información contenida en los ficheros o sistemas de
- información
  - Por parte del personal de la organización
  - Por parte de personas ajenas a la organización
- Copia no autorizada de información
  - Por parte del personal de la organización
  - Por parte de personas ajenas a la organización
- Error en la distribución
  - De informes
  - De soportes
- Error en la manipulación
  - De informes
  - De soportes
- Obtención de información desde soportes desechados
- Obtención de información desde equipos o soportes destinados a su reutilización
- Descifrado de la información
  - Por descubrimiento de claves
  - Por conocimiento directo de las claves

Incidencias que afectan a la integridad de los datos

- Modificación no autorizada de la información

    - Por parte del personal de la organización
    - Por parte de personas ajenas a la organización
- Destrucción parcial o total de la información
    - Por fallos de hardware
    - Por fallos de software
    - Por desastres naturales
    - Por fallos en la manipulación por parte del personal de la empresa
    - Por fallos en la manipulación por parte de personal externo

Incidencias que afectan a la autenticación de usuarios

- Reasignación de clave de usuario
    - Perdida de contraseña por parte de los usuarios
    - Olvido de la contraseña
    - Sospecha de clave comprometida
    - Uso indebido de contraseñas
- Suplantación del usuario autorizado
    - Por cesión de la clave.
    - Por robo de la clave de acceso.
    - Por violación de los controles de acceso
    - Aparición de datos no creados por el usuario
- Bloqueo de cuentas de usuarios
- Por fallos en los programas o dispositivos de control de acceso lógico
- Por fallos en la gestión del control de accesos
    - Modificaciones no autorizadas de permisos de acceso lógico a los ficheros
    - Bajas de personas no comunicadas
    - Autorizaciones de acceso improcedentes
    - Acceso no autorizado a dependencias que contienen sistemas de información
    - Acceso no autorizado a información con datos sensibles

Incidencias relacionadas con la LOPD

- No existencia de fichero inscrito en la AEPD.
- Ejercicio de derechos
    - Acceso
    - Rectificación
    - Cancelación
    - Oposición
- Incumplimiento del principio de calidad de los datos
    - Datos erróneos del afectado
    - Tratamiento para una finalidad no autorizada
    - Recogida fraudulenta de datos
- Incumplimiento del deber de informar
- Incumplimiento de la recogida del consentimiento del afectado
- Incumplimiento del deber de secreto
- Incumplimiento del documento de seguridad
- Cesión ilegítima de datos a terceros
- Transferencia internacional de datos no autorizada por la AEPD.

Otro tipo de incidencias

- Petición de recuperación de datos
- Recuperación de datos
- Fallo en el procedimiento de copias de seguridad

- Error en el desarrollo de la aplicación con pérdida o alteración de información
- Infección en los sistemas de información por software malicioso (virus informáticos)
- Incumplimiento de la política de uso de los sistemas de información
- Incumplimiento de la normativa de seguridad
- Intrusión en los sistemas de información.