UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

Diseño de una herramienta de BI (Business Intelligence) basada en Excel para el análisis de indicadores de competitividad empresarial

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Miret Conejero, José Juan

Tutor: Conesa García, María Pilar

2014

Resumen

El proceso de la toma de decisiones dentro de las organizaciones puede resultar altamente complejo debido a la gran cantidad de información generada. Por este motivo son necesarios los cuadros de mando, herramientas encargadas de ayudar a la conversión de la información en indicadores que generan conocimiento.

Se pretende realizar una herramienta Business Intelligence que facilite la toma de decisiones tanto a nivel gerencial como a nivel técnico a partir de los datos de auditorías de la Norma UNE-ISO 27.001, de auditorías de cumplimiento con la Ley Orgánica de Protección de Datos y de resultados de Tests de Intrusión. Para ello haremos uso de la herramienta Microsoft Excel, disponible en la suite ofimática Microsoft Office.

Palabras clave: Inteligencia Empresarial, Cuadro de mando, Microsoft Excel, Seguridad de la Información.

Abstract

The decision-making process within organizations can be highly complex due to the large amount of information that has beenis generated. Therefore, dashboards, tools for assisting the conversion of information on indicators that generate knowledge, are needed.

The aim is to make a Business Intelligence tool to facilitate decision-making, both, at management level and at technical level of data from audits data of the UNE-ISO 27001, compliance audits with the Ley Orgánica de Protección de Datos and from Penetration Tests results. To do thisFor that purpose, we will use the Microsoft Excel programme, available in the office suite Microsoft Office tool.

Keywords : Business Intelligence, Dashboard, Microsoft Excel, Information Security.

Tabla de contenidos

1. Contexto y objetivos del TFG

Justificación del valor

Las organizaciones cada vez están tomando mayor concienciación sobre la necesidad de tomar medidas en cuanto a privacidad y seguridad informática bien por motivos regulatorios, de imagen, necesidades del mercado e incluso motu-propio. Muestra de ello puede ser la decisión de implantar un Sistema de Gestión de Seguridad de la Información, el cumplir con la Ley Oficial Orgánica de Protección de Datos o emplear aplicar políticas para el bastionado[1] de sus sistemas.

Estas medidas son fruto de toma de decisiones, un proceso complejo de conversión de la información generada dentro de las organizaciones en indicadores que generan conocimiento. Para obtener estos indicadores es necesario cuantificar y establecer criterios para poder realizar una medición.

> *"Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre." - W. Thomson.*

Tanto para la seguridad informática de una organización como para cualquier otro campo de interés, debe buscarse la mejora continua. Para ello, es necesario marcarse una serie de objetivos que deben ser cumplidos y definidos mediante indicadores.

El cuadro de mando se convierte en una herramienta necesaria para este propósito, pues refleja el estado actual y la evolución del elemento medido, además de ser fácilmente entendible para todo aquel que deba interpretarlo, independientemente del nivel de conocimientos técnicos que posea.

Ilustración 1. Cuadro de mando para la monitorización de redes.

Ante las necesidades de una organización cualquiera que se preocupe por la seguridad de su información, buscamos plantear un cuadro de mando que facilite la tarea de calcular el rendimiento de las medidas de mejora que se propongan en esta

[1] se le conoce así, en el ámbito de la seguridad de la información, a las medidas que se deben tomarse para que los sistemas sean más seguros.

materia, y que pueda servir tanto para la detección de posibles resultados negativos como detectar una posible implantación incorrecta de las mismas.

Antecedentes y valoraciones previas

Debido a las prácticas en empresa realizadas en la firma consultora Auren[2], llevo desde abril de 2014 formándome en el Área de la Seguridad de la Información a partir del trabajo realizado en proyectos de:

- Consultoría y auditoría de Sistemas de Gestión de Seguridad de la Información.
- Test de Intrusión Externo.
- Seguridad Gestionada.
- Auditoría de Firma Electrónica para Autoridades de Certificación.
- Auditoría LOPD y RLOPD, LSSI y Cookies.
- Seguridad en transacción de datos para la industria de tarjetas de pago.
- Peritaje informático.

Para la realización de varios informes he utilizado en numerosas ocasiones la herramienta Microsoft Excel para poder tratar la gran cantidad de datos obtenidos, como por ejemplo, el estado de todos los puertos de cada uno de los equipos que forman parte de una red del cliente. Gracias a esto, es posible centrar los esfuerzos en aquellos aspectos que puedan ser considerados de interés para realizar un ataque malicioso. En otras palabras, Business Intelligence a pequeña escala.

Considero que el tema del presente Trabajo Final de Grado despierta interés en mí, pues recoge aspectos que estoy tratando en el día a día desde el punto de vista gerencial, técnico y de implantación, a niveles más amplios de los que he trabajado o que no he podido trabajar en mayor profundidad tanto en la Universidad como en la consultora donde realizo mis prácticas de empresa.

[2] Auren es una firma de prestación de servicios profesionales de auditoría, asesoramiento legal, consultoría y corporate. Actualmente cuenta con casi 700 empleados en España, más de 1.500 en todo el mundo y está presente en más de 60 países.

2. La información en las empresas

Datos, información y sistemas de información

Como punto de partida, debemos tener claros algunos conceptos como qué son los datos, qué se entiende por información y qué es un sistema de información, pues en muchos casos puede llevar a confusión. Para ello, recurriremos a las definiciones propuestas por Kenneth C. Laudon y Jane P. Laudon en su libro "Sistemas de información gerencial, administración de la empresa digital", referencia en el ámbito empresarial y de tecnologías de la información.

La primera definición que nos interesa es la de datos:

> *"Los datos son secuencias de hechos en bruto y representan eventos que ocurren en las organizaciones o en el entorno físico antes de ser organizados y ordenados en una forma que las personas puedan entender y utilizar." - Laudon K. y Laudon J.*

A continuación procedemos con la definición del concepto de información:

> *"Información, son los datos que se han moldeado en una forma significativa y útil para los seres humanos. " - Laudon K. y Laudon J.*

Para poder tratar estos datos y convertirlos en información es necesario un paso intermedio. El encargado de realizar esta transformación es el sistema de información:

> *"Conjunto de componentes interrelacionados que recolectan, procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización, permitiéndole visualizar problemas complejos y crear nuevos productos" - Laudon K. y Laudon J.*

Puede entenderse como un proceso de entrada/salida. El sistema de información es el que se encargaría de tratar los datos, que corresponden a la entrada; para poder obtener un resultado de salida, en este caso la información. Esquemáticamente puede representarse de la siguiente forma.

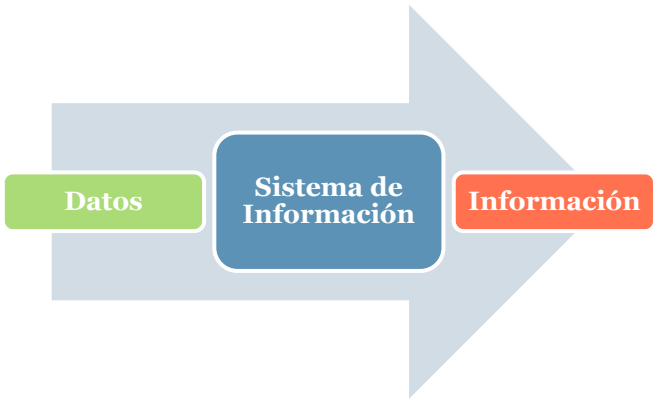


Ilustración 2. Relación entre datos, sistema de información e información.

La importancia de la información

Actualmente, la información es el activo no tangible más importante en las empresas. Ninguna organización puede funcionar sin información o sin gestionarla de forma adecuada, pues representa una desventaja competitiva frente a las demás y juega un papel muy importante en cuanto a la correcta toma de decisiones estratégicas.

Resulta evidente que se tomen medidas para proteger dicha información en aras de impedir que aquellos datos sensibles puedan ser perdidos o que pasen a estar en propiedad de la competencia. Si bien pueden existen existir políticas dentro de las compañías donde se contempla la posibilidad de que un empleado descontento pueda provocar una fuga de información, también se debe tener en cuenta que el robo se realice desde el exterior mediante un ciberataque.

Ilustración 3. Un pentester[3] en su puesto de trabajo.

Actualmente los ciberataques están siendo un auténtico quebradero de cabeza tanto para las empresas como para los gobiernos. En febrero de 2015, el Ministerio de Asuntos Exteriores y de Cooperación del Gobierno de España dio a conocer los datos correspondientes al número de ciberataques recibidos durante el año 2014, donde España ocupa el tercer puesto a nivel mundial, registrando más de 70.000 incidencias. Éstas afectaron tanto a la administración pública como a empresas y particulares.

En el siguiente apartado se introducirán algunas de las normas, estándares y legislaciones más representativas, aplicables en el ámbito de la seguridad de la información.

[3] profesional encargado de realizar las pruebas de test de intrusión.

3. Estándares y legislación relevantes

A continuación se procede a describir algunas de las normas y marcos de trabajo referentes en el ámbito de la Seguridad de la Información, así como la principal legislación aplicable en España. Muchos de los aspectos que se tratan en esta sección son utilizados posteriormente en la elaboración del cuadro de mando aunque no son el objetivo de este trabajo, por lo que en el Anexo I se proporciona bibliografía básica para poder profundizar en aquellos aspectos que se consideren oportunos.

Norma ISO 27.001

Qué es y en qué consiste

La ISO[4] 27001 se centra en los Sistemas de Gestión de Seguridad de la Información, donde se proporciona una serie de requisitos para poder establecer, implementar y realizar un proceso de mejora continua del mismo.

Un Sistema de Gestión de Seguridad de la Información, en adelante SGSI, engloba el diseño, implantación y mantenimiento de un conjunto de procesos para preservar y gestionar de forma eficiente la confidencialidad, integridad y disponibilidad y así reducir los riegos de seguridad y asegurar la continuidad de negocio. Adicionalmente, el SGSI debe actualizarse y adaptarse a todos aquellos cambios que se puedan dar tanto a nivel interno como externo a la organización.

Esta mejora se realiza en base a un procedimiento cíclico, repetitivo en el tiempo, conocido como PDCA: **P**lan-**D**o-**C**heck-**A**ct, en español traducido como planificar, hacer, comprobar y Actuar. Estas cuatro etapas pueden apreciarse en la siguiente ilustración.

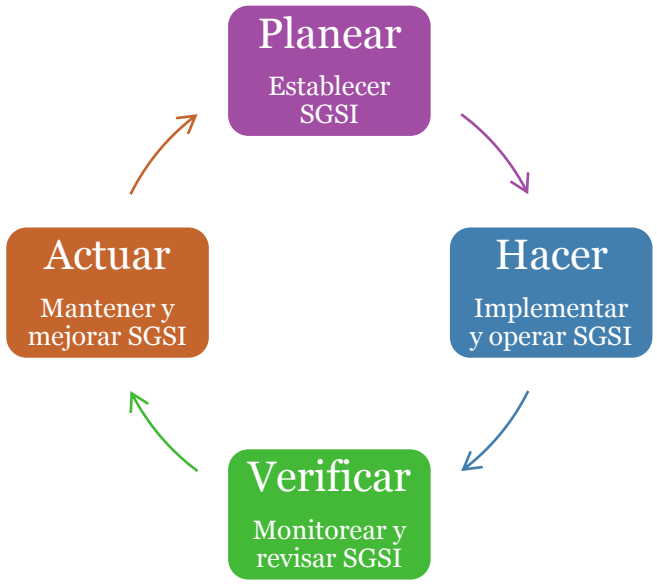


Ilustración 4. Esquema del modelo PDCA para el SGSI.

[4] abreviatura inglesa para referirse a la Organización Internacional de Normalización.

Para establecer un SGSI se tiene en cuenta el papel de cada uno de los miembros de la organización, donde resulta determinante el rol que realiza la Dirección. Ésta es la encargada tanto de revisar que los objetivos del SGSI estén alineados con los de la organización, como revisar los planes de mejora o asignar los recursos necesarios.

Partes en la que se divide la Norma UNE-ISO/IEC 27001:2014

En la primera parte de la norma ISO se definen los fundamentos y principios, el modelo PDCA anteriormente explicado y así como la aplicabilidad y sus límites. Está compuesto por los apartados de introducción, alcance, norma para la consulta y términos y definiciones.

La segunda parte corresponde a los controles de gestión del sistema asociados al modelo PDCA y está compuesto por los apartados de marco general del SGSI, responsabilidad de la dirección, auditoría interna, revisión del SGSI y proceso de mejora.

La tercera parte está compuesta por tres anexos. El primero de ellos, Anexo A, establece un total de 114 controles y objetivos [5]de control clasificados en 14 dominios sobre los cuales se auditaría una entidad que hubiera adaptado este modelo:

1. Políticas de seguridad de la información

2. Organización de la seguridad de la información

3. Seguridad relativa a los recursos humanos

4. Gestión de activos

5. Control de acceso

6. Criptografía

7. Seguridad física y del entorno

8. Seguridad de las operaciones

9. Seguridad de las comunicaciones

10. Adquisición, desarrollo y mantenimiento de los sistemas de información

11. Relación con proveedores

12. Gestión de incidentes de seguridad de la información

13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

14. Cumplimiento

Ilustración 5. Dominios de Seguridad de la ISO 27001.

Los dos anexos restantes, Anexo B y Anexo C, son meramente informativos y hacen referencia a principios de la cultura de la seguridad y correspondencias con otros Sistemas de Gestión.

[5] serán utilizados como indicadores en la herramienta Business Intelligence diseñada.

Ventajas que conlleva la Norma

Que una empresa decida implantar esta norma ISO es una muestra del nivel de compromiso con uno o varios de los pilares básicos de la seguridad de la información (confidencialidad, integridad o disponibilidad), o bien de la privacidad de los mismos, sobretodo enfocado a datos de carácter personal.

Los beneficios más destacables que aporta a la organización la implantación de esta norma ISO son la mayor facilidad para identificar los riesgos y establecer controles para poder gestionarlos o mitigarlos; poder elegir si aplicar los controles a todas las áreas o únicamente aquellas que se deseen y una mayor confianza por parte de los clientes y posibles clientes. Adicionalmente, puede ser un requisito para poder trabajar como proveedor de servicios para otras organizaciones.

Adaptación y certificación en España

La **A**sociación **E**spañola de **Nor**malización y Certificación, conocida por las siglas AENOR, es una entidad privada, independiente y sin ánimo de lucro, encargada de la normalización y certificación en España, aunque existen otras muchas entidades acreditadas para llevar a cabo auditorías de certificación tanto en España como a nivel internacional, existiendo un reconocimiento mutuo entre ellas. AENOR es la responsable legal de la redacción de las normas UNE (Una Norma Española), con valor en territorio español y reconocidas a nivel internacional.

En noviembre de 2014 publicó la Norma UNE-ISO 27.001:2014, norma de la familia de la ISO 27.000, certificable y con correspondencia control a control de la ISO/IEC 27001:2013. Ésta Norma deja obsoleta a la anterior UNE-ISO/IEC 27.001:2007, que mantenía correspondencia con la ISO/IEC 27001:2005[6].

COBIT 5

Qué es y en qué consiste

COBIT**,** abreviatura de **C**ontrol **Ob**jectives for **I**nformation and related **T**echnology[7], es el resultado de los trabajos por parte de ISACA, una asociación independiente sin ánimo de lucro, para crear un único *framework*[8] de negocio para el gobierno y la gestión de las Tecnologías de la Información en las organizaciones. Actualmente se encuentra en la versión 5, que fue publicada en 2012. Esta versión de COBIT se basa en su predecesora, COBIT 4.1, y la amplía integrando marcos como ITIL o normas ISO del ámbito TI.

La misión de COBIT, tal y como se recoge en el documento del framework, se resume en:

[6] este aspecto se verá reflejado como un indicador del cuadro de mando de la herramienta.
[7] traducido al español como Objetivos de Control para Información y Tecnologías Relacionadas.
[8] se traduce al español como marco de trabajo. Esto es un conjunto de conceptos, prácticas y criterios como referencia, para enfrentar y resolver nuevos problemas de índole similar.

Investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores.

Una de las principales características que presenta COBIT 5 es que es genérico, por lo que puede ser aplicado a cualquier organización independientemente de su tamaño, sector o fin. Su alto grado de aceptación es debido a que recoge buenas prácticas, herramientas analíticas y diversos modelos para aportar confianza y valor a los Sistemas de Información, además de buscar maximizar el valor de la propiedad intelectual, la gestión del riesgo y seguridad, y asegurar el cumplimiento a través de la gobernanza y la gestión de TI. En la siguiente gráfica se muestran los cinco principios en los que se basa COBIT 5.

Ilustración 6. Gráfica de los cinco principios en los que se basa COBIT 5.

Ventajas y desventajas

Entre los beneficios que aporta la implantación de COBIT 5, según ISACA, encontramos los que se muestran a continuación:

- Mantener información de alta calidad para apoyar las decisiones de negocio.
- Lograr los objetivos estratégicos a través del uso efectivo e innovador de TI.
- Lograr la excelencia operativa a través de la aplicación confiable, eficiente de la tecnología.
- Mantener TI relacionados con el riesgo a un nivel aceptable.
- Optimizar el coste de los servicios de TI y tecnología.

- Soporte cumplimiento de las leyes, reglamentos, acuerdos contractuales y políticas.

En cambio, COBIT también presenta inconvenientes, que a su vez es una de sus principales ventajas: es demasiado genérico. Esto impide encontrar un estándar que pueda cubrir todos los aspectos necesarios de una organización a nivel de gestión, desarrollo, calidad, etc. Además, existe un punto adicional a tener en cuenta ya que se necesita un esfuerzo considerable por parte de la organización para poder adaptarse completamente a los requisitos que exige COBIT 5.

ITIL v3

Qué es y en qué consiste

ITIL, abreviatura de **I**nformation **T**echnology **I**nfrastructure **L**ibrary[9], es una serie de conceptos y buenas prácticas para la gestión de servicios de tecnologías, así como el desarrollo de Tecnologías de la Información y todas las operaciones relacionadas con ésta. En líneas generales, se asemeja a COBIT en su búsqueda de la calidad y eficiencia, pero se distancia de éste en que ITIL sí que describe detalladamente cada uno de los procedimientos para la gestión. Se encuentra vigente la versión 3 que fue publicada en 2011 y es propiedad de Axelos Ltd desde 2013.

ITIL se sustenta en la ISO 20.000 y consta de cinco volúmenes basados en el ciclo de vida del servicio: estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio.

Ilustración 7. Los cinco volúmenes en los que se basa ITIL.

[9] traducido al español significa "Biblioteca de Infraestructura de Tecnologías de Información".

Ventajas y desventajas

Estos procedimientos que se describen, al igual que los distintos procesos, tareas y listas de control no son específicos para cada organización, por lo que deben ser integrados. Para ello, ITIL contempla mecanismos para hacer un seguimiento del cumplimiento y poder medir las mejoras realizadas.

Aunque ITIL v3 aporte beneficios en cuestión de mejora de la calidad y optimización de costes del servicio, cuenta con una serie de desventajas que en muchas ocasiones resultan decisivas. Algunas de éstas son el cambio de cultura de la organización, pues es necesaria una implicación desde la directiva a los empleados; el tiempo y dinero que es necesario invertir y por último que los resultados no se aprecien de manera inmediata.

Ley Orgánica de Protección de Datos

La Ley Orgánica de Protección de Datos de Carácter Personal, también conocida por LOPD, fue aprobada el 13 de diciembre de 1999. Ésta se basa en el artículo 18 de la Constitución Española de 1978, correspondiente al derecho de la intimidad, para poder garantizar y proteger los datos personales, libertades públicas y los derechos fundamentales de honor, intimidad y privacidad.

Su actividad regulatoria está fundamentada en el tratamiento de los datos y ficheros de carácter personal, independientemente del soporte, quedando fuera del marco normativo aquellos datos que estén destinados para uso doméstico y aquellos que contengan datos de terrorismo y delincuencia organizada.

El encargado de velar por el cumplimiento de esta Ley es la **A**gencia **E**spañola de **P**rotección de **D**atos (AEPD), ente público nacido en 1993 y con sede en Madrid. Es independiente de la Administración y lleva a cabo su actividad en el conjunto del territorio nacional, actuando con personalidad jurídica propia y plena. La AEPD, aunque pueda actuar de oficio, está sujeta a las solicitudes por parte de los ciudadanos.

Todo ciudadano tiene derechos fundamentales en cuanto a la Protección de Datos de carácter personal. Estos se conocen por derechos ARCO, sigla que corresponde a las iniciales de cada uno de los siguientes:

- Derecho de **A**cceso: debe poder acceder libre y gratuitamente a sus datos de carácter personal.
- Derecho de **R**ectificación: debe poder corregir y modificar datos inexactos y garantizar la certeza de los mismos.
- Derecho de **C**ancelación: deben poder suprimirse los datos que resulten inadecuados o excesivos.
- Derecho de **O**posición: debe poder cesarse el tratamiento de los datos de carácter personal una vez sea solicitado.

Los ficheros con datos de carácter personal deben ser inscritos en el Registro General de Protección de Datos[10], órgano de la Agencia Española de Protección de

[10] órgano de la AEPD al que corresponde velar por la publicidad de la existencia de los ficheros y tratamientos de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos ARCO.

Datos. Para realizar dicha inscripción, se debe cumplimentar y remitir a la agencia un formulario electrónico NOTA (**No**tificaciones **T**elemáticas a la **A**EPD), disponible de forma gratuita en la web de la Agencia.

No solo por motivos éticos o legales las personas, instituciones o cualquier otra organización deben cumplir con la LOPD, pues las infracciones van acompañadas de una sanción económica para los titulares de los ficheros acorde a la gravedad de la misma:

- Infracciones leves: puede ir desde un apercibimiento hasta multas entre 900 y 40.000 euros. Ejemplos de actuaciones que pueden considerarse como leves son el no remitir a la AEPD las notificaciones, no solicitar la inscripción de los ficheros de datos de carácter personal en el Registro General de Protección de Datos o el no informar debidamente de la recogida de datos personales.
- Infracciones graves: estas sanciones barajan cifras entre los 40.001 y 300.000 euros y castigan, entre otros, el tratar o recabar datos de carácter personal sin el consentimiento del afectado o impedir el ejercicio de los derechos ARCO.
- Infracciones muy graves: las sanciones oscilan entre los 300.001 y 600.000 euros y se centran en castigar la recogida de datos de forma engañosa o fraudulenta, la cesión de datos personales a terceros fuera de los casos permitidos legalmente o no cesar en el tratamiento ilícito de los datos cuando así lo exija la AEPD.

4. Seguridad Informática

Elementos esenciales en la Seguridad Informática

Casi todo el mundo tiene una idea intuitiva de lo que significa seguridad informática a pesar de la dificultad que implica aportar una definición exacta. Una de las más aceptadas es la referente al hecho de que un sistema informático se encuentre libre de peligro o riesgo, aunque otras apuntan a grados de seguridad e incluso la no existencia de sistemas informáticos seguros.

> *"El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él" - Eugene Spafford.*

Para que un sistema informático se considere seguro debe contar con las siguientes características recogidas bajo las siglas, en inglés, de CIA:

- **C**onfidentiality (confidencialidad): únicamente está permitido el acceso a la información mediante una autorización, y además, se debe realizar de forma controlada.
- **I**ntegrity (integridad): solo está permitida la modificación de la información por las personas autorizadas.
- **A**vailability (disponibilidad): la información del sistema debe permanecer siempre accesible y mediante autorización.

Test de intrusión

Cuál es su objetivo

El objetivo principal de la realización de un test de intrusión es la mejora de la confidencialidad, integridad y disponibilidad de los sistemas informáticos. Adicionalmente, su realización aporta una serie de ventajas entre las que destacan las siguientes:

- Proporciona un conocimiento del grado de vulnerabilidad del sistema de información, imprescindible para poder aplica medidas correctivas.
- Permite detectar sistemas vulnerables en peligro debido a su desactualización.
- Identifica configuraciones erróneas que pudieran desembocar en fallos de seguridad (servicios, servidores, switches, routers, firewalls, etc.).
- Descubre fallos de seguridad que hayan podido surgir a raíz de algún cambio de configuración.
- Aproximación realista a la exposición global del sistema, pues se utilizan herramientas y metodologías de las que suelen valerse los hackers en sus ataques.

Tipos de pruebas

En cuanto a las clases de pruebas existentes, éstas las podemos separar en dos tipos dependiendo desde dónde se realizan las pruebas y de cuánta información se disponga.

Si hablamos desde dónde se están realizando las pruebas, tenemos dos tipos de test de intrusión:

- Externo: intenta simular las condiciones con las que se encontraría un atacante cualquiera desde fuera de la red de la organización.
- Interno: intenta comprobar el nivel de dificultad que tendría un atacante para obtener una elevación de privilegios[11] algún otro tipo de ataque una vez conectado a una sede de la entidad.

Si hablamos de la información disponible, tenemos tres tipos:

- Caja negra: el cliente que ha contratado los servicios no proporciona ningún tipo de información. Esto simularía las condiciones de un ataque real.
- Caja blanca: se proporciona toda la información y características referentes a los servicios publicados. Permite centrarse en aspectos concretos en los que pueda haber una vulnerabilidad.
- Caja gris: sería el caso donde no se aporta toda la información y poder abarcar, más o menos, los objetivos de los dos anteriores.

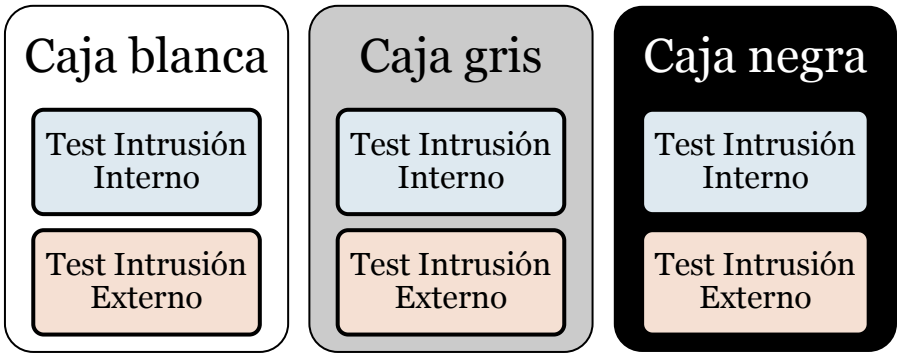


Ilustración 8. Esquema de los distintos tipos de test de intrusión.

Metodologías y frameworks

Existe una gran cantidad de marcos de trabajo que proponen metodologías para realizar de forma adecuada las auditorías técnicas de seguridad. Los más conocidos y aceptados por los pentesters son OSSTMM, ISSAF y OWASP.

OWASP (Open Web Application Security Project[12]) a diferencia de los otros dos, OSSTMM (Open Source Security Testing Methodology Manual[13]) y ISSAF (Information

[11] proceso llevado a cabo para pasar de ser usuario sin privilegios a administrador del sistema.
[12] traducido al español como Proyecto Abierto de Seguridad de Aplicaciones Web.
[13] traducido como Manual de la Metodología Abierta de Testeo de Seguridad.

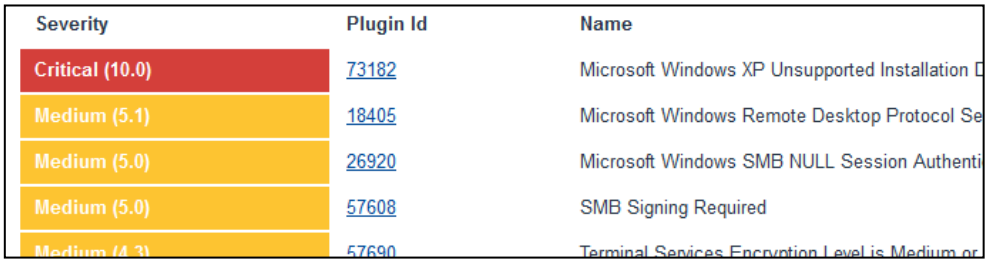
Systems Security Assessment Framework[14]), está más enfocado a la parte de pruebas de seguridad de aplicaciones web.

Aunque lo aconsejable es utilizar un framework, lo normal es combinar varios, elegir aquellos aspectos que puedan ser útiles para el proyecto de auditoría técnica de seguridad y descartar aquellos otros que puedan dañar los entornos de producción en la fase explotación de vulnerabilidades.

En el anexo I hay disponible bibliografía al respecto de estos marcos de trabajo para poder consultarse en mayor profundidad.

Cómo cuantificar el nivel de vulnerabilidad

Ante la complejidad que presenta el cuantificar cuan vulnerable es una red, una web o una aplicación, existen varias métricas que intentan ayudar a ello. Una de las más aceptadas por la cantidad de información que utiliza y porque las principales herramientas de análisis de vulnerabilidades (p.e. Nessus) la utilizan, es CVSS.



Severity	Plugin Id	Name
Critical (10.0)	73182	Microsoft Windows XP Unsupported Installation D
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Se
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authenti
Medium (5.0)	57608	SMB Signing Required
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or

Ilustración 9. Captura de un reporte de la herramienta Nessus donde se indica el CVSS, entre paréntesis, al lado del nivel de severidad.

CVSS (Common Vulnerability Scoring System[15]) es un estándar propiedad de FIRST (Forum of Incident Response and Security Teams) que se encuentra actualmente en la versión 2.0 desde 2007. Éste tiene en cuenta para cuantificar la gravedad de la vulnerabilidad tres componentes:

- Métricas base: es común para todas las vulnerabilidades y se centra en el daño que puede ocasionar a la confidencialidad, integridad y disponibilidad. Para conseguir este objetivo, se basan aspectos como si el ataque se produce de forma remota o local, la dificultad que conlleva la explotación de ésta por parte de un atacante y el tipo de acceso que debe realizar (p.e. debe ser administrador).
- Métricas temporales: se tiene en cuenta la existencia o no de algún parche o cambio de configuración para poder remediar el problema de seguridad en cuestión. Se tienen en cuenta factores como la facilidad de explotación mediante la existencia de exploits[16], en qué grado puede solucionar la liberación de un parche y cuanta gente puede conocer su existencia.

[14] traducido del inglés como Marco de Evaluación de Seguridad de Sistemas de Información.
[15] traducido al español como Sistema de Puntuación de Vulnerabilidad Común.
[16] fragmento de código diseñado con la intención de explotar alguna vulnerabilidad.

- Métricas de entorno: para esta parte se considera el entorno y sus usuarios afectados, enfocado a factores como los costes que pueden ocasionar, qué porcentaje del sistema se vería afectado y cuán importante sería el activo afectado.

De esta forma, podemos diferenciar el nivel de severidad o criticidad de las vulnerabilidades como:

- Débil: de 0 a 2,99.
- Media: de 3 a 6,99.
- Alta: de 7 a 8,99.
- Crítica: de 9 a 10.

Ejemplos de problemas de seguridad en las empresas

Existen multitud de casos famosos en que un ataque informático pone en juego la confidencialidad de los datos que se encuentran en los servidores de una compañía. Uno de los ejemplos más recientes y relevantes fue el ataque durante noviembre de 2014 a la compañía nipona SONY. Las consecuencias del ciberataque fueron considerables: servidores detenidos hasta conocer el alcance y fiabilidad de la red, filtración de películas que estaban preparadas para su estreno, filtración de correos electrónicos comprometedores de altos cargos, así como centenares de documentos como pasaportes digitalizados, sueldos o presupuestos de futuras películas.

Otro ejemplo reciente con el que se puede llegar a entender la importancia de la protección, no solo de la información, sino también el de las redes y cualquier tipo de dispositivo que forme parte de la propia red de la empresa, es el ataque que afectó durante julio de 2014 a empresas energéticas de Estados Unidos y de varios países de la Unión Europea. Según informó Symantec, empresa referente en el sector de la seguridad informática, el ataque se realizó mediante el uso de un sofisticado troyano y se consiguió acceder tanto al sistema informático como al sistema encargado del suministro eléctrico. Este ataque, que fue atribuido al grupo hacker conocido como Energetic Bear (también conocido como Dragonfly), tuvo como objetivo el espionaje industrial, aunque tenía capacidad de sabotaje y podría haber dejado sin suministro de energía a aquellos países afectados. En la siguiente ilustración se muestran los principales países afectados, donde destaca España, el principal receptor de estos ataques.

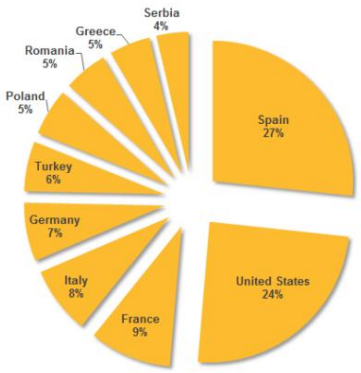


Ilustración 10. Los principales países afectados por el robo de información.

Los ataque informáticos pueden afectar desde gobiernos hasta pequeñas empresas o usuarios privados. Los motivos que empujan a la realización de estos ataques pueden ir desde el hacktivismo[17], obtener información por parte de la competencia e incluso demostrar la propia valía como hacker.

Queda patente la necesidad de realizar labores de bastionado[18] y mantenimiento en los sistemas de información para evitar intrusiones en las redes de las organizaciones. Para ello deben realizarse cada cierto tiempo auditorías de seguridad, tanto internas como externas. Hay que tener en cuenta que lo que hoy es seguro, mañana puede dejar de serlo.

[17] acrónimo de hacker y activista, se basan en la utilización no violenta de herramientas informáticas con fines políticos.
[18] vocablo utilizado para referirse a la protección de los sistemas.

5. Business Intelligence: estado del arte

Introducción a Business Intelligence

Business Intelligence (Inteligencia de Negocio), también conocida por sus siglas BI, se puede definir como:

> *"La habilidad corporativa para tomar decisiones. Esto se logra mediante el uso de metodologías, aplicaciones y tecnologías que permiten reunir, depurar, transformar datos, y aplicar en ellos técnicas analíticas de extracción de conocimiento" - O. Parr.*

Estas herramientas y metodologías tienen en común características como el fácil acceso a la información, poder manejar los datos de la manera que se desee para que puedan servir al apoyo de toma de decisiones y que el usuario que tiene que interpretar los datos pueda entenderlos independientemente de sus capacidades o habilidades con la herramienta en cuestión. Respecto a este último punto, debe tenerse en cuenta que el responsable de escoger la opción que sea más conveniente o beneficiosa para la organización no tiene por qué tener conocimientos técnicos. De aquí la importancia de que sean fáciles de manejar.

Business Intelligence sería la primera de las etapas en la toma de decisiones según Kenneth C. Laudon y Jane P. Laudon, ya citados anteriormente en el presente trabajo, en su obra "Sistemas de información gerencial, administración de la empresa digital". Esta etapa de "inteligencia" permite descubrir, identificar y comprender, paso previo y fundamental para realizar el diseño de una solución, poder elegir la mejor solución y finalmente implantarla.

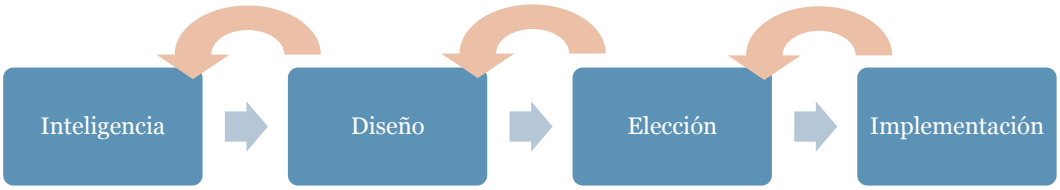


Ilustración 11. Etapas del proceso de toma de decisiones.

Cuadro de mando e indicadores

El cuadro de mando integral es una herramienta creada por dos profesores de la Universidad de Harvard en 1990, Robert S. Kaplan y David P. Norton y fue presentada posteriormente en 1992.

Kaplan y Norton propusieron una forma de gestionar una organización que no tenía en cuenta únicamente los indicadores financieros y que pudiera recoger todo tipo de aspectos que supusieran una ventaja competitiva. Durante la década de 1990 se consolidó y fue ampliamente utilizado por las compañías con indicadores a partir de

datos de distinta naturaleza: finanzas, comerciales, producción, logística, calidad, etc. Actualmente, es una herramienta fundamental.

Además de ayudar a la toma de decisiones tal y como se ha comentado en anteriores apartados, también ayuda a medir el nivel de cumplimiento y desempeño en cuanto a las estrategias y objetivos marcados por parte de las organizaciones. Visualmente se pueden detectar de forma inmediata las desviaciones que se produzcan.

Para que todo cuadro de mando sea efectivo para la organización que lo utilice, debe cumplir los siguientes requisitos:

- La información que se muestra debe ser relevante.
- Debe actuar como una herramienta de diagnóstico. Aquí se encuentran reflejados todos aquellos parámetros que muestren que ayuden a realizar un seguimiento del cumplimiento de objetivos, independientemente de si estos son positivos o negativos para la organización, pues pueden ser claves para su futuro a corto y largo plazo.
- Ser un apoyo para asignar responsabilidades para conseguir alcanzar objetivos. Clave para la mejora continua de la empresa.
- Ante todo debe facilitar la toma de decisiones

Ilustración 12. Ejemplo de un cuadro de mando.

Herramientas disponibles en el mercado

Qué es el Cuadrado Mágico de Gartner

Hoy en día resulta difícil realizar un análisis sobre la situación de alguna herramienta o servicio relacionado con las Tecnologías de la Información sin citar el Cuadrado Mágico de Gartner.

Gartner Inc. es una consultora que se dedica a investigar y aconsejar a los profesionales de las TIC[19] mediante informes que ayudan a la toma de decisiones en cuanto apostar por el uso de alguna tecnología, invertir en algo que pueda estar de moda en años venideros, etc.

El Cuadrado Mágico de Gartner es una gráfica donde se representa, atendiendo a la visión global que puede tener la compañía y la habilidad de ejecución, en cuatro cuadrantes la situación de los productos o tecnologías objeto del análisis. De esta forma los podemos ver en uno de estos:

- Niche players[20]: los fabricantes están abordando bien aspectos específicos, pero no tienen la funcionalidad deseada.
- Visionaires[21]: aunque su nivel de madurez no es el que se espera para poder ser una solución fiable para una empresa, son los más innovadores.
- Challengers[22]: si bien son productos muy completos, estos no llegan por ahora a ser una solución fiable por el momento.
- Leaders[23]: dan respuesta a todas o casi todas las necesidades que se puedan plantear en una empresa.

Las herramientas líder según Gartner

A continuación se muestra el último Cuadrado Mágico correspondiente a las herramientas de Business Intelligence:

Ilustración 13. Cuadrado Mágico de febrero de 2015 para herramientas de BI.

[19] abreviatura de las Tecnologías de la Información y la Comunicación.
[20] puede traducirse al español como jugadores o participantes de nicho.
[21] traducido al español como visionarios.
[22] traducido al español como aspirantes.
[23] traducido al español como líderes.

Si bien existe una gran cantidad de herramientas que cubren las necesidades básicas, resulta crucial elegir la mejor. A la hora de elegir la mejor alternativa nos centraríamos en las del cuadrante de líderes: Tableau, Qlik, Microsoft, MicroStrategy, IBM, Oracle, SAS y SAP.

Dentro de este grupo de elegidas, deberían ponderarse distintos criterios que puedan aportar un valor añadido, la gratuidad o no de la licencia, número de usuarios permitidos, si cuenta con el soporte de una compañía de prestigio, si recibe actualizaciones, etc.

A continuación, podemos observar la evolución que ha habido en el liderazgo del sector en los últimos años. A la izquierda se muestra el cuadrado correspondiente a 2014 y a la derecha el de 2015:

Ilustración 14. Comparativa de los Cuadrados Mágicos entre los años 2014 (izq.) y 2015 (der.).

En general, el grueso del mercado ha tendido hacia el centro de la tabla. Podemos observar cómo se mantiene el producto de Tableau y le siguen, a mayor distancia, Qlick y Microsoft.

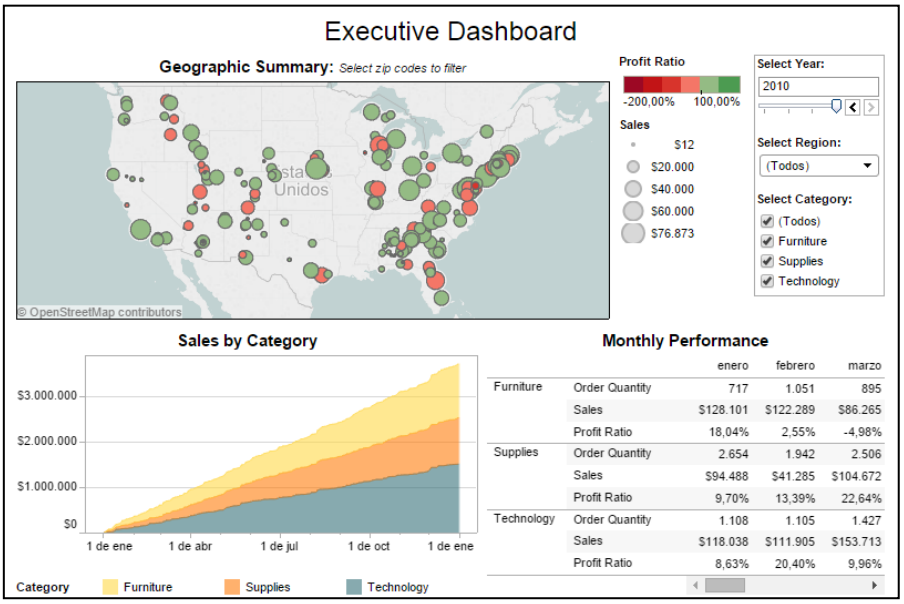


Ilustración 15. Captura de pantalla de la demo online de Tableau Business Intelligence.

6. La herramienta diseñada y su uso

En este apartado se centrará en tratar la utilidad de la herramienta diseñada y se explicará el contenido e información que aportan cada uno de sus componentes e indicadores a una organización.

Utilidad de la herramienta

El objetivo de esta herramienta es fusionar todo el potencial que puede aportar Business Intelligence y la universalidad de la suite ofimáticas Microsoft Office para ayudar a la toma de decisiones en el área de la seguridad de la información de cualquier empresa.

En principio, esta herramienta tiene una doble intencionalidad. Por un lado tiene como objetivo servir de apoyo en la toma de decisiones dentro del Área de TI[24] de las empresas (Business Intelligence), y por otro, la presentación de los resultados por parte de una posible empresa consultora de seguridad de la información.

Este documento Excel, incluyendo únicamente los resultados finales de las auditorías realizadas por ésta o por una entidad de certificación, debe ser capaz de indicar cuáles son los puntos fuertes y débiles, en qué aspecto se debe invertir más en el área TI, qué se quiere potenciar o si la organización cumple con las leyes vigentes contempladas.

A nivel interno, el documento Excel cubre varios apartados:

1. Se muestra el estado del cumplimiento de cada uno de los servicios profesionales contratados.
2. Para cada servicio se muestran las gráficas que ayudarán a la toma de decisiones. Se muestra el estado actual, los datos históricos, adaptaciones a nuevas normas, el estado de actuaciones acometidas para poder subsanar las no conformidades detectadas.
3. Un informe de resultados, en formato imprimible para papel en formato DIN-A4, donde aparezcan los resultados. De esta forma, se pueden mostrar los datos actuales y/o históricos, ordenarlos según el criterio deseado ser estudiados.
4. Un informe de resultados, también imprimible en DIN-A4, con las gráficas del cuadro de mando para poder entregadas durante una reunión o presentar los datos delante los socios de la organización.

Plataforma y diseño

Microsoft Excel, además de ser ampliamente utilizado en las empresas como sistema de apoyo a la toma de decisiones, ha sido el software elegido para el diseño de la

[24] nombre por el que se le conoce al departamento de la empresa encargado a las distintas labores relacionadas con las Tecnologías de la Información.

herramienta fundamentalmente por dos razones. La primera de ellas es relativa a la facilidad de uso y potencia que tiene el software de hojas de cálculo de Microsoft. La segunda, y la más importante, es la gran cantidad de usuarios que tienen una licencia de esta suite ofimática.

Teniendo en cuenta únicamente los usuarios con licencia verificada, estamos hablando de 9,2 millones de activaciones únicamente de la versión Home (más económica y con menos características disponibles) y, si contamos todas las activaciones de todas las versiones de Microsoft Office 2013, de acuerdo con las fuentes de Microsoft, son más de 1.200 millones de personas. Esto significa que a nivel mundial 1 de cada 7 personas dispone de una licencia válida de Office. Adicionalmente este formato sería también compatible con otras herramientas ofimáticas de software libre, como Openoffice lo que incrementa más aún si cabe su difusión.

Este uso masivo, añadido a que los ficheros pueden ser abierto con mayor o peor acierto con software tanto gratuito como no privativo, hace que el fichero de la herramienta de nuestro cuadro de mando sea accesible para cualquier usuario independientemente de sistema operativo o dispositivo desde el cual se decida abrir.

No sólo es de los más utilizados, sino que es una de las aplicaciones más potentes para poder trabajar los datos enfocados a Business Intelligence. Tal y como se comentó en la sección anterior del presente trabajo, Microsoft Excel se encuentra entre los líderes en el Cuadrado Mágico de Gartner.

Visión global de la herramienta

Una vez se accede al fichero de la herramienta diseñada se observa a primera vista la pantalla que se muestra a continuación, correspondiente a la pestaña de "CUADRO MANDO GENERAL", y cuyo contenido se detallará en el siguiente apartado.

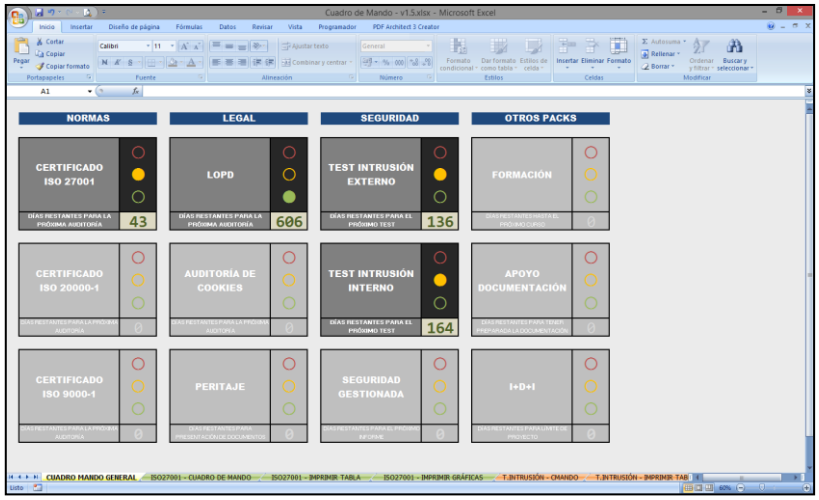


Ilustración 16. Visión global al acceder a la herramienta.

Podemos observar un conjunto de pestañas; existe una pestaña principal "CUADRO MANDO GENERAL" y tres pestañas por cada uno de los servicios contratados: una para cuadro de mando y dos para impresión de informes. Los colores han sido asignados aleatoriamente sin seguir ningún criterio más allá que se permita distinguir el texto y cada uno de los distintos servicios.

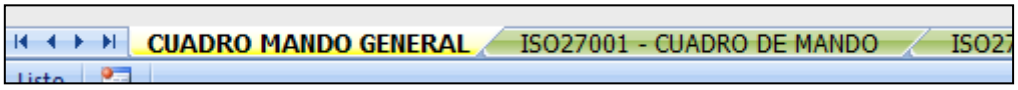


Ilustración 17. Detalle de las pestañas de las hojas de cálculo.

En cuanto a comportamiento de la herramienta, todos los elementos, a excepción de los filtros para que puedan ser seleccionados y ordenados aquellos datos que se deseen, están bloqueados con contraseña para evitar que alguna fórmula se edite por error o de forma malintencionada.

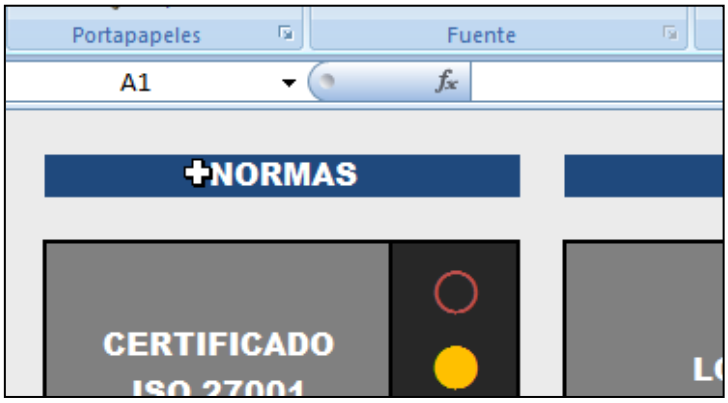


Ilustración 18. Detalle de celdas bloqueadas.

Explicación del cuadro de mando general

Como se ha comentado en el apartado anterior, cuando se accede al fichero Excel, lo primero que se observa es la pestaña de "CUADRO MANDO GENERAL". En ella pueden verse todos los servicios que ofrece la empresa consultora.

Ilustración 19. Contenido de la pestaña "CUADRO MANDO GENERAL".

Podemos observar cuatro columnas con una serie de ítems relacionados:

- Normas: aquellas Normas con las que la Consultora dispone de profesionales para su implantación y/o auditoría.
- Legal: todo aquello que tenga que ver con legislación en el territorio español y esté relacionado con los sistemas de información de las organizaciones.
- Seguridad: aquellos servicios de hacking ético para comprobar las debilidades y fortalezas ante un ataque y los mecanismos de control de fuga de información. También está incluida la seguridad gestionada[25].
- Otros packs: incluye aquellos proyectos que pueden ser contratados ad-hoc a solicitud del cliente y que se ofrecen de forma personalizada atendiendo a las características de éste.

Fijándonos en los paquetes de servicio, podemos observar dos tipos:

- Servicios contratados: se ven más nítidos y cuentan con un semáforo de cumplimiento y un contador donde se informan de los días restantes para subsanar un problema o hasta la próxima auditoría o revisión. El semáforo de cumplimiento es un indicador que igual que los semáforos para la circulación vial, reflejan tres estados que se deducen de forma involuntaria: el rojo indica incumplimiento, el ámbar riesgo y el verde cumplimiento.
- Servicios ofrecidos: se ven menos nítidos y son los que no han sido contratados pero que forman parte de los servicios ofertados por la empresa consultora.

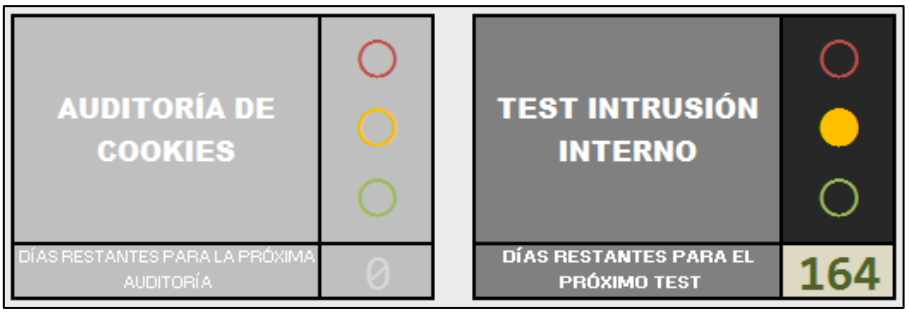


Ilustración 20. Detalle de los servicios ofrecidos (izq.) y servicios contratados (der.).

A partir de lo que se muestra en esta pestaña, incluso sin saber de qué trata cada uno de los paquetes contratados, se puede obtener la siguiente información:

- Si se cumple o no con los requisitos de la Norma ISO 27.001.
- Los días que quedan para subsanar las no conformidades detectadas respecto a la próxima auditoría ISO 27.001.
- Si se cumple con la Ley Orgánica de Protección de Datos.
- El tiempo restante hasta la próxima auditoría.
- Una estimación del nivel de seguridad informática, desde dentro y desde fuera.
- Los días que quedan hasta el próximo test de intrusión interno y externo.

[25] servicio consistente en la revisión de eventos registrados en los sistemas de forma remota para controlar la seguridad y otros aspectos que puedan afectar a la confidencialidad, integridad y disponibilidad.

Explicación del cuadro de mando de la ISO 27.001

A continuación se mostrarán las cuatro pestañas que conforman el bloque de la ISO 27001. Una corresponde con el Cuadro de Mando, otras dos facilitan la impresión de informes y gráficas, y por último, una hoja oculta con todos los cálculos para poder utilizar tablas dinámicas.

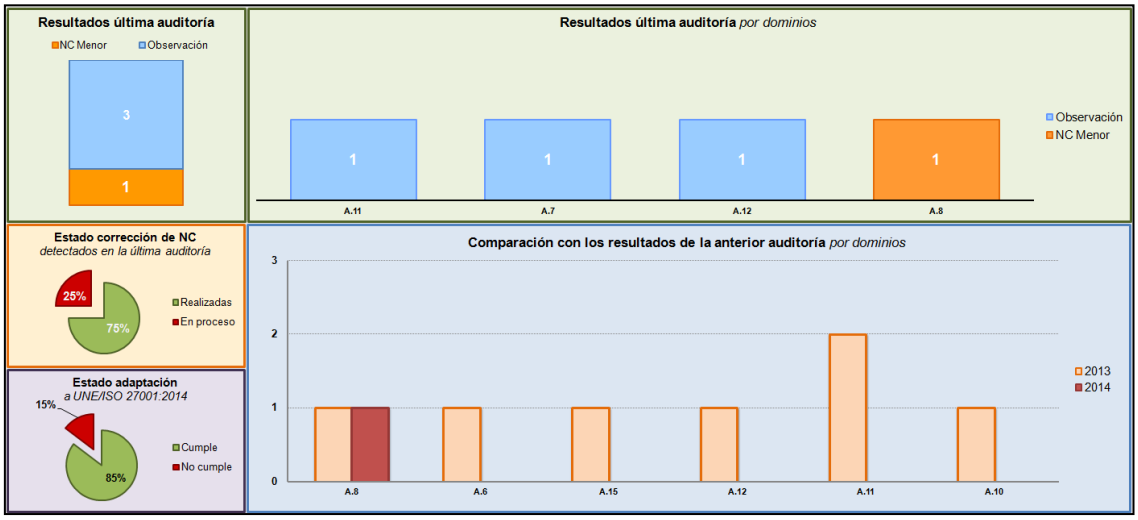


Ilustración 21. Contenido de la pestaña " ISO27001 - CUADRO DE MANDO".

Las gráficas con fondo de color verde (fila superior) reflejan los datos del último informe de cumplimiento emitido por Aenor o la entidad de certificación que haya considerado el cliente. En naranja (parte central de la columna de la izquierda) se muestra el proceso de corrección de las no conformidades detectadas, en morado (parte inferior izquierda) el estado de adaptación a la nueva versión de la Norma y en azul (parte inferior derecha) el histórico de los resultados para cada uno de los dominios.

Resultados de la última auditoría (pestaña 1)

En la Ilustración 22 (siguiente página) puede apreciarse la cantidad de no conformidades mayores, el número de no conformidades menores y el total de observaciones indicadas en el informe a nivel global. En caso de no existir alguna de estas no conformidades, no se verían reflejadas en el gráfico (p.e. en la siguiente ilustración no aparecen no conformidades mayores).

Ilustración 22. Indicador de resultados de la última auditoría.

La misma información, la encontramos a la derecha pero desglosada por dominios (grupos de controles). No sólo sabemos la cantidad de los que están incorrectos, sino que además sabemos dónde se localizan y podemos centrarnos en los aspectos que precisen una actuación más inmediata, dónde mejorar, etc.

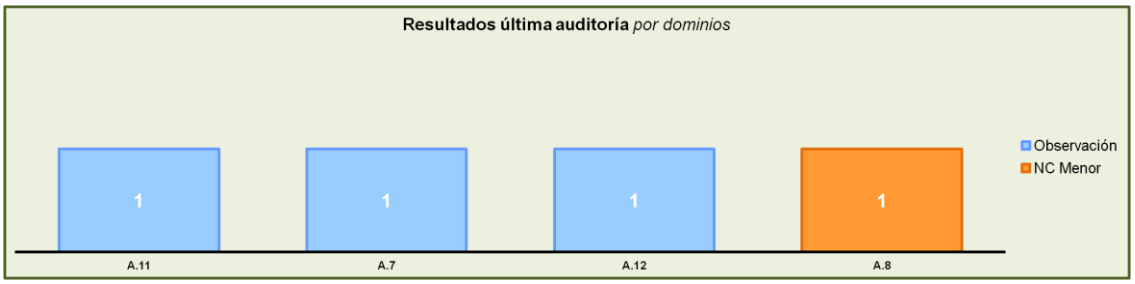


Ilustración 23. Indicador de resultados de la última auditoría por dominios.

Datos históricos (pestaña 1)

Como podemos ver en la gráfica de la Ilustración 23, donde se comparan los resultados de la auditoría actual con la anterior, puede apreciarse si existe una mejora, si ha aumentado el número de no conformidades, si se han visto afectados nuevos dominios o si se mantienen las no conformidades por el motivo que fuere, que posteriormente debería ser analizado.

Con estos tres componentes del cuadro de mando ya se podría disponer de un entendimiento global del estado actual del SGSI y cuáles son sus puntos débiles.

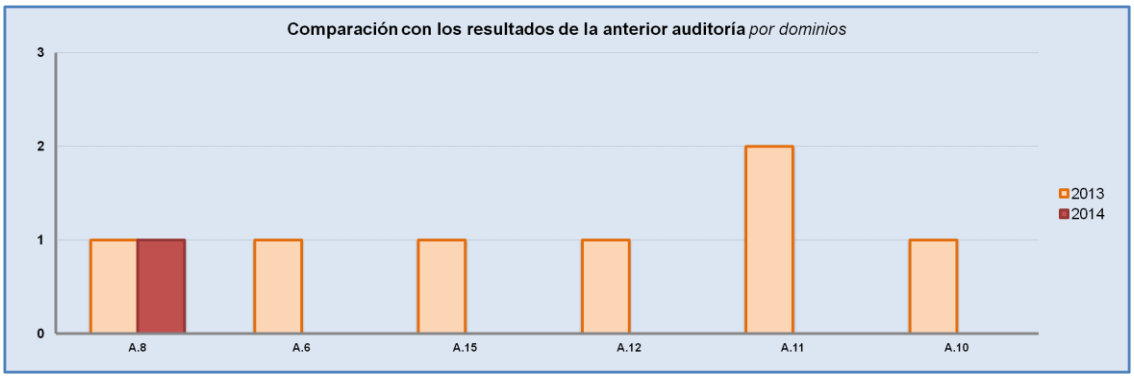


Ilustración 24. Comparación con los resultados con el año anterior.

Corrección de no conformidades (pestaña 1)

Si bien se establece un período de tiempo para poder corregir las no conformidades detectadas por la autoridad de certificación, éstas no se suelen corregir de forma inmediata por lo que se realiza lo que se conoce como un Plan de Acciones Correctivas. Esta gráfica nos permitiría saber en qué punto nos encontramos respecto a la aplicación efectiva de estas medidas.

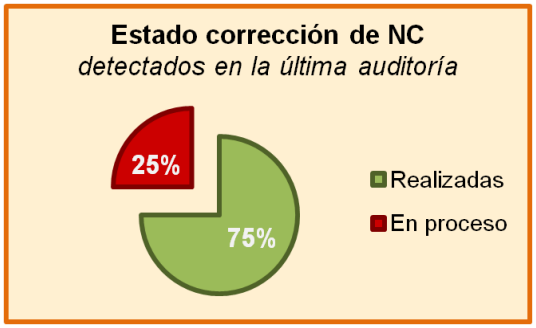


Ilustración 25. Gráfica del estado de corrección de las no conformidades detectadas.

Adaptación a la nueva Norma (pestaña 1)

Desde finales de 2014, cuando se publicó la nueva versión de la ISO 27001 por parte Aenor, ésta pasó ser la nueva norma a auditar. Gran parte de los controles se mantienen de una a otra versión, pero hay controles nuevos y otros que han desaparecido. Esta gráfica refleja el estado de adaptación a la nueva versión.

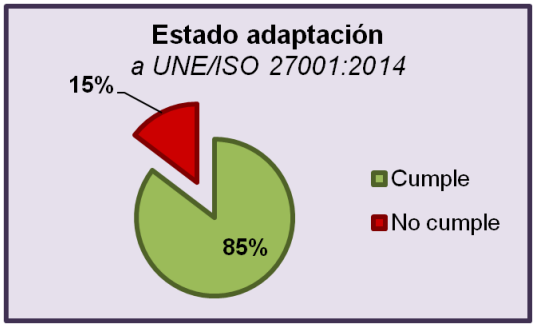


Ilustración 26. Gráfica del estado de adaptación a la nueva versión de la ISO.

Informes y gráficas (pestañas 2 y 3)

Aquí es donde la empresa de consultoría introduce los datos de los informes emitidos por la entidad de certificación. Esta información, tal y como se indicó anteriormente, se procesa mediante tablas dinámicas en una hoja oculta. Al cliente le sirve para imprimir en formato Din-A4 (Ilustración 27, en la siguiente página).

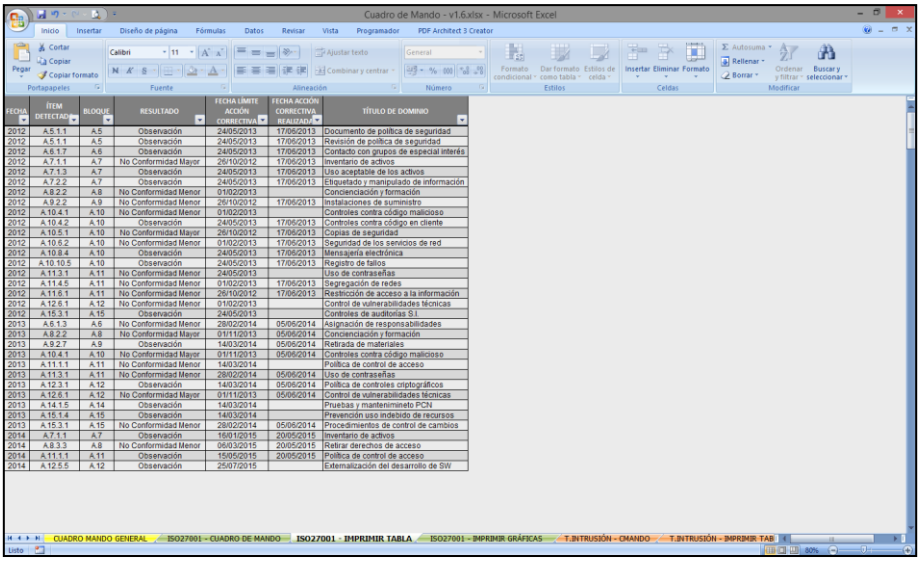


Ilustración 27. Vista de la pestaña "ISO27001 - IMPRIMIR TABLA".

En la tabla hay que introducir:

- Año en que se realiza la auditoría por parte de la entidad de certificación.
- El ítem detectado, tal y como aparece en el informe. Automáticamente se clasifica en el bloque que le corresponde.
- Indicar el grado de incumplimiento: observación, no conformidad menor y no conformidad mayor.
- Fecha límite que se le ha concedido para realizar todas las acciones correctivas.
- Fecha de la acción correctiva realizada, en el caso que se haya realizado. Debe dejarse en blanco si no se ha acometido ninguna mejora. Esta sería la correspondiente a la fecha de la auditoría interna realizada por la empresa consultora.
- Descripción para facilitar la comprensión de la observación o la no conformidad detectada.

Como se introdujo en la vista global de la herramienta, todas las hojas han sido bloqueadas evitando su edición. En aquellas hojas empleadas para imprimir tablas, los filtros sí se encuentran habilitados para por elegir qué valores mostrar y ordenarlos según los criterios que se estimen oportunos, tal y como se muestra en la siguiente ilustración (ver ilustración 28, en la siguiente página).

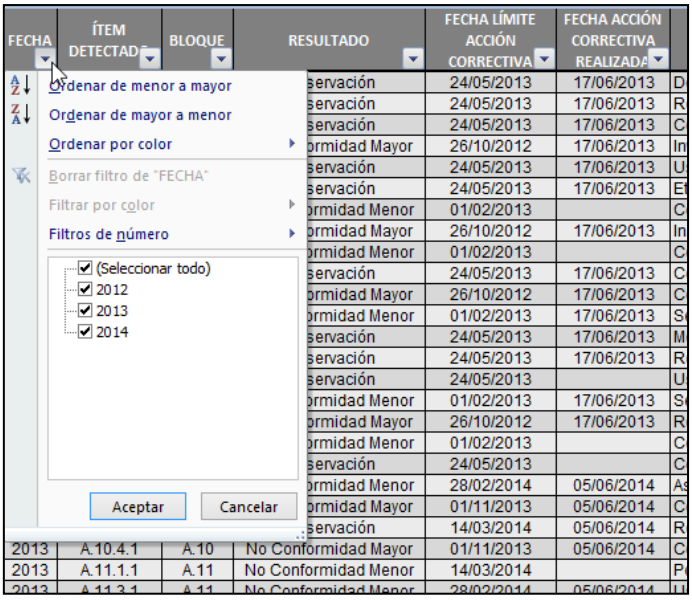


Ilustración 28. Detalle en los filtros en la pestaña "ISO27001 - IMPRIMIR TABLA".

Una vez impreso en papel, el informe quedaría tal y como se muestra en la siguiente captura de pantalla (ver ilustración 29, en la siguiente página):

DOCUMENTO CONFIDENCIAL | INFORME UNE-ISO 27001 | EMBOTELLADORA S.A.

FECHA	ÍTEM DETECTADO	BLOQUE	RESULTADO	FECHA LÍMITE ACCIÓN CORRECTIVA	FECHA ACCIÓN CORRECTIVA REALIZADA	TÍTULO DEL DOMINIO
2012	A.5.1.1	A.5	Observación	24/05/2013	17/06/2013	Documento de política de seguridad
2012	A.5.1.1	A.5	Observación	24/05/2013	17/06/2013	Revisión de política de seguridad
2012	A.6.1.7	A.6	Observación	24/05/2013	17/06/2013	Contacto con grupos de especial interés
2012	A.7.1.1	A.7	No Conformidad Mayor	26/10/2012	17/06/2013	Inventario de activos
2012	A.7.1.3	A.7	Observación	24/05/2013	17/06/2013	Uso aceptable de los activos
2012	A.7.2.2	A.7	Observación	24/05/2013	17/06/2013	Etiquetado y manipulado de información
2012	A.8.2.2	A.8	No Conformidad Menor	01/02/2013		Concienciación y formación
2012	A.9.2.2	A.9	No Conformidad Menor	26/10/2012	17/06/2013	Instalaciones de suministro
2012	A.10.4.1	A.10	No Conformidad Menor	01/02/2013		Controles contra código malicioso
2012	A.10.4.2	A.10	Observación	24/05/2013	17/06/2013	Controles contra código en cliente
2012	A.10.5.1	A.10	No Conformidad Mayor	26/10/2012	17/06/2013	Copias de seguridad
2012	A.10.6.2	A.10	No Conformidad Menor	01/02/2013	17/06/2013	Seguridad de los servicios de red
2012	A.10.8.4	A.10	Observación	24/05/2013	17/06/2013	Mensajería electrónica
2012	A.10.10.5	A.10	Observación	24/05/2013	17/06/2013	Registro de fallos
2012	A.11.3.1	A.11	No Conformidad Menor	24/05/2013		Uso de contraseñas
2012	A.11.4.5	A.11	No Conformidad Menor	01/02/2013	17/06/2013	Segregación de redes
2012	A.11.6.1	A.11	No Conformidad Menor	26/10/2012	17/06/2013	Restricción de acceso a la información
2012	A.12.6.1	A.12	No Conformidad Menor	01/02/2013		Control de vulnerabilidades técnicas
2012	A.15.3.1	A.15	Observación	24/05/2013		Controles de auditorías S.I.
2013	A.6.1.3	A.6	No Conformidad Menor	28/02/2014	05/06/2014	Asignación de responsabilidades
2013	A.8.2.2	A.8	No Conformidad Mayor	01/11/2013	05/06/2014	Concienciación y formación
2013	A.9.2.7	A.9	Observación	14/03/2014	05/06/2014	Retirada de materiales
2013	A.10.4.1	A.10	No Conformidad Mayor	01/11/2013	05/06/2014	Controles contra código malicioso
2013	A.11.1.1	A.11	No Conformidad Menor	14/03/2014		Política de control de acceso
2013	A.11.3.1	A.11	No Conformidad Menor	28/02/2014	05/06/2014	Uso de contraseñas
2013	A.12.3.1	A.12	Observación	14/03/2014	05/06/2014	Política de controles criptográficos
2013	A.12.6.1	A.12	No Conformidad Mayor	01/11/2013	05/06/2014	Control de vulnerabilidades técnicas
2013	A.14.1.5	A.14	Observación	14/03/2014		Pruebas y mantenimineto PCN
2013	A.15.1.4	A.15	Observación	14/03/2014		Prevención uso indebido de recursos
2013	A.15.3.1	A.15	No Conformidad Menor	28/02/2014	05/06/2014	Procedimientos de control de cambios

Informe generado el 14/06/2015 | Página 1 de 2

Ilustración 29. Informe imprimible en formato DIN-A4.

En la pestaña "ISO27001 - IMPRIMIR GRÁFICAS" encontramos los mismos gráficos del cuadro de mando de la norma. Únicamente se han reducido y se ha incluido las cabeceras y los pies de página para que el cliente lo pueda imprimir en formato Din-A4. En la siguiente captura se muestra esta pestaña (Ilustración 30).

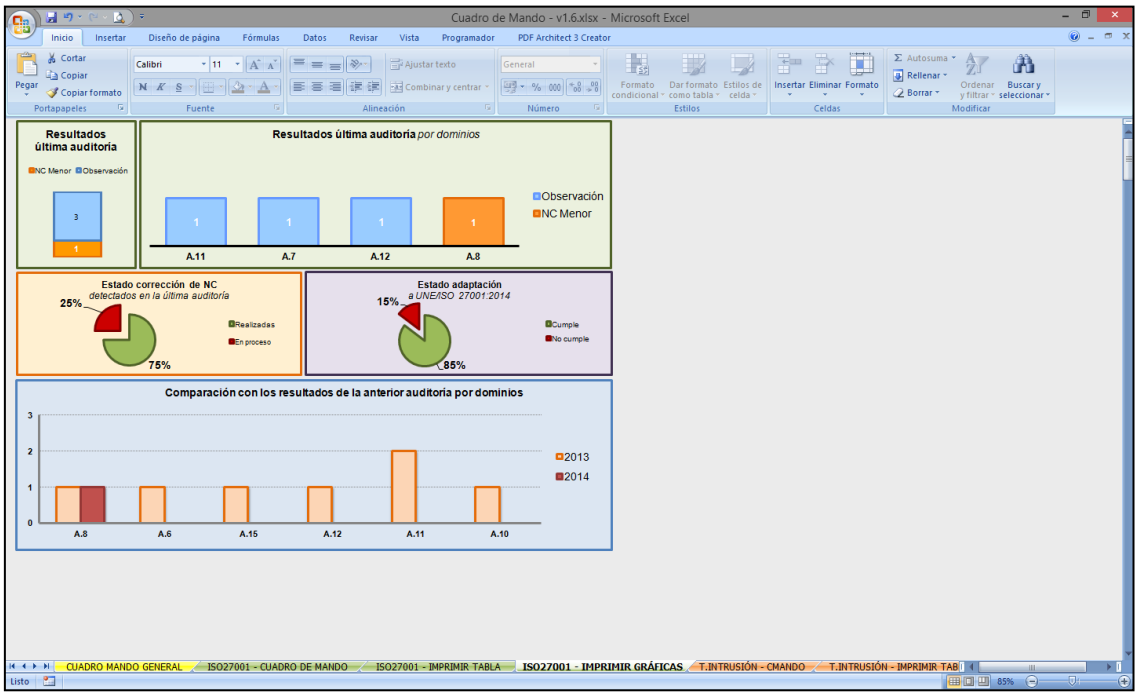


Ilustración 30. Pestaña "ISO27001 - IMPRIMIR GRÁFICAS"

Una vez impreso o guardado en formato PDF, el informe quedaría tal y como se muestra en la siguiente captura de pantalla.

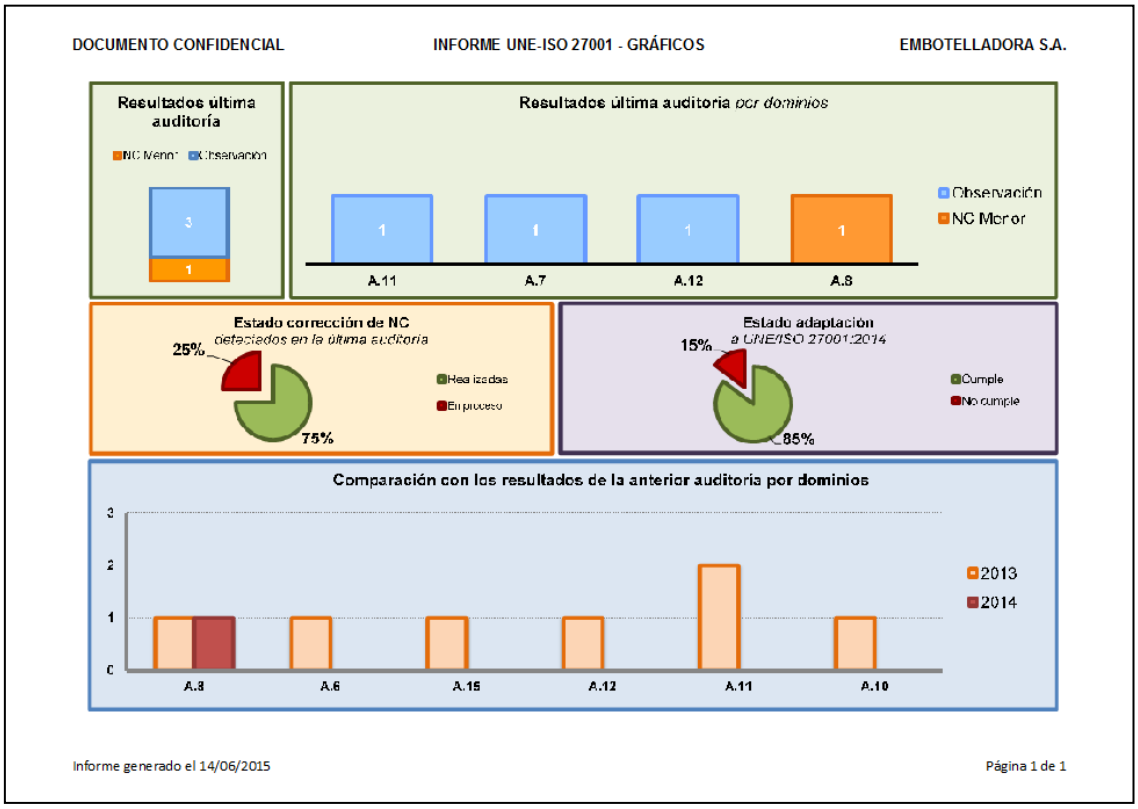


Ilustración 31. Informe imprimible en formato DIN-A4.

Ambos informes son útiles para poder estudiar los resultados en reuniones bien en formato papel o presentados por pantalla (p.e. proyector) y que sean repartidos a los asistentes. Debe tenerse en cuenta que toda la información proporcionada será clave para las decisiones que se tomen.

Cálculos intermedios (pestaña 4)

El desarrollo de este bloque de pestañas ha resultado especialmente laborioso pues, aunque se obtiene mucha información, ésta se obtiene manipulando pocos datos de entrada y todos ellos a través de tablas dinámicas para que se puedan reflejar todos los datos y referencias. Además, Excel no posee todas las facilidades que sí que aportan otras herramientas destinadas a Business Intelligence, por lo que ha supuesto un plus de esfuerzo en el diseño.

Al introducir los datos en "ISO27001 - IMPRIMIR TABLA", la columna bloque se rellena automáticamente. Este dato es necesario para poder realizar una clasificación correcta de los dominios, y para ello se ha tratado el contenido de "Ítem detectado" como una cadena y se le han aplicado condiciones tal y como se puede observar en la siguiente captura.

```
=SI(IZQUIERDA(resultados27Kv2005[[#Esta fila];[ÍTEM DETECTADO]];1)="A"; SI(DERECHA(IZQUIERDA(resultados27Kv2005[[#Esta fila];[ÍTEM DETECTADO]];4);1)="."; IZQUIERDA(resultados27Kv2005[[#Esta fila];[ÍTEM DETECTADO]];3);IZQUIERDA(resultados27Kv2005[[#Esta fila];[ÍTEM DETECTADO]];4)); IZQUIERDA(resultados27Kv2005[[#Esta fila];[ÍTEM DETECTADO]];1))
```

Ilustración 32. Detalle de las condiciones de la columna "Bloque" de la pestaña de informe.

A continuación se muestra una imagen global para que se pueda apreciar cómo se han preparado los datos para que se actualicen todos de forma automática y se les puedan aplicar los filtros adecuados.

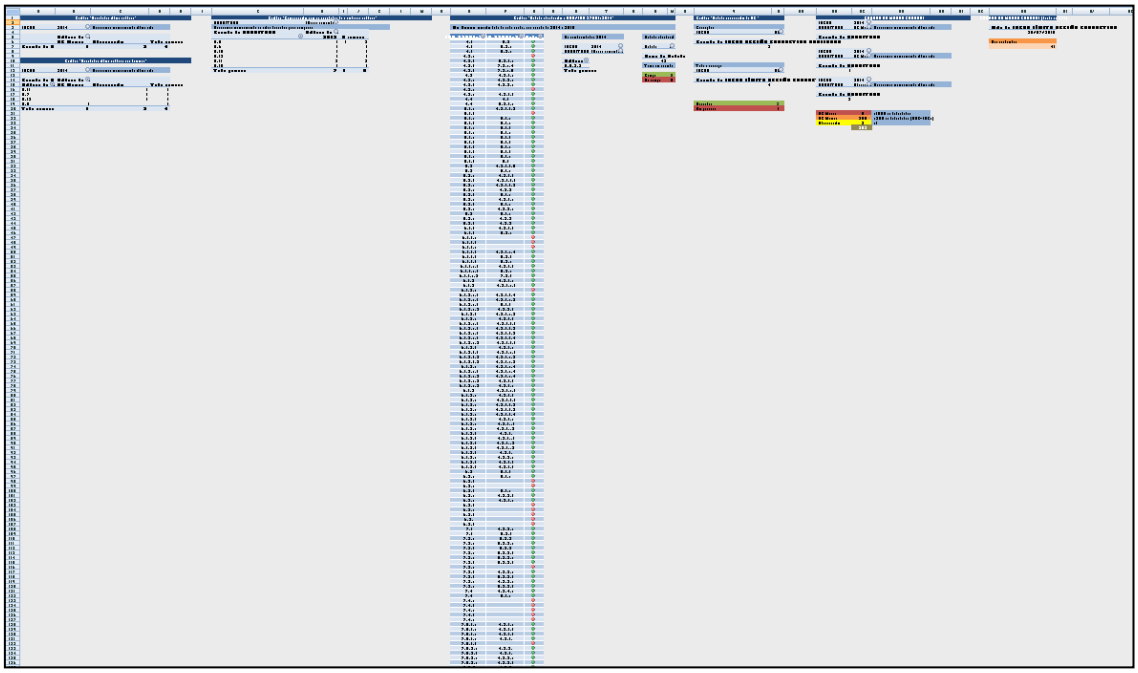


Ilustración 33. Pestaña oculta donde se realizan los cálculos intermedios.

Ahora se procederá a mostrar una por una todas las tablas dinámicas utilizadas para la generación del cuadro de mando. Estas se encuentran en la pestaña oculta "ISO27001 - CALC".

Gráfica "Resultados última auditoría"				
FECHA	2014	Seleccionar manualmente último año		
	Rótulos de columna			
	NC Menor	**Observación**		**Total general**
Cuenta de RESULTADO	**1**		**3**	**4**

Ilustración 34. Tabla dinámica para los resultados de la última auditoría.

Gráfica "Resultados última auditoría por dominios"			
FECHA	2014	Seleccionar manualmente último año	
Cuenta de RESULTADO	**Rótulos de columna**		
Rótulos de fila	**NC Menor**	**Observación**	**Total general**
A.11		1	1
A.7		1	1
A.12		1	1
A.8	1		1
Total general	**1**	**3**	**4**

Ilustración 35. Tabla dinámica para los resultados de la última auditoría por dominios.

Gráfica "Comparación con los resultados de la anterior auditoría"

RESULTADO	(Varios elementos)		
Seleccionar manualmente los años deseados para comparar			
Cuenta de RESULTADO	**Rótulos de columna**		
	2013	**2014**	**Total general**
A.8	1	1	2
A.6	1		1
A.15	1		1
A.12	1		1
A.11	2		2
A.10	1		1
Total general	**7**	**1**	**8**

Ilustración 36. Tabla dinámica para compara los resultados históricos.

Gráfica "Estado adaptación a UNE/ISO 27001:2014"

No tocar ningún dato de esta parte, solo aplicable de 2014 a 2015

ISO 27001:2014	ISO 27001:2005	Estado
4.1	8.3	
4.1	8.3.a	
4.1	8.3.e	
4.2.a		
4.2.b	5.2.1.c	
4.2.b	7.3.c.4	
4.2.b	7.3.c.5	
4.3	4.2.1.a	
4.3.a	4.2.3.e	
4.3.b	4.2.3.e	
4.3.c		
4.3.c	4.3.1.b	
4.4	4.1	
4.4	5.2.1.a	
5.1.a	4.2.1.b.3	
5.1.b		
5.1.c	5.1.e	

No conformidades 2014

FECHA	2014
RESULTADO	(Varios elementos)

Rótulos de fila
A.8.3.3
Total general

Estado adaptación

Estado	1

Suma de Estado
43

Tiene en cuenta los nue

Cumple	250
No cumple	43

Ilustración 37. Tabla dinámica ver el estado de adaptación a la nueva versión de la Norma.

Gráfica "Estado corrección de NC "

Corregidos

FECHA	2014

Cuenta de FECHA ACCIÓN CORRECTIVA REALIZADA
3

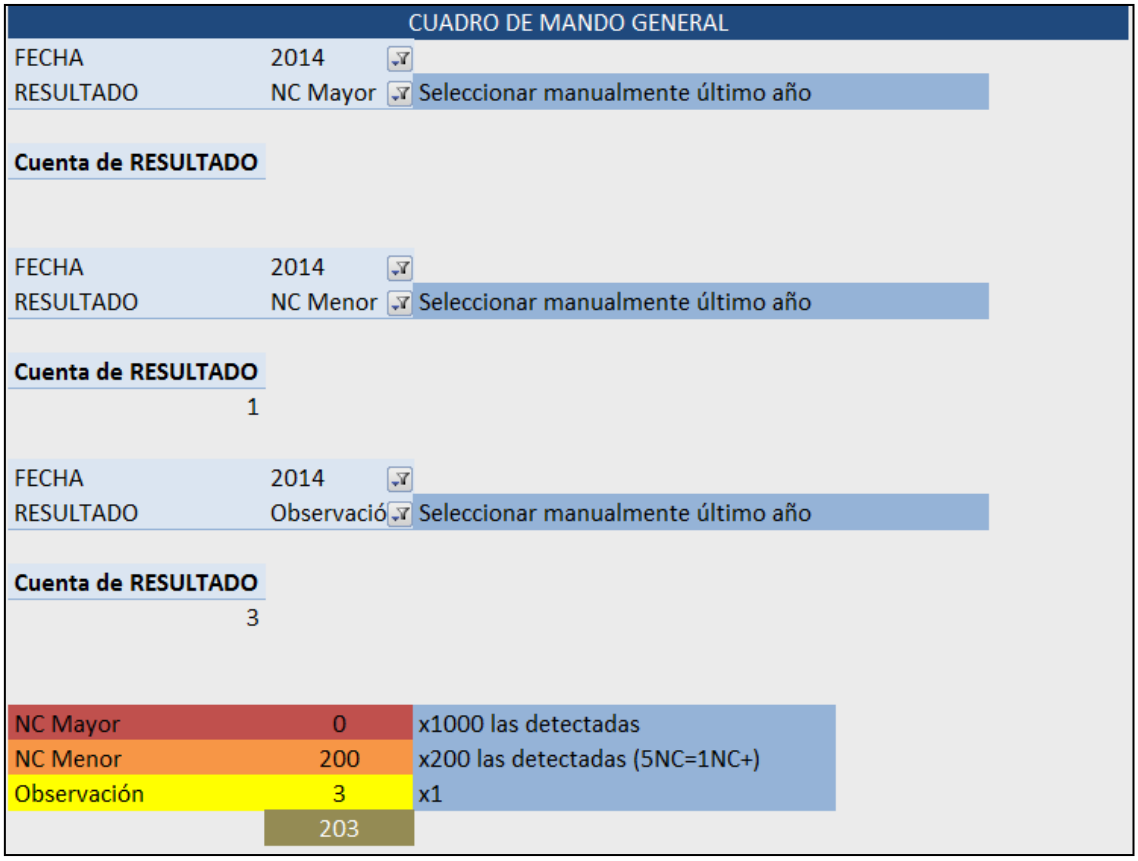
Total a corregir

FECHA	2014

Cuenta de FECHA LÍMITE ACCIÓN CORRECTIVA
4

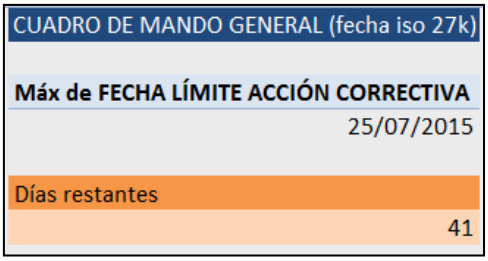
Realizadas	3
En proceso	1

Ilustración 38. Tablas dinámicas para poder mostrar el estado de las correcciones.



CUADRO DE MANDO GENERAL		
FECHA	2014	
RESULTADO	NC Mayor	Seleccionar manualmente último año
Cuenta de RESULTADO		
FECHA	2014	
RESULTADO	NC Menor	Seleccionar manualmente último año
Cuenta de RESULTADO		
1		
FECHA	2014	
RESULTADO	Observació	Seleccionar manualmente último año
Cuenta de RESULTADO		
3		
NC Mayor	0	x1000 las detectadas
NC Menor	200	x200 las detectadas (5NC=1NC+)
Observación	3	x1
	203	

Ilustración 39. Tablas para el semáforo de cumplimiento del Cuadro de Mando General.



CUADRO DE MANDO GENERAL (fecha iso 27k)
Máx de FECHA LÍMITE ACCIÓN CORRECTIVA
25/07/2015
Días restantes
41

Ilustración 40. Cálculos para la cuenta atrás del Cuadro de Mando General.

Cabe destacar la dificultad que ha presentado el mapeo, plasmado en la Ilustración 37, de la nueva norma con la antigua. Debido a las limitaciones que presenta Excel, se ha tenido que realizar una correspondencia uno a uno (1 a 1) con todos los controles en vez de una lista con uno a muchos (1 a n) que hubiera resultado más rápido y cómodo.

Determinar una no conformidad depende en última instancia del criterio del auditor. Aún así, se puede determinar de forma aproximada el nivel de cumplimiento con la nueva norma en base a:

- Cuando haya correspondencia con la antigua versión y esta no tenga una no conformidad, en la nueva versión se indicará como correcto cumplimiento.
- Cuando haya correspondencia con la antigua versión y esta tenga una no conformidad, en la nueva versión se heredará.
- Si el control es nuevo, y no hay equivalencia con la versión antigua, se asumirá la no conformidad.

Finalmente, remitiéndonos a la Ilustración 39, en este apartado se realiza una ponderación de los resultados para poder tener en cuenta, por ejemplo, que 5 no conformidades menores puedan contabilizarse como una mayor a la hora de realizar la valoración global del semáforo de la pestaña de Cuadro de Mando General.

Explicación del cuadro de mando de Test de Intrusión

En este bloque se ha decido fusionar el Test de Intrusión Interno y Externo. Al igual que con la ISO 27001 existe una hoja para el Cuadro de Mando, dos dedicadas para la impresión de informes y graficas y otra hoja oculta donde se alojan las tablas dinámicas y cálculos intermedios.

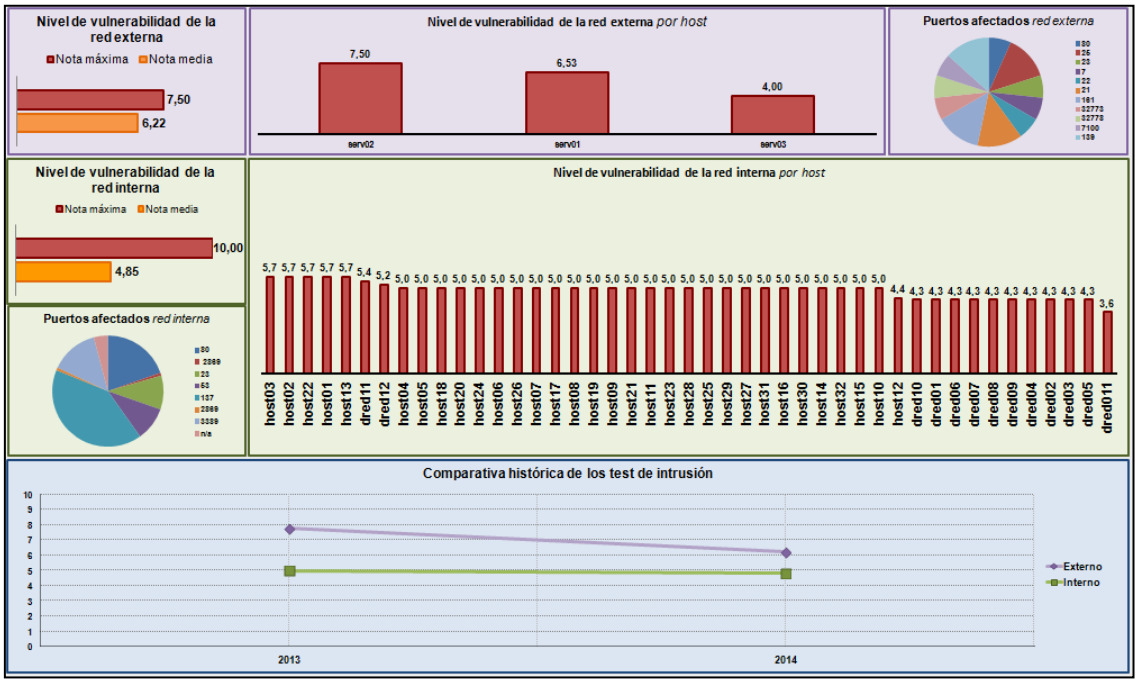


Ilustración 41. Contenido de la pestaña "T.INTRUSIÓN - CMANDO".

Con la intención de poder diferenciar cada bloque se ha decidido que las gráficas con fondo morado correspondan al test de intrusión externo, las de fondo verde a las de la red interna y la azul es una comparativa de los resultados de años anteriores.

Test de Intrusión Externo (pestaña 1)

La información sobre la red externa la podemos encontrar en la fila superior del cuadro de mando. En primer lugar tenemos una gráfica donde se puede ver la nota máxima y la nota media de las vulnerabilidades detectadas, de esta muestra el estado global y si existe alguna que sea crítica (ver ilustración 42, en la siguiente página).

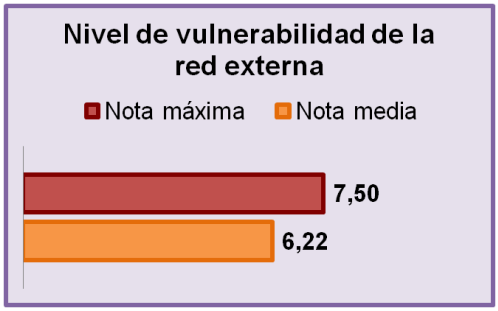


Ilustración 42. Indicador general de las vulnerabilidades de la red externa.

Ahora nos centraremos en dónde están localizadas las vulnerabilidades. Para ello se muestra la nota media obtenida por cada uno de los hosts.

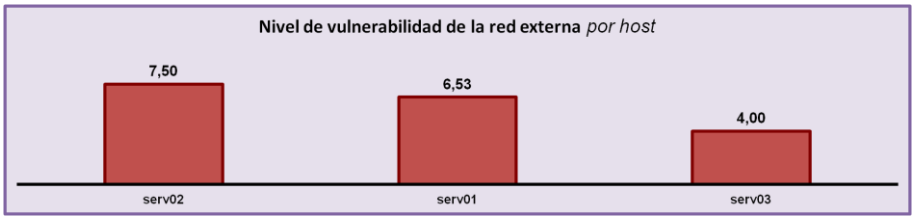


Ilustración 43. Indicador de las vulnerabilidades de la red externa por cada host analizado.

Adicionalmente se muestran los puertos donde se han detectado las vulnerabilidades, pues el personal con un perfil más técnico puede reconocer algunos de los puertos comunes[26] e identificar a primera vista los servicios afectados.

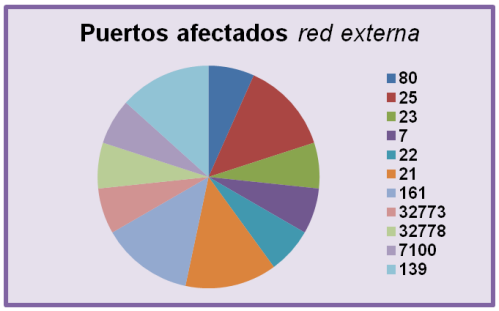


Ilustración 44. Gráfica de los puertos con vulnerabilidades detectadas en la red externa.

Test de Intrusión Interno (pestaña 1)

Se muestran los mismos elementos anteriormente explicados, pero ahora a nivel de la red interna.

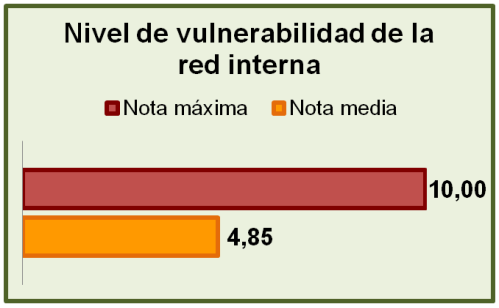


Ilustración 45. Indicador general de las vulnerabilidades de la red interna.

[26] se incluye una lista con los puertos comunes (o bien-conocidos) en el Anexo V.

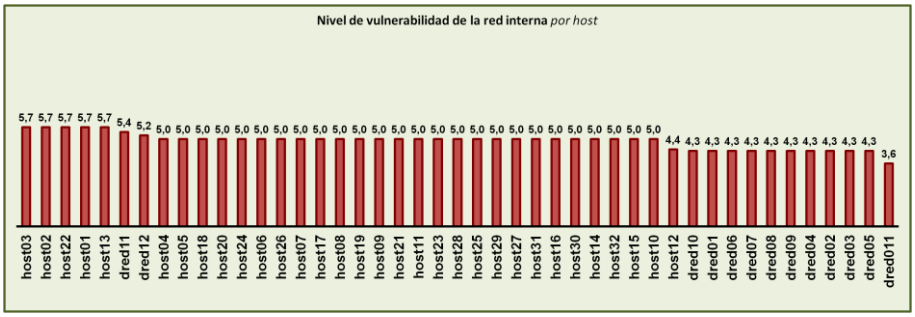


Ilustración 46. Indicador de las vulnerabilidades de la red interna por cada host analizado.

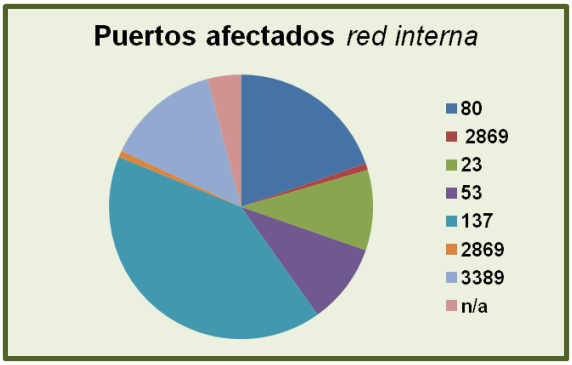


Ilustración 47. Gráfica de los puertos con vulnerabilidades detectadas en la red interna.

Entre otras cosas, estas gráficas puede revelar la existencia de malas configuraciones en la red de la empresa o la presencia de sistemas obsoletos que por su coste o la falta de tiempo han sido imposibles de cambiar o actualizar.

Por lo general, no es tan prioritaria la seguridad de una red interna como a la externa, pero estos problemas pueden dar pie a que un empleado descontento o un atacante con intenciones maliciosas que consiga acceder desde el exterior, puede obtener información sensible, boicotear los servicios, parar una línea de producción, etc. con los riesgos que puede conllevar a nivel de seguridad de maquinaria, personal o las pérdidas económicas.

Datos históricos (pestaña 1)

Finalmente se muestra la gráfica comparativa de los test interno y externo de los últimos años. Resulta útil para la evaluación de la mejora continua pues permite comprobar si las mejoras están siendo adecuadas o si hay que incrementar los esfuerzos.

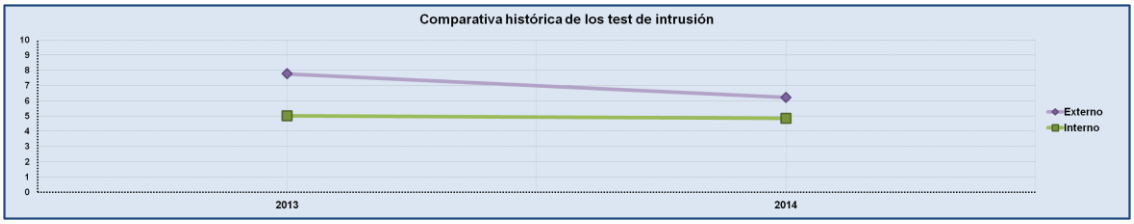
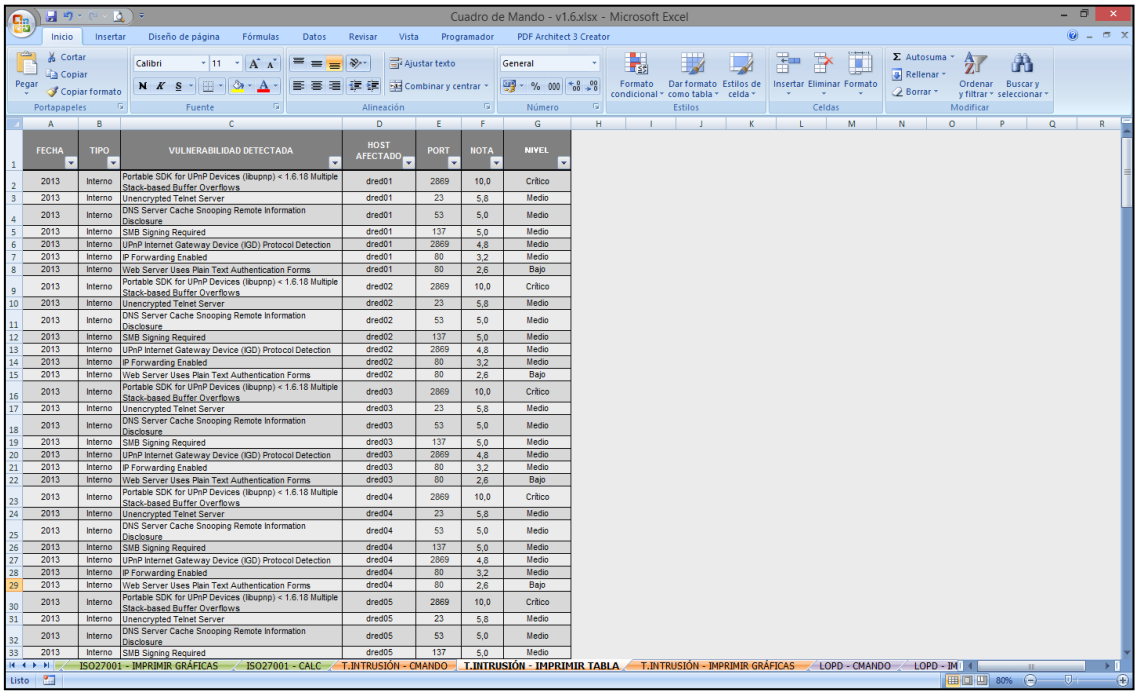


Ilustración 48. Comparación con los resultados de años anteriores.

Como se ha comentado en anteriores apartados del presente trabajo, es prácticamente imposible conseguir la seguridad total en los sistemas, pero si se puede trabajar para reducir los riesgos.

Impresión de informes y documentos (pestañas 2 y 3)

Desde las pestañas de imprimir la tabla y las gráficas se pueden obtener informes imprimibles en formato Din-A4. Además, mediante los filtros se permite mostrar los valores deseados y ordenarlos se crea conveniente.



FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred01	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred01	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred01	53	5,0	Medio
2013	Interno	SMB Signing Required	dred01	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred01	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred01	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred01	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred02	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred02	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred02	53	5,0	Medio
2013	Interno	SMB Signing Required	dred02	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred02	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred02	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred02	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred03	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred03	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred03	53	5,0	Medio
2013	Interno	SMB Signing Required	dred03	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred03	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred03	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred03	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred04	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred04	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred04	53	5,0	Medio
2013	Interno	SMB Signing Required	dred04	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred04	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred04	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred04	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred05	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred05	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred05	53	5,0	Medio
2013	Interno	SMB Signing Required	dred05	137	5,0	Medio

Ilustración 49. Vista de la pestaña " T.INTRUSIÓN - IMPRIMIR TABLA".

La empresa consultora debe introducir los siguientes datos en la tabla:

- Año en que se realiza el test de intrusión.
- La tipología del test: interno o externo.
- La vulnerabilidad detectada. Esta información ha sido extraída de Nessus, una herramienta automática de detección de vulnerabilidades.
- El host donde se ha detectado la vulnerabilidad, pues puede repetirse en varios de los sistemas al tener las mismas características y configuraciones. Puede indicarse el nombre o la dirección IP.
- Puerto donde se ha detectado la vulnerabilidad.
- La nota obtenida en el CVSS de Nessus. El icono de la columna de riesgo se actualiza automáticamente según sea el riesgo: débil, medio, alto o crítico.

En cuanto a los gráficos, son los mismos del cuadro de mando del test de intrusión pero adaptados para que puedan caber en papel tamaño folio.

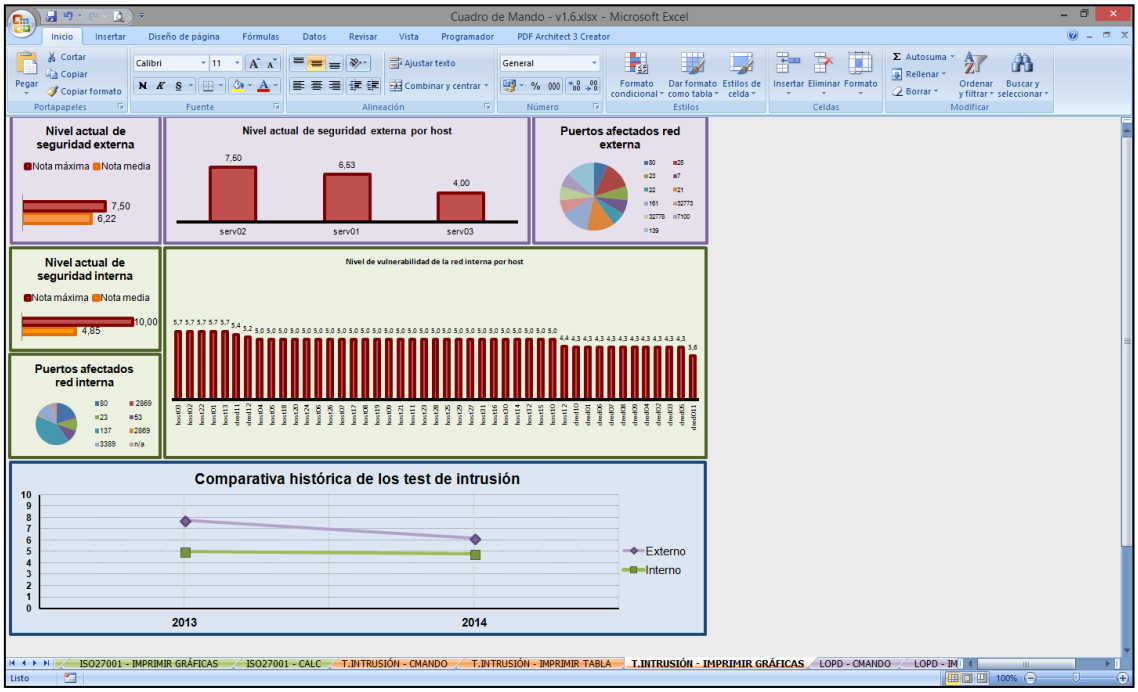


Ilustración 50. Vista de la pestaña " T.INTRUSIÓN - IMPRIMIR GRÁFICAS".

Tanto el informe impreso de la tabla como el de las gráficas siguen el mismo diseño que el de la ISO 27001. Puede observarse en el Anexo III cómo quedarían ambos al ser impresos a partir de los datos del caso de estudio del apartado 7 del presente trabajo.

Cálculos intermedios (pestaña 4)

A continuación, a modo de demostración del trabajo realizado, se incluyen las capturas de las tablas dinámicas ocultas.

Nivel actual de seguridad externa	
FECHA	2014
TIPO	Externo
Valores	
Nota media	**Nota máxima**
6,22	7,50

Ilustración 51. Tabla dinámica para la gráfica de nivel de seguridad de la red externa.

Nivel actual de seguridad externa por host	
FECHA	2014
TIPO	Externo
Rótulos de fila	**Promedio de NOTA**
serv02	7,50
serv01	6,53
serv03	4,00
Total general	**6,22**

Ilustración 52. Tabla dinámica para la gráfica de nivel de seguridad por hosts de la red externa.

Puertos afectados red externa	
FECHA	2013
TIPO	Externo
Rótulos de fila	**Cuenta de PORT**
80	1
25	2
23	1
7	1
22	1
21	2
161	2
32773	1
32778	1
7100	1
139	2
Total general	**15**

Ilustración 53. Tabla dinámica para la gráfica de los puertos con vulnerabilidades detectadas en la red externa.

Nivel actual de seguridad interna por host	
FECHA	2014
TIPO	Interno
Valores	
Nota media	**Nota máxima**
4,85	10,00

Ilustración 54. Tabla dinámica para la gráfica de nivel de seguridad de la red interna.

Nivel actual de seguridad interna por host	
FECHA	2014
TIPO	Interno
Rótulos de fila	**Promedio de NOTA**
host03	5,7
host02	5,7
host22	5,7
host01	5,7
host13	5,7

Ilustración 55. Tabla dinámica para la gráfica de nivel de seguridad por hosts de la red interna.

Puertos afectados red interna	
FECHA	2014
TIPO	Interno
Rótulos de fila	**Cuenta de PORT**
80	24
2869	1
23	12
53	12
137	50
2869	1
3389	17
n/a	5
Total general	**122**

Ilustración 56. Tabla dinámica para la gráfica de los puertos con vulnerabilidades detectadas en la red interna

Comparativa años			
Promedio de NOTA	**Rótulos de columna**		
Rótulos de fila	**Externo**	**Interno**	**Total general**
2013	7,77	5,02	5,31
2014	6,22	4,85	4,90
Total general	**7,39**	**4,94**	**5,12**

Ilustración 57. Tabla dinámica para obtener la gráfica de comparación de datos históricos.

Dias hasta próximo test	
Interno	26/10/2015
Externo	23/11/2015
Externo	133
Interno	161

Ilustración 58. Cálculos para la cuenta atrás del Cuadro de Mando General.

Explicación del cuadro de mando de LOPD

Como en los casos anteriores encontramos cuatro hojas: una contiene el cuadro de mando, otra corresponde a una tabla para poder imprimir los informes, una hoja con las mismas gráficas que en el cuadro de mando preparadas para ser impresas en

formato folio y una última que permanecerá oculta con todos los cálculos para poder tener tablas dinámicas.

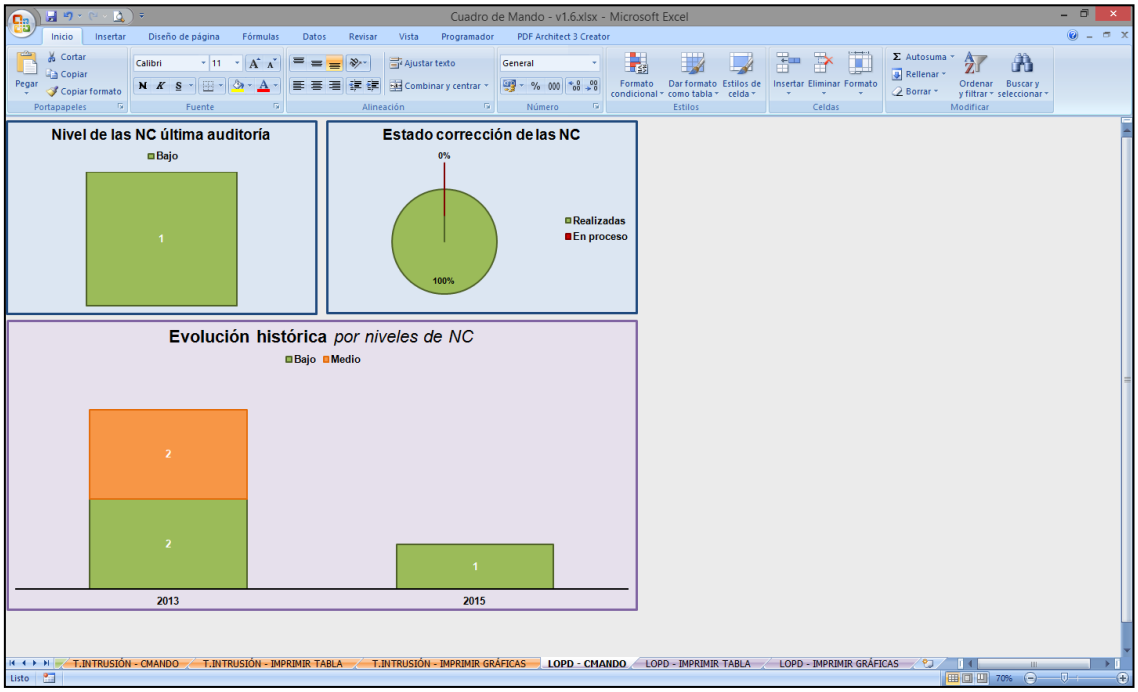


Ilustración 59. Contenido de la pestaña "LOPD - CMANDO".

Las gráficas con el color azul de fondo reflejan los datos del último informe de la auditoría interna realizada por parte de la consultora y en morado se muestra la comparativa histórica.

Puede que sea el cuadro de mando más sencillo, pues sólo necesita indicar el cumplimiento o las no conformidades detectadas para que se puedan corregir. Cabe destacar que en principio no debería aparecer ninguna, aunque esto resulta muy complicado por la multitud de factores que pueden afectar a las organizaciones.

Resultados de la última auditoría (pestaña 1)

A continuación se muestra el primero de los indicadores. Aquí se muestra el número de no conformidades atendiendo al criterio del auditor para ser clasificadas en los niveles de alto, medio y bajo. Para realizar esta clasificación se tienen en cuenta las características de la empresa, dónde se ha detectado el problema, el número de afectados, etc.

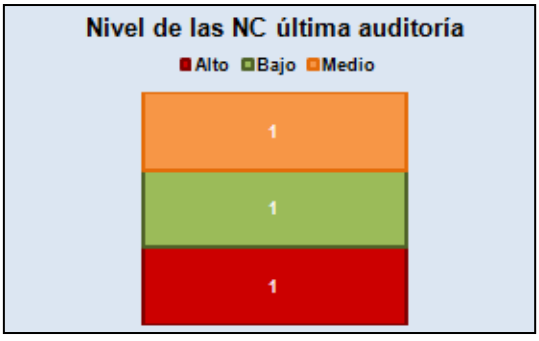


Ilustración 60. Indicador de no conformidades detectadas.

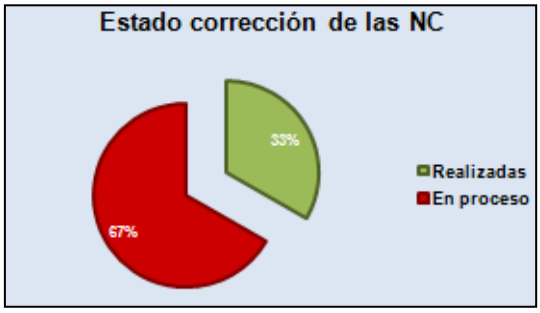


Ilustración 61. Indicador del estado de las correcciones de las no conformidades detectadas.

Datos históricos (pestaña 1)

A continuación se muestra la gráfica comparativa de los resultados de los distintos años de los que se dispone informe de auditoría. En este caso es bianual.

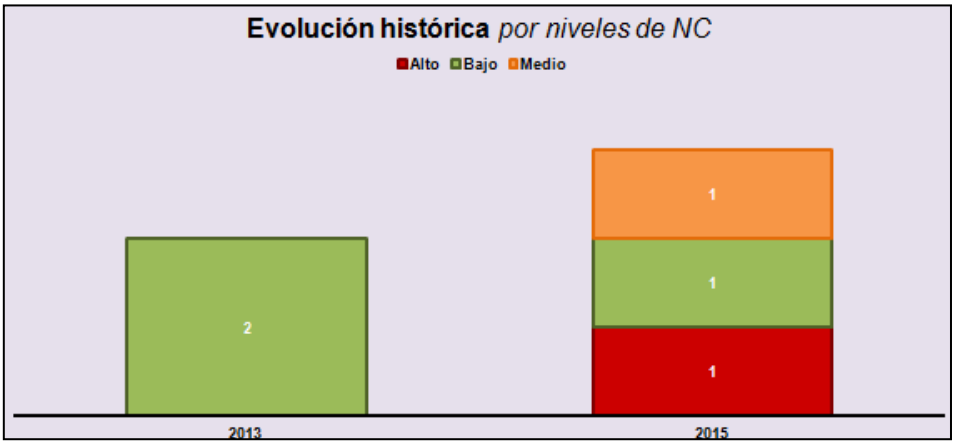


Ilustración 62. Gráfica de la evolución de los incumplimientos detectados.

Impresión de informes y documentos (pestañas 2 y 3)

Desde esta pestaña, el responsable decide qué datos imprimir y cómo ordenarlos. Como en todos los casos anteriores, están adaptados para formato Din-A4.

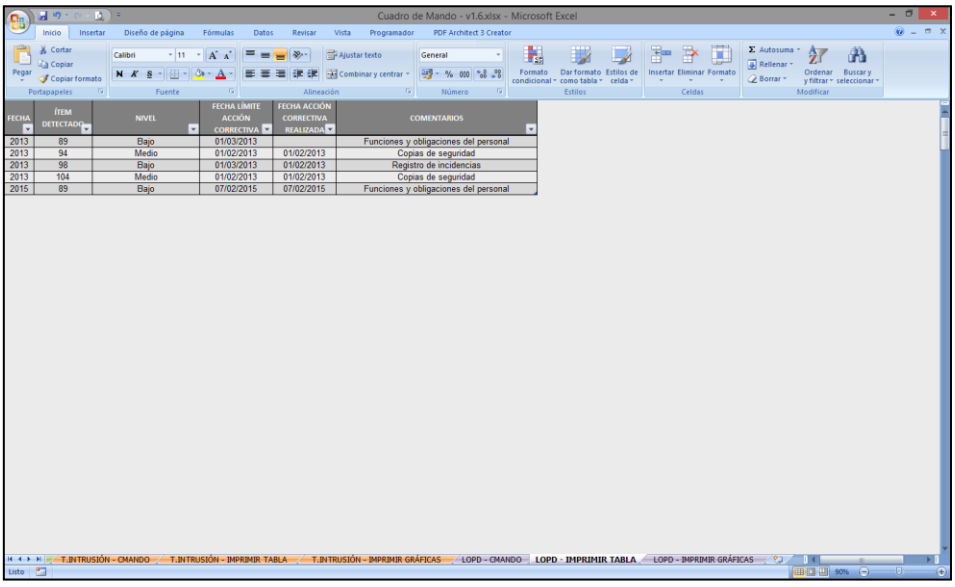


Ilustración 63. Vista general de la pestaña "LOPD - IMPRIMIR TABLA".

En la tabla hay que introducir:

- Año en que se realiza la auditoría.
- El número del artículo del artículo/reglamento en el que se ha detectado la no conformidad.
- Indicar el grado de incumplimiento: bajo, medio o alto.
- Fecha límite que se le ha concedido para realizar todas las acciones correctivas.
- Incluir una vez que se ha llevado a cabo esta acción, la fecha en la que se ha comprobado por parte de la consultora, que se cumple con el control de la norma.
- Si procede, incluir algún comentario.

Son los mismos gráficos del apartado del cuadro de mando de la LOPD, únicamente se han incluido las cabeceras y los pies de página para que el cliente lo pueda imprimir en formato Din-A4.

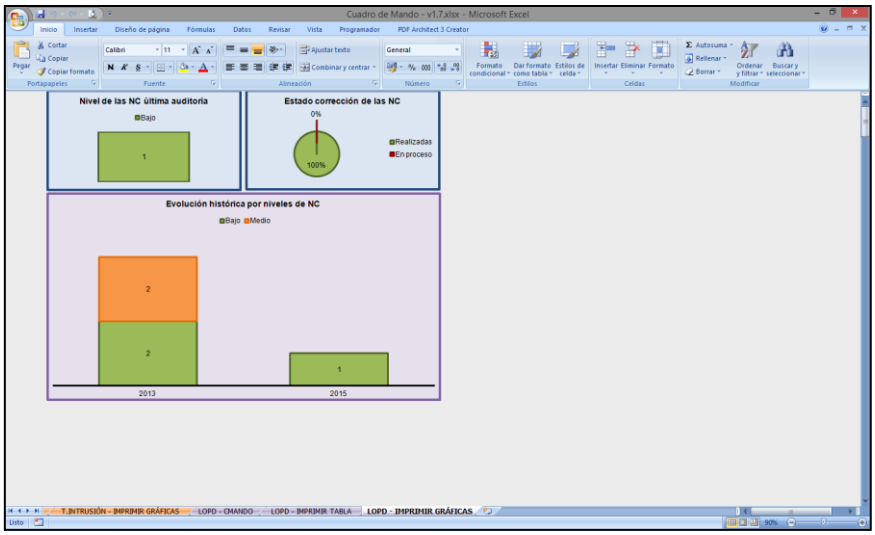


Ilustración 64. Vista general de la pestaña "LOPD - IMPRIMIR GRÁFICAS".

Puede observarse en el Anexo IV cómo quedarían ambos al ser impresos a partir de los datos del caso de estudio del apartado 7 del presente trabajo.

Cálculos intermedios (pestaña 4)

A continuación se mostrarán las diferentes capturas correspondientes a las tablas dinámicas y cálculos realizados para poder diseñar los distinto indicadores del cuadro demando.

Gráfica "Resultados última auditoría"		
FECHA	2015	
	Rótulos de columna	
	Bajo	Total general
Cuenta de NIVEL	1	1

Ilustración 65. Tabla dinámica para las no conformidades detectadas.

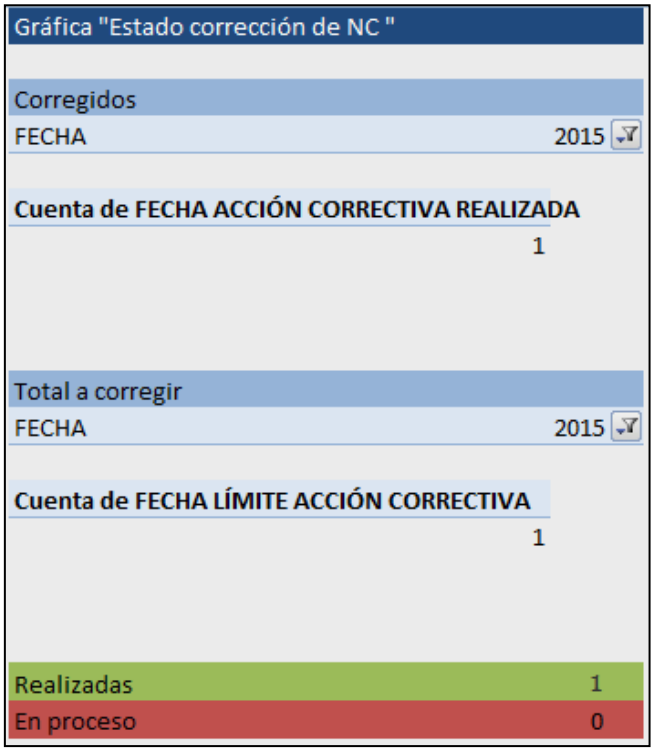


Ilustración 66. Tablas dinámicas para mostrar el estado de las correcciones realizadas.

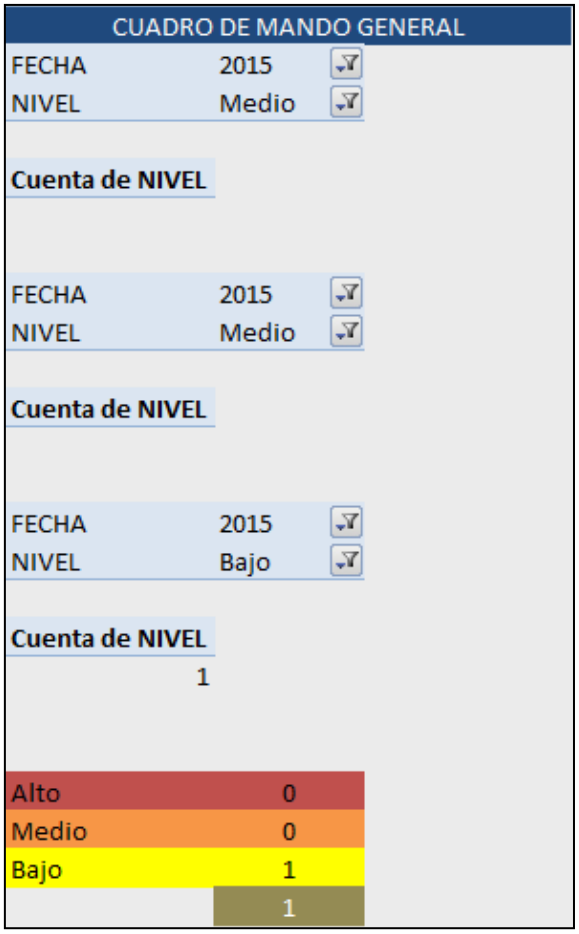


Ilustración 67. Tablas dinámicas para el semáforo de cumplimiento del Cuadro de Mando General.

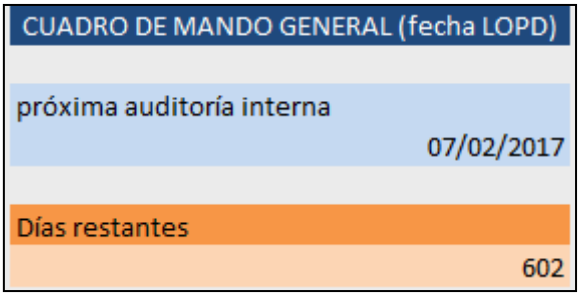


Ilustración 68. Cálculos para la cuenta atrás del Cuadro de Mando General.

CUADRO DE MANDO GENERAL (fecha LOPD)

Cuenta de NIVEL	Rótulos de columna		
Rótulos de fila	Bajo	Medio	Total general
2013	2	2	4
2015	1		1
Total general	3	2	5

Ilustración 69. Tabla dinámica para obtener la gráfica de comparación de datos históricos.

7. Caso de estudio

Metodología del caso

Una vez explicada la herramienta introduciremos una aplicación práctica utilizando la metodología del caso de estudio[27].

Ante la imposibilidad de contar con datos de un cliente real por motivos de seguridad, privacidad y acuerdos de confidencialidad; se ha decidido generar resultados que puedan ser reales y/o cercanos a una situación de un cliente de una empresa consultora. Adicionalmente, estos datos han sido cotejados por expertos que han comprobado que los resultados generados podrían ser aproximados a un caso real.

Historia de Embotelladora S.A.

Embotelladora S.A. es una empresa familiar, fundada por Antonio Botella, que cuenta con más de 30 años de vida en la Comunidad Valenciana. Ha sabido sobrevivir a crisis, la competencia de las grandes marcas y el cambio generacional sin estancarse en el pasado.

Antonio tenía claro que en un mercado tan competitivo era imposible sobrevivir únicamente del agua y siempre supo invertir dónde y cuando tocaba. En la década de los 80 supo como satisfacer las necesidades de gran parte de las comarcas de la provincia y en los 90, mediante alianzas y trabajar con marcas blancas, consiguió estar en los mercados de media España.

Los problemas surgieron al entrar en el año 2002. Antonio, cercano a la jubilación, inició una revolución tecnológica para adaptarse a los nuevos tiempos y poder tener un inventario actualizado, intercomunicar los departamentos, tener una página web, etc. Quería copiar los pasos que estaban marcando los grandes pero sin que la empresa perdiera sus raíces.

Su preocupación principal era conseguir el logro de sus objetivos estratégicos a través del uso efectivo e innovador de esas nuevas tecnologías y así lograr excelencia operativa y mejorar de la calidad de la información para dar soporte a la toma de decisiones.

El hijo de Antonio, Toni Botella, toma el mando de la compañía en 2010 y decidió mantener una línea continuista y de mejora de la imagen de la compañía, siendo muestra de ello el proceso realizado para obtener una nueva ISO: la 27001. A pesar de la crisis económica, Embotelladora S.A. no se ha visto muy afectada y se encuentra

[27] es una metodología introducida aproximadamente en 1914 por la Universidad de Harvard para que los estudiantes de Derecho, durante su aprendizaje, se enfrentaran a situaciones reales donde debieran tomar decisiones, emitir juicios fundamentados, etc. Gracias a su éxito pasó a aplicarse en otros campos de enseñanza y en la actualidad es de uso común en universidades y escuelas de negocios.

entre las 100.000 empresas más importantes de España pero muy lejos de las grandes marcas.

A finales de 2012 llegó una oferta para suministrar como marca blanca de un supermercado de gran importancia a nivel nacional. Las negociaciones no llegaron a buen puerto, y en el órgano directivo de la compañía se sospecha que esta situación se debe a una filtración, pues en los último trimestre del 2012 perdió una serie de contratos se consideraban cerrados debido a la posesión por parte de la competencia de ciertos datos estratégicos extremadamente confidenciales de Embotelladora S.A.

Ante este escenario, Toni se reunió con el responsable del área de TI para ver qué solución había ante esta posible fuga de información. El responsable, Marco Bol, le propuso recurrir a los servicios de Consultora S.L.

Marco se puso en contacto con Consultora S.L y solicitó un presupuesto para llevar a cabo una serie de proyectos relativos a seguridad de la información, concretamente para realizar Test de Intrusión, tanto a nivel externo como interno, incluyendo un análisis detallado de la configuración de los servidores y dispositivos de red. Una vez aprobado, se procedió de forma inmediata a la ejecución de las pruebas y los informes reflejaron que efectivamente había graves problemas de seguridad en el ámbito técnico de sistemas y redes, en gran parte debidos a los dos servidores al estar obsoletos y configurados por defecto.

Como resultado de los trabajos realizados, se evidenció la falta de ciertos logs[28] necesarios en distintos sistemas de información para poder obtener un registro de las conexiones a los servidores críticos. Como recomendación de Consultora S.L., éstos se activaron y configuraron adecuadamente, y a través de ellos fue posible identificar el punto de entrada del atacante y solucionar el problema existente relativo a la fuga de datos. Ante el buen trabajo realizado por Consultora S.L, Embotelladora S.A. decidió contratarle más servicios: la auditoría interna respecto del estándar ISO 27001 para corregir las no conformidades arrastradas, un informe de cumplimiento con la LOPD y replicar los test de intrusión anualmente.

Ya en 2015, tras la realización de la auditoría bianual de LOPD, el consultor senior de Consultora S.L., para aportar valor añadido a sus servicios, decidió que además de los informes que entregaba habitualmente como conclusión de cada uno de sus trabajos, informaría de la situación actual en la que se encuentran sus clientes respecto a cada uno de los servicios contratados. La empresa embotelladora recibirá una hoja en formato Excel donde podría consultar de forma centralizada todos los resultados de tal forma que les ayude a tomar una decisión en cuanto a inversión económica y dedicación de esfuerzos en cuestión de Seguridad de la Información. Además, podría ser clave para evitar un estancamiento en la mejora continua de la citada embotelladora.

[28] traducido al español como bitácora, son ficheros que sirven para registrar los eventos acontecidos en el sistema.

Presentación de resultados

Marco Bol, nada más recibir el documento Excel, analizó los cuadros de mando de la herramienta (pueden verse en mayor detalle en los anexos II, III y IV).

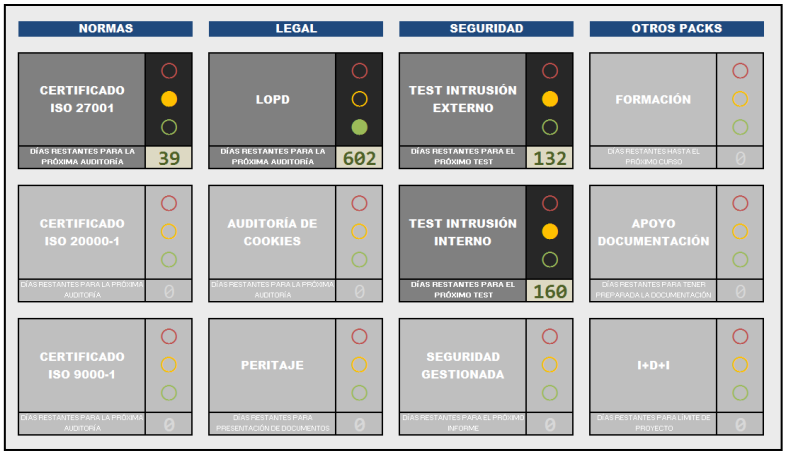


Ilustración 70. Cuadro de Mando General.

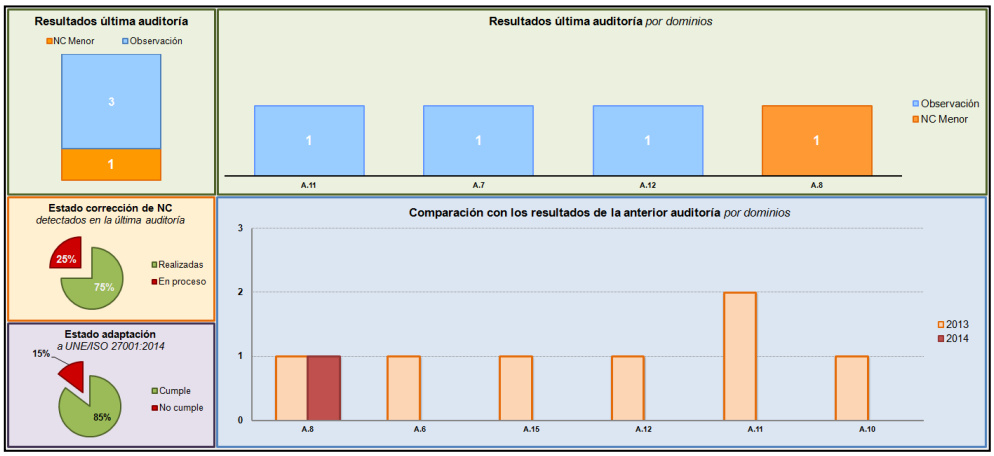


Ilustración 71. Cuadro de Mando de la ISO 27001.

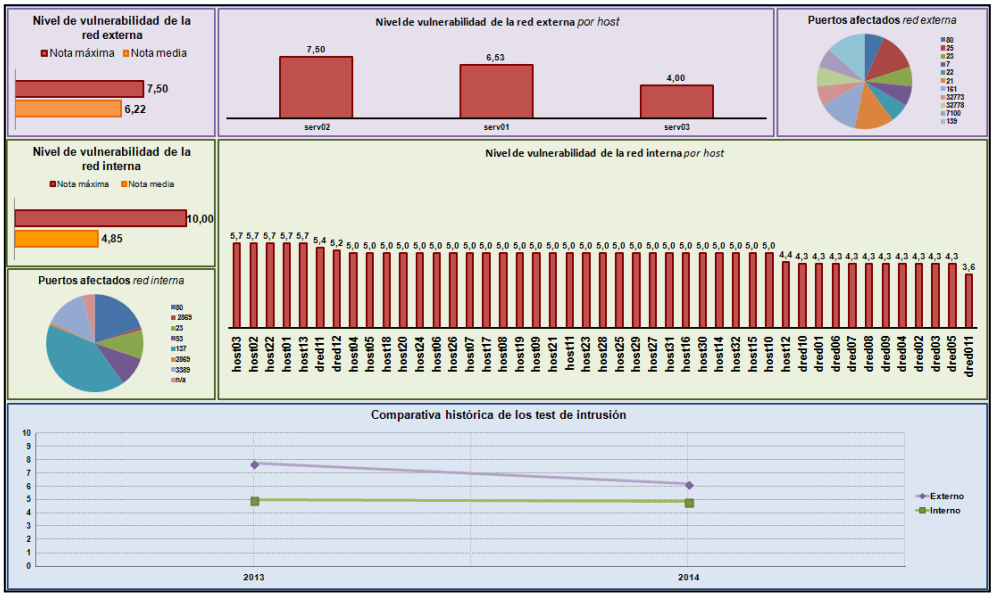


Ilustración 72. Cuadro de Mando del Test de Intrusión.

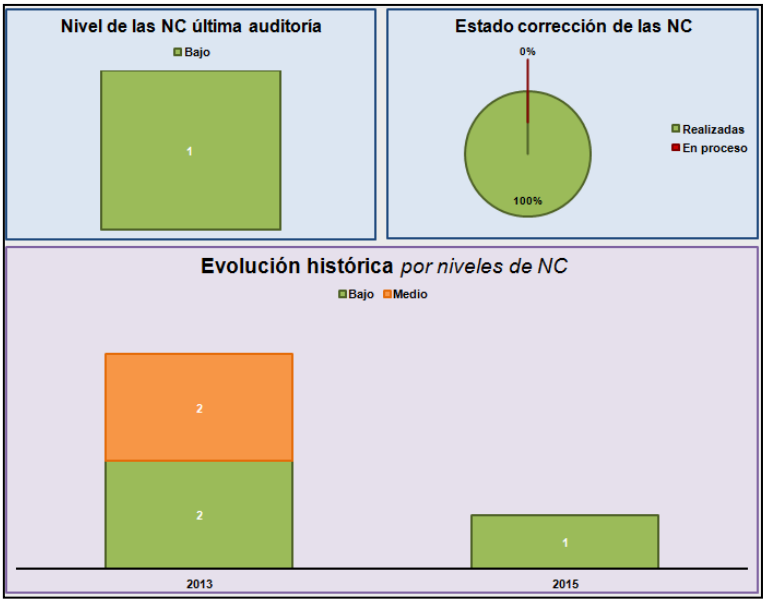


Ilustración 73. Cuadro de Mando de la LOPD.

A partir del análisis y con los informes generados desde la herramienta, Marco Bol concluyó que en cuanto a:

ISO 27001:

- Es donde deben centrarse los esfuerzos de su departamento, pues dispone poco más de un mes para la próxima auditoría y se descuidó dominio técnico. Si bien se han hecho esfuerzos y se ha corregido la mayor parte de las no conformidades, hay bastantes controles nuevos que podrían decantar la propuesta para la no renovación del certificado.

- Hay que ponerse en contacto con Consultora S.L. para realizar una nueva auditoría interna.

LOPD:

- Su departamento ha realizado un buen trabajo corrigiendo todo lo que se indicó en anteriores informes de cumplimiento.

- Sería conveniente que los empleados recién incorporados recibieran un cursillo básico para mantener el nivel de cumplimiento en materia de protección de datos en futuros informes.

Seguridad de la red externa:

- Se ha mejorado en casi dos puntos la seguridad a nivel externo. Se han corregido algunas configuraciones de los dos servidores principales, pero se encuentran obsoletos. En el nuevo servidor se ha detectado un número menor de vulnerabilidades, sería conveniente retirar los viejos y sustituirlos.

- Debe configurarse la configuración de los puertos. Existen puertos abiertos correspondientes a servicios que se han deshabilitado y que posteriormente no fueron estar cerrados.

Seguridad de la red interna:

- Se ha empeorado en cuestión de seguridad interna de un año a otro, a pesar del enorme trabajo realizado tras la fuga de información. Parece ser que una de las razones puede ser que algunos equipos están obsoletos.

- Aún existen equipos con Windows XP en bastantes salas. Paulatinamente, a lo largo del segundo semestre, se deberían cambiar en favor de Windows 7 pues XP no dispone de soporte de Microsoft desde 2014 y cuenta con vulnerabilidades críticas. Esto afecta al presupuesto en curso por lo que necesitarán que el departamento de finanzas compruebe la viabilidad de la inversión.

- Debe revisarse la configuración de los puertos y aprovechar para revisar los privilegios de los usuarios, pues no le consta que se utilizaran algunos de los puertos detectados como abiertos.

- Se debería aplazar la realización del test de intrusión interno a diciembre de 2015, una vez se haya finalizado la transición a Windows 7 y se hayan solventado aquellos problemas de seguridad más importantes.

A Marco le pareció realmente útil el cuadro de mandos proporcionado por Consultora S.L., pues con él ha podido tomar decisiones con más agilidad y también ha facilitado la comunicación tanto con sus superiores (por la facilidad para generar informes y el uso de pocos indicadores pero muy claros) como con sus subalternos (por disponer de un cuadro de mando para cada normativa o ítem analizado sabía con rapidez cuales eran los trabajadores directamente relacionados con el indicador a mejorar o resolver). La utilización del cuadro de mandos ha resultado mucho más fácil que analizar los resultados de informes de Auditorías de LOPD, de AENOR o de hojas y hojas con vulnerabilidades detectadas.

Marco se reunirá con Toni y el resto de los departamentos afectados para plantear las propuestas de modificaciones y/o mejoras y el efecto que sobre los presupuestos del año que viene puede tener cada una de las medidas que entiende que serían claves para la seguridad de la compañía.

8. Conclusiones

Valoraciones finales para la empresa-cliente

Como se ha comentado en el presente trabajo, Business Intelligence proporciona metodologías, aplicaciones y tecnologías que, como se ha podido evidenciar, permiten reunir, depurar y transformar los datos para poder extraer conocimiento y servir de soporte en la toma de decisiones y por lo tanto pueden ser de gran ayuda para la mejora de la estrategia de la empresa a todos los niveles y por lo tanto su competitividad. En este caso, nos hemos centrado en una área de interés, TIC, que tiene importantes repercusiones sobre el resto de la organización. Los datos han sido obtenidos a partir de las distintas auditorías relacionadas con el ámbito de las tecnologías de la información, y en concreto, de la privacidad y seguridad.

Mediante Microsoft Excel se ha Diseño una herramienta Business Intelligence que no solo sirve para poder analizar mediante indicadores la competitividad empresarial dentro del ámbito de la seguridad del área de TI o de la privacidad y tratamiento de los datos de los que se dispone, sino que también se busca mejorar la gestión de los distintos sistemas con los que cuentan las organizaciones y poder propulsar un cambio de cultura en la empresa.

Aunque su diseño implica la dedicación de muchas horas, pues se deben tomar muchos aspectos en cuenta, se ha conseguido el objetivo de facilitar la recopilación de la información y abstraer ideas, proporcionando además presentar informes y distribuir toda la información que se tenía de forma mucho más clara y accesible para todo el personal independientemente de si se tienen o no conocimientos al respecto. Se consigue "rebajar" la exigencia del conocimiento en la materia hasta el punto en el que, con pocos conocimientos en el área analizada, se puede entender si se va en la buena dirección o se presentan debilidades o desviaciones respecto a los objetivos marcados.

Valoraciones finales para la empresa- consultora

Adicionalmente, este trabajo realizado para la elaboración de los cuadros de mandos que hemos presentado puede servir para la elaboración de otros indicadores para otras Normas ISO, heredando así los componentes de las distintas pestañas, en cuestión de gráficas, informes, pies de página, etc. Por lo que el esfuerzo únicamente se centraría en la introducción de los datos y en la elaboración de que indicadores necesitaríamos disponer para hacer un buen seguimiento de la nueva norma así como la realización de mapeos con nuevas versiones de normas. Por ello para la empresa oferente de este tipo de servicio la disponibilidad de una herramienta como la desarrollada en este trabajo puede mejorar la calidad del servicio que ofrece y optimizar el coste del servicio y de la que en alguna proporción podría beneficiarse el cliente.

Cabe destacar que este tipo de herramientas suelen desarrollarse a nivel interno en las empresas consultoras, a menor escala, y no es fácil encontrar documentos en la red donde se recoja, ni parcialmente, la funcionalidad proporcionada. Por ello, la elaboración y desarrollo de este trabajo fin de grado pueda dar como resultado una herramienta que podría comercializarse en el mercado

Valoraciones personales

Personalmente, me hubiera gustado haber podido desarrollar más la herramienta a nivel visual, poder dedicar más tiempo a la creación de nuevos indicadores, abarcar más Normas o realizar más mapeos e incluso entre distintas como pueda ser la ISO 27001 y la 9000. Ante la falta de tiempo y la imposibilidad de hacer un trabajo acotado dentro de las 300 horas correspondientes al Trabajo Final de Grado, se ha decido limitarlo.

Dejando de lado estos detalles, me ha gustado la temática y el enfoque que me ha permitido darle mi tutora a la idea inicial propuesta, pudiendo sentirme más cómodo tanto para la redacción como para el desarrollo de la herramienta. Adicionalmente, me ha resultado útil para aprender y profundizar en Business Intelligence, estudiar aspectos que desconocía y que eran necesarios reflejarlos en cada una de las pestañas de la herramienta. Todo ello sin contar la experiencia obtenida en Microsoft Excel. Como conclusión personal creo que este trabajo me ha permitido profundizar y ver con otras perspectivas el trabajo que actualmente estoy realizando en la consultora y al que me gustaría dedicar los esfuerzos de mi próximos años

Agradecimientos

Me gustaría agradecer a la Universidad Politécnica de Valencia, y en concreto a la Escuela Técnica Superior de Informática, estos años en los que no solo me he podido formar a nivel práctico y teórico, sino que también he adquirido conocimientos transversales y he podido acceder al mercado laboral, en el sector que deseaba e incluso antes de acabar la carrera.

Si bien estoy muy agradecido a buena parte de profesores de la ETSINF, me gustaría dar especialmente las gracias a aquellos con los que he coincidido en la especialización de Sistemas de Información y a mi tutora del Trabajo Final de Grado, Pilar Conesa, por la dirección, dedicación y esfuerzos realizados.

Fuera del ámbito universitario quiero agradecer a Auren, sobre todo a José Miguel Cardona y a Josep Cunyat, que me abrieran las puertas para realizar las prácticas de empresa y por formarme junto a un gran equipo de profesionales.

Finalmente, quiero dedicar este trabajo mi familia, a Júlia y a todos los amigos que me llevo de esta etapa de mi vida. Muchas gracias por todo.

9. Bibliografía

ABANLEX ABOGADOS. "Infracciones / Sanciones" <http://www.abanlex.com/areas-de-practica/proteccion-de-datos/servicios-abanlex/infracciones-sanciones/> [Consulta: 11 de marzo de 2015].

AENOR (2007). "Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. UNE-ISO/IEC 27001:2007". Madrid: AENOR.

AENOR (2014). "Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. UNE-ISO/IEC 27001:2014". Madrid: AENOR.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. "Principales derechos". <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/index-ides-idphp.php> [Consulta: 11 de marzo de 2015].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. "Inscripción de Ficheros". <https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/index-ides-idphp.php> [Consulta: 11 de marzo de 2015].

ARBOLEYA, H. et al. (2011). “Ingeniería de proyectos de explotación de información para PyMEs”. Red de Universidades con Carreras en Informática (RedUNCI). <http://sedici.unlp.edu.ar/bitstream/handle/10915/20017/Documento_completo.pdf?sequence=1>.

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD (AEC). Centro de conocimiento <http://www.aec.es/web/guest/centro-conocimiento/> [Consulta: 8 de marzo de 2015].

AXELOS. "ITIL". <https://www.axelos.com/best-practice-solutions/itil> [Consulta: 7 de mayo de 2015].

BITCOMPANY. <http://www.bitcompany.biz/wp-content/uploads/2012/02/que-es-itil.gif> [Consulta: 7 de mayo de 2015].

BSI GROUP (2013). "ISO-IEC 27001 Features and Benefits". <http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISOIEC27001-Features-and-Benefits-UK-EN.pdf>.

BSI GROUP (2013). "Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013. ISO/IEC 27001 Mapping guide". <http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf >.

BSI GROUP (2013). "Sistema de gestión ISO/IEC 27001 de Seguridad de la Información". <http://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/> [Consulta: 11 de marzo de 2015].

CALZADA, LETICIA y ABREU, J.L. (2009). "El impacto de las herramientas de inteligencia de negocios en la toma de decisiones de los ejecutivos". Daena: International Journal of Good Conscience. 4(2), p.16-52.

CAO, JAVIER (2011). "Medición de un SGSI: diseñando el cuadro de mandos (I)" en *INCIBE*<https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Medicion_de_un_SGSI_disenando_el_cuadro_de_mandos_I> [Consulta: 14 de marzo de 2015].

CORLETTI, ALEJANDRO y DE ALBA MUÑOZ, CARMEN (2008). "UNE–ISO/IEC 27001:2005 & LOPD (II)" en *Revista Dintel*. Normas y Estándares, pp.144-148. <http://www.revistadintel.es/Revista1/DocsNum20/Normas/Corletti.pdf>.

DIARIO ABC (2014). "El FBI confirma que investiga el ataque informático a Sony" en *ABC*.es <http://www.abc.es/tecnologia/20141202/rc-confirma-investiga-ataque-informatico-201412020132.html> [Consulta: 14 de marzo de 2015].

ELEVEN PATHS (2014). "Ocho siglas relacionadas con las vulnerabilidades (III): CVSS".<http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=1>. [Consulta: 11 de marzo de 2015].

ESPAÑA. Ley Orgánica 15/1999, de 13 de desembre, de Protección de Datos de Carácter Personal. *BOE*, 14 de desembre de 1999, núm. 298, p. 43088-43099 <https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf>.

GARTNER (2015). "Magic Quadrant for Business Intelligence and Analytics Platforms". <https://www.gartner.com/technology/reprints.do?id=1-2ACLP1P&ct=150220&st=sb> [Consulta: 2 de mayo de 2015].

GONZÁLEZ, M. (2015). "España es, tras EE UU y Reino Unido, el país que sufre más ciberataques" en El País. <http://politica.elpais.com/politica/2015/02/05/actualidad/1423136881_175042.html> [Consulta: 14 de marzo de 2015].

HERNÁNDEZ, M. et al. (2000). "Casos prácticos de administración y organización de empresas". Getafe (Madrid). Ediciones Pirámide, Grupo Anaya.

INFORMATION WEEK (2014). "Gartner BI Magic Quadrant: Winners & Losers" <http://www.informationweek.com/big-data/big-data-analytics/gartner-bi-magic-quadrant-winners-and-losers/a/d-id/1114013> [Consulta: 2 de mayo de 2015].

ISACA. "COBIT". <https://cobitonline.isaca.org/> [Consulta: 7 de mayo de 2015].

JIMÉNEZ, R. (2015). "Los háckers difunden películas de Sony y datos personales de actores" en *El País*. <http://tecnologia.elpais.com/tecnologia/2014/12/01/actualidad/1417419360_876637.html> [Consulta: 14 de marzo de 2015].

LAUDON, K. y LAUDON, J. (2008). "Sistemas de Información Gerencial. Administración de la empresa digital". México. Pearson Educación.

LUCKEVICH, M., MISNER, S. y VITT, E. (2003). "Business intelligence: técnicas de análisis para la toma de decisiones estratégicas". España. McGraw-Hill Interamericana de España.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. "NVD Common Vulnerability Scoring System Support v2" <https://nvd.nist.gov/cvss.cfm> [Consulta: 11 de marzo de 2015].

MICROSOFT. "Microsoft by the Numbers". <http://news.microsoft.com/bythenumbers/index.HTML> [Consulta: 8 de mayo de 2015].

MIFSUD, ELVIRA (2012). "MONOGRÁFICO: Introducción a la seguridad informática - Seguridad de la información / Seguridad informática" en *Observatorio Tecnologógico*. <http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=1> [Consulta: 2 de mayo de 2015].

PALOP, F. y VICENTE, J. M. (1999). "Vigilancia tecnológica e inteligencia competitiva. Su potencial para la empresa española". Departamento de Tecnología Electrónica Universidad de Valladolid.

SERVICIO DE INNOVACIÓN EDUCATIVA (2008). "El Método del Caso" en *Universidad Politécnica de Madrid*. p.4. <http://innovacioneducativa.upm.es/guias/MdC-guia.pdf >.

SYMANTEC (2014). "Dragonfly Western Energy Companies Under Sabotage" <http://blog.elevenpaths.com/2014/04/ocho-siglas-relacionadas-con-las.html> [Consulta: 14 de marzo de 2015].

10. Anexos

Anexo I. Bibliografía recomendada

Ante la imposibilidad de abarcar adecuadamente a nivel teórico en la profundidad que merecen algunos de los aspectos tratados, se adjunta la siguiente bibliografía con la intención de ampliar aquellos temas que se consideren oportunos.

ARIÑO, M. (2005). "Toma de decisiones y gobierno de organizaciones". Bilbao. Ediciones Deusto, Planeta de Agostini Profesional y Formación.

BREWSTER, E. et al. (2009). "IT Service Management. A Guide for ITIL Foundation Exam Candidates". Reino Unido. CPI Antony Rowe Ltd.

ISACA. Recursos de COBIT en español. <http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx>.

ISAF. Repositorio en *Sourceforge*. < http://sourceforge.net/projects/isstf/>.

ISECOM. Open Source Security Testing Methodology Manual (OSSTMM). <http://www.isecom.org/research/osstmm.html>

LIEBOWITZ, J. (2006). "Strategic Intelligence: Business Intelligence, Competitive Intelligence, and Knowledge Management". Auerbach Publications.

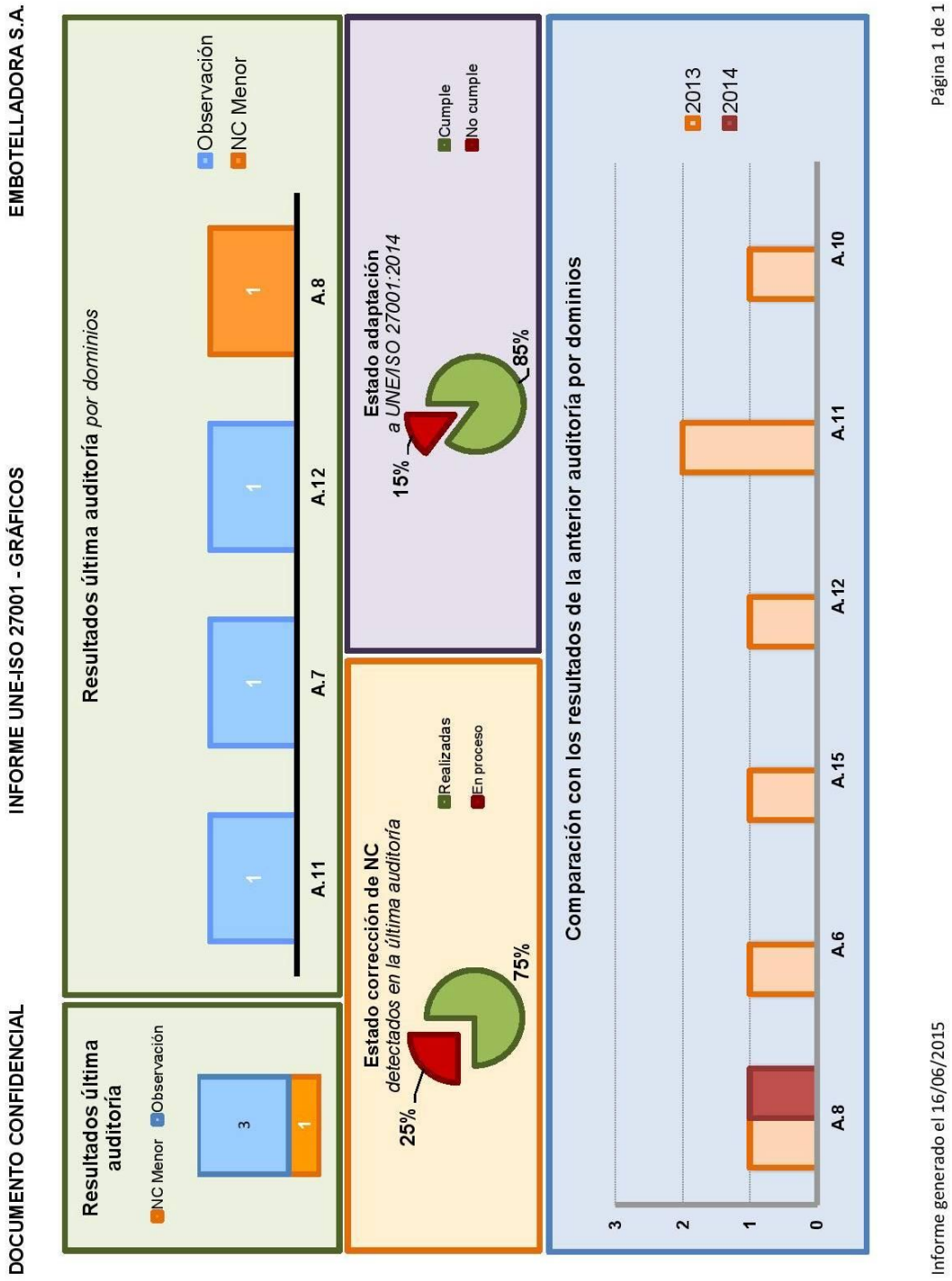
MUÑIZ, L. (2013). "Tablas Dinámicas con Excel aplicadas a la gestión ". Barcelona. Profit Editorial.

OWASP. <https://www.owasp.org/index.php/Main_Page>.

RAMOS, S. (2011). "Microsoft Business Intelligence: vea el cubo medio lleno". Albatera (Alicante). SolidQ.

RIPOLL, I. Web personal <http http://personales.upv.es/iripoll/>.

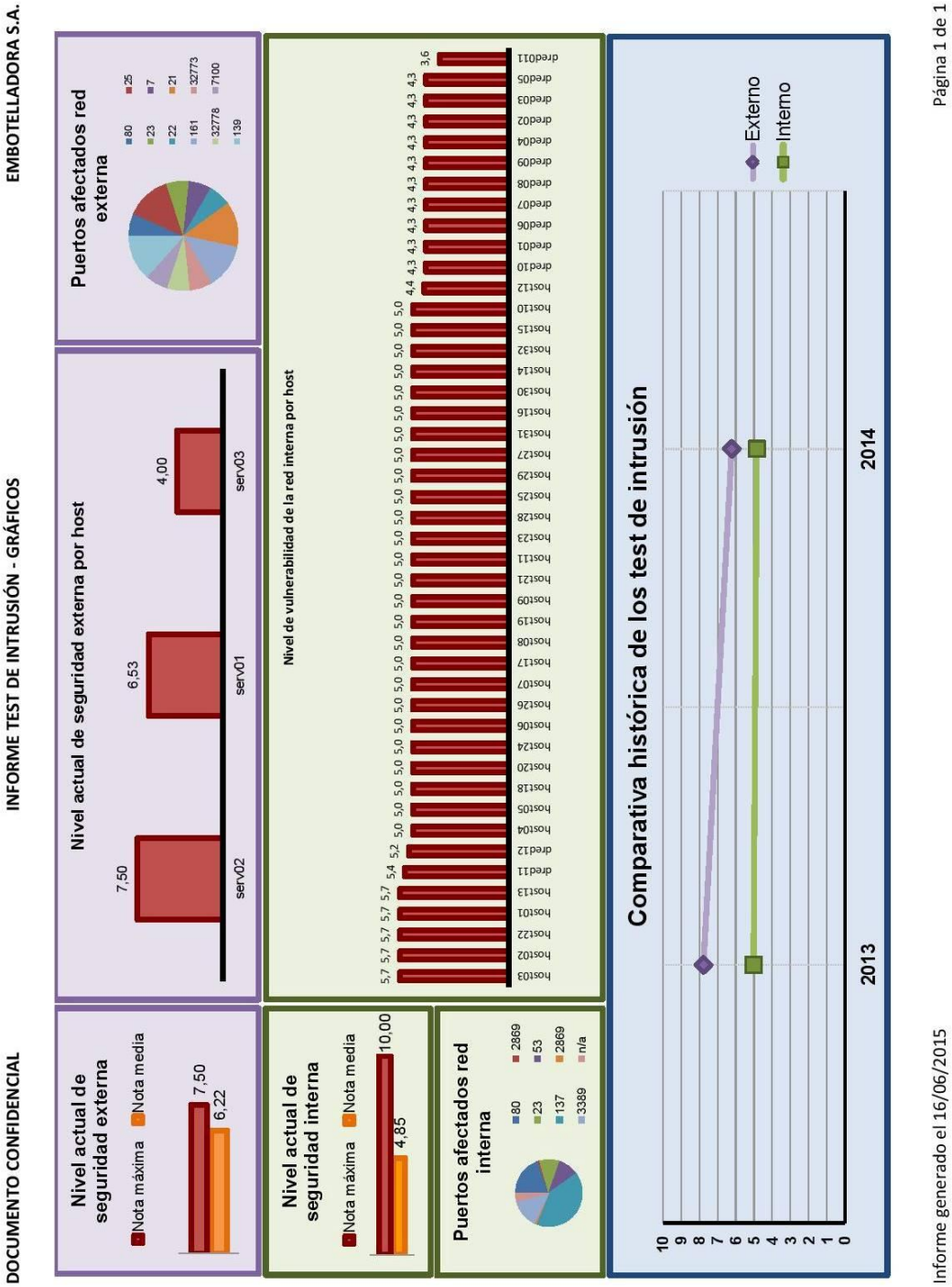
Anexo II. Informes generados para la ISO 27.001



FECHA	ÍTEM DETECTADO	BLOQUE	RESULTADO	FECHA LÍMITE ACCIÓN CORRECTIVA	FECHA ACCIÓN CORRECTIVA REALIZADA	TÍTULO DEL DOMINIO
2012	A.5.1.1	A.5	Observación	24/05/2013	17/06/2013	Documento de política de seguridad
2012	A.5.1.1	A.5	Observación	24/05/2013	17/06/2013	Revisión de política de seguridad
2012	A.6.1.7	A.6	Observación	24/05/2013	17/06/2013	Contacto con grupos de especial interés
2012	A.7.1.1	A.7	No Conformidad Mayor	26/10/2012	17/06/2013	Inventario de activos
2012	A.7.1.3	A.7	Observación	24/05/2013	17/06/2013	Uso aceptable de los activos
2012	A.7.2.2	A.7	Observación	24/05/2013	17/06/2013	Etiquetado y manipulado de información
2012	A.8.2.2	A.8	No Conformidad Menor	01/02/2013		Concienciación y formación
2012	A.9.2.2	A.9	No Conformidad Menor	26/10/2012	17/06/2013	Instalaciones de suministro
2012	A.10.4.1	A.10	No Conformidad Menor	01/02/2013		Controles contra código malicioso
2012	A.10.4.2	A.10	Observación	24/05/2013	17/06/2013	Controles contra código en cliente
2012	A.10.5.1	A.10	No Conformidad Mayor	26/10/2012	17/06/2013	Copias de seguridad
2012	A.10.6.2	A.10	No Conformidad Menor	01/02/2013	17/06/2013	Seguridad de los servicios de red
2012	A.10.8.4	A.10	Observación	24/05/2013	17/06/2013	Mensajería electrónica
2012	A.10.10.5	A.10	Observación	24/05/2013	17/06/2013	Registro de fallos
2012	A.11.3.1	A.11	No Conformidad Menor	24/05/2013		Uso de contraseñas
2012	A.11.4.5	A.11	No Conformidad Menor	01/02/2013	17/06/2013	Segregación de redes
2012	A.11.6.1	A.11	No Conformidad Menor	26/10/2012	17/06/2013	Restricción de acceso a la información
2012	A.12.6.1	A.12	No Conformidad Menor	01/02/2013		Control de vulnerabilidades técnicas
2012	A.15.3.1	A.15	Observación	24/05/2013		Controles de auditorías S.I.
2013	A.6.1.3	A.6	No Conformidad Menor	28/02/2014	05/06/2014	Asignación de responsabilidades
2013	A.8.2.2	A.8	No Conformidad Mayor	01/11/2013	05/06/2014	Concienciación y formación
2013	A.9.2.7	A.9	Observación	14/03/2014	05/06/2014	Retirada de materiales
2013	A.10.4.1	A.10	No Conformidad Mayor	01/11/2013	05/06/2014	Controles contra código malicioso
2013	A.11.1.1	A.11	No Conformidad Menor	14/03/2014		Política de control de acceso
2013	A.11.3.1	A.11	No Conformidad Menor	28/02/2014	05/06/2014	Uso de contraseñas
2013	A.12.3.1	A.12	Observación	14/03/2014	05/06/2014	Política de controles criptográficos
2013	A.12.6.1	A.12	No Conformidad Mayor	01/11/2013	05/06/2014	Control de vulnerabilidades técnicas
2013	A.14.1.5	A.14	Observación	14/03/2014		Pruebas y mantenimineto PCN
2013	A.15.1.4	A.15	Observación	14/03/2014		Prevención uso indebido de recursos
2013	A.15.3.1	A.15	No Conformidad Menor	28/02/2014	05/06/2014	Procedimientos de control de cambios

FECHA	ÍTEM DETECTADO	BLOQUE	RESULTADO	FECHA LÍMITE ACCIÓN CORRECTIVA	FECHA ACCIÓN CORRECTIVA REALIZADA	TÍTULO DEL DOMINIO
2014	A.7.1.1	A.7	Observación	16/01/2015	20/05/2015	Inventario de activos
2014	A.8.3.3	A.8	No Conformidad Menor	06/03/2015	20/05/2015	Retirar derechos de acceso
2014	A.11.1.1	A.11	Observación	15/05/2015	20/05/2015	Política de control de acceso
2014	A.12.5.5	A.12	Observación	25/07/2015		Externalización del desarrollo de SW

Anexo III. Informes generados para la Test de Intrusión



FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred01	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred01	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred01	53	5,0	Medio
2013	Interno	SMB Signing Required	dred01	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred01	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred01	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred01	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred02	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred02	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred02	53	5,0	Medio
2013	Interno	SMB Signing Required	dred02	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred02	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred02	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred02	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred03	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred03	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred03	53	5,0	Medio
2013	Interno	SMB Signing Required	dred03	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred03	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred03	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred03	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred04	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred04	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred04	53	5,0	Medio

FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2013	Interno	SMB Signing Required	dred04	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred04	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred04	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred04	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred05	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred05	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred05	53	5,0	Medio
2013	Interno	SMB Signing Required	dred05	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred05	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred05	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred05	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred06	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred06	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred06	53	5,0	Medio
2013	Interno	SMB Signing Required	dred06	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred06	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred06	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred06	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred07	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred07	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred07	53	5,0	Medio
2013	Interno	SMB Signing Required	dred07	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred07	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred07	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred07	80	2,6	Bajo

FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred08	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred08	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred08	53	5,0	Medio
2013	Interno	SMB Signing Required	dred08	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred08	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred08	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred08	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred09	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred09	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred09	53	5,0	Medio
2013	Interno	SMB Signing Required	dred09	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred09	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred09	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred09	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred10	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred10	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred10	53	5,0	Medio
2013	Interno	SMB Signing Required	dred10	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred10	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred10	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred10	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred11	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred11	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred11	53	5,0	Medio

FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2013	Interno	SMB Signing Required	dred11	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred11	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred11	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred11	80	2,6	Bajo
2013	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred12	2869	10,0	Crítico
2013	Interno	Unencrypted Telnet Server	dred12	23	5,8	Medio
2013	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred12	53	5,0	Medio
2013	Interno	SMB Signing Required	dred12	137	5,0	Medio
2013	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred12	2869	4,8	Medio
2013	Interno	IP Forwarding Enabled	dred12	80	3,2	Medio
2013	Interno	Web Server Uses Plain Text Authentication Forms	dred12	80	2,6	Bajo
2014	Interno	Unencrypted Telnet Server	dred01	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred01	53	5,0	Medio
2014	Interno	SMB Signing Required	dred01	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred01	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred01	80	2,6	Bajo
2014	Interno	Unencrypted Telnet Server	dred02	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred02	53	5,0	Medio
2014	Interno	SMB Signing Required	dred02	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred02	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred02	80	2,6	Bajo
2014	Interno	Unencrypted Telnet Server	dred03	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred03	53	5,0	Medio
2014	Interno	SMB Signing Required	dred03	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred03	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred03	80	2,6	Bajo

FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2014	Interno	Unencrypted Telnet Server	dred04	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred04	53	5,0	Medio
2014	Interno	SMB Signing Required	dred04	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred04	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred04	80	2,6	Bajo
2014	Interno	Unencrypted Telnet Server	dred05	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred05	53	5,0	Medio
2014	Interno	SMB Signing Required	dred05	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred05	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred05	80	2,6	Bajo
2014	Interno	Unencrypted Telnet Server	dred06	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred06	53	5,0	Medio
2014	Interno	SMB Signing Required	dred06	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred06	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred06	80	2,6	Bajo
2014	Interno	Unencrypted Telnet Server	dred07	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred07	53	5,0	Medio
2014	Interno	SMB Signing Required	dred07	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred07	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred07	80	2,6	Bajo
2014	Interno	Unencrypted Telnet Server	dred08	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred08	53	5,0	Medio
2014	Interno	SMB Signing Required	dred08	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred08	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred08	80	2,6	Bajo
2014	Interno	Unencrypted Telnet Server	dred09	23	5,8	Medio

FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred09	53	5,0	Medio
2014	Interno	SMB Signing Required	dred09	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred09	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred09	80	2,6	Bajo
2014	Interno	Unencrypted Telnet Server	dred10	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred10	53	5,0	Medio
2014	Interno	SMB Signing Required	dred10	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred10	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred10	80	2,6	Bajo
2014	Interno	Unencrypted Telnet Server	dred11	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred11	53	5,0	Medio
2014	Interno	SMB Signing Required	dred011	137	5,0	Medio
2014	Interno	IP Forwarding Enabled	dred011	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred011	80	2,6	Bajo
2014	Interno	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows	dred12	2869	10,0	Crítico
2014	Interno	Unencrypted Telnet Server	dred12	23	5,8	Medio
2014	Interno	DNS Server Cache Snooping Remote Information Disclosure	dred12	53	5,0	Medio
2014	Interno	SMB Signing Required	dred12	137	5,0	Medio
2014	Interno	UPnP Internet Gateway Device (IGD) Protocol Detection	dred12	2869	4,8	Medio
2014	Interno	IP Forwarding Enabled	dred12	80	3,2	Medio
2014	Interno	Web Server Uses Plain Text Authentication Forms	dred12	80	2,6	Bajo
2013	Externo	BSD Based telnetd telrcv Function Remote Command Execution	serv01	7	5,0	Medio
2013	Externo	Cisco Aironet Telnet Invalid Username/Password DoS	serv01	23	5,0	Medio
2013	Externo	OpenSSH < 3.4 Multiple Remote Overflows	serv01	22	10,0	Crítico
2013	Externo	ProFTPD STAT Command Remote DoS	serv01	21	7,1	Alto

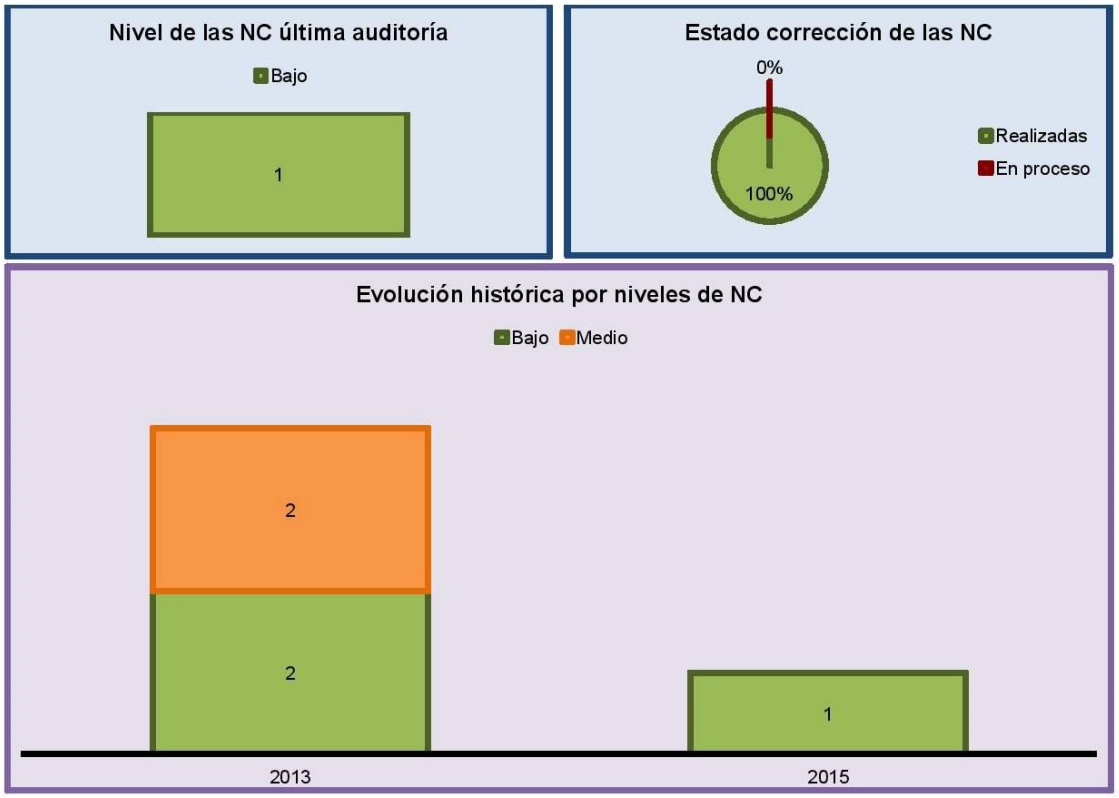
FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2013	Externo	Multiple FTPD glob Command Arbitrary Command Execution	serv01	21	7,5	Alto
2013	Externo	Sendmail < 8.11.2 -bt Option Local Overflow	serv01	25	7,2	Alto
2013	Externo	Sendmail Custom DNS Map TXT Query Overflow	serv01	25	7,5	Alto
2013	Externo	SNMP Agent Default Community Names	serv01	161	7,5	Alto
2013	Externo	Multiple Vendor Malformed SNMP Message-Handling DoS	serv01	161	10,0	Crítico
2013	Externo	Solaris cachefsd fscache_setup Function Remote Overflow	serv01	32773	10,0	Crítico
2013	Externo	Solaris snmpXdmid Long Indication Event Overflow	serv01	32778	10,0	Crítico
2013	Externo	X Font Service Crafted XFS Query Remote Overflow	serv01	7100	10,0	Crítico
2013	Externo	oops WWW Proxy Server Reverse DNS Response Overflow	serv02	80	7,5	Alto
2013	Externo	Microsoft Windows SMB Log In Possible	serv02	139	10,0	Crítico
2013	Externo	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration	serv02	139	2,3	Bajo
2014	Externo	ProFTPD STAT Command Remote DoS	serv01	21	7,1	Alto
2014	Externo	Multiple FTPD glob Command Arbitrary Command Execution	serv01	21	7,5	Alto
2014	Externo	Multiple Vendor Malformed SNMP Message-Handling DoS	serv01	161	5,0	Medio
2014	Externo	oops WWW Proxy Server Reverse DNS Response Overflow	serv02	80	7,5	Alto
2014	Externo	SSH Protocol Version 1 Session Key Retrieval	serv03	22	4,0	Medio
2013	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the	host01	3389	5,1	Medio
2013	Interno	Microsoft Windows SMB NULL Session Authentication	host01	137	5,0	Medio
2013	Interno	SMB Signing Required	host01	137	5,0	Medio
2013	Interno	Terminal Services Encryption Level is Medium or Low	host01	3389	4,3	Medio
2013	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host01	3389	3,3	Medio
2013	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	host02	3389	5,1	Medio
2013	Interno	Microsoft Windows SMB NULL Session Authentication	host02	137	5,0	Medio
2013	Interno	SMB Signing Required	host02	137	5,0	Medio
2013	Interno	Terminal Services Encryption Level is Medium or Low	host02	3389	4,3	Medio

FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2013	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host02	3389	3,3	Medio
2013	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	host03	3389	5,1	Medio
2013	Interno	Microsoft Windows SMB NULL Session Authentication	host03	137	5,0	Medio
2013	Interno	SMB Signing Required	host03	137	5,0	Medio
2013	Interno	Terminal Services Encryption Level is Medium or Low	host03	3389	4,3	Medio
2013	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host03	3389	3,3	Medio
2013	Interno	SMB Signing Required	host04	137	5,0	Medio
2013	Interno	SMB Signing Required	host05	137	5,0	Medio
2013	Interno	SMB Signing Required	host06	137	5,0	Medio
2013	Interno	SMB Signing Required	host07	137	5,0	Medio
2013	Interno	SMB Signing Required	host08	137	5,0	Medio
2013	Interno	SMB Signing Required	host09	137	5,0	Medio
2013	Interno	SMB Signing Required	host10	137	5,0	Medio
2013	Interno	SMB Signing Required	host11	137	5,0	Medio
2013	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	host12	3389	5,1	Medio
2013	Interno	Microsoft Windows SMB NULL Session Authentication	host12	137	5,0	Medio
2013	Interno	SMB Signing Required	host12	137	5,0	Medio
2013	Interno	Terminal Services Encryption Level is Medium or Low	host12	3389	4,3	Medio
2013	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host12	3389	3,3	Medio
2013	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	host13	3389	5,1	Medio
2013	Interno	Microsoft Windows SMB NULL Session Authentication	host13	137	5,0	Medio
2013	Interno	SMB Signing Required	host13	137	5,0	Medio
2013	Interno	Terminal Services Encryption Level is Medium or Low	host13	3389	4,3	Medio
2013	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host13	3389	3,3	Medio
2013	Interno	SMB Signing Required	host14	137	5,0	Medio

FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2013	Interno	SMB Signing Required	host15	137	5,0	Medio
2013	Interno	SMB Signing Required	host16	137	5,0	Medio
2013	Interno	SMB Signing Required	host17	137	5,0	Medio
2013	Interno	SMB Signing Required	host18	137	5,0	Medio
2013	Interno	SMB Signing Required	host19	137	5,0	Medio
2013	Interno	SMB Signing Required	host20	137	5,0	Medio
2013	Interno	SMB Signing Required	host21	137	5,0	Medio
2013	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	host22	3389	5,1	Medio
2013	Interno	Microsoft Windows SMB NULL Session Authentication	host22	137	5,0	Medio
2013	Interno	SMB Signing Required	host22	137	5,0	Medio
2013	Interno	Terminal Services Encryption Level is Medium or Low	host22	3389	4,3	Medio
2013	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host22	3389	3,3	Medio
2014	Interno	Microsoft Windows XP Unsupported Installation Detection	host01	n/a	10,0	Crítico
2014	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	host01	3389	6,4	Medio
2014	Interno	Microsoft Windows SMB NULL Session Authentication	host01	137	5,0	Medio
2014	Interno	SMB Signing Required	host01	137	5,0	Medio
2014	Interno	Terminal Services Encryption Level is Medium or Low	host01	3389	4,3	Medio
2014	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host01	3389	3,3	Medio
2014	Interno	Microsoft Windows XP Unsupported Installation Detection	host02	n/a	10,0	Crítico
2014	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	host02	3389	6,4	Medio
2014	Interno	Microsoft Windows SMB NULL Session Authentication	host02	137	5,0	Medio
2014	Interno	SMB Signing Required	host02	137	5,0	Medio
2014	Interno	Terminal Services Encryption Level is Medium or Low	host02	3389	4,3	Medio
2014	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host02	3389	3,3	Medio
2014	Interno	Microsoft Windows XP Unsupported Installation Detection	host03	n/a	10,0	Crítico

FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2014	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	host03	3389	6,4	Medio
2014	Interno	Microsoft Windows SMB NULL Session Authentication	host03	137	5,0	Medio
2014	Interno	SMB Signing Required	host03	137	5,0	Medio
2014	Interno	Terminal Services Encryption Level is Medium or Low	host03	3389	4,3	Medio
2014	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host03	3389	3,3	Medio
2014	Interno	SMB Signing Required	host04	137	5,0	Medio
2014	Interno	SMB Signing Required	host05	137	5,0	Medio
2014	Interno	SMB Signing Required	host06	137	5,0	Medio
2014	Interno	SMB Signing Required	host07	137	5,0	Medio
2014	Interno	SMB Signing Required	host08	137	5,0	Medio
2014	Interno	SMB Signing Required	host09	137	5,0	Medio
2014	Interno	SMB Signing Required	host10	137	5,0	Medio
2014	Interno	SMB Signing Required	host11	137	5,0	Medio
2014	Interno	Microsoft Windows SMB NULL Session Authentication	host12	137	5,0	Medio
2014	Interno	SMB Signing Required	host12	137	5,0	Medio
2014	Interno	Terminal Services Encryption Level is Medium or Low	host12	3389	4,3	Medio
2014	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host12	3389	3,3	Medio
2014	Interno	Microsoft Windows XP Unsupported Installation Detection	host13	n/a	10,0	Crítico
2014	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	host13	3389	6,4	Medio
2014	Interno	Microsoft Windows SMB NULL Session Authentication	host13	137	5,0	Medio
2014	Interno	SMB Signing Required	host13	137	5,0	Medio
2014	Interno	Terminal Services Encryption Level is Medium or Low	host13	3389	4,3	Medio
2014	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host13	3389	3,3	Medio
2014	Interno	SMB Signing Required	host14	137	5,0	Medio
2014	Interno	SMB Signing Required	host15	137	5,0	Medio
2014	Interno	SMB Signing Required	host16	137	5,0	Medio

FECHA	TIPO	VULNERABILIDAD DETECTADA	HOST AFECTADO	PORT	NOTA	NIVEL
2014	Interno	SMB Signing Required	host17	137	5,0	Medio
2014	Interno	SMB Signing Required	host18	137	5,0	Medio
2014	Interno	SMB Signing Required	host19	137	5,0	Medio
2014	Interno	SMB Signing Required	host20	137	5,0	Medio
2014	Interno	SMB Signing Required	host21	137	5,0	Medio
2014	Interno	Microsoft Windows XP Unsupported Installation Detection	host22	n/a	10,0	Crítico
2014	Interno	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	host22	3389	6,4	Medio
2014	Interno	Microsoft Windows SMB NULL Session Authentication	host22	137	5,0	Medio
2014	Interno	SMB Signing Required	host22	137	5,0	Medio
2014	Interno	Terminal Services Encryption Level is Medium or Low	host22	3389	4,3	Medio
2014	Interno	Terminal Services Encryption Level is not FIPS-140 Compliant	host22	3389	3,3	Medio
2014	Interno	SMB Signing Required	host23	137	5,0	Medio
2014	Interno	SMB Signing Required	host24	137	5,0	Medio
2014	Interno	SMB Signing Required	host25	137	5,0	Medio
2014	Interno	SMB Signing Required	host26	137	5,0	Medio
2014	Interno	SMB Signing Required	host27	137	5,0	Medio
2014	Interno	SMB Signing Required	host28	137	5,0	Medio
2014	Interno	SMB Signing Required	host29	137	5,0	Medio
2014	Interno	SMB Signing Required	host30	137	5,0	Medio
2014	Interno	SMB Signing Required	host31	137	5,0	Medio
2014	Interno	SMB Signing Required	host32	137	5,0	Medio


Nivel de las NC última auditoría
Bajo
1
Estado corrección de las NC
0%
100%
Realizadas
En proceso
Evolución histórica por niveles de NC
Bajo
Medio
2
2
1
2013
2015

DOCUMENTO CONFIDENCIAL **INFORME LOPD** **EMBOTELLADORA S.A.**

FECHA	ÍTEM DETECTADO	NIVEL	FECHA LÍMITE ACCIÓN CORRECTIVA	FECHA ACCIÓN CORRECTIVA REALIZADA	COMENTARIOS
2013	89	Bajo	01/03/2013		Funciones y obligaciones del personal
2013	94	Medio	01/02/2013	01/02/2013	Copias de seguridad
2013	98	Bajo	01/03/2013	01/02/2013	Registro de incidencias
2013	104	Medio	01/02/2013	01/02/2013	Copias de seguridad
2015	89	Bajo	07/02/2015	07/02/2015	Funciones y obligaciones del personal

Anexo V. Puertos comunes

A continuación se muestra una lista de puertos comunes o bien conocidos para ser usados tanto por servicios TCP o UDP.

Puerto/protocolo	Descripción
1/tcp	Multiplexor TCP
7/tcp	Protocolo Echo (Eco) Responde con eco a llamadas remotas
9/tcp	Protocolo Discard Elimina cualquier dato que recibe
13/tcp	Protocolo Daytime Fecha y hora actuales
17/tcp	Quote of the Day (Cita del Día)
19/tcp	Protocolo Chargen Generador de caracteres
20/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - datos
21/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - control
22/tcp	SSH, scp, SFTP
23/tcp	Telnet manejo remoto de equipo, inseguro
25/tcp	SMTP Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)
37/tcp	time (comando)
43/betocp	nicname
53/udp	DNS Domain Name System (Sistema de Nombres de Dominio), por ejemplo BIND9
53/tcp y udp	FaceTime
67/udp	BOOTP BootStrap Protocol (Server), también usado por DHCP
68/udp	BOOTP BootStrap Protocol (Client), también usado por DHCP
69/udp	TFTP Trivial File Transfer Protocol (Protocolo Trivial de Transferencia de Ficheros)
70/tcp	Gopher
79/tcp	Finger
80/tcp	HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) (WWW)
88/tcp	Kerberos Agente de autenticación
110/tcp	POP3 Post Office Protocol (E-mail)
111/tcp	sunrpc
113/tcp	ident (auth) antiguo sistema de identificación
119/tcp	NNTP usado en los grupos de noticias de usenet
123/udp	NTP Protocolo de sincronización de tiempo
135/tcp	epmap
137/tcp	NetBIOS Servicio de nombres
138/tcp	NetBIOS Servicio de envío de datagramas
139/tcp	NetBIOS Servicio de sesiones
143/tcp	IMAP4 Internet Message Access Protocol (E-mail)
161/udp	SNMP Simple Network Management Protocol
162/tcp	SNMP-trap
177/tcp	XDMCP Protocolo de gestión de displays en X11
389/tcp	LDAP Protocolo de acceso ligero a Bases de Datos
443/tcp	HTTPS/SSL usado para la transferencia segura de páginas web

Puerto/protocolo	Descripción
445/tcp	Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot) o también es usado por Microsoft-DS compartición de ficheros
465/tcp	SMTP Sobre SSL. Utilizado para el envío de correo electrónico (E-mail)
500/udp	IPSec ISAKMP, Autoridad de Seguridad Local
512/tcp	exec
513/tcp	Rlogin
514/udp	syslog usado para logs del sistema
520/udp	RIP Routing Information Protocol (Protocolo de Información de Enrutamiento)
591/tcp	FileMaker 6.0 *(alternativa para HTTP, ver puerto 80)*
631/tcp	CUPS sistema de impresión de Unix
666/tcp	identificación de Doom para jugar sobre TCP
690/tcp	VATP (Velneo Application Transfer Protocol) Protocolo de comunicaciones de Velneo
993/tcp	IMAP4 sobre SSL (E-mail)
995/tcp	POP3 sobre SSL (E-mail)
1080/tcp	SOCKS Proxy
1337/tcp	suele usarse en máquinas comprometidas o infectadas
1352/tcp	IBM Lotus Notes/Domino RCP
1433/tcp	Microsoft-SQL-Server
1434/tcp	Microsoft-SQL-Monitor
1494/tcp	Citrix MetaFrame Cliente ICA
1512/tcp	WINS Windows Internet Naming Service
1521/tcp	Oracle listener por defecto
1701/udp	Enrutamiento y Acceso Remoto para VPN con L2TP.
1720/udp	H.323
1723/tcp	Enrutamiento y Acceso Remoto para VPN con PPTP.
1761/tcp	Novell Zenworks Remote Control utility
1863/tcp	MSN Messenger
1935/tcp	FMS Flash Media Server
2049/tcp	NFS Archivos del sistema de red
2082/tcp	cPanel puerto por defecto
2083/tcp	CPanel puerto por defecto sobre SSL
2086/tcp	Web Host Manager puerto por defecto
2427/udp	Cisco MGCP
3030/tcp y udp	NetPanzer
3074/tcp	Xbox Live
3074/udp	Xbox Live
3128/tcp	HTTP usado por web caches y por defecto en Squid cache
3128/tcp	NDL-AAS
3306/tcp	MySQL sistema de gestión de bases de datos
3389/tcp	RDP (Remote Desktop Protocol) Terminal Server
3396/tcp	Novell agente de impresión NDPS

Puerto/protocolo	Descripción
3690/tcp	Subversion (sistema de control de versiones)
4662/tcp	eMule (aplicación de compartición de ficheros)
4672/udp	eMule (aplicación de compartición de ficheros)
4899/tcp	RAdmin (Remote Administrator), herramienta de administración remota (normalmente troyanos)
5000/tcp	Universal plug-and-play
5060/udp	Session Initiation Protocol (SIP)
5190/tcp	AOL y AOL Instant Messenger
5222/tcp	Jabber/XMPP conexión de cliente
5223/tcp	Jabber/XMPP puerto por defecto para conexiones de cliente SSL
5269/tcp	Jabber/XMPP conexión de servidor
5432/tcp	PostgreSQL sistema de gestión de bases de datos
5517/tcp	Setiqueue proyecto SETI@Home
5631/tcp	PC-Anywhere protocolo de escritorio remoto
5632/udp	PC-Anywhere protocolo de escritorio remoto
5400/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5500/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5600/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5700/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5800/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5900/tcp	VNC protocolo de escritorio remoto (conexión normal)
6000/tcp	X11 usado para X-windows
6112/udp	Blizzard
6129/tcp	Dameware Software conexión remota
6346/tcp	Gnutella compartición de ficheros (Limewire, etc.)
6347/udp	Gnutella
6348/udp	Gnutella
6349/udp	Gnutella
6350/udp	Gnutella
6355/udp	Gnutella
6667/tcp	IRC IRCU Internet Relay Chat
6881/tcp	BitTorrent puerto por defecto
6969/tcp	BitTorrent puerto de tracker
7100/tcp	Servidor de Fuentes X11
7100/udp	Servidor de Fuentes X11
8000/tcp	iRDMI por lo general, usado erróneamente en sustitución de 8080. También utilizado en el servidor de streaming ShoutCast.
8080/tcp	HTTP HTTP-ALT ver puerto 80. Tomcat lo usa como puerto por defecto.
8118/tcp	privoxy
9009/tcp	Pichat peer-to-peer chat server
9898/tcp	Gusano Dabber (troyano/virus)

Puerto/protocolo	Descripción
10000/tcp	Webmin (Administración remota web)
19226/tcp	Panda Security Puerto de comunicaciones de Panda Agent.
12345/tcp	NetBus en:NetBus (troyano/virus)
25565/tcp	Minecraft Puerto por defecto usado por servidores del juego.
31337/tcp	Back Orifice herramienta de administración remota (por lo general troyanos)
45003/tcp	Calivent herramienta de administración remota SSH con análisis de paquetes.

11. Índice de ilustraciones