Departamento de Informática
INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN

PROYECTO FIN DE CARRERA

AUDITORÍA INFORMÁTICA Y APLICACIÓN A UN CASO EN UNA EMPRESA REAL

Autor: Jorge Barrio Ibánez
NIA: 100040188

Tutor: Miguel Ángel Ramos González

Leganés, febrero de 2014

Título: AUDITORÍA INFORMÁTICA Y APLICACIÓN A UN CASO EN UNA EMPRESA REAL
Autor: JORGE BARRIO IBÁÑEZ
Director: MIGUEL ÁNGEL RAMOS GONZÁLEZ

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 2014 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Al fin, este parece el fin de un camino iniciado ya hace demasiado tiempo. Momentos duros, mucho trabajo... y por fin la recompensa.

En primer lugar quería agradecer a Miguel Ángel, sus consejos, atención, disponibilidad y paciencia en todo momento. Ha sido el culpable de que pudiera realizar este proyecto y finalizar la carrera.

También a mi amigo Dani por su apoyo constante, un referente donde fijarme y darme cuenta que todo es posible. Vicente, gracias por tus consejos y ayuda diarios.

Por último a mis padres, que me aguantaron durante todo este tiempo.

Gracias a todos.

Contenido

Ilustraciones

1. Resumen

El proyecto trata sobre la realización de una auditoría informática a una reconocida empresa del sector tecnológico. Tanto el nombre de la empresa como los datos técnicos tanto de procedimientos, sistemas, puestos,... serán ficticios por cuestiones de confidencialidad.

Dentro de la auditoría, se abordará tanto la parte teórica sobre lo que consiste en realizar una auditoría, hasta la realización de un estudio en profundidad sobre la empresa en lo que se refiere a la seguridad física y la seguridad a mantener sobre procedimientos y sistemas.

Para realizar esto, nos apoyaremos en los siguientes marcos: LOPD, ISO 27001 y COBIT 4.1, aunque especialmente usaremos la norma 27001 gracias a los controles que posee para su implementación. Gracias a estos mecanismos, podremos seguir un guión sobre las diferentes pautas a realizar y las recomendaciones a seguir para conseguir reunir toda la información necesaria y así poder detectar posibles deficiencias.

Una vez concluido el proceso de auditoría, realizaremos un informe sobre posibles deficiencias encontradas así como las recomendaciones más apropiadas para solucionarlas.

El proyecto no busca errores para culpabilizar o buscar responsables, sino que pretende ser una guía para la mejora de la seguridad en todos los sentidos.

2. Abstract

The project is carried out on the implementation of a computer auditing to a recognized company in the technology sector. Both the name of the company and the technical data of procedures, systems, jobs,... will be fictitious for confidentiality reasons.

Within the audit, it will be discussed both the theory part of what an audit is, until the realization of a detailed study of the company in terms of physical security and security to hold in procedures and systems.

To accomplish this, we'll rely on the following frames: LOPD, ISO 27001 and COBIT 4.1, although we use especially ISO 27001 thanks to its checks for implementation. With these techniques, we can follow a script about the different controls to be made and the recommendations for gathering all the necessary information and be able to identify possible deficiencies.

Once concluded the audit process, we'll make a report on any deficiencies found as well as the most appropriate recommendations to resolve them.

The project doesn't look up errors to blame or find responsible, but is intended to be a guide to improvement of security every way.

3. Introducción General

Desde hace ya varios años es impensable conocer el funcionamiento de una empresa sin el uso de las nuevas tecnologías integradas con los sistemas de información. Este hecho lleva consigo la necesidad de utilizar unas normas y seguir unas pautas de actuación para cumplir ciertos niveles de seguridad.

Desde que las diversas entidades de negocio de una empresa se fueron apoyando conjuntamente en la informática, el proceso de la auditoría toma un valor indispensable. Se tienen que cumplir una serie de normas en lo referente tanto a la seguridad física como a la seguridad de las operaciones y procedimientos internos.

En la actualidad, casi todas las empresas de medio-gran tamaño realizan sus propias auditorías externas, internas, o ambas. Esto les facilita el cumplir con todos los requerimientos legales que se les exigen y hace que mejore el funcionamiento de la empresa.

La motivación que nos ha llevado a la realización de este proyecto está en el hecho de estar trabajando en el departamento de sistemas de una reconocida empresa dedicada al ámbito tecnológico desde hace más de 4 años.

Desde aquí hemos podido observar la importancia de llevar un control sobre la seguridad fisca y sobre los sistemas de información. Estas auditorías resultan un punto de control muy importante sobre el funcionamiento interno de la empresa y de los medios de actuación de los empleados, dado que a menudo perdemos la conciencia sobre si lo que hacemos lo realizamos correctamente.

A veces suele ocurrir que estos procesos sobre la seguridad son esquivados o se buscan soluciones parche para salir del paso, en vez de buscar soluciones académicas y con vistas a solucionar posibles problemas futuros. En la medida en la que unas veces por prisas y otras por desconocimiento, a veces se adoptan soluciones en las que incurrimos en el uso de malas prácticas.

En este proyecto explicaremos qué es una auditoría informática, así como los marcos que se suelen usar para realizarla: LOPD, ISO 27001 y requisitos de seguridad física. También detallaremos los tipos de auditoría, los elementos que se precisan y las fases que se siguen para realizarla. Gracias a los marcos anteriormente utilizados y la ayuda del manual del uso de activos de *EMPRESA_X* establecemos los requisitos necesarios para cumplir con las normas de seguridad adecuadas.

Una vez explicado esto, explicaremos los procedimientos y el funcionamiento de los diferentes elementos y sistemas de información que existen y realizaremos una auditoría de software y comunicaciones sobre los elementos más importantes de la red.

Con estas dos partes, evaluamos un presupuesto sobre los costes de realizar dicha auditoría teniendo en cuenta las condiciones ideales y evaluaremos un informe de recomendaciones.

El objetivo de este proyecto es encontrar deficiencias en los procesos de actuación y de seguridad, agujeros de seguridad o malas prácticas en las que un usuario malintencionado o hacker pudiera hacer un daño a la empresa. También debemos

encontrar posibles debilidades que estén haciendo a la empresa perder recursos debido a malos hábitos.

Sobre la empresa a la que auditaremos, no podemos dar toda la información fidedigna y exacta, ya que incurriríamos en faltas sobre confidencialidad y facilitaríamos las debilidades a posibles atacantes. Por esto, en todo el documento denominaremos a nuestra empresa con el nombre *EMPRESA_X*.

4. Auditoría Informática

La auditoría informática es un elemento que aunque sea o parezca poco importante es esencial para determinar vulnerabilidades y deficiencias existentes en los sistemas de información en la actualidad.

Básicamente consiste en recoger, agrupar y evaluar las evidencias para ver si un sistema de información cumple con ciertos niveles de seguridad como la salvaguarda de documentación, controlar que el uso de recursos se gestionen correctamente y el mantenimiento de la integridad de los datos.

(Cocomsys, 2014)

Gracias a la auditoría, podemos explorar a fondo todo el funcionamiento de nuestros sistemas de información y poder detectar si estamos incurriendo en fallos o si tenemos agujeros de seguridad o errores de procedimiento.

Este proyecto va a tratar pues de analizar los sistemas de información de una empresa de la que no daremos datos identificativos y poder hacer una auditoría general de los sistemas que se utilizan, a fin de detectar posibles problemas o situaciones en la que se estén produciendo fallos de seguridad.

4.1. Introducción

4.1.1. Definición

Actualmente existen muchas definiciones, según donde consultemos o sobre qué es lo que auditemos, y nunca parece que haya una que refleje fielmente lo que es.

La **RAE** nos da esta definición: "*Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse*".

(RAE, 2014)

Esta definición es muy general y se puede aplicar a muchas materias distintas. No existe de modo específico una definición exacta sobre auditoría informática.

Por tanto, el objetivo es el de realizar un análisis de nuestros sistemas empleando o no el uso de programas informáticos.

Podemos entonces definir auditoría informática como **el conjunto de procedimientos y técnicas para evaluar, controlar un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente**.

(Acha Iturmendi, 1994)

4.1.2. Objetivo

Gracias a los conocimientos teóricos sobre auditoría en la Universidad Carlos III y a mi experiencia laboral en diversas empresas en departamentos de sistemas, voy a realizar este proyecto para mejorar eficiencia, eficacia, rentabilidad, seguridad y aseguramiento de la calidad sobre los sistemas informáticos existentes.

Todos los sistemas de información pueden tener debilidades de seguridad ya que la tecnología avanza a pasos agigantados y al gran número de desarrollos a nivel de software que se van creando. Es por ello por lo que debemos realizar análisis periódicos sobre los sistemas que tenemos y sobre los que vayamos añadiendo.

El objetivo de esta auditoría no es detectar fallos para encontrar un culpable, sino para que haya una mejora de rendimiento en todos los procesos en los que ocurra y una mejora sobre la seguridad de forma que estemos cubiertos por un posible ataque informático. Asimismo, gracias a la auditoría revisaremos las posibles deficiencias que haya en cuanto a seguridad física que tenga la empresa.

4.1.3. Ámbito de actuación

Fase en que se diseñan los límites de la auditoría en cuanto a la profundidad y la cantidad de tiempo para llevarla a cabo.

Es un apartado que es de difícil aplicación, ya que debemos de establecer unos límites que sean lo suficientemente amplios para comprender todas las necesidades que tenemos y no ser demasiado extenso para que no se alargue en el tiempo y las posibles soluciones que adoptemos no se vean obsoletas.

El alcance sobre la auditoría que realizaremos irá desde la propia seguridad física: control de acceso, identificación, elementos de seguridad pasivos y activos,... así como la seguridad de los sistemas de información en los PCs, servidores y elementos de comunicación. También evaluaremos que los procesos de gestión y procedimentales sean los correctos.

Respecto a los departamentos a evaluar serán todos: IT, Administración, Ventas, Marketing y Club, así como la delegación en Portugal. También evaluaremos los diferentes elementos que aunque no pertenezcan a un departamento único, serán del conjunto de la empresa.

4.1.4. Regulación

En España, no existe una normativa estricta relacionada con la auditoría informática, de hecho, no todos los profesionales que realizan auditorías tienen formación ni experiencia que garanticen que se hagan buenas auditorías.

Existe por tanto, este vacío sobre quién debe hacer las auditorías. A pesar de esto, existen diferentes metodologías a seguir que nos puedan asegurar cumplir con los objetivos de seguridad.

4.2. Tipos de auditoría informática: interna y externa

Existen dos tipos de auditorías según su origen:

Auditoría informática interna:

Esta auditoría se lleva a cabo dentro de la propia empresa, realizada por personal que pertenece a la empresa auditada. A pesar de ser realizada internamente, esta debe realizarse siempre siendo real e independiente.

Se reportarán los resultados al más alto nivel de la dirección de la organización y tendrá la función de asesora de control. Los miembros que realicen la auditoría deben cumplir una serie de pautas:

- Dependencia del orden superior
  Los auditores deberán depender directamente del director general o del comité de administración, pero nunca del departamento de informática o algún miembro de dicho departamento.

- Conocimiento de los auditores
  Dado que los auditores deben de tener conocimientos sobre los sistemas de información, es posible que estos provengan del departamento de informática. Es fundamental la labor de objetividad dado que auditarán en mayor o menor medida sus propios sistemas.

- Relación entre auditores
  Se debe evitar que los auditores tengan algún tipo de amistad o algún tipo de afecto hacia los trabajadores a los que auditarán. Esto repercutirá en la objetividad y la utilidad de la auditoría.

- No realizar otras funciones
  Los empleados encargados de realizar la auditoría no podrán realizar otra actividad incompatible al mismo tiempo.

Todas estas recomendaciones anteriores son necesarias, si bien existen otras dos que son aconsejables:

  - Contratación de personal externo
    Es bueno que se contrate a algún auditor externo como apoyo a los auditores internos, ya que estos a veces no son profesionales con conocimientos amplios ni tienen un conocimiento sobre otras entidades, como los externos.

  - Conocimiento sobre la propia empresa
    La auditoría interna tiene la ventaja de que los auditores tienen un gran conocimiento sobre todo lo que rodea a la empresa sobre los sistemas de información. También pueden conocer deficiencias que se estén produciendo y que sean difícilmente detectadas por un auditor externo.

Auditoría informática externa:

Esta auditoría tiene por objetivo realizar un estudio más en profundidad teniendo en cuenta que los encargados de realizar esta auditoría no tendrán contacto previo con ningún trabajador de la empresa auditada. Esto aumentará en mayor medida el nivel sobre la imparcialidad y objetividad de dicha auditoría. Detallaremos a continuación las características más importantes:

- Elección de la empresa

Como hemos indicado en la auditoría interna, uno de sus puntos desfavorables son los lazos que puedan existir entre los auditores con personal del departamento de informática. Esto no debe ocurrir en este caso.

- Proceso de contratación

La empresa auditada, deberá tener en cuenta en el momento de contratar a la empresa auditora varios factores como: ámbito, alcance, duración, resultados, coste,...

Es indispensable cerrar bien las condiciones del contrato, así como el aseguramiento del cumplimiento de los compromisos.

- Plan de trabajo previo

Será recomendable revisar posibles auditorías internas o externas anteriores, para apoyarnos en ellas sin perder la independencia y mejorar los procesos.

Comparando la auditoría externa con la interna, podemos destacar lo siguiente:

- ✓ Es recomendable si las circunstancias lo permiten, la combinación de los dos tipos de auditoría.
- ✓ Los auditores internos podrán complementar a los externos, y esto repercutirá en un mayor conocimiento y una mayor objetividad de los procesos.

(Lucena Prats, 2006)

4.3. El auditor informático

El auditor informático es la persona que va a revisar la seguridad, el control interno, la efectividad, la gestión del cambio y la integridad de la información. Será el encargado del control y la verificación de dichos controles.

La persona que realice el papel de auditor, deberá de cumplir ciertos aspectos como:

- conocimientos generales actualizados y especializados sobre toda clase de sistemas técnicos y tecnologías de la información
- conocimientos sobre normas y estándares aplicados a la auditoría informática
- conocimientos sobre organización en la empresa y procesos de los sistemas de información
- conocimientos sobre herramientas de control, monitorización y gestión de procesos,...

- conocimientos sobre la gestión de diversos sistemas como: sistemas operativos, bases de datos, cifrado de datos, redes locales,...

Junto con los aspectos anteriores, también deberá tener conocimientos sobre técnicas de evaluación de riesgos, muestreo, cálculos por operación, recopilación de información, análisis e interpretación de datos,...

(Jazmin, 2009)

4.4. Etapas de la metodología

Para la realización de la auditoría, debemos de seguir una serie de etapas para conseguir que la evaluación se realice correctamente. El buen análisis y estructuración de las etapas en el inicio de la auditoría hará que realicemos una auditoría lo más eficientemente posible.

4.4.1. Fase I. Definición de alcance y objetivos

En la primera fase se definen dos puntos imprescindibles como alcance y objetivos. Ambos puntos deberán ser analizados correctamente ya que una mala definición condicionará el resto de la auditoría.

Alcance

El alcance de la auditoría vendrá definido por los siguientes factores:

- entorno, límites y profundización de actuación en la realización de la auditoría informática
- acuerdo por escrito (auditor-cliente) si existen aéreas especiales o diversas sedes a auditar
- definir qué materias pueden ser auditables

Objetivos

El auditor debe analizar con gran exactitud los requerimientos del cliente y deberá hacer cumplir todos los procedimientos para alcanzar esos objetivos. Dentro de los objetivos diferenciaremos entre dos:

► ***Objetivos generales***

- controles generales: modo de funcionamiento, controles técnicos y sobre procedimientos

- comprobar las normas: propias de las instalaciones informáticas y procedimientos generales y específicos del departamento de informática

- comprobar que no existan contradicciones con otras normas

- comunicación con las personas que tengan poder de decisión en la empresa y a quien irá dirigido

► ***Objetivos específicos***

- ver la necesidad de auditar un procedimiento de gran complejidad
- contrastar los informes de la auditoría interna con la externa
- evaluación del funcionamiento de determinadas áreas en un departamento
- implementar el aumento de la seguridad, fiabilidad y calidad
- trabajar sobre la disminución de costes o plazos

4.4.2. Fase II. Estudio inicial

En esta segunda fase se buscará examinar la situación general de funciones y actividades generales de la informática. Los auditores deberán tener amplios conocimientos y definir los siguientes apartados:

- estructura organizativa del departamento de informática a auditar
- aplicaciones informáticas: procedimientos informáticos realizados en la empresa como los relacionados con Bases de Datos, Ficheros, ERP,...
- organigrama: estructura informática de la organización a auditar
- departamentos: describir sus funciones y sus relaciones jerárquicas
- flujos de información, tanto horizontales y oblicuos como extra departamentales y verticales
- número de puestos de trabajo y personas por puesto de trabajo

4.4.3. Fase III. Entorno operacional

En la fase operacional se mostrará el análisis físico del funcionamiento de la organización, así como los diferentes elementos hardware y software que lo componen.

- situación geográfica: situación del CPD, modo de funcionamiento y responsables
- inventario, análisis y configuración del hardware y software existente en la empresa
- esquema del mapa de conexionado de red y configuración

Para las aplicaciones de BBDD y ficheros estableceremos los siguientes requisitos:

- analizaremos la cantidad, el volumen y complejidad de las aplicaciones así como su diseño
- documentación: mejora la posible resolución de problemas
- complejidad de BBDD y ficheros: tamaño, número de accesos y actualización

4.4.4. Fase IV. Determinación de recursos de la Auditoría Informática

A partir del estudio inicial, se determinan los recursos humanos y materiales que se requieren para realizar la auditoría:

Recursos materiales:

- la mayoría serán proporcionados por la empresa auditada
- software y hardware: paquetes de utilidades de auditoría y herramientas para llevarla a cabo como PC, impresora,...

Recursos humanos:

- dependerá de la profundidad y áreas a auditar

A continuación detallaremos los perfiles profesionales de los auditores:

Profesión	Actividades y Conocimientos deseados
Informático Generalista	Con amplia experiencia en diferentes ramas (ej. explotación, desarrollo, sistemas,...)
Experto en Desarrollo de Proyectos	Amplia experiencia como jefe de proyectos. Conocedor de las metodologías y técnicas más importantes de desarrollo
Técnico de Sistemas	Experto en S.O. y software básico. Amplios conocimientos de Explotación
Experto en BBDD y su administración	Amplia experiencia en BBDD y su mantenimiento, así como en los productos utilizados para ellos. Conocimientos de explotación
Experto en Software de Comunicaciones	Conocimientos profundos de redes, líneas de comunicaciones, teleproceso,...
Experto en Explotación	Experiencia como responsable de algún CPD y en automatización de trabajos
Técnico de Organización	Buen coordinador y organizador. Especialista en el análisis de flujos de información
Técnico de Evaluación de Costes	Economista con conocimientos de informática

Tabla 1: Perfiles

4.4.5. Fase V. Actividades de la Auditoría Informática

En esta fase se definen técnicas y métodos a tener en cuenta para la recogida de información sobre los empleados y la organización:

Revisión

- análisis de la propia información y la obtenida en la auditoría
- entrevistas

  - con método preestablecido y preparación
  - gran elaboración de preguntas y orden
  - checklist: cuestionario minucioso, ordenado y estructurado por materias

- simulación

- muestreos

Herramientas

- cuestionario general
- cuestionario-checklist
- simuladores (aplicaciones generadores de datos)
- paquetes de Auditoría (generadores de programas)

  - rastrear los caminos de los datos
  - utilizados principalmente en auditorías no de informática
  - paquetes de parametrización de librerías

Otras actividades a tener en cuenta

- ***Movilización***. Mantener una reunión de planificación inicial para determinar el proceso más eficaz y rentable de obtención de información y el uso de especialistas y herramientas necesarias
- ***Entorno de control***. Registrar y evaluar el entorno de control de la empresa
- ***Información del negocio/sector***

  - Planificar la utilización de tecnología
  - Obtener comprensión del negocio, estructura, riesgos
  - Discutir preocupaciones, necesidades y expectativas

- ***Información sobre los sistemas y el entorno informático***

  - Evaluando los controles de supervisión

- ***Estrategia de auditoría.*** Reunión de planificación
- ***Preparar los programas de auditoría.*** Para las áreas de auditoría, analizando los riesgos de error y fraudes identificados
- ***Preparar un plan de tareas***

  - Calendario e información a recibir del cliente
  - Plan de tareas, con asignación de tiempos
  - Roles y responsabilidades de miembros del equipo auditor y estrategia de comunicación para revisar, asignar tareas y acordar objetivos
  - Establecer medidas para supervisar el progreso, incluyendo reuniones periódicas

- ***Comunicación del plan***

  - Informar a los miembros del equipo
  - Presentar al cliente el plan de auditoría a seguir

- ***Ejecución***

  - Documentar, evaluar y probar los controles de supervisión de las aplicaciones ejecutadas
  - Informar al cliente sobre estado del trabajo y conclusiones alcanzadas

- ***Otros procedimientos de auditoría.*** Informes finales
- ***Revisión.*** Completar los pasos y tareas del trabajo
- ***Finalización***

- Completar y revisar el tratamiento informático. Responder a excepciones
- Aspectos críticos importantes han sido resueltos, documentados y comunicados al cliente y al equipo
- Carta de manifestaciones del cliente
- Firma del auditor

- ***Información al cliente.*** Comunicar las debilidades significativas de control interno y las recomendaciones oportunas
- ***Evaluaciones.*** Calidad del servicio en relación con las expectativas del cliente

4.4.6. Fase VI. Informe final

- Titulo o Identificación del Informe: distinguirlo de otros informes
- Fecha de comienzo
- Miembros del equipo que realizarán la auditoría
- Nombre de la entidad auditada
- Seleccionar a los destinatarios que recibirán el informe
- Se finaliza con:
  - nombre, dirección y datos de registro del auditor
  - firma del auditor
  - fecha de emisión del Informe
- Objetivos y Alcance de la auditoría
  - estándares, especificaciones, prácticas y procedimientos utilizados
  - excepciones aplicadas
- Limitaciones encontradas y objetivos no auditados
- Materias consideradas en la auditoría
  - situación actual: hechos importantes y consolidados
  - tendencias de situación futura
  - puntos débiles y amenazas:
    - · hecho encontrado
    - · consecuencias del hecho
    - · repercusión del hecho (influencias sobre otros aspectos)
    - · conclusión del hecho
  - recomendaciones
  - redacción de la carta de presentación

4.4.7. Fase VII. Carta de Introducción o Presentación del Informe Final

La carta de presentación del Informe Final reflejará los siguientes atributos:

- Resumen en 3 o 4 folios del contenido del informe final
- Incluye fecha, naturaleza, objetivos y alcance de la auditoría
- Cuantifica la importancia de la áreas analizadas
- Proporciona una conclusión general, concretando las áreas de gran debilidad

- Presenta las debilidades en orden de importancia

Además hay que tener en cuenta que no se escribirán recomendaciones.

(Lombardi Pereira, 2010)
(Universidad de Belgrano, 2013)

4.5. Marcos y Referencias para la Auditoría Informática

A continuación explicaremos dos de los marcos que seguiremos para realizar la auditoría en EMPRESA_X: LOPD y la norma ISO 27001. También explicaremos otro marco utilizado ampliamente llamado COBIT, aunque no lo usaremos en la aplicación de este trabajo.

4.5.1. LOPD

La ley orgánica de Protección de Datos de Carácter Personal tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

(BOE, 1999)

Se entiende por "datos de carácter general personal" cualquier información concerniente a personas físicas identificadas o identificables:

- nombre, apellidos, DNI, dirección, datos bancarios, fotografía, huellas, voz, dirección de e-mail e imágenes.
- entre los datos de carácter personal hay unos especialmente sensibles que tienen mayores restricciones según la LOPD: ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual.

  ► Sólo pueden recogerse datos de carácter personal cuando sean pertinentes y no excesivos.

  ► Sólo pueden usarse los datos personales para la finalidad con la que fueron recogidos.

  ► Los datos serán cancelados cuando dejen de ser necesarios para la finalidad con la que fueron obtenidos.

  ► Los datos deben ser en todo momento exactos y reflejar la situación real del afectado.

El Reglamento de desarrollo de la LOPD 1720/2007 contiene lo siguiente:

- Especificaciones sobre el Documento de Seguridad
- Datos acerca de la Inscripción de Ficheros
- Especificaciones sobre los Procedimientos que deben existir

Previamente a la recogida de datos personales, el afectado debe ser informado de:

1. La existencia de un fichero que contendrá sus datos.

2. La posibilidad de ejercer sus derechos sobre los datos (rectificación, cancelación, acceso y oposición).

3. El nombre de la entidad y la dirección a la que pertenece el responsable del fichero.

► El tratamiento de datos personales requerirá el consentimiento inequívoco del afectado.

► Aquellos que intervengan en el tratamiento de los datos personales están obligados a guardar secreto profesional.

► Los datos personales sólo podrán ser comunicados o cedidos a un tercero para el cumplimiento de los fines autorizados.

Derechos ***A.R.C.O.*** de los interesados:

- Derecho de Acceso. Informar gratuitamente de todos los datos que se poseen sobre el interesado.
- Derecho de Rectificación. Corregir los datos que sean inexactos o incompletos.
- Derecho de Cancelación. Bloqueo de los datos cuando no sean adecuados impidiendo su tratamiento.
- Derecho de Oposición. Cese del tratamiento de los datos en casos con finalidad comercial o cuando no es necesario su consentimiento para el tratamiento.

(INTECO, 2014)

4.5.1.1. Controles LOPD

La LOPD no tiene unos controles asociados que nos permitan evaluar con certeza si se cumplen las obligaciones de la ley, así que nos apoyaremos para su comprobación en la herramienta "Evalúa" de la AEPD. Así pues, enumeraremos las normas que se siguen diferenciados en varios puntos:

(AEPD, 2013)

CONTROLES LOPD SOBRE EMPRESA_X

Registro de Ficheros
• En *EMPRESA_X*, se tratan datos de carácter personal necesarios para las reparaciones de los productos. Dicho tratamiento de datos personales se realiza en varios ficheros, los cuales están dentro de la política de respaldo y se mantienen en el tiempo como indica la ley. • También se almacenan datos sobre datos personales relativos a concursos o promociones que se realizan en el departamento de marketing. Igualmente, se guardan dichos datos. • Otros documentos son los relativos a los empleados de la empresa en el departamento de recursos humanos.

- La información tratada es notificada a la AEPD para su inscripción en el Registro General de Protección de Datos.

Información y Consentimiento

- Los datos relacionados con clientes son obtenidos directamente por los empleados de *EMPRESA_X* mediante una llamada telefónica. La recogida de datos se hace con el consentimiento de la persona afectada informándole sobre el contenido de la ley.
- No se recogen datos personales protegidos, como sexo, religión, afiliación política,... ni comisión de infracciones penales o administrativas. Tampoco se recopilan datos sobre menores de edad.
- Los datos también son tratados por terceras empresas, en el caso de *EMPRESA_X* son las empresas de mensajería y reparaciones las que colaboran.
- Sobre el proceso de toma de datos, se informa a la persona a la que pertenecen, de los aspectos básicos de protección de datos vía telefónicamente. Toda esta información es grabada telefónicamente y la persona afectada es avisada previamente de este hecho.
- Cuando se reciben datos de un tercero, se informa a la persona de los aspectos sobre la protección de datos en el plazo máximo de 3 meses a partir de la recogida.

Principios

- Los datos recogidos son los estrictamente necesarios para las finalidades propias de la organización de las que se informa al interesado en la recogida.
- Los datos recogidos se almacenan hasta que concluya la obligación legal y acabe ésta y se bloquearán hasta su borrado definitivo.
- Se dispone de un sistema para corregir errores y cancelar los datos cuando ya no se necesiten. Existe un método para la notificación de la cancelación o rectificación en caso de modificar los datos en un tercero.
- Respecto a los datos personales, se conoce su deber de secreto y confidencialidad y se hará hincapié de su importancia a las personas que traten la información.

Derechos A.R.C.O.

- Se conocen los derechos que la LOPD otorga a las personas y cuyos datos trata.
- Se facilitan los procedimientos para facilitar y garantizar el ejercicio de los derechos de oposición, acceso, rectificación y cancelación. Entre ellos, cómo se realizarán y los tiempos en llevarse a cabo. Dichos derechos se realizarán cuando quiera el afectado y serán gratuitos.
- Será posible el uso de los servicios anteriores en procesos automatizados siempre previa identificación del afectado.
- Se sigue un procedimiento sobre qué realizar en el caso de solicitud de acceso a los datos personales. Se conoce quién tiene la posesión de los datos, cómo los ha obtenido y si se han comunicado a terceros. Se tiene el compromiso de contestar en 1 mes y ofrecer el acceso en 10 días.

- Si se solicita la rectificación o cancelación de los datos personales, se atenderán en un plazo de 10 días.
- Si alguien solicita dejar de usar sus datos, se excluirán del tratamiento en 10 días.
- Si alguien revoca el consentimiento del tratamiento de datos, se atenderá la petición en 10 días.

Relación con Terceros

- Se realiza una comunicación sobre los datos de carácter general a terceros, solicitándose un consentimiento para realizarlo. Esta comunicación se regula por un contrato detallado donde se establecen las condiciones precisas conforme a la LOPD. En el contrato se prevé la prestación de servicios por parte de terceros. Los datos no se externalizan fuera de España.

Seguridad

- El nivel máximo de seguridad de los ficheros tratado es *bajo* y se adoptan las medidas de seguridad previstas en el reglamento de la LOPD.
- Se dispone de un documento de seguridad con las medidas relativas a la LOPD.
- Los empleados tienen el conocimiento sobre las obligaciones de seguridad.
- Cuando se contrata o diseña un software, se verifica que se cumplen las medidas de seguridad.
- Respecto a los datos personales en soportes no automatizados, se procede a su custodia y salvaguarda.

4.5.2. ISO 27001:2005

La norma ISO 27001 es un estándar internacional para la seguridad de la información que tiene como fin proteger la confidencialidad, integridad y disponibilidad de la información de un Sistema de Gestión de la Seguridad de la Información (SGSI).

La norma 27001 es parte de un conjunto de estándares definidos por la serie 27000 que engloba a más normas especializadas. La serie 27000 describe de forma general una introducción de los Sistemas de Gestión de la Seguridad de la Información y del ciclo Plan-Do-Check-Act.

La norma 27001:2005 tiene como referencia el estándar **ISO/IEC 27001** y cuyo objetivo se centra en los requisitos necesarios para cumplir con la seguridad. Además añade en su Anexo A los objetivos de control y controles que se desarrollan ampliamente en la ISO 27002:2005.

Ya que esta norma se centra ampliamente en la seguridad sobre un SGSI, a continuación detallaremos qué es un SGSI además de explicar todos los elementos que lo forman.

SGSI (Sistema de Gestión de la Seguridad de la Información)

Presentación

Un Sistema de Gestión de la Seguridad de la Información tiene como fin la protección de la información de una organización frente al uso, divulgación e interrupción no autorizada.

Objetivos

1- Asegurar la confidencialidad, disponibilidad e integridad de los datos.

2- Conocer y gestionar los riesgos en materia de seguridad de la información.

3- Facilitar el conocimiento a todo el personal implicado de la Política de Seguridad implantada en la organización.

4- Mejora continua en el tiempo

Importancia de la seguridad de la información

Un Sistema de Información se considera seguro si se encuentra libre de todo riesgo y daño. Es imposible garantizar la seguridad o la inviolabilidad absoluta de un sistema informático, por ello el objetivo que pretendemos es la gestión de la seguridad.

La seguridad de la información se entiende como la preservación de las siguientes características:

- Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas.
- Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, cuando lo necesiten.

Adicionalmente, deberán considerarse los conceptos de:

- ✓ Autenticidad y No Repudio: asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- ✓ Auditabilidad: considera que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- ✓ Protección frente a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Además, se debe impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- ✓ Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la organización.
- ✓ Confiabilidad de la información: que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Organización

En cuanto a la organización, podemos establecer 4 etapas diferenciadas de actuación:

Planificar (Plan) -> Planificación de los servicios

Realizar (Do) -> Realización de la gestión de los servicios

Actuar (Act) -> Mejora continua

Comprobar (Check) -> Medir y/o verificar

Comité de Seguridad

El Comité de Seguridad tendrá las siguientes funciones:

1. Revisar y proponer para su aprobación, la Política y las funciones generales en materia de seguridad de la información.

2. Supervisar cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

3. Tomar conocimiento y supervisar la investigación y monitorización de los incidentes relativos a la seguridad.

4. Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.

5. Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.

6. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

7. Promover la difusión y apoyo a la seguridad de la información.

8. Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información de la empresa frente a interrupciones imprevistas.

Además del Comité de Seguridad, en la organización deberá existir la figura del *Responsable de Seguridad*.

Responsable de Seguridad

Es la persona que cumple la función de supervisar el cumplimiento de la Política de Seguridad y de asesorar en materia de seguridad de la información a los integrantes de la empresa que así lo requieran.

Sus funciones serán las de implantar, coordinar y controlar las medidas definidas en las políticas, estándares y procedimientos de seguridad de la información.

El *Responsable de Seguridad* asistirá al personal de la empresa en materia de seguridad de la información y coordinará la interacción con especialistas y con los propietarios de la información, analizará el riesgo de los accesos de terceros a la

información y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

La organización deberá tener definida una Política de Seguridad que englobará todas las normas que se seguirán tanto para trabajadores, activos y procedimientos.

Importancia de la Política de Seguridad

La Política de Seguridad es un conjunto de normas que explican las directrices principales de seguridad de la información y de las comunicaciones a seguir por todos los usuarios y que serán objeto del debido control, monitorización y auditoría por parte de la empresa.

Aunque sean los miembros de la Dirección de la empresa los máximos responsables de liderar e implantar los debidos controles de seguridad de la información, su cumplimiento será responsabilidad de todos y cada uno de los que trabajan o colaboran en las actividades de la empresa.

Para conseguir la implantación efectiva de los objetivos que plantea la presente Política de Seguridad, se aportarán los medios y recursos necesarios, extendiendo su consecución progresivamente a todas las áreas de acuerdo con un modelo de mejora continua, que hará especial énfasis en la formación de los recursos humanos y en la medida de los resultados.

Respuesta frente a un incidente

Un incidente de seguridad es cualquier evento adverso en un sistema de información, aplicación, red,... que pueda comprometer la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información.

Puede ser causado mediante la explotación de alguna vulnerabilidad existente en los sistemas o por un intento o amenaza de romper los mecanismos de seguridad implantados.

Es obligatorio para todo el personal de la empresa notificar cualquier incidencia que afecte a la seguridad de los datos o presunción/sospecha de la misma, que se produzca en los sistemas de información y recopilar toda la información posible para analizar el problema.

Todos los empleados y contratistas de la empresa deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

La comunicación inmediata, por parte de los usuarios a los responsables de seguridad de cualquier evento, tal como: anomalía informática o de comunicaciones, mal funcionamiento, pérdida de control de los programas, desconexión súbita del sistema, comunicación externa sospechosa, presencia física de desconocidos no identificados en las dependencias,... se realizará a través del correo electrónico.

El procedimiento de comunicación y respuesta a incidentes deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el *Responsable de Seguridad* sea informado tan pronto como se haya detectado.

El Comité de Seguridad tomará razón de cualquier incidente evaluado como crítico, analizando y tomando las medidas para su corrección y prevención en el futuro.

Copias de Seguridad

Para garantizar la recuperación de los datos de los usuarios, en caso de pérdida o destrucción, se seguirán las siguientes reglas:

- Todos los usuarios deberán realizar copias de seguridad de sus unidades de almacenamiento locales (disco duro o dispositivos de almacenamiento internos o externos) de acuerdo con las instrucciones y medios facilitados.
- Los datos almacenados centralmente serán objeto, asimismo, de la realización de copias de seguridad.
- Las copias de seguridad serán custodiadas y conservadas de acuerdo a las instrucciones y medios de la empresa.
- La información almacenada en los ordenadores de los usuarios y que no haya sido copiada en los servidores no tiene garantizada su disponibilidad.

Se deben de seguir ciertas recomendaciones en lo que se refiere al uso de Internet, correo electrónico y protección contra virus, así como seguir unas buenas prácticas en el uso de los activos.

Navegación por Internet

Para garantizar el debido acceso a Internet y sus recursos por parte de los usuarios, se seguirán las reglas siguientes:

- La navegación por Internet se ajustará a las necesidades del desempeño de cada usuario, reconociéndose el valor y utilidad de sus contenidos y servicios a efectos de eficacia y eficiencia interna y externa.
- Queda terminantemente restringido el acceso de los usuarios a aquellas zonas de Internet consideradas inseguras o inapropiadas, de acuerdo con las prácticas de buen uso reconocidas y distribuidas.
- Para cumplir todo lo anterior, se establecerá la navegación a Internet a través de un proxy configurado a tal fin. Y para restringir la navegación por contenido, se configurará un filtro en el firewall.

Virus, Espías y Spam

Los virus actúan de muy diversas formas, pero la mayoría de las veces aprovechan debilidades del sistema operativo, fallos de diseño que se suelen denominar agujeros de seguridad.

- Es muy importante mantener actualizado el sistema operativo y en general todas las aplicaciones que se utilicen.
- La forma más habitual de ubicación de los virus es en archivos adjuntos de mensajes de correo de usuarios desconocidos.

- Para que se hagan efectivos los daños de los virus, es necesario que se activen, abriendo (ejecutando) el archivo que contiene el código dañino.
- No se deben abrir ficheros adjuntos que no provengan de una dirección de confianza. Hay que tener especialmente cuidado con los programas distribuidos de forma gratuita.

Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su consentimiento para su posible explotación fraudulenta.

- La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirla a empresas publicitarias u otras organizaciones enteradas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software.
- Pueden tener acceso por ejemplo a: el correo electrónico y contraseñas, dirección IP y DNS, teléfono, país, páginas que se visitan, qué tiempo se está en ellas y con qué frecuencia se regresa, qué software está instalado en el equipo y cual se descarga, qué compras se hacen por Internet, tarjeta de crédito y cuentas de banco.
- Los programas espía pueden ser instalados en un ordenador mediante un virus, un troyano que se distribuye por correo electrónico, o bien pueden estar ocultos en la instalación de un programa aparentemente inocuo.

Principales síntomas de infección:

- Cambio de la página de inicio, la de error y búsqueda del navegador
- Aparición de ventanas "pop-ups", incluso sin estar conectadas y sin tener el navegador abierto, la mayoría de temas comerciales
- Barras de búsquedas que no se pueden eliminar
- La navegación por la red se hace cada día más lenta, y con más problemas
- Es notable que tarda más en iniciar el ordenador
- Al hacer click en un vínculo, el usuario retorna de nuevo a la misma página que el software espía hace aparecer
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar
- Denegación de servicios de correo y mensajería instantánea

Los antivirus son capaces de eliminar programas espía. Se recomienda no usar un solo programa antiespía, sino una combinación de varios, que ofrece una protección mucho más compleja.

Como Spam se conoce al envío masivo e indiscriminado de mensajes de correo electrónico a direcciones capturadas en la Red.

- Aunque los mensajes con virus también se pueden considerar correo Spam, la mayoría del Spam consiste en mensajes comerciales que nos ofrecen muy variados servicios.
- El Spam que no lleva virus no es peligroso, pero sí muy molesto, ya que el resultado es que cuando consultamos nuestro correo cada vez encontramos más mensajes basura, mensajes con los que o bien quieren darnos a conocer los servicios que ofrecen o intentan contagiarnos un virus.
- Nuestra dirección la han obtenido de forma ilegal, "escuchando la red" o captándola de algún formulario.

El **Spam es ilegal**, por lo que podemos emprender acciones legales contra sus emisores, pero probablemente abandonemos, ya que las direcciones de origen que se usan siguen complejos redireccionamientos, o se trata de empresas en otros países, o no reconocen que sea suyo,...

- Podemos también intentar que dejen de enviarnos mensajes utilizando ese vínculo tan ad hoc que casi todos ponen al final del mensaje y que dice algo como: "Si desea que no le enviemos más mensajes, pulse aquí..."
- Con muchos de los remitentes esto funcionará, pero muchos otros usan ese vínculo para ¡hacernos caer en la trampa! Usan el vínculo para asegurarse de que la dirección está viva.
- Lo mejor en estos casos es eliminar los mensajes, para lo que las reglas de los clientes de correo resultan muy útiles, al hacer que se eliminen automáticamente cuando se reciben. Podemos añadir fácilmente una regla para la dirección desde la que hemos recibido un mensaje no deseado, de forma que se elimine cualquier mensaje que se reciba en el futuro desde esa dirección. Problema: las empresas van cambiando de dirección porque saben que se usan estas reglas.

Correo electrónico y Contraseñas

Para garantizar el debido uso del correo electrónico por parte de los usuarios, se seguirán las siguientes reglas:

- Las cuentas de correo electrónico asignadas a los usuarios para el desempeño de sus actividades profesionales son propiedad de la empresa.
- A todos los usuarios de las cuentas de correo electrónico de la empresa se les asigna una dirección electrónica y una contraseña, que serán estrictamente personales e intransferibles.
- La contraseña será configurada por el usuario de acuerdo con las instrucciones incluidas en la Política de uso de activos.
- Las contraseñas deberán renovarse periódicamente y no compartirlas.

Como reglas generales se recomienda:

1. No abrir nunca o reenviar mensajes de correo de remitentes desconocidos.

2. No abrir nunca o reenviar mensajes de correo de remitentes conocidos pero con asuntos en idiomas diferentes.

3. No abrir nunca los ficheros adjuntos de correos de procedencia dudosa.

4. No usar la misma contraseña para todo. Si alguien encuentra esta contraseña, esta persona podría tener la posibilidad de ingresar a cualquier elemento protegido.

5. Tratar de memorizar la contraseña sin escribirla. Alguien podría encontrar, intencionadamente o no, el pedazo de papel donde se escribió la contraseña.

(El portal de ISO 27001 en Español, 2014)

4.5.2.1. Controles 27001:2005

De acuerdo con todo lo anterior, podemos establecer una serie de controles definidos en el Anexo A de la ISO 27001 desde los capítulos A5 hasta la A15 y desarrollado más ampliamente en la ISO 27002.

Explicaremos a continuación los controles que se utilizan y cuáles de ellos se cumplen o no en la empresa a la que auditamos. Gracias a estos controles, tendremos una guía para auditar en parte todos nuestros sistemas y así ayudarnos a encontrar posibles deficiencias que pudieran existir.

Los controles sombreados en amarillo claro corresponden a controles que ya no están disponibles en la nueva versión de 2013.

CONTROLES ISO 27001:2005 SOBRE EMPRESA_X

CUMPLIMIENTO		
CONTROL	**?**	**OBSERVACIONES**
A.5 **Política de seguridad**		
A.5.1 **Política de seguridad de la información** Objetivo: *Proporcionar indicaciones para la gestión y soporte de la seguridad de la información de acuerdo con los requisitos empresariales y con la legislación y las normativas aplicables.*		
A.5.1.1 *Documento de política de seguridad de la información*	☑	La empresa dispone de un **documento de política de seguridad** de la información que se actualiza regularmente y que es accesible por los empleados.
A.5.1.2 *Revisión de la política de seguridad de la información*	☑	El documento de seguridad de la información se actualiza regularmente o cuando existe algún cambio importante.

Tabla 2: Controles_A5

A.6 **Aspectos organizativos de la seguridad de la información**		
A.6.1 **Organización interna** Objetivo: *Gestionar la seguridad de la información dentro de la organización.*		
A.6.1.1 *Comité de gestión de seguridad de la información*	☑	Existe un **comité de seguridad** encargado de realizar sugerencias o detectar posibles deficiencias, las cuáles serán notificadas a los trabajadores.
A.6.1.2 *Coordinación de la seguridad de la información*	☑	El comité de seguridad se reúne periódicamente para evaluar posibles cambios teniendo en cuenta los roles y funciones de cada trabajador.
A.6.1.3 *Asignación de responsabilidades relativas a la*	☑	Las responsabilidades de cada trabajador relativas a la seguridad de la información son establecidas por el comité.

seguridad de la información		
A.6.1.4 *Proceso de autorización de recursos para el procesado de la información*	☑	Cada nuevo objeto añadido al sistema de seguridad de la información es definido en las políticas de seguridad de la organización.
A.6.1.5 *Acuerdos de confidencialidad*	☑	Se revisan y establecen periódicamente los acuerdos de confidencialidad tanto con los trabajadores de la empresa como con colaboradores externos.
A.6.1.6 *Contacto con las autoridades*	☑	Se establecen los contactos pertinentes con las autoridades competentes.
A.6.1.7 *Contacto con grupos de especial interés*	☑	Se mantiene contacto y asesoramiento con empresas y consultorías sobre seguridad de la información y auditoría.
A.6.1.8 *Revisión independiente de la seguridad de la información*	☑	Se establecen periódicamente controles sobre la gestión de seguridad de la información a través de entidades independientes.
A.6.2 **Terceros** Objetivo: *Mantener la seguridad de la información de la organización y de los dispositivos de procesado de la información que son objeto de acceso, tratamiento, comunicación o gestión por terceros.*		
A.6.2.1 *Identificación de los riesgos derivados del acceso de terceros*	☑	Se definen los riesgos que implican la obtención de datos de la empresa por parte de terceros, y se establecen los controles pertinentes.
A.6.2.2 *Tratamiento de la seguridad en la relación con los clientes*	☑	Antes de facilitar cualquier tipo de documentación o acceso a los activos al cliente, se cumplen los requisitos de seguridad. Para ello, se firma un acuerdo de confidencialidad entre la empresa y el cliente.
A.6.2.3 *Tratamiento de la seguridad en contratos con terceros*	☑	Se establecen los requisitos de seguridad adecuados para los acuerdos con terceros en cualquiera de los casos de intercambio o acceso a la información o activos. Al igual que en el caso anterior, se firma un contrato de confidencialidad.

Tabla 3: Controles_A6

A.7 **Gestión de activos**		
A.7.1 **Responsabilidad sobre los activos** Objetivo: *Conseguir y mantener una protección adecuada de los activos de la organización.*		
A.7.1.1 *Inventario de activos*	☑	Existe un inventario sobre todos los activos de la empresa identificados en un fichero actualizable. **(*)** **Política de activos (16.1)**
A.7.1.2 *Propiedad de los activos*	☑	Cada uno de los activos o recursos de información tienen un propietario asignado, ya sea persona física o departamento.
A.7.1.3 *Uso aceptable de los activos*	☑	Quedan identificadas y documentadas las reglas para el **uso aceptable de la información y de los activos (4.5.6)** asociados con los recursos.
A.7.2 **Clasificación de la información** Objetivo: *Asegurar que la información recibe un nivel adecuado de protección.*		
A.7.2.1 *Directrices de clasificación*	☑	La información está clasificada según su valor, requisitos legales, sensibilidad y criticidad para la organización.
A.7.2.2 *Etiquetado y manipulado de la información*	☑	La información sensible está debidamente etiquetada según un sistema de clasificación esquemática para la organización.

Tabla 4: Controles_A7

A.8 **Seguridad ligada a los recursos humanos**
A.8.1 **Antes del empleo** Objetivo: *Asegurar que los empleados, los contratistas y los terceros entienden sus responsabilidades, y son*

adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos.		
A.8.1.1 *Funciones y responsabilidades*	☑	La responsabilidad de los empleados, contratistas y terceros se definen de acuerdo a la política de seguridad de la información de la organización.
A.8.1.2 *Investigación de antecedentes*	☑	Los datos sobre los candidatos al puesto de trabajo, contratistas o terceros se llevan a cabo dentro de la legislación vigente.
A.8.1.3 *Términos y condiciones de contratación*	☑	Tanto los candidatos, contratistas o terceros deben aceptar y firmar el acuerdo de responsabilidades de acuerdo a la seguridad de la información.
A.8.2 **Durante el empleo** Objetivo: *Asegurar que todos los empleados, contratistas y terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización, en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano.*		
A.8.2.1 *Responsabilidades de la Dirección*	☑	La dirección exige tanto a sus empleados, como contratistas y terceros, el cumplimiento de los procedimientos y políticas de la seguridad de la información.
A.8.2.2 *Concienciación, formación y capacitación en seguridad de la información*	☑	Tanto los empleados como los contratistas y terceros reciben la adecuada formación e información sobre nuevos cambios de procedimientos o políticas sobre seguridad periódicamente.
A.8.2.3 *Proceso disciplinario*	☑	Existe un proceso disciplinario ubicado en el reglamento de seguridad de la información de la empresa para los empleados que provoquen alguna violación de la seguridad.
A.8.3 **Cese del empleo a cambio de puesto de trabajo** Objetivo: *Asegurar que los empleados, contratistas y terceros abandonen la organización o cambien de puesto de trabajo de una manera ordenada.*		
A.8.3.1 *Responsabilidad del cese o cambio*	☑	Las condiciones por las que se produce un cese del empleo o cambio de puesto de trabajo están debidamente definidas por contrato.
A.8.3.2 *Devolución de activos*	☑	Tanto los empleados como contratistas y terceros deben devolver los activos al finalizar su empleo y/o contrato.
A.8.3.3 *Retirada de los derechos de acceso*	☑	Los derechos de acceso a la información de los empleados, contratistas o terceros serán retirados una vez concluida la relación laboral.

Tabla 5: Controles_A8

A.9 **Seguridad física y ambiental**		
A.9.1 **Áreas seguras** Objetivo: *Prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la organización.*		
A.9.1.1 *Perímetro de seguridad física*	☑	Cada uno de los puntos donde se encuentran alojados recursos de información se encuentran debidamente securizados mediante puertas, muros, o puntos con control de acceso.
A.9.1.2 *Controles físicos de entrada*	☑	Las áreas seguras están securizadas de forma que sólo pueda acceder personal autorizado.
A.9.1.3 *Seguridad de oficinas, despachos e instalaciones*	☑	Existen las diferentes medidas de seguridad de acceso sobre oficinas, despachos, salas,...
A.9.1.4 *Protección contra las amenazas externas y de origen ambiental*	☑	Existe una protección contra elementos naturales tales como: fuego, inundación, explosión,...
A.9.1.5 *Trabajo en áreas seguras*	☑	Existen las medidas de seguridad física necesarias para trabajar en las áreas seguras.
A.9.1.6 *Áreas de acceso público y de*	☑	Existe un control sobre la seguridad física en torno a las zonas de carga y descarga, para que el personal no autorizado no pueda acceder.

carga y descarga		
A.9.2 **Seguridad de los equipos** Objetivo: *Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización.*		
A.9.2.1 *Emplazamiento y protección de equipos*	☑	Los equipos están protegidos ante posibles amenazas medioambientales así como de accesos no autorizados.
A.9.2.2 *Instalaciones de suministro*	☑	Los equipos están debidamente protegidos contra fallos eléctricos.
A.9.2.3 *Seguridad del cableado*	☑	Tanto el cableado eléctrico como de telecomunicaciones está debidamente protegido y asegurado.
A.9.2.4 *Mantenimiento de los equipos*	☑	Los equipos reciben periódicamente un mantenimiento hardware que asegura su integridad y disponibilidad.
A.9.2.5 *Seguridad de los equipos fuera de las instalaciones*	☑	Los equipos situados fuera de la oficina o del reciento, o sin son activos que se sacan fueran de la oficina, cumplen con los requerimientos sobre seguridad establecidos.
A.9.2.6 *Reutilización o retirada segura de equipos*	☑	Todos los activos hardware y software que contengan datos sensibles son debidamente eliminados o destruidos para que no puedan ser accedidos, adjuntándose un justificante de destrucción de activos.
A.9.2.7 *Retirada de materiales propiedad de la empresa*	☑	Ninguno de los activos de la empresa puede sacarse de la oficina salvo autorización previa del responsable encargado.

Tabla 6. Controles_A9

A.10 **Gestión de comunicaciones y operaciones**		
A.10.1 **Responsabilidades y procedimientos de operación** Objetivo: *Asegurar el funcionamiento correcto y seguro de los recursos de procesamiento de la información.*		
A.10.1.1 *Documentación de los procedimientos de operación*	☑	La documentación sobre los procesos y procedimientos se realiza periódicamente y está a disposición de los empleados.
A.10.1.2 *Gestión de cambios*	☑	Los cambios producidos en los recursos y los sistemas de tratamiento de información son controlados.
A.10.1.3 *Segregación de tareas*	☑	Las tareas y áreas de responsabilidad están definidas, para que no se produzcan fugas o accesos no autorizados a la información.
A.10.1.4 *Separación de los recursos de desarrollo, prueba y operación*	☑	Se separan los recursos de desarrollo, de pruebas y de operación para reducir los accesos no autorizados o indebidos.
A.10.2 **Gestión de la provisión de servicios por terceros** Objetivo: *Implantar y mantener el nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros.*		
A.10.2.1 *Provisión de servicios*	☑	Se comprueban que los controles de seguridad, definiciones de los servicios y los niveles de provisión relacionados con terceros han sido implantados y mantenidos.
A.10.2.2 *Supervisión y revisión de los servicios prestados por terceros*	☑	Los servicios, informes y registros proporcionados por un tercero son revisados regularmente mediante auditorías.
A.10.2.3 *Gestión de cambios en los servicios prestados por terceros*	☑	Se gestionan los cambios en la provisión del servicio, mantenimiento, mejora de políticas y controles de seguridad.
A.10.3 **Planificación y aceptación del sistema** Objetivo: *Minimizar el riesgo de fallos de los sistemas.*		
A.10.3.1 *Gestión de capacidades*	☑	Se supervisan regularmente las actividades de los empleados sobre los recursos, realizando proyecciones de requisitos futuros.
A.10.3.2 *Aceptación del sistema*	☑	Se establecen las condiciones que deben cumplir los nuevos recursos, actualizaciones o mejoras sobre los procesos de gestión de los sistemas.
A.10.4 **Protección contra código malicioso y descargable**		

Objetivo: *Proteger la integridad del software y de la información.*		
A.10.4.1 *Controles contra el código malicioso*	☑	Se establecen los respectivos controles de detección, prevención y corrección para evitar el uso de código malicioso y su concienciación al usuario.
A.10.4.2 *Controles contra el código descargado en el cliente*	☑	El código descargable utilizado para el desarrollo de los programas, está sujeto al cumplimiento de las normas existentes.
A.10.5 **Copias de seguridad** Objetivo: *Mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información.*		
A.10.5.1 *Copias de seguridad de la información*	☑	Se tiene una política definida sobre las copias de seguridad. El backup se realiza periódicamente y se verifica su integridad y disponibilidad. **(*)** **Política de Backup (16.2)**
A.10.6 **Gestión de la seguridad de las redes** Objetivo: *Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.*		
A.10.6.1 *Controles de red*	☑	Se establecen diferentes sistemas para el control y la seguridad de la red y la información en tránsito. **(*)** **Herramientas de Control (16.3)**
A.10.6.2 *Seguridad de los servicios de red*	☑	Se establecen los requisitos de seguridad y gestión de la red, y se especifican dónde y quién los realiza.
A.10.7 **Manipulación de los soportes** Objetivo: *Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización.*		
A.10.7.1 *Gestión de soportes extraíbles*	☑	Se establece una gestión para controlar los soportes extraíbles.
A.10.7.2 *Retirada de soportes*	☑	Los soportes que no serán utilizados, se deberán retirar conforme a un procedimiento de baja de activos.
A.10.7.3 *Procedimientos de manipulación de la información*	☑	Se establecen procedimientos seguros para la manipulación y almacenamiento de la información.
A.10.7.4 *Seguridad de la documentación del sistema*	☑	La documentación está protegida contra accesos no autorizados.
A.10.8 **Intercambio de información** Objetivo: *Mantener la seguridad de la información y del software intercambiados dentro de una organización y con un tercero.*		
A.10.8.1 *Políticas y procedimientos de intercambio de información*	☑	Se establecen controles y procedimientos para el intercambio de información en los procesos de comunicación. **(*)** **Política Cloud (16.4)**
A.10.8.2 *Acuerdos de intercambio*	☑	Se establecen acuerdos para el intercambio de información entre la organización y terceros.
A.10.8.3 *Soportes físicos en tránsito*	☑	Los soportes físicos que salen de la organización están securizados ante accesos no autorizados.
A.10.8.4 *Mensajería electrónica*	☑	La información transmitida a través de mensajería electrónica está debidamente protegida.
A.10.8.5 *Sistemas de información empresariales*	☑	Se implantan políticas de seguridad para proteger la información que existe en el intercambio de información empresarial.
A.10.9 **Servicios de comercio electrónico** Objetivo: *Garantizar la seguridad de los servicios de comercio electrónico, y el uso seguro de los mismos.*		
A.10.9.1 *Comercio electrónico*	☑	La información transmitida a través del correo electrónico sobre redes públicas está debidamente protegida.
A.10.9.2 *Transacciones en línea*	☑	La información transmitida a través de transacciones en línea está debidamente protegida para evitar la pérdida de datos, revelación,...
A.10.9.3 *Información puesta a disposición pública*	☑	La información puesta de disposición pública es protegida a fin de evitar posibles modificaciones no autorizadas.
A.10.10 **Supervisión**		

Objetivo: *Detectar las actividades de procesamiento de la información no autorizadas.*		
A.10.10.1 *Registro de auditorías*	☑	Se lleva a cabo un registro sobre las auditorías realizadas en el pasado a fin de llevar un control y supervisión en el momento.
A.10.10.2 *Supervisión del uso del sistema*	☑	Se lleva a cabo un registro sobre la supervisión del uso de los recursos de la información.
A.10.10.3 *Protección de la información de los registros*	☑	Todo lo relativo a la gestión de los registros de información se protege para evitar el acceso o uso indebido.
A.10.10.4 *Registros de administración y operación*	☑	Se registran las actividades del administrador del sistema y/o operador. **(*)** **Política de Control (16.5)**
A.10.10.5 *Registro de fallos*	☑	Los fallos son registrados y documentados para su posterior análisis y solución.
A.10.10.6 *Sincronización del reloj*	☑	Los relojes de todos y cada uno de los sistemas están debidamente sincronizados por una fuente interna y externa NTP.

Tabla 7. Controles_A10

A.11 **Control de acceso**		
A.11.1 **Requisitos de negocio para el control de acceso** Objetivo: *Controlar el acceso a la información.*		
A.11.1.1 *Política de control de acceso*	☑	Se lleva a cabo una política de control de acceso basada en los intereses de la organización.
A.11.2 **Gestión de acceso de usuario** Objetivo: *Asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas.*		
A.11.2.1 *Registro de usuario*	☑	Existen unos controles para: alta, modificación y baja de los usuarios en los diferentes sistemas de control y de información. **(*)** **Procedimientos (16.6)**
A.11.2.2 *Gestión de privilegios*	☑	La asignación de privilegios está restringida y controlada.
A.11.2.3 *Gestión de contraseñas de usuario*	☑	La gestión de contraseñas es un proceso controlado. **(*)** **Política de Contraseñas (16.7)**
A.11.2.4 *Revisión de los derechos de acceso de usuario*	☑	La dirección debe revisar los permisos de acceso de los usuarios regularmente.
A.11.3 **Responsabilidades de usuario** Objetivo: *Prevenir el acceso de usuarios no autorizados, así como evitar el que se comprometa o se produzca el robo de la información o de los recursos de procesamiento de la información.*		
A.11.3.1 *Uso de contraseña*	☑	Se instruye al usuario y se aplican requerimientos de contraseñas conforme a las buenas prácticas.
A.11.3.2 *Equipo de usuario desatendido*	☑	Los equipos desatendidos tienen la protección suficiente.
A.11.3.3 *Política de puesto de trabajo despejado y pantalla limpia*	☑	El puesto de trabajo está libre de utensilios inútiles, y se establece una política sobre soportes extraíbles.
A.11.4 **Control de acceso a la red** Objetivo: Prevenir el acceso no autorizado a los servicios en red.		
A.11.4.1 *Política de uso de los servicios en red*	☑	Los usuarios sólo tienen permisos para los recursos que le son necesarios. **(*)** **Permisos de Usuario (16.8)**
A.11.4.2 *Autenticación de usuario para conexiones externas*	☑	Se lleva a cambo un procedimiento para que un usuario fuera de la organización pueda acceder a los recursos. **(*)** **Política de Acceso Remoto (16.9)**
A.11.4.3 *Identificación de los equipos en las redes*	☑	Cada uno de los equipos conectados a la red se encuentra registrado y localizado.
A.11.4.4	☑	Se controla el acceso físico y lógico a los puertos de diagnóstico y

Diagnóstico remoto y protección de los puertos de configuración		configuración.
A.11.4.5 *Segregación en las redes*	☑	Tanto los grupos de servicio como los usuarios y sistemas en la red están segregados.
A.11.4.6 *Control de la conexión a la red*	☑	Se establece un control y registro sobre las conexiones de cada usuario en la red. **(*)** **Control de Red por Usuario (16.10)**
A.11.4.7 *Control de encaminamiento (routing) de red*	☑	Se establece un control y seguimiento sobre las rutas que existen entre los diferentes recursos con la fuente de información para evitar usos indebidos.
A.11.5 **Control de acceso al sistema operativo** Objetivo*: Prevenir el acceso no autorizado a los sistemas operativos.*		
A.11.5.1 *Procedimientos seguros de inicio de sesión*	☑	Los accesos a los diferentes sistemas operativos se controlan y son seguros.
A.11.5.2 *Identificación y autenticación de usuario*	☑	Cada usuario tiene un identificador propio que le sirve para autenticarse en los diferentes sistemas.
A.11.5.3 *Sistema de gestión de contraseñas*	☑	Los sistemas de control de contraseñas son seguros y robustos, y pueden ser modificados interactivamente.
A.11.5.4 *Uso de los recursos del sistemas*	☑	Se controla el acceso a ciertas aplicaciones o programas que puedan invalidar la seguridad de los recursos.
A.11.5.5 *Desconexión automática de sesión*	☑	Las sesiones inactivas durante un periodo indefinido se cierran solas.
A.11.5.6 *Limitación del tiempo de conexión*	☑	Se establecen para ciertas aplicaciones críticas la limitación de uso en el tiempo.
A.11.6 **Control de acceso a las aplicaciones y a la información** Objetivo: *Prevenir el acceso no autorizado a la información que contienen las aplicaciones.*		
A.11.6.1 *Restricción del acceso a la información*	☑	Establecemos un control para restringir el acceso a la información de ciertas aplicaciones de acuerdo con la política de control.
A.11.6.2 *Aislamiento de sistemas sensibles*	☑	Los entornos sensibles están en lugares aislados y tienen accesos restringidos.
A.11.7 **Ordenadores portátiles y teletrabajo** Objetivo: *Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y servicios de teletrabajo.*		
A.11.7.1 *Ordenadores portátiles y comunicaciones móviles*	☑	Se establecen las respectivas medidas de seguridad para entornos móviles, ya sean ordenadores portátiles y dispositivos móviles. **(*)** **Seguridad en Dispositivos Móviles (16.11)**
A.11.7.2 *Teletrabajo*	☑	Se establece una política sobre las directrices a seguir en el uso del teletrabajo.

Tabla 8. Controles_A11

A.12 **Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A.12.1 **Requisitos de seguridad de los sistemas de información** Objetivo: *Garantizar que la seguridad está integrada en los sistemas de información.*		
A.12.1.1 *Análisis y especificación de los requisitos de seguridad*	☑	Cuando se diseñan o incorporan nuevos sistemas de información a la organización, se produce un análisis y especificación sobre los requisitos de seguridad necesarios.
A.12.2 **Tratamiento correcto de las aplicaciones** Objetivo: *Evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones.*		
A.12.2.1	☑	Se garantiza que la entrada de los datos en las aplicaciones es

Validación de los datos de entrada		validada.
A.12.2.2 *Control del procesamiento interno*	☑	En las aplicaciones se realiza la comprobación de validación a fin de evitar acciones malintencionadas.
A.12.2.3 *Integridad de los mensajes*	☑	Se cumplen todos los requisitos de seguridad para asegurar que la información es accedida por quien debe.
A.12.2.4 *Validación de los datos de salida*	☑	Se controlan los datos que genera la aplicación en la salida.
A.12.3 **Controles criptográficos** Objetivo: *Proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos.*		
A.12.3.1 *Política de uso de los controles criptográficos*	☑	Se establece una política de uso de controles criptográficos para preservar la información.
A.12.3.2 *Gestión de claves*	☑	Se establece una herramienta para la gestión de claves para dar soporte.
A.12.4 **Seguridad de los archivos de sistema** Objetivo: *Garantizar la seguridad de los archivos de sistema*		
A.12.4.1 *Control de software en explotación*	☑	Se lleva a cabo un control sobre la instalación de software en las máquinas.
A.12.4.2 *Protección de los datos de prueba del sistema*	☑	Los datos de prueba seleccionados son protegidos y controlados.
A.12.4.3 *Control de acceso al código fuente de los programas*	☑	Se restringe el acceso al código fuente de los programas.
A.12.5 **Seguridad en los procesos de desarrollo y soporte** Objetivo: *Mantener la seguridad del software y de la información de las aplicaciones.*		
A.12.5.1 *Procedimientos de control de cambios*	☑	Se controlan los procedimientos de implantaciones de cambio.
A.12.5.2 *Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo*	☑	Se revisan las aplicaciones de negocio exhaustivamente al realizar algún cambio sobre el sistema operativo.
A.12.5.3 *Restricciones a los cambios en los paquetes de software*	☑	Se establece un control riguroso sobre los cambios de software que se efectúan.
A.12.5.4 *Fugas de información*	☑	Deben evitarse situaciones que produzcan fugas de información.
A.12.5.5 *Externalización del desarrollo de software*	☑	La externalización del desarrollo de software es controlada.
A.12.6 **Gestión de la vulnerabilidad técnica** Objetivo: *Reducir los riesgos resultantes de la explotación de la vulnerabilidades técnicas publicadas*		
A.12.6.1 *Control de las vulnerabilidades técnicas*	☑	Se tiene conocimiento sobre las vulnerabilidades existentes en los sistemas utilizados, evaluando su situación y adoptando las medidas correctivas.

Tabla 9. Controles_A12

A.13 **Gestión de incidentes de seguridad de la información**		
A.13.1 **Notificación de eventos y puntos débiles de la seguridad de la información** Objetivo: *Asegurarse de que los eventos y las vulnerabilidades de la seguridad de la información, asociados con los sistemas de información, se comunican de manera que sea posible emprender las acciones correctivas oportunas.*		
A.13.1.1 *Notificación de los eventos de*	☑	Todos los eventos relacionados con la seguridad de la información deben comunicarse mediante los canales adecuados. **(*)** **Alta de**

seguridad de la información		**Incidencias (16.12)**
A.13.1.2 *Notificación de los puntos débiles de la seguridad*	☑	Cualquier organización o persona que trabaje con materiales de información de la organización, está obligada a notificar cualquier punto débil que exista.
A.13.2 **Gestión de incidentes de seguridad de la información y mejoras** Objetivo: *Garantizar que se aplica un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información.*		
A.13.2.1 *Responsabilidades y procedimientos*	☑	Se establecen los procedimientos y responsabilidades para que exista una adecuada rapidez en los incidentes de seguridad.
A.13.2.2 *Aprendizaje de los incidentes de seguridad de la información*	☑	Se establece un procedimiento que cuantifica el coste de los incidentes.
A.13.2.3 *Recopilación de evidencias*	☑	Cuando existe la implicación de otra entidad o persona que sea necesario adoptar acciones legales, se aportan evidencias conforme a la ley.

Tabla 10. Controles_A13

A.14 **Gestión de la continuidad**		
A.14.1 **Aspectos de seguridad de la información en la gestión de la continuidad del negocio** Objetivo: *Contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación.*		
A.14.1.1 *Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.*	☒	Debe crearse un plan sobre la continuidad de negocio que contemple los requisitos de seguridad de la información necesarios.
A.14.1.2 *Continuidad del negocio y evaluación de riesgos*	☑	Se evalúan los posibles eventos que retrasan o causan interrupciones en los procesos de negocio, así como la probabilidad, efectos y consecuencias de estos.
A.14.1.3 *Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información*	☒	Debe realizarse un plan para la restauración y disponibilidad de los proceso de negocio si ocurren interrupciones o fallos en estos.
A.14.1.4 *Marco de referencia para la planificación de la continuidad del negocio*	☒	Debe establecerse un procedimiento de referencia para la continuidad del negocio de manera que cumpla con los requisitos y tenga en cuenta las prioridades.
A.14.1.5 *Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio*	☒	Los planes de continuidad deben ser probados y actualizados regularmente.

Tabla 11. Controles_A14

A.15 **Cumplimiento**		
A.15.1 **Cumplimiento de los requisitos legales** Objetivo: *Evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad*		
A.15.1.1 *Identificación de la legislación aplicable*	☑	Todos los requisitos necesarios y su enfoque en la organización están debidamente definidos, documentados y actualizados.
A.15.1.2 *Derecho de propiedad intelectual (DPI)*	☑	Se implantan procedimientos adecuados para garantizar los requisitos legales y reglamentarios sobre el uso del material, a fin de evitar problemas con los derechos intelectuales y uso de licencias software/hardware.
A.15.1.3 *Protección de los documentos*	☑	Los documentos de la organización están protegidos contra la pérdida, destrucción o falsificación de acuerdo con los requisitos legales.

de la organización		
A.15.1.4 *Protección de datos y privacidad de la información personal*	☑	Se garantiza la protección y privacidad de la información de acuerdo con los requisitos legales.
A.15.1.5 *Prevención del uso indebido de los recursos de tratamiento de la información.*	☑	Se impide que los usuarios usen los recursos de información para usos indebidos.
A.15.1.6 *Regulación de los controles criptográficos*	☑	Los controles criptográficos se utilizan de acuerdo a los requisitos legales.
A.15.2 **Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico** Objetivo: *Asegurar que los sistemas cumplen las políticas y normas de seguridad de la organización*		
A.15.2.1 *Cumplimiento de las políticas y normas de seguridad*	☑	Los directores se aseguran que los planes de seguridad en su área se cumplen.
A.15.2.2 *Comprobación del cumplimiento técnico*	☑	Se comprueba periódicamente que los sistemas de información cumplen las normas de aplicación de la seguridad.
A.15.3 **Consideraciones sobre la auditoría de los sistemas de información** Objetivo: *Lograr que el proceso de auditoría de los sistemas de información alcance la máxima eficacia con las mínimas interferencias.*		
A.15.3.1 *Controles de auditoría de los sistemas de información*	☒	Los requisitos y actividades de auditoría sobre sistemas operativos deben ser planificados para minimizar el riego de interrupciones.
A.15.3.2 *Protección de las herramientas de auditoría de los sistemas de información*	☑	El acceso a las herramientas de auditoría está controlado para evitar su uso indebido.

Tabla 12. Controles_A15

4.5.3. ISO 27001:2013

En la nueva versión, hay varios cambios que mencionaremos a continuación:

- Las partes de definiciones de la versión 2005 han sido eliminadas o reubicadas en la ISO/IEC 27000.
- El modelo Plan-Do-Check-Act ha sido eliminado, ya que se considera que lo realmente importante es la mejora continua, y además existen otros modelos que pueden servir.
- Otro factor que cambia es el orden en que aparecen los requisitos: ahora el orden es irrelevante y lo importante es que se cumplan una vez realizada la implementación del SGSI.
- El número de secciones ha aumentado mientras que el número de controles con respecto a 2005 se ha reducido.

Los controles que se detallan a continuación se han añadido en la nueva versión 2013.

4.5.3.1. Controles 27001:2013

CONTROLES ISO 27001:2013 SOBRE EMPRESA_X

CUMPLIMIENTO		
CONTROL	**?**	**OBSERVACIONES**
A.14.2.1 *Política de desarrollo seguro. Reglas para el desarrollo de software y sistemas de información.*	☑	Existe una metodología a seguir para la creación de nuevo software u otros proyectos.
A.14.2.5 *Los procedimientos del sistema de desarrollo. Principios para la ingeniería de sistemas*	☑	Se lleva a cabo el desarrollo de proyectos conforme a las normas y estándares existentes.
A.14.2.6 *Entorno de desarrollo seguro. Establecer y proteger el entorno de desarrollo*	☑	Se llevan a cabo las correspondientes medidas para asegurar en entorno protegido y se actualizan periódicamente.
A.14.2.8 *Sistema de pruebas de seguridad. Las pruebas de funcionalidad de seguridad.*	☑	Se realizan cada cierto tiempo pruebas referidas a la seguridad y se documentan.
A.16.1.4 *Evaluación y decisión de los eventos de seguridad de información. Esto es parte de la gestión de incidentes.*	☑	Una vez detectada cualquier deficiencia en los procesos de seguridad, se analiza y de lleva a cabo una acción correctiva.
A.17.2.1 *Disponibilidad de instalaciones de procesamiento de información. Lograr redundancia.*	☑	Se analiza la posibilidad de establecer elementos redundantes que permitan la ejecución de tareas ante cualquier tipo de desastre.

Tabla 13. Controles_2013

4.5.4. COBIT 4.1

COBIT es un marco de referencia fundamentalmente para implementar las buenas prácticas y desarrollo de políticas en la organización, elaborado por ISACA. Formalmente serviría para investigar, desarrollar y promover un marco de trabajo autoritativo, actualizado e internacionalmente aceptado para el control de gobierno de TI para la adopción de las empresas y para el uso diario de los administradores de empresas, profesionales de TI y auditorías. Este control está definido por COBIT 4.1 y contiene 4 dominios, con varios procesos de TI por cada dominio:

1. Planear y Organizar

2. Adquirir e Implementar

3. Entregar y Dar Soporte

4. Monitorear y Evaluar

En total, de los cuatro dominios anteriores resultan 210 controles u objetivos de control, de los que la empresa debería de ejecutarlos para cumplir los objetivos.

Existe una nueva versión denominada COBIT 5.0, la cual tiene diversos cambios en lo que se refiere a cantidad y distribución de procesos. Existe un nuevo dominio dedicado a Evaluar, Dirigir y Monitorear que cubre alguna función de los ya existentes. Por tanto, se reorganizan los cuatro anteriores con diferentes procesos.

Aunque no es necesario para la implementación de COBIT el uso de un software para tal fin, existe uno llamado *COBIT Assesor* para realizar un seguimiento a las tareas.

No nos detendremos en este proyecto en explicar a fondo este marco, sólo lo mencionamos de forma superficial para uso informativo.

(ISACA, 2013)
(Marroquín Rivera & Rivas Merino, 2009)

4.5.5. Herramientas y técnicas para la Auditoría Informática

Dentro de las posibles formas de abordar la realización de una auditoría prestamos atención a un software llamado *PILAR*.

Este software permite la ejecución de un proyecto de Análisis de Riesgos mediante la metodología Magerit. Si queremos realizar un análisis de costes exhaustivo sobre nuestra entidad, será un buen método, aunque no es objeto de este proyecto.

(Ministerio de Hacienda, 2014)

La metodología Magerit sobre la que se basa PILAR trata de abordar el análisis de riesgos con un método definitivo. Dicha metodología se puede definir en estos puntos esenciales:

1. Identificar los activos

2. Establecer las dependencias de los activos

3. Valorar los activos

4. Dimensiones: evaluar confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad

5. Enumerar posibles amenazas

6. Determinar el impacto sobre los activos

7. Establecer salvaguardas sobre los activos

8. Detectar carencias y establecer mejoras

9. Análisis del coste-beneficio de las salvaguardas

10. Plan de acción y establecimiento de las salvaguardas

(Huerta, 2012)

4.5.6. Uso aceptable de activos

4.5.6.1. Objeto

El objeto de este documento es establecer las reglas principales de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

4.5.6.2. Ámbito de la aplicación

La dirección de *EMPRESA_X* proporciona las directrices específicas a los empleados implicados que tienen relación con los activos de la organización. Los empleados deben ser conscientes de las limitaciones existentes en el uso de la información, siendo estos responsables del uso de los recursos que exponen en este documento.

Los sistemas de información de *EMPRESA_X* así como los servicios que éstos prestan deben usarse de forma profesional. La organización asume los costes asociados al uso del correo electrónico, las comunicaciones y el acceso a Internet con fines profesionales.

No se permite el uso de estos servicios para fines ajenos a los intereses de *EMPRESA_X* o cualquier otro uso que infrinja las leyes.

4.5.6.3. Referencias

· Manual de Gestión de la Calidad y Seguridad de *EMPRESA_X* (EMPRESA_X, 2014)
· Norma *UNE-ISO 27001:2005* (ISO/IEC, 27001:2005, 2005) y *UNE-ISO 27001:2013* (ISO/IEC, 27001:2013, 2013)

4.5.6.4. Definiciones

No aplica.

4.5.6.5. Diagrama del proceso

La presente tabla describe los distintos flujos del proceso en la organización:

Proceso: **USO ACEPTABLE DE ACTIVOS**	
RESPONSABLES	· Director Gerente · Responsable de Seguridad
ENTRADAS	· Políticas de la empresa
SALIDAS	· Aceptación política de uso
REGISTROS	· Recibí de política de uso de activos
ACTIVIDADES DE SEGUIMIENTO	· Planificación del Sistema de Gestión · Revisión por la dirección
INFRAESTRUCTURAS Y EQUIPOS	· No necesario
CUALIFICACION PERSONAL	· A todos los interesados
DOCUMENTOS SOPORTE	· Legislación · Informes de Auditorías · Evaluación de riesgos

Tabla 14. Uso_Aceptable

4.5.6.6. Procedimiento

► *SEGURIDAD DE LA RED Y LOS SISTEMAS DE INFORMACIÓN*

La información que se encuentra alojada en los sistemas de *EMPRESA_X* debe tratarse como información interna. Hay que prestar especial atención en el tratamiento de la información relacionada con los clientes, bases de datos de proveedores o datos de carácter personal en general.

Internet es la fuente principal de amenazas que pueden exponer a la organización a riesgos relacionados con virus, spyware, spam y otras amenazas que ponen en peligro la confidencialidad, integridad y disponibilidad de la información.

Hay que tratar la información en formato electrónico con precaución, garantizando que ninguna persona no autorizada tiene acceso a los sistemas o datos de *EMPRESA_X*. Igualmente no se tiene que intentar acceder a documentos o sistemas para los cuales no se tiene permiso de acceso.

Bajo ninguna circunstancia se debe hacer:

- Utilizar un programa que no esté previamente instalado en tu PC.
- Utilizar un disco o un dispositivo extraíble en tu PC sin que previamente haya sido escaneado por un antivirus o su uso haya sido aprobado por *EMPRESA_X*.
- Descargar programas u otro material de Internet para utilizarlo en los sistemas de información.
- Hay que prestar especial atención con los archivos adjuntos en los correos electrónicos y otros programas de comunicación. Son una fuente potencial de virus o código malicioso. Por lo tanto nunca se tiene que abrir un archivo adjunto del que se desconozca su procedencia o su contenido sea sospechoso.

Nunca se debe intentar evitar los sistemas de seguridad de la empresa o de acceso a aéreas restringidas de la red. (ej. Carpetas del servidor con permisos de acceso). Cualquier intento constituye una violación de esta política.

► *CONTRASEÑAS*

Las contraseñas son un elemento crítico para la seguridad de la empresa. Las contraseñas se deben mantener en secreto. No se deben escribir o compartir con otras personas.

En el caso de que una persona necesite acceder a ciertos sistemas, el *Responsable de Seguridad* o *Administración* será el encargado de autorizar este acceso, si ha sido debidamente autorizado.

No se compartirán contraseñas con otros usuarios, ni se utilizarán contraseñas genéricas o de grupos. La contraseña identifica únicamente al usuario que la utiliza y se responsabiliza de la misma.

Todas las contraseñas de usuario deben cumplir con las siguientes características:

- Tener al menos una longitud de 6 caracteres
- Tener al menos un carácter numérico
- Incluir mayúsculas y minúsculas
- No formar parte de diccionarios (español o extranjero)
- No deben ser patrones fácilmente deducibles.
- No deben ser información personal como fecha de nacimiento, nombres de familia, mascotas,...

Aunque el sistema no requiera el cambio de contraseña, se recomienda su cambio al menos 1 vez al año. No puede utilizarse la contraseña utilizada anteriormente como contraseña actual. Esta responsabilidad recae sobre el *administrador del sistema*.

En caso de sospecha de que la contraseña haya sido comprometida o utilizada indebidamente por otra persona, se debe informar al *Responsable de Seguridad* sobre este incidente.

Se debe bloquear el PC en caso de ausencia de su puesto de trabajo, evitando que cualquier otro usuario pueda acceder a la información por la ausencia de éste.

Las contraseñas se almacenarán en un repositorio seguro controlado por el *Responsable de Seguridad* de *EMPRESA_X*.

► *CORREO ELECTRÓNICO Y MENSAJERÍA INSTANTÁNEA*

EMPRESA_X utiliza el email y la mensajería instantánea (ej. *GroupWise Messenger*) como medios de comunicación para las actividades de la organización. El uso personal de estas herramientas no está prohibido, aunque en ningún caso debe interferir con el desempeño de sus tareas.

Como recomendaciones y normas de uso se expone lo siguiente:

- Se debe evitar enviar archivos adjuntos de gran tamaño (más de *30 MB*)
- No se deben enviar presentaciones o mensajes de carácter lúdico que puedan herir la sensibilidad de algún empleado
- Identificar siempre destinatario y emisor del correo
- No hay que utilizar software de mensajería instantánea que previamente no se haya aprobado

Los mensajes de correo electrónico pueden utilizarse para exigir responsabilidad legal, por lo tanto deben aplicarse los mismos estándares y protocolos que para la correspondencia manuscrita. Nunca hay que enviar un correo electrónico que pueda dañar la imagen de *EMPRESA_X* o que no se pueda justificar.

Si se desea enviar información confidencial por email, debe enviarse de forma segura, es decir, cifrada o con contraseña. Es recomendable comprimir la información y protegerla mediante contraseña. En el caso de envío cifrado de información es posible acordar con el receptor el uso del software libre utilizado para el cifrado.

No se debe enviar por email la siguiente información:

- Material que viole las obligaciones de confidencialidad tanto con *EMPRESA_X* como con cualquier tercera parte interesada, así como incumplimiento de propiedad intelectual, copyright o cualquier otra normativa.
- Material difamatorio
- Material ofensivo
- Material falso tanto de *EMPRESA_X* como de cualquier empleado
- Cualquier otro material que pueda considerarse ilegal y que no esté contemplado en algunos de los puntos anteriores.

Los sistemas de comunicación de *EMPRESA_X* no se han de utilizar para cualquier propósito comercial que no esté dentro del ámbito de la organización.

No se puede leer, grabar o copiar cualquier mensaje que haya sido enviado a un empleado sin el consentimiento de éste.

En caso de tener alguna duda acerca del uso del correo electrónico con fines comerciales contactar con el *Responsable de Seguridad.*

► *USO DE INTERNET E INTERCAMBIO DE INFORMACIÓN*

Los principios de uso del correo electrónico y mensajería instantánea se aplican al uso de Internet y al intercambio de información.

Debemos ser conscientes de la importancia de Internet en el mundo empresarial. Hay que tener en cuenta la gran cantidad de información que contiene la red. Por tanto se deben comprobar y verificar las fuentes de información obtenida.

Para transacciones bancarias se utilizarán los acuerdos regulados con la entidad bancaria manteniendo siempre los niveles adecuados de seguridad antes de realizar cualquier operación.

Siempre que se envíe información a clientes de *EMPRESA_X* se deberá tener en cuenta el nivel de confidencialidad de la información. Hay que tener como referencia el marco legal del *R.D. 1720/2007* por el que se aprueba el desarrollo del reglamento de la *ley orgánica 15/1999 de protección de datos de carácter personal*.

En la obtención de información de las páginas web se puede infringir el copyright de dicha página. Se debe comprobar este punto antes de obtener la información.

Queda prohibida la visita de sitios, descarga de material, transferencia, almacenamiento de datos o imágenes que se encuadren dentro de estas categorías:

- Material difamatorio
- Material ofensivo, vulgar u obsceno
- Cualquier tipo de material que pueda considerarse ilegal

No se puede utilizar el sistema para acceder a juegos online.

EMPRESA_X se reserva el derecho de monitorizar el uso de Internet de acuerdo a la legislación y regulaciones vigentes. En caso de duda del nivel de privacidad, no se debe utilizar el servicio para acceder a algunos de los sitios web mencionados anteriormente.

► *ACCESO A LOS DATOS DE CARÁCTER PERSONAL*

Los accesos a datos de carácter personal se regirán mediante los acuerdos contractuales establecidos con los clientes en el marco de la *Ley Orgánica de Protección de Datos y su Reglamento*.

La violación de esta política constituye una falta grave que puede conllevar acciones legales por parte de las autoridades competentes.

► *USO DE LAS APLICACIONES WEB EN REMOTO*

El uso de aplicaciones web (aplicaciones de gestión, webmail,...) desde ubicaciones fuera de la oficina, y especialmente cuando estas son accedidas desde otros equipos (ordenadores personales, ordenadores públicos), expone a la organización a diferentes riesgos de seguridad tales como que personas que no tienen autorización vean información confidencial o tengan acceso a archivos temporales.

Para evitar esto se exponen las siguientes normas:

- Comprobar que no haya nadie observando la información mostrada en pantalla
- No descargar información en equipos que no sean propiedad de *EMPRESA_X*. Es posible que queden copias en las carpetas temporales de los sistemas a las que otras personas pueden tener acceso.
- Cerrar todas las sesiones utilizando los comandos habilitados para ello. Evitar dejar cualquier sesión abierta, explorador, carpetas temporales.
- Apagar el equipo siempre que sea posible.

► *DISPOSITIVOS MÓVILES*

Las normas expuestas anteriormente para la utilización del correo electrónico e Internet se utilizarán para cualquier otro medio de comunicación en dispositivos móviles como PDAs, BlackBerry, teléfonos móviles,...

El robo es una amenaza de seguridad añadida sobre estos dispositivos. El usuario debe mantener un PIN de protección, contraseña o cifrado. Si uno de estos dispositivos se pierde o es robado, se debe comunicar inmediatamente a la *Dirección* de *EMPRESA_X* así como al *Responsable de Seguridad*.

► *PROTECCIÓN SOFTWARE MALICIOSO*

Todos los equipos que tengan acceso a la red deben tener instalado un software antivirus. Este tiene que estar activado y actualizado. Ningún usuario debe intentar desactivar la protección.

Cualquier sistema infectado con virus debe desconectarse inmediatamente de la red y debe informarse al *Responsable de Seguridad* del incidente. Los equipos que hayan sido infectados no volverán a conectarse a la red hasta que los técnicos responsables hayan verificado que el virus o cualquier otro código malicioso hayan sido eliminados.

Existen miles de email que contienen virus. Si se recibe un correo con algún archivo adjunto con terminación .exe, o con un texto que no resulta familiar, o simplemente se tiene sospecha del email recibido, en ningún caso debe abrirse, e informar inmediatamente al *Responsable de Seguridad*.

- *HARDWARE Y SOFTWARE*

Los equipos y el software utilizado en *EMPRESA_X* son propiedad de la organización. Al abandonar la organización todo el equipamiento software, documentos y manuales deben ser devueltos.

EMPRESA_X debe cumplir con los términos de las licencias software que se adquieren, controlando la distribución y el uso del software. Bajo ninguna circunstancia se puede copiar el software, ya que esto supondría una violación de la licencia pudiendo provocar fallos en los sistemas de información.

Los ordenadores portátiles pueden salir fuera de las instalaciones de *EMPRESA_X*. Se deben ejercer todas las medidas de precaución posibles al utilizar estos equipos fuera de las instalaciones.

Nunca se deben dejar los equipos portátiles dentro del maletero de un coche, habitación de hotel o cualquier otro lugar desatendido.

- *ALMACENAMIENTO DE LA INFORMACIÓN*

Las copias de seguridad de la información de *EMPRESA_X* deben realizarse en las ubicaciones previstas para tal fin por la *Dirección*. Las carpetas locales de cada PC deben considerarse como ubicaciones temporales. Toda la información debe copiarse a las carpetas compartidas en el servidor tan pronto como sea posible, o en cualquier caso en un plazo máximo de 1 semana desde la creación del archivo.

El servidor de *EMPRESA_X* dispone de varias carpetas pertenecientes a los distintos departamentos. La gestión de los privilegios de estas carpetas es responsabilidad del *Responsable de Seguridad*, asignando a cada usuario según su perfil y funciones en la empresa acceso a determinadas carpetas.

Es importante realizar copias de respaldo de los archivos de correo de forma regular.

El almacenamiento de información confidencial en los discos duros locales u ordenadores portátiles, debe ser mínima. Debe minimizarse la duplicidad de la información.

► *ESCRITORIOS Y PANTALLAS LIMPIAS*

Cada empleado es responsable de mantener su entorno de trabajo limpio. Se recomienda seguir las siguientes normas:

- Se debe asegurar de guardar de manera segura cualquier información confidencial en cualquier soporte.
- No dejar olvidados documentos confidenciales en impresoras o faxes compartidos.
- Se asegurará de destruir cualquier información en papel o cualquier soporte físico que pueda tener información confidencial cuando deje de ser necesaria.

Los empleados serán responsables de bloquear su puesto de trabajo informático cuando lo abandonen antes incluso del bloqueo automático del sistema por inactividad. El objeto de esta medida es que la información visible no pueda ser comprometida.

4.5.6.7. Responsabilidades

El *Responsable de Seguridad* es el responsable de controlar y coordinar la aplicación del presente procedimiento.

4.5.6.8. Formatos

Formato: *Aceptación de la política de uso de activos*

Todos los formatos correspondientes a este procedimiento operativo se encuentran en la carpeta de formatos originales.

4.5.6.9. Historial de modificaciones

REV	FECHA	MODIFICACION
0	03/06/2013	Elaboración inicial del procedimiento
1	01/12/2013	Actualización de políticas de seguridad

Tabla 15. Modificaciones

5. Revisión del Hardware

· Listar todo el hardware y uso

En este punto enumeraremos todo el hardware existente en la empresa a la que estamos auditando, indicando el modelo de servidor, sistema operativo y una breve descripción sobre su uso.

Servidores:

SERVIDOR	MODELO	SISTEMA OPERATIVO	DESCRIPCION
ESDTA	Hp DL 360G6	Linux SUSE 10.3 Novell Network 6.5 eDirectory	Servidor de ficheros de datos. Novell Enterprise OES2 eDirectory
ESACD	Dell PowerEdge 2950	Windows Server 2008 Std. SP2	Tiphone VoIP para CallCenter
ESGW	Dell PowerEdge R710	Linux SUSE 10.3	Servidor Novell GroupWise v8
ESIMG	Dell PowerEdge 1950	Novell Network 6.5 eDirectory	Servidor de ficheros multimedia. Novell Enterprise OES2 eDirectory
ESPING	Virtual Machine	Linux SUSE 9.0 2.6.5-52	BASH scripts para monitorización
ESEDI	Hp DL 120G7	Windows Server 2008 R2 Std. SP2	Planificador de procesos EDI con clientes y proveedores
CONTROL	IBM ThinkCenter M52	Windows XP Pro. SP3	Control de acceso y presencia
NETXUS	IBM xSeries 306	Windows Server 2000 Pro.	Planificador de procesos Netxus para intercambio de información con Ventas
PROXY	Dell PowerEdge 2850	Linux Debian 2.6.26-2	Proxy Internet Squid 3.0
ESMIS	Virtual Machine	Windows Server 2003 SP2	Reporte financiero MIS /Alea
ESTS1	Virtual Machine	Windows Server 2003 SP2	Terminal Server IT
ESTS3	Virtual Machine	Windows Server 2003 SP2	Terminal Server Ventas
ESTS4	Hp DL 360R05	Windows Server 2003 SP2	Terminal Server CallCenter
ESTS5	Virtual Machine	Windows Server 2003 SP2	Terminal Server Administración
ESTS8	Hp DL 360G7	Windows Server 2008 R2 Std. SP2	Terminal Server Administración. Secondary Domain Controller & Secondary DNS/DHCP
ESCTL	Dell PowerEdge 1950	Linux Debian 2.6.5	Control SPAM / Amavis – Spamassain
ESBES	Virtual Machine	Windows Server 2008 R2 Std. SP2	BlackBerry Enterprise Server
ESSD	Dell PowerEdge 1950	Windows Server 2003 SP2	Alta incidencias IT ServiceDesk
ESBKP	Hp DL 180G6	Windows Server 2008 R2 Std. SP2	Aplicación BackupExec y WSUS
NAGIOS	Virtual Machine	Linux OpenSuse 2.6.37	Monitorización de sistemas Nagios
ES-DIVA	Virtual Machine	Windows XP Pro. SP3	Reporte financiero DIVA
SpareLoad	IBM ThinkCenter M52	Linux Suse 2.6.4	Backup correo RELOAD
PTTS	Dell PowerEdge 2950	Windows Server 2003 SP2	Terminal Server Portugal
PTFS	Dell PowerEdge 2950	Novell Network 6.5 eDirectory	Servidor de ficheros de datos y GroupWise
PTIMG	Dell PowerEdge	Novell Network 6.5	Servidor de ficheros multimedia

	2950	eDirectory	
ESXi1	IBM Express x3550	Linux RedHat 2.4.21-57	ESX VMWare Hosting
ESXi2	IBM Express x3550	Linux RedHat 2.4.21-57	ESX VMWare Hosting
ESXi3	IBM Express x3550	Linux RedHat 2.4.21-57	ESX VMWare Hosting
ESVC	Virtual Machine	Windows Server 2008 R2 Std. SP2	Gestión de ESX VCenter
ESRSA	Virtual Machine	Windows Server 2003 SP2	Aplicación acceso remoto RSA
ESBDSAC	IBM x3250M3	Windows Server 2008 R2 Std. SP2	Datos clientes SQL Server
ESWWW	IBM x3250M3	Windows Server 2008 R2 Std. SP2	Servidor Web IIS
ESDC	Virtual Machine	Windows Server 2008 R2 Std. SP2	Primary Domain Controller & Primary DNS/DHCP

Tabla 16. Hardware_1

Equipos:

EQUIPO	MODELO	SISTEMA OPERATIVO	DESCRIPCION
PCs Marketing	HP-Compaq Elite 8100/8200	Windows 7 Pro. SP1	Multimedia y ofimático
PCs Ventas	Dell Latitude D630/D620 HP-Compaq Elite 8100/8200	Windows XP SP3 Windows 7 Pro. SP1	Multimedia y ofimático
PCs Club	IBM ThinkCenter M52	Windows XP SP3	Multimedia y ofimático
ThinClient	Dell Wyse S10	Nativo	Conexión RDP
Portátiles I	Dell Precission D320	Windows XP SP3	Multimedia y ofimático
Portátiles II	Dell Latitude D510	Windows 7 SP1	Multimedia y ofimático
Portátiles III	Dell Precission D330	Windows 7 SP1	Multimedia y ofimático

Tabla 17. Hardware_2

Hardware de Red:

EQUIPO	MODELO	DESCRIPCION
Switches	HP Procurve 5406zl / 2610	Switch de red
Router Internet	Nativo	Jazztel
Router ADSL	Nativo	Telefónica
Firewall	SonicWall NSA 3500	Firewall de red
Teléfonos IP	Taridan Telecom T207M	Teléfono IP
Medidor Tª	Geist GBB15-P	Mide la temperatura/humedad del CPD
Monitores	Lg, Hp, Dell...	Monitores para estaciones de trabajo
Móviles	BlackBerry 9320, 9800	Móviles de empresa
PDAs	Motorola MC55A0	PDAs de agentes comerciales
Controladora Wifi	HP MSM710	Controlador de puntos de acceso Wifi
APs Wifi	HP MSM320 / HP MSM422	Puntos de acceso Wifi

Tabla 18. Hardware_3

Impresoras:

EQUIPO	MODELO	DESCRIPCION
Impresora I	Ricoh Aficio MP C3300	Impresora Administración/Ventas/Marketing
Impresora II	HP Laserjet 4250	Impresora Administración
Impresora III	HP Laserjet 4250	Impresora Contabilidad
Impresora IV	Ricoh Aficio MP 161	Impresora Marketing/Ventas

Impresora V	Ricoh Aficio MP C3003	Impresora Club
Impresora VI	Ricoh Aficio MP 161	Impresora Club

Tabla 19. Hardware_4

Líneas y conexiones:

TIPO	SUMINISTRADOR	DESCRIPCION
Internet	Jazztel	Línea de comunicación simétrica de Internet. 50MB
Europa1	Colt Telecom	Línea de comunicación punto a punto a sede Europea1. 20MB
Europa2	Colt Telecom	Línea de comunicación punto a punto a sede Europea2. 20MB
Sede1	Colt Telecom	Línea de comunicación punto a punto a Sede1. 20MB.
Sede2	Jazztel	Línea de comunicación punto a punto a Sede2. 50MB
ADSL	Telefónica España	Línea ADSL para conexiones Wifi. 6MB
ADSL2	Jazztel	Línea ADLS para conexiones Wifi. 20MB

Tabla 20. Hardware_5

· Hacer estadísticas de uso y personas

En la siguiente tabla detallaremos para cada servidor, quién lo gestiona y quién tiene acceso. Para indicar quién lo gestiona, definiremos los siguientes usuarios y a qué departamento pertenecen:

T1 -> Técnico1 (IT)
T2 -> Tecnico2 (IT)
T3 -> Técnico3 (IT)
T4 -> Técnico4 (IT)
C1 -> Consultor externo
C2 -> Consultor externo
E1 -> Técnico externo
R1 -> RRHH (Administración)
A1 -> Financiero (Administración)

SERVIDOR	Quién lo administra	Usuarios que lo utilizan	Tipo de uso
ESDTA	T1, T2, C1	80	Acceso al sistema y unidades de red
ESACD	T1, T2, E1	15	Acceso a la aplicación de telefonía Tiphone
ESGW	T1, T2, C1	80	Acceso al cliente de correo GroupWise
ESIMG	T1, T2, C1	30	Acceso a unidades de red
ESPING	T1, T2	40	Mensajes sobre alertas de sistemas
ESEDI	T1, T2, T3	10	El sistema recepciona los pedidos de clientes
CONTROL	T1, T2, R1	80	Monitoriza el acceso y control a la oficina
NETXUS	T1, T2, T3	20	Descarga de pedidos de clientes a las PDAs
PROXY	T1, T2	80	Acceso a Internet
ESMIS	T1, T2, C2, A1	4	Acceso a aplicación financiera
ESTS1	T1, T2, T3, C1	3	Acceso a herramientas IT en Terminal Server
ESTS3	T1, T2	5	Acceso a herramientas Ventas en Terminal Server
ESTS4	T1, T2	6	Acceso a herramientas CallCenter en Terminal Server
ESTS5	T1, T2	8	Acceso a herramientas de Administración en Terminal Server
ESTS8	T1, T2, T3	11	Acceso a herramientas de Administración en Terminal Server
ESCTL	T1, T2, C1	80	Control de SPAM de correo externo

ESBES	T1, T2, T3	25	Gestión de dispositivos BlackBerry
ESSD	T1, T2, T3	80	Acceso a la aplicación de alta de incidencias
ESBKP	T1, T2	80	Actualizaciones Windows y Backup de datos
NAGIOS	T1, T2	80	Monitorización de sistemas y servicios
ES-DIVA	T1, T2, A1	3	Acceso a la aplicación de reporte de información
SpareLoad	T1, T2, C1	80	Almacena una copia semanal del buzón de correo
PTTS	T1, T2	6	Acceso a herramientas Portugal en Terminal Server
PTFS	T1, T2, C1	6	Acceso a unidades de red y cliente de correo GroupWise
PTIMG	T1, T2, C1	6	Acceso a unidades de red
ESXi1	T1, T2	80	Almacenamiento de máquinas virtuales
ESXi2	T1, T2	80	Almacenamiento de máquinas virtuales
ESXi3	T1, T2	80	Almacenamiento de máquinas virtuales
ESVC	T1, T2	80	Aplicación de gestión VMware vSphere 5
ESRSA	T1, T2, C1	24	Acceso a la aplicación de gestión de token RSA
ESBDSAC	T1, T2, T4	30	Acceso a BBDD de clientes y proveedores
ESWWW	T1, T2, T4	80	Acceso a gestión servidor web
ESDC	T1, T2	80	Gestión de DHCP/DNS y GPO

Tabla 21. Uso_1

EQUIPO	Quién lo administra	Usuarios que lo utilizan	Tipo de uso
PCs Marketing	T1, T2, T3	Individual	Acceso a cada PC de Marketing
PCs Ventas	T1, T2, T3	Individual	Acceso a cada PC de Ventas
ThinClient	T1, T2, T3	Individual	Acceso a cada ThinClient
Portátiles I	T1, T2, T3	Individual	Acceso a cada Portátil
Portátiles II	T1, T2, T3	Individual	Acceso a cada Portátil
Portátiles III	T1, T2, T3	Individual	Acceso a cada Portátil

Tabla 22. Uso_2

EQUIPO	Quién lo administra	Usuarios que lo utilizan	Tipo de uso
Switches	T1, T2, C1	80	Acceso a la gestión de los switches de red
Router Internet	T1, T2, C1	80	Acceso al router de Internet
Router ADSL	T1, T2	80	Acceso a la gestión del router ADSL
Firewall	T1, T2, C1	80	Acceso a la gestión del Firewall
Teléfonos IP	T1, T2, T3	80	Acceso a la configuración de teléfonos IP
Medidor Tª	T1, T2, C1	3	Acceso a la monitorización de temperatura del CPD
Monitores	T1, T2, T3	Individual	Monitor conectado al equipo
Dispositivos móviles	T1, T2, T3	40	Acceso a la gestión de dispositivos BlackBerry
PDAs	T1, T2, T3	24	Acceso a la configuración de PDAs
Controladora Wifi	T1, T2	80	Acceso a la gestión de la controladora Wifi
APs Wifi	T1,T2	80	Acceso a la gestión de los puntos de acceso Wifi

Tabla 23. Uso_3

EQUIPO	Quién lo administra	Usuarios que lo utilizan	Tipo de uso
Impresora I	T1, T2	80	Impresión a color y fax
Impresora II	T1, T2	15	Impresión de documentos

Impresora III	T1, T2	3	Impresión de documentos
Impresora IV	T1, T2	30	Impresión de documentos
Impresora V	T1, T2	30	Impresión a color y fax
Impresora VI	T1, T2	15	Impresión de documentos y fax

Tabla 24. Uso_4

· Sistemas claves

SERVIDOR	ACCESO	SISTEMA	COMPLEJIDAD	CADUCIDAD
ESDTA	Individual	Novell	Alta	90 días
Esta contraseña nos permite el acceso individual de cada usuario a su perfil en el sistema. Una vez que autentique, nos dará acceso a las unidades de red de las que tenemos permisos.				
ESACD	Individual	Windows	Baja	No caduca
Esta contraseña permite el acceso a la unidad mapeada que contiene el acceso para la aplicación Tiphone con la que se accede al sistema de CallCenter.				
ESGW	Individual	Novell	Alta	No caduca
Esta contraseña permite el acceso a la aplicación GroupWise de correo interno. Esta contraseña puede no existir si tenemos configurado la autenticación contra el usuario de Novell automáticamente.				
ESIMG	Individual	Novell	Alta	90 días
Esta contraseña permite el acceso a ciertas unidades de red.				
ESPING	Único	Linux	Media	No caduca
Esta contraseña permite el acceso al servidor donde están alojados los script de monitorización.				
ESEDI	Individual	Windows	Baja	No caduca
Esta contraseña permite el acceso al servidor donde se alojan los procesos automatizados de EDI.				
CONTROL	Único	Windows	Baja	No caduca
Esta contraseña permite el acceso al servidor donde se aloja el programa encargado de control de acceso.				
NETXUS	Único	Windows	Baja	No caduca
Esta contraseña permite el acceso al servidor donde se alojan los procesos automatizados que se descargan en las PDA.				
PROXY	Individual	Linux	Media	No caduca
Esta contraseña permite el acceso al servidor donde se aloja el servicio proxy para la navegación de todos los usuarios.				
ESMIS	Único	Windows	Baja	No caduca
Esta contraseña permite el acceso al servidor donde se alojan los procesos automatizados de informe financiero.				
ESTS1	Individual	AD Windows	Media	90 días
Esta contraseña permite el acceso al terminal server donde se alojan aplicaciones para IT.				
ESTS3	Individual	AD Windows	Media	90 días
Esta contraseña permite el acceso al Terminal Server donde se alojan aplicaciones para Ventas.				
ESTS4	Individual	Windows	Baja	No caduca
Esta contraseña permite el acceso al Terminal Server donde se alojan aplicaciones para CallCenter.				
ESTS5	Individual	AD Windows	Media	90 días
Esta contraseña permite el acceso al Terminal Server donde se alojan aplicaciones para Administración.				
ESTS8	Individual	AD Windows	Media	90 días
Esta contraseña permite el acceso al terminal server donde se alojan aplicaciones para Administración.				
ESCTL	Individual	Linux	Media	No caduca
Esta contraseña permite el acceso a la aplicación que gestiona el servicio antispam.				
ESBES	Único	Windows	Baja	No caduca
Esta contraseña permite el acceso al servidor que gestiona los dispositivos BlackBerry.				
ESSD	Individual	AD Windows	Media	90 días
Esta contraseña permite el acceso a la aplicación que gestiona el alta de incidencias informáticas. El usuario se autenticará sobre el dominio Active Directory.				
ESBKP	Único	Windows	Baja	No caduca
Esta contraseña permite el acceso a la aplicación que gestiona los backup sobre los datos.				
NAGIOS	Único	Linux	Media	No caduca
Esta contraseña permite el acceso al servidor donde se encuentra la aplicación de monitorización Nagios.				
NE-DIVA	Único	Windows	Baja	No caduca
Esta contraseña permite el acceso al servidor que realiza reportes de cierta información financiera.				
SpareLoad	Único	Linux	Media	No caduca
Esta contraseña permite el acceso al servidor que gestiona el backup semanal del GroupWise.				

PTTS	Individual	Windows	Baja	No caduca
Esta contraseña permite el acceso al terminal server donde se alojan aplicaciones para Portugal.				
PTFS	Individual	Novell	Alta	90 días
Esta contraseña establece los permisos necesarios para el acceso a ciertas unidades de red.				
PTIMG	Individual	Novell	Alta	90 días
Esta contraseña permite el acceso a ciertas unidades de red.				
ESXi1	Individual	Linux	Media	No caduca
Esta contraseña permite el acceso a la gestión del ESX a través de vSphere 5.				
ESXi2	Individual	Linux	Media	No caduca
Esta contraseña permite el acceso a la gestión del ESX a través de vSphere 5.				
ESXi3	Individual	Linux	Media	No caduca
Esta contraseña permite el acceso a la gestión del ESX a través de vSphere 5.				
ESVC	Individual	AD Windows	Media	90 días
Esta contraseña permite el acceso a la gestión del clúster ESX a través de vSphere 5.				
ESRSA	Único	Windows	Baja	No caduca
Esta contraseña permite el acceso al servidor que gestiona los token RSA de acceso remoto.				
NEBDSAC	Único	Windows	Baja	No caduca
Esta contraseña permite el acceso al servidor que aloja la BBDD de clientes.				
NEWWW	Único	Windows	Baja	No caduca
Esta contraseña permite el acceso al servidor que aloja el servidor Web.				
ESDC	Individual	AD Windows	Media	90 días
Esta contraseña permite el acceso al servidor que aloja el controlador de dominio.				

Tabla 25. Claves_1

EQUIPO	ACCESO	SISTEMA	COMPLEJIDAD	CADUCIDAD
PCs Marketing	Individual	AD Windows	Media	90 días
Esta contraseña permite el acceso al PC.				
PCs Ventas	Individual	Nativo	Alta	No caduca
Esta contraseña permite el acceso al PC.				
ThinClient	Genérico	Nativo		
Este sistema no requiere contraseña, ya que solo hace una conexión RDP a un servidor.				
Portátiles I	Individual	Windows	Baja	90 días
Esta contraseña permite el acceso al portátil.				
Portátiles II	Individual	Windows	Baja	90 días
Esta contraseña permite el acceso al portátil.				
Portátiles III	Individual	Windows	Baja	90 días
Esta contraseña permite el acceso al portátil.				

Tabla 26. Claves_2

EQUIPO	ACCESO	SISTEMA	COMPLEJIDAD	CADUCIDAD
Switches	Individual	Nativo	Alta	No caduca
Esta contraseña permite el acceso a la gestión de los switches de red.				
Router Internet	Genérico	Nativo	Media	No caduca
Esta contraseña permite el acceso a la gestión del router de acceso a internet.				
Router ADSL	Genérico	Nativo	Media	No caduca
Esta contraseña permite el acceso a la gestión del router ADSL de acceso a internet.				
Firewall	Individual	Nativo	Alta	No caduca
Esta contraseña permite el acceso a la gestión del firewall de red.				
Teléfonos IP	Genérico	Nativo	Baja	No caduca
Esta contraseña permite el acceso a la gestión de los teléfonos IP.				
Medidor Tª	Genérico	Nativo	Baja	No caduca
Esta contraseña permite el acceso a la gestión del medidor de temperatura del CPD.				
Monitores	Genérico	Nativo		
Los monitores no requieren contraseña para su manejo.				
Dispositivos móviles	Genérico	Windows	Baja	90 días
Esta contraseña permite el acceso a la aplicación de gestión de dispositivos BlackBerry.				
PDAs	Genérico	Nativo	Baja	No caduca
Esta contraseña permite el acceso a la gestión de las PDAs.				

Controladora Wifi	Genérico	Nativo	Media	No caduca
Esta contraseña permite el acceso a la gestión de la controladora Wifi				
APs Wifi	Genérico	Nativo	Media	No caduca
Esta contraseña permite el acceso a la gestión de los APs Wifi.				

Tabla 27. Claves_3

EQUIPO	ACCESO	SISTEMA	COMPLEJIDAD	CADUCIDAD
Impresora I	Individual	Nativo	Baja	No caduca
Esta contraseña permite el acceso a la gestión de la impresora.				
Impresora II	Individual	Nativo		
Esta impresora no tiene permisos para impresión.				
Impresora III	Individual	Nativo		
Esta impresora no tiene permisos para impresión.				
Impresora IV	Individual	Nativo		
Esta impresora no tiene permisos para impresión.				
Impresora V	Individual	Nativo	Baja	No caduca
Esta contraseña permite el acceso a la gestión de la impresora.				
Impresora VI	Individual	Nativo	Baja	No caduca
Esta contraseña permite el acceso a la gestión de la impresora.				

Tabla 28. Claves_4

· Mapa de conexiones

En este apartado mostraremos en detalle el conexionado lógico de la empresa. Nuestra empresa tiene conectividad con varias sedes tanto europeas como nacionales. Existen 2 conexiones punto a punto con ambas sedes europeas y nacionales para el acceso a los diferentes sistemas de información y aplicaciones.

No mostraremos direcciones IP públicas, direccionamientos, servicios publicados en Internet ni otros datos identificativos que pudieran razones de seguridad.

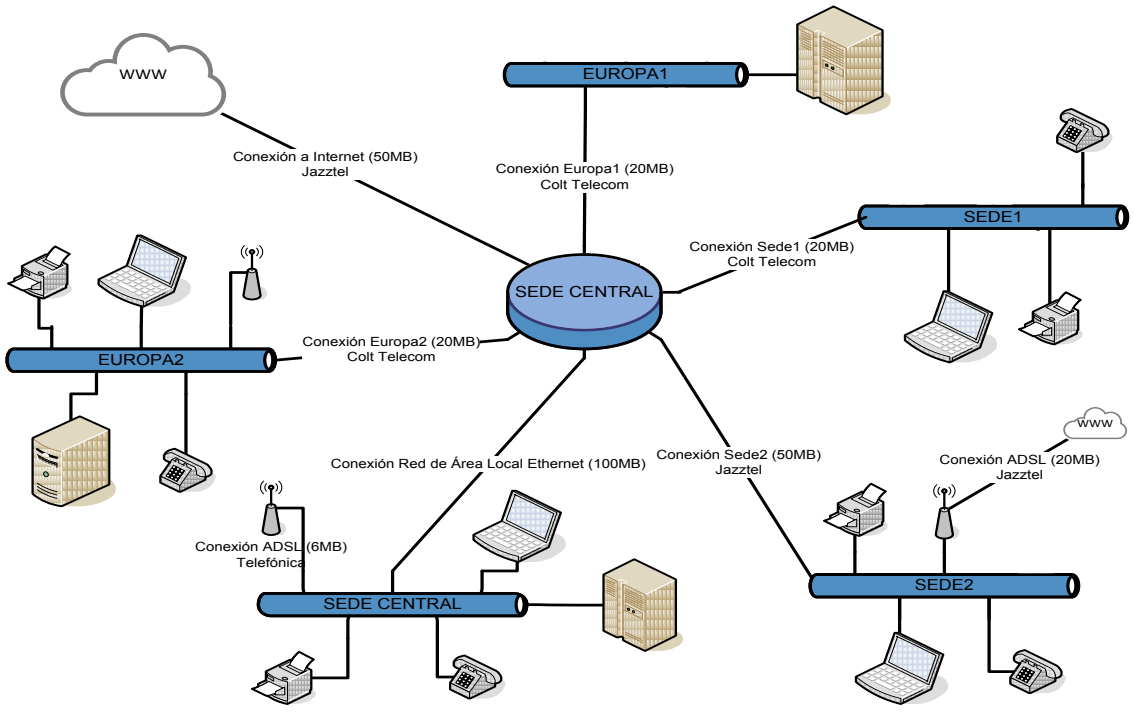

Tabla 29. Esquema_lógico_1

En cuanto a la infraestructura física de nuestros sistemas, se establece de dos formas bien diferenciadas según la importancia que tengan los servicios.

Existe un sistema virtualizado que contiene la mayoría de los servidores en producción y servidores físicos independientes que usaremos para los sistemas más importantes.

A continuación se detalla el sistema virtualizado. Está compuesto por 3 ESX formando un clúster, gestionado por VMware vSphere 5.1. En todos estos sistemas utilizaremos todas las mejoras para gestionar la carga de trabajo y la alta disponibilidad para aumentar el rendimiento y la seguridad.

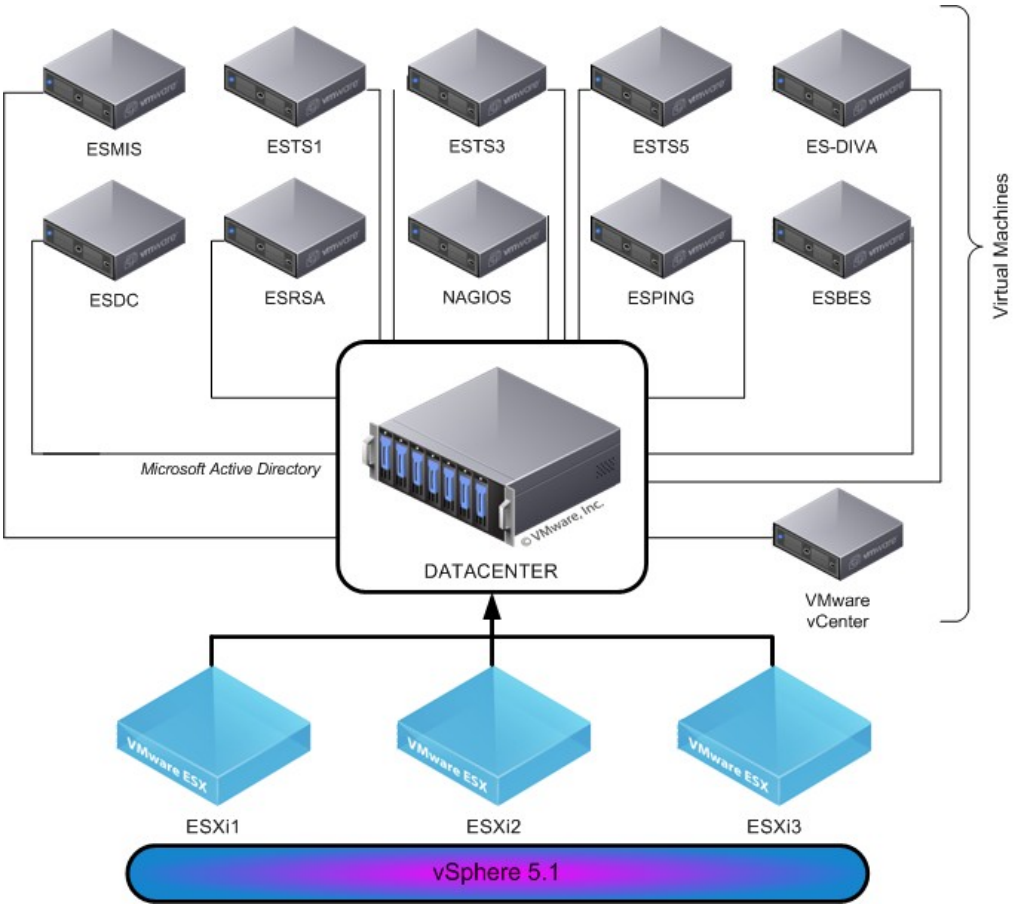

Tabla 30. Esquema_lógico_2

Es este gráfico se detalla a grandes rasgos el conexionado de la infraestructura de la empresa. Tanto los servidores físicos como el entorno de virtualización están en VLANs separadas del resto.

Cada departamento, así como los diferentes sistemas estarán a su vez en VLANs diferentes, para aislar el tráfico, todo ello conectado a su vez con switches.

Es importante hacer referencia a los servidores ESWWW y ESBDSAC que estarán aislados en una DMZ, ya que alojan servicios importantes que están expuestos al exterior.

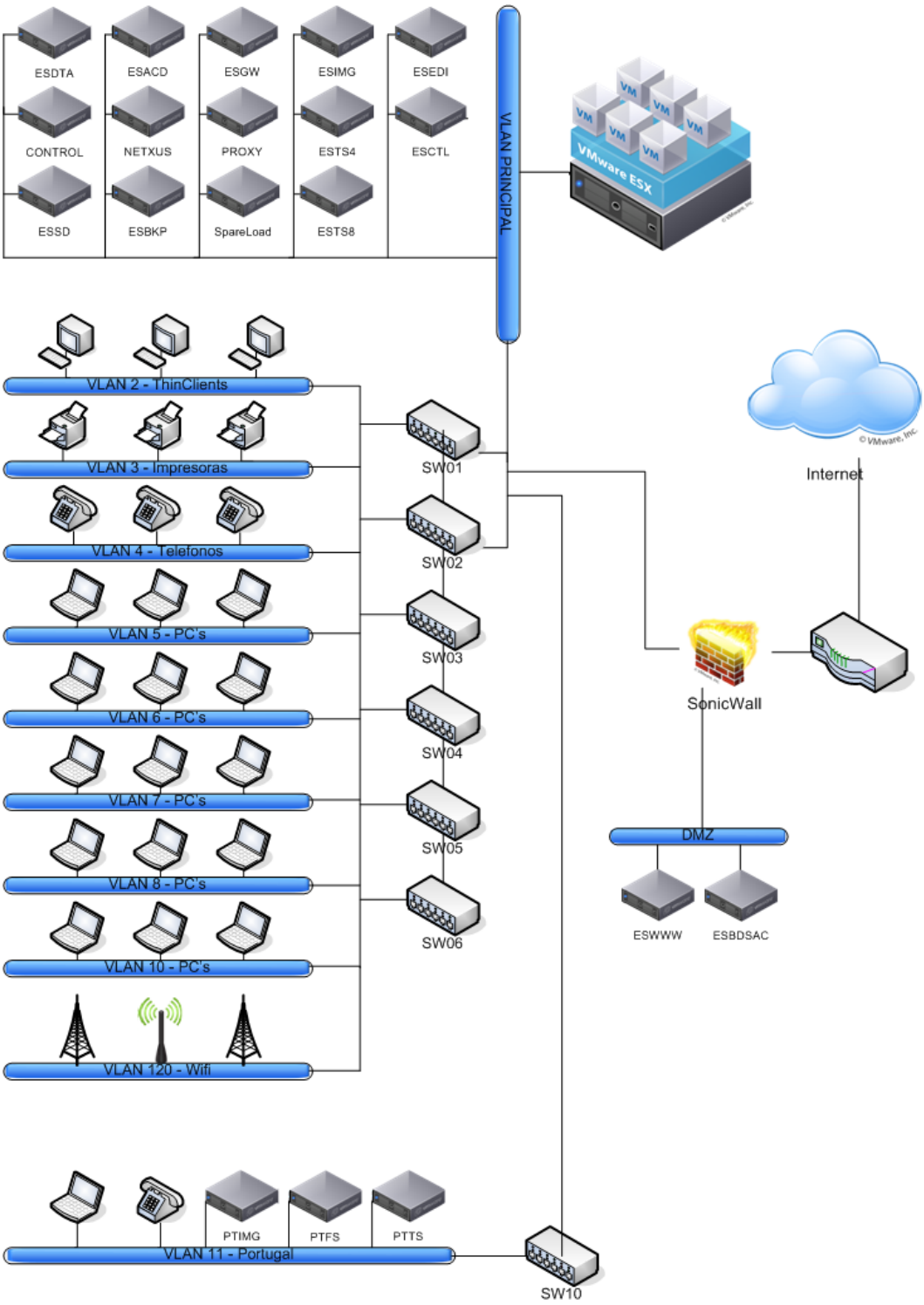

Tabla 31. Esquema_lógico_3

· Prioridades

A la hora de desarrollar nuevos sistemas tendremos en cuenta la prioridad que nos ocupe. Esta prioridad se establecerá dependiendo de si los sistemas forman parte del propio negocio de la empresa o si son sistemas de apoyo o monitorización respecto a los ya existentes. Teniendo en cuenta esto, establecemos que los servicios más importantes serán montados en servidores físicos, y los menos en la herramienta de virtualización que tenemos.

Para los servidores físicos se contratará en el momento de la compra un soporte de mantenimiento especial, por si ocurriese cualquier tipo de problema, tener una respuesta inmediata del fabricante.

· Modificaciones

Para establecer una rutina de seguridad sobre los servidores establecemos los siguientes pasos a llevar a cabo:

- En los equipos virtualizados realizamos cada cierto tiempo snapshots del estado de las máquinas. Estos snapshots forman parte del backup semanal que realizaremos.

- En los servidores físicos comprobamos cada cierto tiempo si se han producido problemas mediante el análisis de los logs y también los incluiremos dentro de la política de backup.

En ambos casos se configura que las alertas importantes que generen los sistemas sean enviados por correo electrónico a los técnicos.

· Probar el hardware: pruebas en paralelo y benchmarks

Antes de configurar cualquier programa software, al igual que la instalación de nuevo hardware, se establece un periodo de prueba en el que se prueban los sistemas antes de su puesta en producción.

Dentro de estas pruebas, intentaremos reflejar las condiciones que se producirán en un futuro y así adelantarnos a posibles problemas que existan.

· Comprobar su vida real

Respecto a todos los servidores y hardware físico que se utilizan en la organización y que están en producción, es de obligatoriedad que estén en garantía. Esto implica que si ocurre algún tipo de problema como: rotura de disco, fallo de hardware, error en los sistemas operativos,... se tenga un soporte del fabricante o de una empresa de soporte que se encargue de la incidencia y de la solución del problema.

Por ello, se configuran en la herramienta de gestión de hardware y software (ServiceDesk Plus) todos los contratos de mantenimiento así como los periodos de garantía de los activos.

Gracias a esto, el sistema notificará a los técnicos con suficiente antelación si los periodos de vencimiento están próximos, y actuar en consecuencia.

6. Auditoría sobre el Hardware

En este punto analizaremos mediante herramientas software de auditoría los elementos más sensibles en la organización. Para ello, usaremos dos conocidas aplicaciones: Microsoft Baseline Security Analizer 2.3 y OpenVAS 6 para detectar posibles vulnerabilidades en nuestros servidores.

A continuación detallaremos un pequeño resumen sobre las deficiencias encontradas más importantes. Las etiquetaremos en color rojo y amarillo según la gravedad que nosotros hemos considerado.

SERVIDOR	MBSA (Microsoft Baseline Security Analyzer) *sobre servidores Windows	OpenVAS (Open Vulnerability Assessment System)	Otros factores
ESDTA	-	Revisar 123/udp, 8009/tcp y 8009/tcp	Actualizar parches del S.O. (Linux)
ESACD	Revisar configuración completa. Firewall, parches y permisos, accesos de usuarios e instancia SQL	Sin problemas de seguridad	-
ESGW	-	Revisar 2049/udp y 123/udp	
ESIMG	-	Revisar 80/tcp, 443/tcp, 2200/tcp, 389/tcp y 8009/tcp	Actualizar parches del S.O. (Linux y Novell)
ESPING	-	Sin problemas de seguridad	
ESEDI	Revisar configuración completa. Firewall, parches y permisos, accesos de usuarios e instancia SQL	Revisar software HP	-
CONTROL	Cumple bien casi en la totalidad. Revisar accesos de usuarios	Sin problemas de seguridad	-
NETXUS	Revisar configuración completa (Windows no soportado). Firewall, parches y accesos de usuarios	Revisar 21/tcp, 80/tcp, 445/tcp y 3389/tcp	Actualizar el sistema operativo
PROXY	-	Revisar 8080/tcp	Actualizar parches del S.O. (Linux)
ESMIS	Cumple bien casi en la totalidad. Revisar accesos de usuarios e IIS	Sin problemas de seguridad	-
ESTS1	Cumple bien en la totalidad	Sin problemas de seguridad	-
ESTS3	Cumple bien casi en la totalidad. Revisar accesos de usuarios	Sin problemas de seguridad	-
ESTS4	Cumple bien casi en la totalidad. Revisar accesos de usuarios e instancia SQL	Revisar software HP	-
ESTS5	Cumple bien casi en la totalidad. Revisar accesos de usuarios	Sin problemas de seguridad	-
ESTS8	Cumple bien casi en la totalidad. Revisar accesos de usuarios	Sin problemas de seguridad	-
ESCTL	-	Sin problemas de seguridad	Actualizar parches del S.O. (Linux)
ESBES	Cumple bien casi en la totalidad. Revisar permisos y accesos de usuarios e instancia SQL	Revisar 9000/tcp y 443/tcp	-
ESSD	Cumple bien casi en la totalidad. Revisar permisos y accesos de usuarios	Sin problemas de seguridad	-
ESBKP	Cumple bien casi en la totalidad. Revisar permisos y accesos de usuarios e instancia SQL	Revisar 81/tcp, 8080/tcp, 443/tcp y 3000/tcp	-
NAGIOS	-	Revisar 80/tcp	Actualizar parches

			del S.O. (Linux)
ES-DIVA	Cumple bien casi en la totalidad. Revisar accesos de usuarios	Revisar 3389/tcp	-
SpareLoad	-	Revisar 2049/tcp	Actualizar parches del S.O. (Linux)
PTTS	Cumple bien casi en la totalidad. Revisar permisos y accesos de usuarios	Sin problemas de seguridad	
PTFS	-	Revisar 8009/tcp, 53/tcp, 80/tcp, 443/tcp, 2200/tcp, 389/tcp y 2049/tcp	Actualizar parches del S.O. (Linux)
PTIMG	-	Revisar 8009/tcp, 53/tcp, 80/tcp, 443/tcp, 2200/tcp, 389/tcp y 2049/tcp	Actualizar parches del S.O. (Linux)
ESXi1	-	Sin problemas de seguridad	Actualizar parches VMware
ESXi2	-	Sin problemas de seguridad	Actualizar parches VMware
ESXi3	-	Sin problemas de seguridad	Actualizar parches VMware
ESVC	Cumple bien casi en la totalidad. Revisar accesos de usuarios e instancia SQL	Revisar 9090/tcp	Actualizar a versión 5.5 VMware
ESRSA	Cumple bien casi en la totalidad. Revisar permisos y accesos de usuarios	Sin problemas de seguridad	-
ESBDSAC	Cumple bien casi en la totalidad. Revisar permisos y accesos de usuarios	Sin problemas de seguridad	-
ESWWW	Cumple bien casi en la totalidad. Revisar accesos de usuarios	Revisar 5556/tcp	-
ESDC	Cumple bien casi en la totalidad. Revisar accesos de usuarios	Sin problemas de seguridad	-

Tabla 32. Vulnerabilidades
* En el Anexo IV encontraremos los reportes sobre los análisis a los servidores.

Respecto a los demás equipos informáticos, indicamos lo siguiente:

- No hemos auditado las máquinas de sobremesa porque tenemos el conocimiento de que están correctamente securizadas tanto en el parcheado de software gracias a la aplicación WSUS así como firewall y permisos de accesos con políticas de seguridad desplegadas a través del dominio de Active Directory.
- Ejecutamos la auditoría sobre los switches, indicándonos resultados correctos.

7. Revisión del Software

Dado que en *EMPRESA_X* no se realiza desarrollo de software a gran escala salvo pequeñas aplicaciones, adecuaremos la revisión del software al desarrollado por terceras empresas para la nuestra.

· Solicitar los esquemas del software

Se documentarán todas las propuestas realizadas de los proveedores con el fin de analizar si se cumplen los requerimientos pedidos. El software desarrollado en la propia empresa se documentará de la misma forma.

· Solicitar programas operativos y de aplicación

Se almacenarán las aplicaciones creadas en un repositorio creado a tal fin. En caso de generar actualizaciones sobre dichos programas, serán correspondientemente almacenadas y documentadas. Se establecerá un procedimiento para poder volver a las versiones anteriores que tuvieran las aplicaciones por si surgieran problemas.

· Solicitar bases de datos

Se solicitará a los gestores de las bases de datos la documentación y los programas fuente utilizados, y se realizarán diversas comprobaciones sobre los ficheros que lo componen. Todos los programas creados se auditarán para asegurar que se cumple con todas las medidas de seguridad requeridas.

· Hacer las pruebas del S.O. con expertos, y con los operadores (observar las reacciones)

Se realizan pruebas con auditores internos y externos sobre seguridad y funcionamiento de los S.O. . y aplicaciones. Se analizarán también las aplicaciones con ciertos usuarios y se evaluarán los resultados.

· Revisión de la vida útil del software

Se lleva un control exhaustivo sobre todas las licencias y software disponible, documentándolos y estableciendo recordatorios cuando dichas licencias caduquen.

También se evaluará el ciclo de vida en el que la aplicación será útil y pueda ser mantenido teniendo en cuenta los costes y la actualización tecnológica.

· Responsables del proyecto

Los responsables del proyecto serán los encargados de supervisar la aplicación y dar solución a posibles actualizaciones o deficiencias.

· Diseñadores

El diseñador documentará en profundidad el funcionamiento de las aplicaciones fielmente a cómo funcionan en realidad. La documentación deberá ser lo suficientemente clara por si en el futuro es necesario modificar el código fuente.

· Probadores

Se documentan y analizan todas las pruebas realizadas antes de que el software sea puesto en producción, ya sean de los propios usuarios o de los técnicos. Si existen problemas o se detectan posibles mejoras, se estudiará su modificación y/o implantación.

· Fundamentos de aplicación

Se comprobará que se cumplen los siguientes requisitos para los que fue diseñada la aplicación como: mantenibilidad, usabilidad, seguridad, rendimiento y diseño.

· Analizar su uso

De todas las aplicaciones diseñadas, se analizará cual es el impacto sobre los usuarios, así como los requerimientos necesarios para su implementación. Se analizará el funcionamiento permanente así como posibles problemas o mejoras que se puedan producir.

8. Auditoría Informática de la Seguridad Física

8.1. Introducción

Primeramente, deberemos preguntarnos qué es la seguridad física. Parece que siempre que pensamos en seguridad informática nos estamos refiriendo a virus, intrusiones en el sistema, robos de contraseñas,... pero eso no lo es todo. La seguridad física comprende todos estos factores además de la integridad de los activos tanto materiales como humanos.

La seguridad 100% de un sistema de información no existe, si bien se puede realizar una tarea que ofrezca un nivel de compromiso importante. También tenemos que considerar que la seguridad conlleva un coste, y no debemos de superar los límites que consideremos adecuados.

Las tareas de la seguridad física comprenden:

- Obtener y procurar mantener un nivel de seguridad física sobre los activos, ubicación de la oficina, seguridad eléctrica y seguridad sobre los sistemas de información.
- Analizar los siguientes recursos: riesgos de los sistemas y riesgos naturales.

8.2. Alcance

Siempre que hablamos de alcance en la seguridad física debemos de establecer unos ciertos límites donde actuar, dependiendo del tamaño de la empresa, campo en el que actúa, nivel de riesgo,... y en función de ello, adoptar las medidas de seguridad necesarias.

Una vez realizada esta pequeña reflexión deberemos de explorar al máximo todos los posibles riegos que podamos tener, siempre dentro de unos límites adecuados.

8.3. Organigrama

Para la realización de una auditoría es esencial conocer desde el principio y tener claro el organigrama de la empresa. Gracias a esto, podremos descubrir de un modo más profundo y esquemático las funciones de cada individuo. Mostramos a continuación el organigrama existente en *EMPRESA_X*.

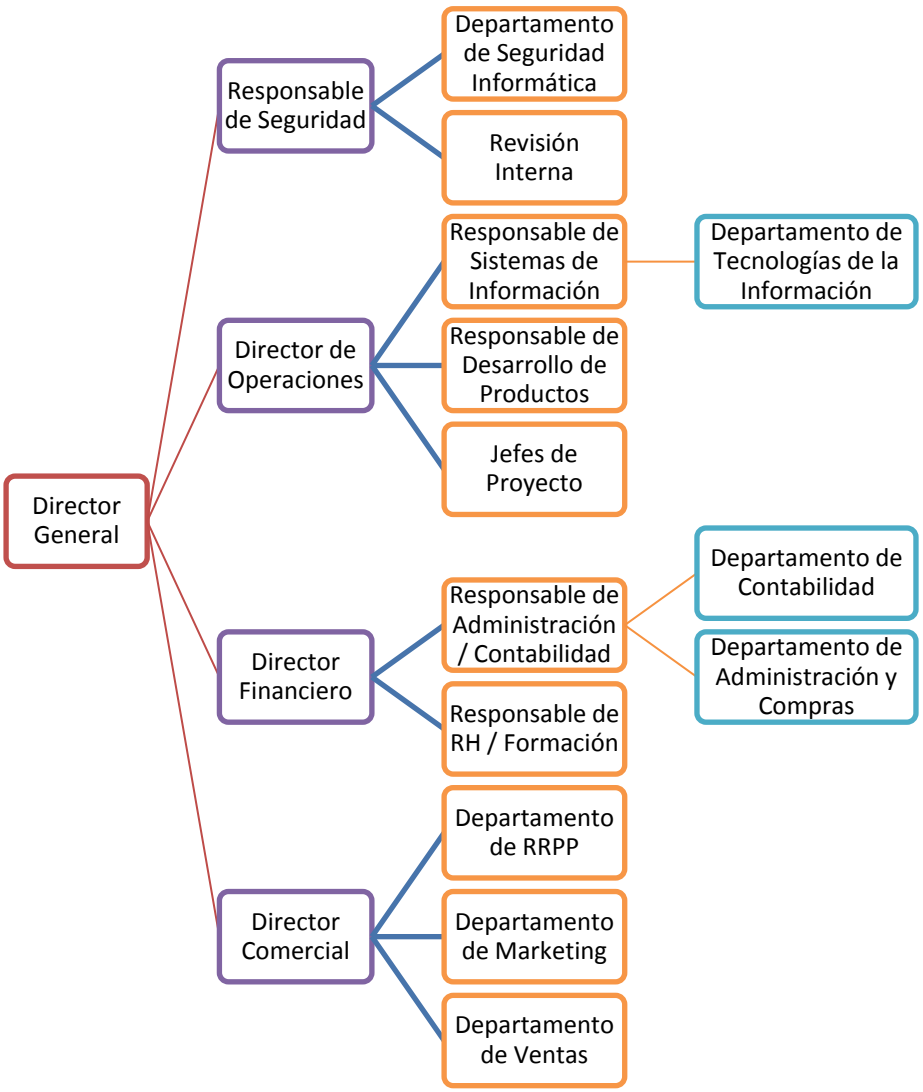

Tabla 33. Organigrama

8.4. Política de Seguridad

La política de seguridad en una empresa es el producto de un acto imprescindible de diseño y puesta en producción de todos los elementos básicos que aseguren la información y datos de un sistema de información. Es nuestra garantía de que los datos o aplicaciones de todo nuestro sistema de información estén a salvo y recuperables de cualquier contratiempo que pueda producirse por causas accidentales o errores humanos.

Los aspectos referidos a la política de seguridad, deberán estar expresamente definidos en un documento que debe ser creado conjuntamente por el *Responsable de Seguridad* y los técnicos.

Dentro de la política de seguridad, tendrá gran importancia la política de backup. En ella se definirá con exactitud la periodicidad con la que el backup será realizado, de qué datos o aplicaciones se realizará, tipo de copia y los responsables que lo llevarán a cabo.

8.5. Normas de Seguridad

Referidos a la política de backup, los soportes sobre los que se realiza la copia deberán de ser etiquetados correctamente aunque reconocibles sólo por los responsables y deberán de ser almacenados de forma segura.

La recuperación de los datos deberá hacerse de forma segura y rápida, asegurándose que los datos se recuperan correctamente.

8.6. Trabajo preparatorio

Será la primera toma de contacto con la empresa auditada, así que podremos tomar unos primeros requerimientos que nos servirán para hacer la planificación inicial. Distinguiremos las siguientes fases:

a) encargo del proyecto

Podemos diferenciar entre encargos específicos que nos pidan por alguna debilidad aparecida o por la necesidad de realizar la auditoría que estaba programada. En ambos casos, tendremos que tener el personal adecuado con los conocimientos pertinentes. Antes de realizar un proyecto de auditoría debemos pensar si seremos capaces de llevarlo a cabo con la infraestructura y personal que tenemos.

Después de analizar la propuesta, pasaremos a realizar una planificación por encima, en la que se deben definir el ámbito, objetivos, plazos de tiempo y costes. Todo ello deberá quedar en un contrato por escrito u otra forma legal.

b) planificación

Procederemos a realizar una planificación que sea acorde con los requerimientos pedidos.

i) responsables

La entidad auditada deberá elegir un responsable del proyecto, que es el que se encargará de la comunicación directa con los auditores, facilitándole todo lo que necesiten. Es la persona que se encargará de establecer las acciones que sean necesarias. También en la empresa auditora, se ha de elegir igualmente un responsable.

ii) código del proyecto

El proyecto debe ser identificable por algún código, según normativa de la entidad.

iii) análisis de objetivos

La finalidad de la auditoría es que se cumplan los objetivos, aunque bien se pueden alcanzar otros que en un principio no estaban planificados. Por tanto, se deben analizar bien los requerimientos que la entidad nos facilita.

iv) profundidad

Una de las cosas que tiene que quedar clara cuando realizamos el análisis tiene que ser hasta donde queremos llegar, es decir, el nivel de profundidad con el que queremos auditar. Para ello tendremos que ver el grado de entrevistas, tamaño de la información, los muestreos, las encuestas,...

v) ámbito

Es uno de los aspectos importantes a tener en cuenta, definir la amplitud de lo que queramos auditar. Deberemos de tener en cuenta tanto los costes económicos como humanos.

8.7. Recopilación de información

Este apartado tratará en conjunto sobre la recopilación de las fuentes de información de las que disponemos. Dichas fuentes serán: documentación facilitada al auditor, la información dada por el propio personal, las revisiones y las pruebas, y las fuentes externas a la entidad. Esta información será la que trataremos para evaluar la seguridad física de la auditoría.

Para la búsqueda de información, será conveniente la realización de cuestionarios adaptables a cada persona, según sea el objetivo, ámbito y profundidad de la auditoría. Detallaremos más adelante mediante una pequeña aplicación, un modelo de cuestionario en el que se reflejarán todos los aspectos relevantes de la Seguridad Física.

Estos cuestionarios deberán ser rellenados por el personal al que queramos auditar y que nos servirán para conocer aspectos no detectados y que utilizará el auditor para realizar las preguntas de forma directa.

8.7.1. La observación

La observación es un proceso muy importante, en el que podremos profundizar mucho para obtener gran cantidad de información.

8.7.2. La documentación

La documentación que se debe solicitar a la entidad auditada dependerá en función de los objetivos, ámbito y profundidad de la auditoría en concreto, pero a rasgos generales, se deben solicitar los siguientes documentos para más adelante proceder a su análisis y revisión. Estos documentos que se pedirán serán:

1) organigrama de la entidad y funciones

Analizar cuál es la dependencia de la entidad informática y verificar que existe un departamento o función de seguridad informática. Si existe departamento de auditoría, verificar que no depende del de informática, y que sus integrantes no se encargan del desarrollo, mantenimiento, seguridad u otra tarea que se pueda auditar.

2) políticas y procedimientos

Se debe asegurar que existen políticas de gestión y actuación, y que los procedimientos que se emplean en los sistemas informáticos son los adecuados. Si no existen estos, se recomienda su creación.

3) planes de seguridad

Verificar que existe un plan de seguridad adecuado para la entidad que sea real y factible. Además, quien lo lleve a cabo sea personal que esté en contacto y lo pueda llevar a cabo.

4) planes de contingencia

Verificar que existe un plan de contingencia adecuado y factible de ejecución, si no, deberá de ajustarse a un valor real. De no existir, se deberá recomendar la creación de uno.

5) actas de Comités

Analizar las decisiones tomadas y que afecten para poder detectar el origen de las debilidades.

6) memorando y comunicados

Es importante conocer los comunicados que la empresa manda a los empleados respecto a las medidas de seguridad. Es importante que los empleados estén debidamente informados sobre las materias de seguridad general y las de seguridad de la información. De no ser así, correríamos un serio peligro.

7) planos de las instalaciones

La entidad deberá contar con unos planos sobre las instalaciones y deberán de ser accesibles por cualquier trabajador para su consulta en la medida en que no requiera una protección especial.

8) contratos

Se deberán conocer los contratos de los trabajadores que estén en contacto con los sistemas de información, para saber si las cláusulas dispuestas como confidencialidad y tratamiento de la información son suficientes.

9) pólizas de seguros

Se deberán presentar todas las pólizas que tenga la empresa y que afecten a la auditoría para averiguar qué sistemas están protegidos, y asegurar que las coberturas son las correctas. Se estudiará si la entidad tiene riesgos altos en algún apartado para un posible refuerzo de seguridad.

10) informes anteriores

Repasaremos informes o auditorías anteriores para averiguar si se ha mejorado en las debilidades encontradas, y además añadir fuentes de información que nos puedan servir sin perder la objetividad en nuestro análisis

8.7.3. Análisis del entorno de las instalaciones

En este punto, analizaremos todos los factores, tanto naturales como no naturales y sociales que pueda tener una entidad. Además de los tipos de riesgos que podamos tener, se realizarán entrevistas para averiguar si tenemos más riegos en las instalaciones.

Al analizar los tipos de riesgos, deberemos definir el grado que afecta a cada uno en la entidad, y lo estableceremos en 5 niveles: muy bajo, bajo, normal, alto y muy alto.

a) naturales

i) terremotos

El riesgo de terremotos es un factor importante que depende del lugar del planeta en el que ocurra. Para ello, deberemos de conocer la situación sísmica del lugar y qué tipo de empresa es, ya que hay empresas más vulnerables que otras.

ii) tormentas eléctricas

Es otro factor importante a tener en cuenta, relacionado con la seguridad eléctrica. A diferencia de los terremotos, podemos y debemos poner los medios adecuados para minimizar los riesgos, siempre teniendo en cuenta el grado de actividad que exista.

iii) temperatura

La temperatura afecta negativamente a los aparatos eléctricos, por lo tanto deberemos de controlarla dentro de unos parámetros aceptables. Gran importancia tiene la sala técnica, donde está guardada gran parte de la información de la empresa. Deberemos de tener controles preventivos que eviten situaciones inesperadas.

iv) humedad

La humedad es otro factor que afecta negativamente a los aparatos eléctricos, por suerte, son pocos los lugares donde tenemos este fenómeno.

v) lluvias

Deberemos de recurrir a datos estadísticos para estudiar los posibles riesgos que tendrá la entidad: si se encuentra en una zona lluviosa, cerca del mar, ríos,...

b) no naturales

i) vibraciones

Se deberá de estudiar si fuera de la entidad, se produce algún tipo de vibración debido a medios de transporte, obras,... Si fuera preciso, se podrían realizar estudios más precisos a fin de detectar las vibraciones.

ii) polvo

Se deberá de estudiar el polvo existente en el ambiente y si existen fuentes cercanas que lo puedan emitir, como parques, fábricas, cercanía de carreteras,...

iii) incendios

Se deberán analizar los riesgos que tiene la entidad en cuanto a posibles incendios que se puedan producir en las cercanías, si existen productos inflamables, medidas de seguridad existentes y cercanía del parque de bomberos.

iv) interferencias

Deberemos analizar si existen interferencias existentes en el ambiente, existencia de antenas de telefonía, ruido eléctrico,... que puedan influir en la salud del personal y en la infraestructura interna.

c) sociales

Se podrá hacer un estudio sobre la situación social del entorno de la empresa y dentro de ella, como niveles de vandalismo, robo,...

8.7.4. El personal involucrado

Lo normal es que exista un equipo de trabajo para llevar a cabo el trabajo de auditoría, la forma de actuar tiene que ser también en forma de grupo con un plan de trabajo y objetivos conjuntos. El conocimiento mínimo de los componentes deberá ser amplio, si bien, sería conveniente que cada componente estuviese especializado en un campo, para ampliar los conocimientos. Los componentes que la realizarán serán los siguientes:

a) gerente

Normalmente, se designará un solo gerente, salvo que la entidad auditada sea muy amplia. Las funciones que realizará serán:

i) Planificación del trabajo

Es esta fase se definirá la estrategia de trabajo a seguir. Deberá de estar planificado por un estamento superior.

ii) Definición de los proyectos

De deben definir conjuntamente con la entidad superior los objetivos de la auditoría.

iii) Elaboración del programa de trabajo

Se definirá la planificación del trabajo de forma definitiva, estableciendo los tiempos y asignación de las tareas.

iv) Dirección del proyecto de auditoría

Existirá un encargado general del proyecto, que llevará a cabo la dirección de la auditoría y el que tomará las decisiones más importantes en caso de dudas.

v) Revisión del informe

La revisión del informe se realizará por todos los miembros del grupo, y tendrá la ventaja del conocimiento de todos los participantes.

vi) Seguimiento de las recomendaciones

Sólo se aplicará un seguimiento si realizamos auditorías internas en el futuro, o si quien realizará nuestra próxima auditoría externa esté formado por las mismas personas.

b) jefe de equipo

Puede haber varios jefes de equipo, siempre que tengamos más de un grupo de trabajo. Esto puede ocurrir si la auditoría se realiza a una entidad grande y/o con varias ubicaciones. Sus roles serán:

i) Colaboración con el gerente

Debe de estar en contacto permanente con el gerente para posibles dudas que surjan.

ii) Supervisión del trabajo de campo

Serán los encargados de la supervisión del trabajo, ayudando en todo lo posible.

iii) Coordinación y revisión del trabajo de los auditores

Encargados de establecer qué trabajo realizarán los auditores y el control que llevarán.

iv) Detección de los puntos importantes para el informe

Deberán conocerse los puntos fuertes, débiles, consideraciones y errores sobre el informe.

v) Propuesta de recomendaciones

Se deben de proponer las recomendaciones o soluciones a partir del informe que se deberán ejecutar para buscar una solución.

vi) Elaboración del borrador del informe

Se elaborará el informe que será entregado a la entidad auditada, con las deficiencias, consideraciones y errores indicados.

c) los auditores

Son los encargados de realizar el trabajo de campo y de realizar las entrevistas y cuestionarios. Estarán en contacto con los gerentes y los jefes de grupo. Sus funciones serán:

i) Colaboración con los jefes de grupo

Tendrán una estrecha colaboración con los jefes de grupo

ii) Realización del trabajo de campo

Como indicamos anteriormente, serán los encargados de la realización de entrevistas, cuestionarios,.. y de pedir la documentación necesaria a los auditados.

iii) Propuesta de sugerencias

Al ser los primeros en realizar la tarea de campo, serán los encargados de proponer sugerencias a los jefes de grupo para que las puedan estudiar.

iv) Propuesta de recomendaciones

Las recomendaciones las propondrán a los jefes de grupo para que éstos las puedan estudiar.

d) auditores junior

Puede haber o no auditores junior en un equipo de trabajo. Estos tendrán poca experiencia y estarán acompañados de auditores profesionales para adquirir madurez y conocimientos.

Por tanto, serán una herramienta de apoyo a los grupos de trabajo existentes.

8.7.4.1. Aspectos del personal/Contrato de seguridad

Todos los trabajadores que efectúen la auditoría deberán de firmar un acuerdo de confidencialidad con la empresa auditada. Deberán mantener el secreto profesional sobre todos los aspectos que se refieran a la seguridad de los auditados.

El personal deberá ser respetuoso con las posibles deficiencias que puedan estar cometiendo los empleados y mantendrá una relación de estrecha colaboración con los auditados.

8.7.5. Teletrabajadores

Depende de la dirección, algunos trabajadores podrán realizar parte o totalmente su jornada de trabajo desde casa. Si esto se produce, se deberá asegurar que los trabajadores tengan las mismas condiciones que si trabajasen en la propia oficina.

Se deberá asegurar la confidencialidad, integridad y disponibilidad de la información como si estuviese en la propia empresa.

Se deberán estudiar los riegos que supone trabajar fuera de la empresa, así como asegurar que tienen los medios adecuados para realizar el trabajo.

8.7.6. Protección contra robos

Todos los equipos informáticos y sistemas de red de la compañía situados en lugares públicos o de paso deberán de estar dotados con dispositivos antirrobo.

Los servidores o sistemas multiusuario se situarán en lugares protegidos dentro de una habitación o sala con los cierres adecuados. Los equipos informáticos portátiles se securizarán con cables de seguridad y todos sus datos deberán estarán cifrados.

No está permitido sacar información o herramientas propias de la empresa fuera del centro de trabajo, salvo autorización expresa. Tanto los equipos portátiles como los dispositivos móviles estarán exentos de esta restricción siempre que tengan las protecciones adecuadas.

8.7.7. Divulgación de información de seguridad

La información relativa a los sistemas y normas de seguridad de la empresa sólo podrá ser conocida por los usuarios de la empresa, y nunca puede ser divulgada a otras personas. El *Responsable de Seguridad* será el encargado de velar por el cumplimiento de esta norma.

8.7.8. Derechos sobre los desarrollos

Mientras que los empleados pertenezcan a la empresa, los posibles proyectos y desarrollos que realicen pertenecerán a la propia compañía. También serán propiedad de la empresa tanto los programas como la documentación que se utilicen para realizarlos.

Asimismo, la compañía se reservará el derecho de uso y acceso de dicha información por parte de los empleados.

8.7.9. Uso personal de la información

No se permitirá el uso de material informático de la empresa para fines personales o de ocio. Solamente se permitirá en casos aislados y siempre con el consentimiento de la compañía. Sólo podrá usarse el software preinstalado en los equipos, el uso de software aparte del instalado no estará permitido.

Dichas excepciones se producirán siempre que no afecte a su trabajo, no ponga en peligro ningún sistema de la compañía y que no conlleve gran cantidad de tiempo.

8.7.10. Conductas inadecuadas

La compañía podrá en cualquier momento retirar o modificar los permisos de los empleados sobre el acceso a los sistemas de información.

No se permitirá que ciertas conductas alteren el funcionamiento interno de la empresa ni que tengan un comportamiento inapropiado.

8.7.11. Aplicaciones que comprometen la seguridad

Salvo autorización expresa por parte del departamento de seguridad, ningún empleado podrá hacer uso de ninguna herramienta software ni hardware que pueda comprometer la seguridad de los sistemas informáticos de la empresa.

Cualquier incidente que se produzca sobre este tipo de materia, supondrá una violación grave de la normativa interna y conllevará la adopción de acciones disciplinarias.

8.7.12. Denuncia obligatoria

Cualquier incidencia que ponga en peligro la información o los sistemas informáticos de la compañía, deberá ser inmediatamente notificada al departamento de seguridad de la compañía.

La omisión con conocimiento sobre dichas acciones, supondrá la toma de acciones legales en consonancia con el reglamento de régimen interno de la empresa.

8.7.13. Sistemas involucrados

Los sistemas involucrados serán todos los ordenadores y sistemas de la red que son administrados por la compañía. También serán de aplicación tanto los diferentes equipos informáticos, soportes sobre los que funcionan y todos los sistemas de servicios o terceros.

8.7.14. Responsabilidades: de los usuarios, propietarios y depositarios

De los propietarios: serán los jefes de departamento y propietarios de la información los que tendrán la responsabilidad de mantener y proteger la información. Estos designarán a los usuarios que deberán de tener acceso, clasificarán el nivel de la confidencialidad y definirán cómo se usará dicha información.

De los depositarios: son los encargados de guardar la información y de procurar mantener el aseguramiento de la integridad y disponibilidad de estos. No deben de permitir que dicha información sea accedida o manipulada por personal que no deba.

De los usuarios: estos serán los responsables de cumplir con las normas establecidas por la empresa en materia de seguridad informática. Cualquier otra gestión de la información será llevada a cabo por su administrador o el propietario de la información.

8.7.15. Copias de seguridad

La copia de seguridad de los elementos de información de la empresa es una práctica imprescindible para el aseguramiento de la información. El backup se realizará sobre todos aquellos datos que tengan gran importancia ya sea tanto por los datos que contienen como por la obligación por ley de almacenar dicha información.

A continuación detallamos cómo realizamos las copias de seguridad y cómo afectan a nuestros servidores.

	Backup incremental					*Backup absoluto*	
SERVIDORES	**L**	**M**	**X**	**J**	**V**	**MENSUAL**	**Tipo de Backup**
SPADTA	☒	☒	☒	☒	☒	☒	Ficheros de recursos de red
ESACD	☒	☒	☒	☒	☒	☒	Ficheros de registro de llamadas
ESGW	☐	☐	☐	☐	☒	☒	Ficheros de la oficina postal
ESIMG	☐	☐	☐	☐	☐	☐	No se hace dado que son ficheros multimedia de gran tamaño.
ESPING	☐	☐	☐	☐	☒	☒	Backup completo de la VM
ESEDI	☒	☒	☒	☒	☒	☒	Backup de ficheros de pedidos
CONTROL	☒	☒	☒	☒	☒	☒	Ficheros de datos de acceso
NETXUS	☒	☒	☒	☒	☒	☒	Ficheros de datos de clientes
PROXY	☒	☒	☒	☒	☒	☒	Logs de acceso a internet
ESMIS	☒	☒	☒	☒	☒	☒	Ficheros de datos financieros
ESTS1	☐	☐	☐	☐	☐	☐	No existen datos relevantes
ESTS3	☒	☒	☒	☒	☒	☒	Ficheros de perfiles de usuario
ESTS4	☒	☒	☒	☒	☒	☒	Ficheros de perfiles de usuario
ESTS5	☒	☒	☒	☒	☒	☒	Ficheros de perfiles de usuario
ESTS8	☒	☒	☒	☒	☒	☒	Ficheros de perfiles de usuario
ESCTL	☐	☐	☐	☐	☒	☒	Ficheros de control de spam
ESBES	☐	☐	☐	☐	☒	☒	Backup completo de la VM
ESSD	☒	☒	☒	☒	☒	☒	BBDD sobre la aplicación
ESBKP	☒	☒	☒	☒	☒	☒	Ficheros de copias secundarias
NAGIOS	☐	☐	☐	☐	☒	☒	Backup completo de la VM
ES-DIVA	☐	☐	☐	☐	☒	☒	Backup completo de la VM
SpareLoad	☐	☐	☐	☐	☒	☒	Ficheros de oficina postal
PTTS	☒	☒	☒	☒	☒	☒	Ficheros de perfiles de usuario
PTFS	☒	☒	☒	☒	☒	☒	Ficheros de recursos de red
PTIMG	☐	☐	☐	☐	☐	☐	No se hace dado que son ficheros multimedia de gran tamaño.
ESXi1	☐	☐	☐	☐	☐	☐	No se realiza
ESXi2	☐	☐	☐	☐	☐	☐	No se realiza
ESXi3	☐	☐	☐	☐	☐	☐	No se realiza
ESVC	☐	☐	☐	☐	☒	☒	Backup completo de la VM
ESRSA	☐	☐	☐	☐	☒	☒	Backup completo de la VM
ESBDSAC	☒	☒	☒	☒	☒	☒	BBDD de clientes
ESWWW	☒	☒	☒	☒	☒	☒	Ficheros de servidor Web
ESDC	☐	☐	☐	☐	☒	☒	Backup completo de la VM

Tabla 34. Copia_Seguridad

Todo este trabajo será realizado y supervisado por el personal del departamento de informática. Al final de cada trabajo, deberán de realizarse pruebas de restauración que permitan comprobar que los backup se han realizado correctamente.

El backup se realiza en dos tipos de formato, tanto a cinta como a dispositivo de almacenamiento local.

8.7.16. Desarrollo del informe

Éste será el último punto en la realización de la auditoría y tratará sobre la realización de un informe sobre todos los datos analizados. Se procederá a comprobar que se cumplen todas las medidas de seguridad exigidas en la toma de requisitos.

En caso de que se produzcan diferencias con lo requerido o se encuentren evidencias de que se estén cometiendo errores, se desglosarán y detallarán buscando posibles soluciones.

Juntando todos los datos anteriores, se presentarán en un informe con las posibles deficiencias encontradas así como recomendaciones y soluciones. Dicho informe se entregará al *Responsable de Seguridad* y a la *Dirección*.

(Enrique Castillo, 2009)

9. Auditoría sobre Aplicaciones

9.1. Introducción

La auditoría de programas es la evaluación de la eficiencia técnica, del uso de los diversos recursos (cantidad de memoria) y del tiempo que utilizan los programas, su seguridad y confiabilidad, con el objetivo de optimizarlos y evaluar el riesgo que tienen para la organización.

9.2. Ámbito

Tiene un mayor grado de profundidad y de detalle que la auditoría de la seguridad física en informática, ya que analiza y evalúa la parte interna del uso de los sistemas informáticos.

9.3. Características de la aplicación

Deben definirse qué características han de tener las aplicaciones que se desarrollan y si es posible llevarlas a cabo. Se analizará su conveniencia en recursos y coste y se comprobará una vez terminado el desarrollo si la aplicación cumple con los requerimientos inicialmente pedidos.

9.4. Manejo de la aplicación

Para lograr que la auditoría de programas sea eficiente, las personas que la realicen han de poseer conocimientos profundos sobre sistemas operativos, sistemas de administración de bases de datos y lenguajes de programación usados en los programas. Asimismo, se deberá comenzar con la revisión de la documentación del mismo.

Para poder llevar a cabo una auditoría adecuada de los programas se necesita que los sistemas estén trabajando correctamente, y que se obtengan los resultados requeridos, ya que al cambiar el proceso del sistema en general se cambiarán posiblemente los programas. Sería absurdo intentar optimizar un programa de un sistema que no está funcionando correctamente.

Para optimizar los programas se deberá tener pleno conocimiento y aceptación del sistema o sistemas que usan ese programa, y disponer de toda la documentación detallada del sistema total.

10. Bibliografía

Gran parte de la bibliografía que usamos la obtenemos de Internet, no obstante, añadiremos algunos libros o revistas que también hemos consultado.

Google
http://www.google.com

Flu-Project.com
http://www.flu-project.com/sobre-flu/herramientas-de-auditoria-de-seguridad

Universidad de Belgrano. Argentina
http://www.ub.edu.ar

Portal ISO 27001 en Español
http://www.iso27000.es

Blog dedicado a las auditorías informáticas
http://auditorinformatico.blogspot.com.es

Noticias sobre seguridad de la información
http://blog.segu-info.com.ar

Agencia Española de Protección de Datos
http://www.agpd.es

Consultoría de seguridad de la información
http://www.audea.com

Wikipedia
http://es.wikipedia.org

Monografías
http://www.monografias.com

Recursos bibliográficos
http://www.slideshare.net

Análisis de riesgos
http://www.securityartwork.es

Análisis de riesgos con Magerit
https://www.ccn-cert.cni.es/

ISACA
https://www.isaca.org

OpenVAS
http://www.openvas.org/

MBSA
http://technet.microsoft.com/es-es/security/cc184924.aspx

Web sobre seguridad informática
http://hackmageddon.com/

Auditoría Informática en la empresa. Acha, J. J. 1994. Paraninfo

Auditoría Informática de la Seguridad Física. Sergio Lucena Prats. 2006

Auditoría Informática: un enfoque práctico. Mario G. Piattini. 1997

Sobre la Auditoría Informática y LOPD desde la experiencia personal y profesional. Germán Rodríguez Ramirez. 2009

Auditoría Práctica de Bases de Datos bajo INFORMIX. Mª Isabel Romero Fernández. 2009

11. Informe y Recomendaciones

11.1. Introducción

Una vez realizada la auditoría sobre *EMPRESA_X*, en este apartado realizaremos un pequeño informe sobre las anomalías encontradas así como soluciones y recomendaciones, a fin de cumplir con todos los requerimientos sobre seguridad informática.

11.2. Objetivo de la auditoría

El principal objetivo de la auditoría realizada en *EMPRESA_X*, es la evaluación de los controles de las normas ISO 27001 y LOPD en su aplicación sobre los Sistemas de Información.

Gracias a estos controles, podemos establecer debilidades y fortalezas sobre los sistemas de seguridad de la información que se realizan en *EMPRESA_X*.

11.3. Alcance de la auditoría

El alcance de la auditoría se ha englobado en los departamentos: Ventas, Marketing, IT, Administración y Portugal y los procesos que serán auditados según la norma ISO 27001 y LOPD.

Dentro de los detalles técnicos de la auditoría, hemos entrado en profundidad sobre la seguridad detallada en los servidores y otros equipos informáticos, como nivel de parches, firmware, firewall,...

No hemos llegado a auditar cada usuario individualizado en lo que se refiere a los permisos, accesos que deba de tener, acceso a documentación,... ya que consideramos que se cumplen perfectamente. Indicamos esto porque somos los encargados en parte del control de los permisos y acceso de los usuarios. Para realizar esto de una manera formal, necesitaríamos analizar con cada usuario individualmente cómo realiza su trabajo y no es el enfoque de este trabajo.

Estos elementos anteriores omitidos de la auditoría lo hacemos porque conocemos en gran medida cómo están securizados los elementos y le damos una mayor importancia a elementos más genéricos sobre la seguridad.

11.4. Equipo auditor

Ya que la auditoría que realizamos no se basa en datos exactamente reales, hemos supuesto que la empresa auditora tendrá los siguientes técnicos especialistas encargados de auditar determinadas áreas:

Auditor 1 -> Informático Generalista
Auditor 2 -> Experto en Desarrollo de Proyectos
Auditor 3 -> Técnico de Sistemas
Auditor 4 -> Experto en BBDD y su Administración
Auditor 5 -> Experto en Software de Comunicación
Auditor 6 -> Experto en Explotación
Auditor 7 -> Técnico de Organización
Auditor 8 -> Técnico de Evaluación de Costes

Normalmente, las auditorías informáticas suelen ser realizados por no más de 3-4 personas en una empresa de la envergadura de *EMPRESA_X*. Para explicar bien las diferentes áreas a auditar, hemos supuesto el uso de muchos auditores.

11.5. Fechas y lugares

Hemos supuesto que la fecha de inicio de la auditoría será el día 15/01/2014 con una fecha de duración prevista de finalización de 24 días. Tanto la duración, como las fecha de inicio y fin de la auditoría son valores definidos entre la empresa auditada y auditora.

El lugar será en la sede de *EMPRESA_X*, si bien, parte del trabajo se realizó de forma remota y la elaboración de informes en el domicilio del auditor.

11.6. Cláusula de Confidencialidad

Es importante indicar una cláusula de confidencialidad entre los auditores y la empresa auditora. En un informe de una auditoría real, definiríamos varios puntos como:

- Reunidos: se establecerán los datos personales de los representantes tanto de la empresa auditora como a la que presta el servicio.
- Exponen: conjunto de normas que deberán de llevar en común ambas empresas referidas al tipo de relación que lleven, tanto de colaboración, jurídica y aspecto de seguridad y confidencialidad.
- Condiciones: definiremos tanto el objeto por el que se presta el servicio así como el periodo de duración que tendrá. También se pueden definir opcionalmente otros aspectos relativos a cláusulas penales, derechos de propiedad y protección de datos, así como el coste de los servicios.

No se presenta ninguna cláusula específica ya que podría variar dependiendo de quién negocie los acuerdos.

11.7. Informe sobre LOPD

Sobre los datos analizados en el punto 4.5.1.1, podemos afirmar que *EMPRESA_X* está cumpliendo con todas las obligaciones de la LOPD que existen actualmente.

En principio, no se han detectado errores que pudieran ser constitutivos de faltas o deficiencias que pudieran detectarse por parte de la AEPD. Gracias a las auditorías externas realizadas se lleva un control detallado sobre las normas a seguir, por tanto, se deberán seguir dichas normas y prestar un especial control sobre cambios en el futuro.

11.8. Informe sobre Controles 27001

Sobre los controles de 27001, diferenciaremos en primer lugar lo referente a la norma 27001:2005. Hemos encontrado alguna deficiencia que debería de ser subsanada próximamente, aunque no parecen graves.

A.14.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.

No existe ningún plan de contingencia ni continuidad de negocio ante posibles impedimentos que la actividad laboral se pueda realizar en las oficinas. Esto es un riesgo alto, ya que la empresa sufriría pérdidas importantes, aunque la posibilidad de problemas de gran naturaleza que impidiesen ejercer la actividad laboral en la empresa es remota.

A.14.1.3. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.

No existe tampoco un plan de continuidad de los procesos de información en caso de catástrofe en la oficina. Esto supone un problema ya que los trabajadores no tendrían posibilidad de realizar su trabajo fuera de la oficina.

A.14.1.4. Marco de referencia para la planificación de la continuidad del negocio.

No existe un marco de referencia a seguir sobre la continuidad del negocio. Esto engloba las anteriores deficiencias.

A.14.1.5. Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.

Al no existir ningún plan sobre continuidad de negocio, tampoco existe un control ni reevaluación sobre dichos controles.

A.15.3.2. Protección de las herramientas de auditoría de los sistemas de información.

No existe un control específico sobre las herramientas a usar para la realización de auditorías.

Respecto a la norma 27001:2013, hemos observado en el punto 4.5.3.1 que se cumplen los nuevos cambios introducidos. Por tanto, nos deberemos de centrar en cumplir las deficiencias anteriores.

11.9. Recomendaciones

Aparte de solucionar las deficiencias encontradas anteriormente, hemos elaborado posibles recomendaciones de seguridad gracias a nuestro conocimiento técnico de la infraestructura.

- Deshabilitar el acceso genérico a los servidores y equipos en modo administrador. Esto es: deshabilitar usuarios como "administrator" o "root", sustituyéndolos por usuarios individuales con los permisos adecuados.

- Establecer acceso web para aplicaciones con puertos más seguros, como 443. Además, no usar estos puerto genéricos como el 80 o 443, sino que utilicemos otros, ej. 9443 o 9080.

- Registrar logs de acceso a todos los sistemas, con el fin de saber todas las modificaciones que hacen los técnicos.

- Habilitar acceso SSH en la medida de lo posible en vez de telnet, que no cifra, y deshabilitarlo para el usuario administrador o root.

- No se realiza un control de los soportes ópticos o memorias USB sobre la posibilidad de extraer información de la compañía. Se debería de bloquear la escritura en estos dispositivos mediante políticas GPO.

- En las conexiones de proveedores o clientes a nuestro sistema para tareas de mantenimiento o control, se deberá restringir la comunicación a “IP” de origen y usaremos NAT, para restringir el acceso.

- Se deberían de activar los firewall de Windows de todos los equipos, analizando previamente las conexiones que deban permitirse.

- Además de como se realiza con WSUS, se debería de encontrar una forma de mantener los servidores de otras plataformas diferentes a Windows correctamente actualizados.

- Revisar los circuitos conectados a la corriente protegida de la UPS, ya que en caso de caída de fluido eléctrico, se penalizará el tiempo de fluido eléctrico en función de los aparatos conectados.

- Revisar el acceso de cada usuario a través de proxy, no existe caducidad de la contraseña. Sería deseable la integración con el Active Directory.

- Es necesario un cambio periódico de las contraseñas de acceso Wifi, ya que podrían ser vulneradas con facilidad, así como un control de qué dispositivos se conectan. En algunos accesos se usa encriptación WEP siendo recomendable WPA2 o similar. También es aconsejable implementar el filtrado por MAC para el acceso de dispositivos.

- Sería deseable un proceso automatizado de chequeo de antivirus en todos los equipos cada cierto tiempo.

- Integrar todos los equipos y servidores dentro del mismo dominio, así nos podremos autenticar con el mismo usuario en todos los sistemas.

12. Conclusiones y Líneas Futuras

La realización de un proyecto de auditoría informática supone un gran reto, ya que hay que realizar un estudio previo sobre cómo queremos enfocarlo y definir bien el alcance sobre el contenido de qué queremos auditar. Para ello, necesitaremos tener un amplio conocimiento sobre los marcos legales que se exigen así como los métodos y metodologías que existen para llevarlos a cabo.

El amplio conocimiento que tenemos de la empresa en parte nos ayuda, ya que no tendremos que realizar múltiples cuestionarios ni entrevistas al personal de la empresa, y podremos enfocarlo así más rápidamente. Por el contrario, al estar dentro de un departamento de IT, nos es difícil abstraernos y ver en una perspectiva global la evaluación sobre la seguridad que debemos de afrontar.

El proceso de realización ha sido extenso en el tiempo, ya que siempre aparecen nuevas normas o sistemas que auditar, y es difícil establecer un punto de corte del que no deberemos pasar. El gran conocimiento técnico sobre el funcionamiento de la organización, hace que sea complejo elaborar un documento válido que presente las deficiencias más importantes y que sean entendibles por las personas encargadas de la toma de decisiones.

En general, como la empresa periódicamente es sometida a auditorías tanto internas como externas, cumple con casi la totalidad de las normas de seguridad sobre la LOPD e ISO 27001. Si bien, existen algunos otros aspectos que deberían ser revisados o actualizados, según se publiquen nuevas normas o se desplieguen nuevas funcionalidades dentro de la empresa.

Lo más importante para no cometer errores en el futuro es establecer las funciones de las que se encargará cada miembro de la organización en general. Es fundamental que cada miembro que tenga algún tipo de responsabilidad en alguna materia sea consciente de las normas que debe cumplir. Sobre los sistemas y su control, siempre deberemos de estar alerta sobre cualquier cambio que se produzca, así como posibles actualizaciones sobre software o hardware. Será necesario tener un conocimiento sobre todo tipo de noticias relativas a seguridad, bien a través, de consultorías, foros, webs especializadas,…

A pesar de un aparente estado de normalidad, nunca deberemos de creernos que cumplimos todos los requerimientos sobre seguridad, ya que esto es una apreciación un tanto peligrosa. Siempre deberemos de estar alerta ante cualquier tipo de incidencia, ya sea en forma de seguridad física así como de procedimientos y de sistemas.

Por último, se puede tomar como referencia este trabajo como una forma de cuantificar qué y cómo debemos de evaluar las medidas de seguridad de una empresa, si bien, deberemos de actualizarla regularmente. Cabe reseñar que esta auditoría ha ayudado a cumplir ciertos objetivos sobre seguridad y a conseguir una labor formativa en mi caso.

En cuanto a nuestra aportación en esta auditoría podemos destacar que gracias a esto hemos conseguido tener una visión más global sobre los problemas de la seguridad en la organización. En el aspecto profesional esto me ha aportado el poder realizar un control y detección de las vulnerabilidades existentes en la empresa y trabajar en la seguridad proactiva. Gracias a esto, puedo llevar un control estructurado sobre las diferentes materias que puedan ser sensibles a problemas.

En el aspecto futuro sobre lo que nos puede ayudar esta auditoría tenemos que comentar que puede funcionar como una guía a seguir para realizar controles periódicos. Podríamos ampliarla renovándola con posibles revisiones de las normas de seguridad que surjan así como usando aplicaciones especializadas en la gestión y el cumplimiento de las normas ISO 27001 y LOPD. En caso de los escáneres de vulnerabilidades podríamos usar algún referente como Nessus.

13. Glosario

AEPD
Agencia Española de Protección de Datos, 24, 25, 169, 170

BASH
Intérprete de comandos para Linux, 52

BBDD
Definido como bases de datos, 19, 57, 77

COBIT
Se define como los Objetivos de Control para Información y Tecnologías Relacionadas, 10, 11, 43, 44

controller
Es el responsable de controlar internamente la gestión económica y financiera de una empresa., 98, 100

CPD
Se define como el Centro de Procesamiento de Datos, 19, 53, 55, 57

DHCP
Servicio de entrega de direcciones IP (Dynamic Host Configuration Protocol), 52, 53, 55, 101

DMZ
Se define a la zona neutral donde se alojan servidores críticos, 59

DNS
Se refiere al Servidor de Nombres (Domain Name System), 31, 52, 53

EDI
Se define como el Intercambio Electrónico de Datos (Electronic Data Interchange), 52, 56

EMPRESA_X
Es como definiremos la empresa auditada durante todo el documento, 45, 46, 47, 48, 49, 50

ERP
Son los sistemas de planificación de recursos empresariales (Enterprise Resource Planning), 19

ESX VMWare
Servidor de virtualización de VMWare, 53

GPO
Conjunto de Políticas de Active Directory, 55, 85, 108, 109, 110, 111, 113, 114, 115, 116, 118, 119, 122, 123, 124

GroupWise
Software para gestionar el correo electrónico, 52, 54, 55, 56

IP
Se refiere a la dirección de red del equipo, 31, 53, 55, 57

ISO 27001
Es un estándar para la seguridad de la información, 10, 11, 26, 42, 45, 80, 82, 86, 87, 167

IT
Definido como las Tecnologías de la Información (Information Technology), 52, 54, 56

Linux
Sistema operativo de código abierto, 52, 53, 56, 57

LOPD
Se define como la Ley Orgánica de Protección de Datos de Carácter Personal, 10, 11, 23, 24, 25, 26, 82, 83, 86, 87, 167, 169

MBSA
Microsoft Baseline Security Analyzer, 62, 81, 106

Nagios
Software de código abierto para la monitorización de sistemas, 52, 55, 56, 62, 77, 146

NAT
Traducción de direcciones de red, 85

Novell
Sistema Operativo, 52, 56, 57

NTP
Es el protocolo de sincronización horaria (Network Time Protocol), 38

Proxy
Servidor intermediario de acceso a Internet, 52

RAE
Definido como Real Academia Española, 14

RRHH
Recursos Humanos, 54, 98, 100

RSA
Es el sistema de seguridad de acceso remoto (Rivest, Shamir y Adleman), 53, 55, 57

S.O.
Forma abreviada para definir Sistemas Operativos, 20, 62, 63, 64

ServiceDesk
Software para la gestión de incidencias, 52, 61

SGSI
Es el Sistema de Gestión de la Seguridad de la Información (Information Security Management System), 42

SLA
Acuerdo de Nivel de Servicio (Service Level Agreement), 101

snapshots
Son las fotos sobre el estado actual de las máquinas, 61

Spam
Se define el correo basura, 30, 31, 32, 46, 52, 54, 77

spyware
Se definen así a los programas espías, 31, 46

Tiphone
Software basado en VoIP, 52, 54, 56

Wifi
Conectividad Wireless usada, 53, 54, 55, 58, 85, 100

WSUS
Es el servidor de actualizaciones de Windows (Windows Server Update Services), 52

14. Referencias

Acha Iturmendi, J. J. (1994). *Auditoría Informática en la empresa.* Paraninfo.

AEPD. (2013). *EVALÚA*. Obtenido de http://www.agpd.es/portalwebAGPD/jornadas/dia_proteccion_2011/responsable/evalua-ides-idphp.php

Anónimo. (2009). *Cuestionario para realizar una auditoría*. Obtenido de gerar961437: http://www.scribd.com/doc/18565564/CUESTIONARIO-PARA-REALIZAR-UNA-AUDITORIA-INFORMATICA

Auditoría Informática y de Sistemas. (2012). *Listas de chequeo o checklist para áreas de cómputo*. Obtenido de http://auditordesistemas.blogspot.com.es/2012/02/listas-de-chequeo-o-checklist-para.html

BOE. (13 de Diciembre de 1999). *Ley Orgánica 15/1999 de Protección de Datos de Carácter General*. Obtenido de http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

Cocomsys. (2014). *Auditoría Informática*. Obtenido de Core of Computer Systems: http://cocomsys.com/cocomsys/auditoria-informatica

El portal de ISO 27001 en Español. (2014). *Sistemas de Gestión de la Seguridad de la Información*. Obtenido de http://www.iso27000.es/

EMPRESA_X. (2014). *Manual de Gestión de la Calidad y Seguridad de EMPRESA_X.* Madrid.

Enrique Castillo, E. (2009). *Planeación de Auditoría de Sistemas Informáticos.* Obtenido de http://www.slideshare.net/vidalcruz/planeacion-de-auditoria-de-sistemas-informaticos

Huerta, A. (13 de Noviembre de 2012). *Analisis de Riesgos con PILAR*. Obtenido de http://www.securityartwork.es/2012/11/13/analisis-de-riesgos-con-pilar-ii/

INTECO. (2014). *LOPD. Derecho y Deberes*. Obtenido de http://www.inteco.es/Formacion/Legislacion/Ley_Organiza_de_Proteccion_de_Datos/Derechos_y_Deberes/

ISACA. (2013). *COBIT 4.1*. Obtenido de http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx

ISO/IEC. (2005). 27001:2005.

ISO/IEC. (2013). 27001:2013.

Jazmin, R. M. (2009). *Perfil del Auditor Informático*. Obtenido de http://www.slideshare.net/rossemarycruces/perfil-del-auditor-informtico

Lombardi Pereira, R. (2010). *Metodología de la Auditoría Informática - Isaca*. Obtenido de http://www.scribd.com/doc/170986549/Metodologia-de-La-Auditoria-Informatica-Isaca

Lucena Prats, S. (2006). Auditoría Informática de la Seguridad Física. PFC UC3M.

Marroquín Rivera, R. A., & Rivas Merino, A. E. (2009). *Administración de Centros de Cómputo.* Obtenido de http://inforemp3.blogspot.com.es/2009/02/la-version-actual-es-cobit-4.html

Ministerio de Hacienda. (2014). *Metodologia de Analisis y Riesgos de los S.I.* Obtenido de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.UpTs5cQz2So

RAE. (2014). *Definición*. Obtenido de http://lema.rae.es/drae/srv/search?id=jHIksgNjM2x53A2fZYh

Universidad de Belgrano. (2013). *Metodología de Auditoría Informática*. Obtenido de http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm

15. Anexo I. Calendario de Trabajo

Respecto al calendario de trabajo distinguiremos el tiempo que nos ha costado la realización de este proyecto y el tiempo que hemos supuesto en que se podría realizar contando con el número de auditores y fases que detallamos.

· La realización de este proyecto nos ha llevado casi un año desde el proceso inicial de analizar, definir e implementar el proyecto. Hemos tenido que definir bien los objetivos y la acotación de los límites de la auditoría. Pensamos que este estudio se podría haber realizado en mucho menos tiempo, pero nos hemos retrasado mucho ya que no teníamos demasiados conocimientos sobre LOPD e ISO 27001.

· Una vez dicho esto, a continuación analizamos el tiempo que nos habría llevado realizar una auditoría real según la metodología aplicada. Los tiempos de duración de cada tarea son orientativos, basándonos en el estudio que habría que realizar en *EMPRESA_X*.

Hemos supuesto la fecha se inicio del proyecto el día 15/01/2014 resultándonos la fecha de finalización según los recursos de los que dispondremos el 17/02/2014.

Nombre de tarea	Duración	Comienzo	Fin
Definicion de alcance y objetivos	**3 días**	**mié 15/01/14**	**vie 17/01/14**
Alcance	1 día	mié 15/01/14	mié 15/01/14
Objetivos Generales	2 días	jue 16/01/14	vie 17/01/14
Objetivos Específicos	2 días	jue 16/01/14	vie 17/01/14
Estudio inicial	**5 días**	**lun 20/01/14**	**vie 24/01/14**
Estudio organizativo	2 días	lun 20/01/14	mar 21/01/14
Estudio funcional	3 días	mié 22/01/14	vie 24/01/14
Entorno operacional	**5 días**	**lun 27/01/14**	**vie 31/01/14**
Estudio de operación e inventario	3 días	lun 27/01/14	mié 29/01/14
Analisis sistemas complejos	2 días	jue 30/01/14	vie 31/01/14
Determinacion de recursos de la Auditoria Infor	**2 días**	**lun 03/02/14**	**mar 04/02/14**
Recursos materiales	2 días	lun 03/02/14	mar 04/02/14
Recursos humanos	2 días	lun 03/02/14	mar 04/02/14
Actividades de la auditoria informatica	**5 días**	**mié 05/02/14**	**mar 11/02/14**
Revision	2 días	mié 05/02/14	jue 06/02/14
Herramientas	2 días	mié 05/02/14	jue 06/02/14
Otros	3 días	vie 07/02/14	mar 11/02/14
Informe final	**2 días**	**mié 12/02/14**	**jue 13/02/14**
Realizacion del informe final	2 días	mié 12/02/14	jue 13/02/14
Carta de Introduccion o Presentacion del Inform	**2 días**	**vie 14/02/14**	**lun 17/02/14**
Informe Final	2 días	vie 14/02/14	lun 17/02/14

Tabla 35. Calendario_1

A priori, y una vez realizados los cálculos de los recursos que tenemos con las tareas que debemos de ejecutar parece que es demasiado tiempo el que nos da.

Ya que nunca hemos realizado ninguna auditoría real a una empresa, no sabemos los resultados esperados que deben salir, no obstante, hemos planteado un sobreasignamiento de tareas y recursos por una razón: así podemos ver más específicamente todas las tareas posibles a auditar así como todo tipo de auditores que puedan realizarlas.

A continuación mostraremos el diagrama de Gantt de todo el proyecto. Según podemos observar, hemos considerado que ciertas tareas se pueden ejecutar al mismo tiempo. Esto es una apreciación ficticia, ya que no podemos saber con exactitud si se podrían producir. Será la realización de la auditoría y su funcionamiento diario la que nos dirá si se cumple el proyecto diseñado.

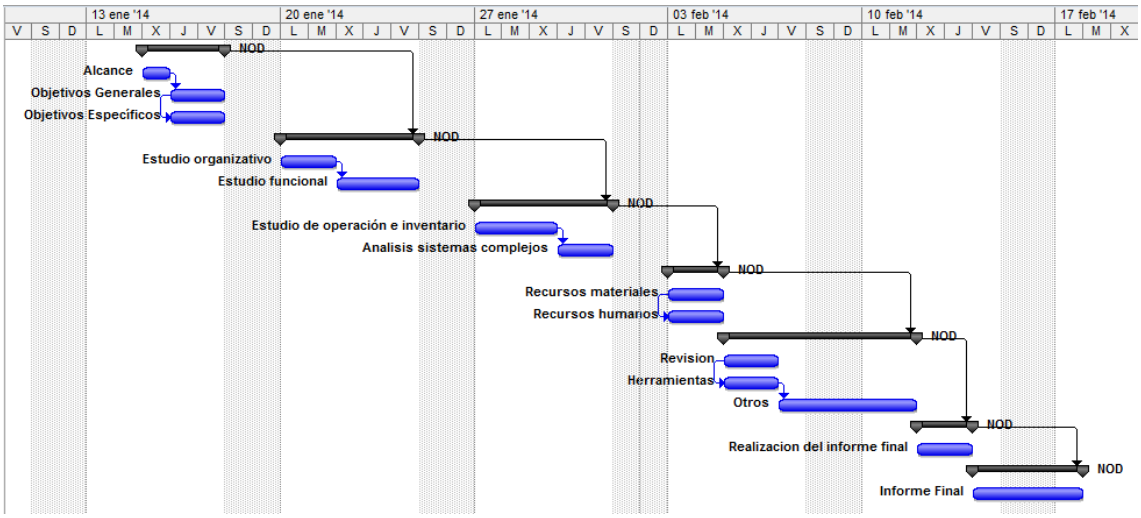

Tabla 36. Calendario_2

Aquí mostramos una tabla indicando por cada auditor, cuántos recursos en horas ha destinado a cada tarea. A pesar de que parece mucho tiempo, ya indicamos anteriormente que lo hacemos para hacernos una idea y mostrar resultados amplios.

Id		Nombre del recurso	Trabajo
1		Informatico Generalista	80,35 horas
		Alcance	*4 horas*
		Objetivos Generales	*8 horas*
		Estudio funcional	*9,95 horas*
		Estudio de operación e inventario	*7,2 horas*
		Recursos materiales	*3,2 horas*
		Recursos humanos	*3,2 horas*
		Revision	*8 horas*
		Otros	*19,2 horas*
		Realizacion del informe final	*9,6 horas*
		Informe Final	*8 horas*
2		Experto en Desarrollo de Proyectos	27,98 horas
		Objetivos Específicos	*8 horas*
		Analisis sistemas complejos	*9,6 horas*
		Revision	*8 horas*
		Realizacion del informe final	*2,38 horas*
3		Tecnico de Sistemas	20,8 horas
		Recursos materiales	*4,8 horas*
		Herramientas	*16 horas*
4		Experto en BD ysu Administracion	16,78 horas
		Estudio de operación e inventario	*9,6 horas*
		Herramientas	*4,8 horas*
		Realizacion del informe final	*2,38 horas*
5		Experto en Software de Comunicaciones	14,4 horas
		Analisis sistemas complejos	*9,6 horas*
		Herramientas	*4,8 horas*
6		Experto en Explotacion	38,72 horas
		Estudio organizativo	*3,2 horas*
		Estudio de operación e inventario	*14,4 horas*
		Analisis sistemas complejos	*9,6 horas*
		Herramientas	*4,8 horas*
		Otros	*6,72 horas*
7		Tecnico de Organización	81,72 horas
		Alcance	*4,8 horas*
		Objetivos Generales	*8 horas*
		Objetivos Específicos	*8 horas*
		Estudio organizativo	*9,6 horas*
		Estudio funcional	*12,45 horas*
		Recursos materiales	*8 horas*
		Recursos humanos	*4,8 horas*
		Revision	*3,2 horas*
		Otros	*5,28 horas*
		Realizacion del informe final	*9,6 horas*
		Informe Final	*8 horas*
8		Tecnico de Evaluacion de Costes	41,6 horas
		Alcance	*3,2 horas*
		Objetivos Generales	*6,4 horas*
		Recursos materiales	*6,4 horas*
		Recursos humanos	*8 horas*
		Realizacion del informe final	*9,6 horas*
		Informe Final	*8 horas*

Tabla 37. Calendario_3

16. Anexo II. Presupuesto

Sobre el presupuesto conviene indicar que los costes por hora, el número de horas y el número de personas involucradas en el proyecto son orientativas y en ningún caso deben de ser un ejemplo sobre el coste total.

Sobre las personas involucradas en la auditoría hay que indicar que todo el personal que interviene son auditores, aunque diferenciaremos entre tipos de auditores según sea su especialidad. Por tanto, en vez de nombrarlos como auditor1, auditor2,... los nombraremos con el tipo de trabajo en el que son especialistas.

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

AUTOR: JORGE BARRIO IBAÑEZ

DEPARTAMENTO IT

DESCRIPCION DEL PROYECTO

- Titulo: **Auditoria Empresa_X**
- Duración (dias): **24 días (15/01/2014 - 17/02/2014)**

PRESUPUESTO TOTAL (EUROS)

Euros: **8.714,06 €**

COSTES DIRECTOS

PERSONAL					
Cantidad	**Recurso**	**Categoría**	**Dedicación (horas)**	**Coste (hora)**	**Coste Total (Euro)**
1	AUDITOR 1	Informático Generalista	80,37	15,00	1.205,50
1	AUDITOR 2	Experto en Desarrollo de Proyectos	27,98	20,00	559,60
1	AUDITOR 3	Técnico de Sistemas	20,8	15,00	312,00
1	AUDITOR 4	Experto en BD y su Administración	16,78	20,00	335,60
1	AUDITOR 5	Experto en Software de Comunicación	14,4	20,00	288,00
1	AUDITOR 6	Experto en Explotación	38,72	25,00	968,00
1	AUDITOR 7	Técnico de Organización	81,72	25,00	2.043,00
1	AUDITOR 8	Técnico de Evaluación de Costes	41,6	25,00	1.040,00
			SUBTOTAL A		**6.751,70 €**

Tabla 38. Presupuesto_1

Desglose por tareas

TAREAS				
Tareas	**Categoría**	**Dedicación (horas)**	**Coste hombre (hora)**	**Coste (Euro)**
Definición de alcance y objetivos		**50,4**		**1.100,00 €**
Alcance		*12*		*260,00*
	Informático Generalista	4	15,00	60,00
	Técnico de Organización	4,8	25,00	120,00
	Técnico de Evaluación de Costes	3,2	25,00	80,00
Objetivos Generales		*22,4*		*480,00*
	Informático Generalista	8	15,00	120,00
	Técnico de Organización	8	25,00	200,00
	Técnico de Evaluación de Costes	6,4	25,00	160,00
Objetivos Específicos		*16*		*360,00*
	Experto en Desarrollo de Proyectos	8	20,00	160,00
	Técnico de Organización	8	25,00	200,00
Estudio Inicial		**35,2**		**780,50 €**
Estudio Organizativo		*12,8*		*320*
	Experto en Explotación	3,2	25,00	80,00
	Técnico de Organización	9,6	25,00	240,00
Estudio funcional		*22,4*		*460,5*
	Informático Generalista	9,95	15,00	149,25
	Técnico de Organización	12,45	25,00	311,25
Entorno operacional		**60**		**1.284,00 €**
Estudio de operación e inventario		*31,2*		*660,00*
	Informático Generalista	7,2	15,00	108,00
	Experto en BD y su Administración	9,6	20,00	192,00
	Experto en Explotación	14,4	25,00	360,00
Análisis sistemas complejos		*28,8*		*624,00*
	Experto en Desarrollo de Proyectos	9,6	20,00	192,00
	Experto en Software de Comunicaciones	9,6	20,00	192,00
	Experto en Explotación	9,6	25,00	240,00
Determinación de Recursos de la Auditoria		**38,4**		**848,00 €**
Recursos materiales		*22,4*		*480*
	Informático Generalista	3,2	15,00	48,00
	Técnico de Sistemas	4,8	15,00	72,00
	Técnico de Organización	8	25,00	200,00
	Técnico de Evaluación de Costes	6,4	25,00	160,00
Recursos humanos		*16*		*368,00*
	Informático Generalista	3,2	15,00	48,00
	Técnico de Organización	4,8	25,00	120,00
	Técnico de Evaluación de Costes	8	25,00	200,00

Actividades de la Auditoria Informática		**80,8**		**1.500,00 €**
Revisión		***19,2***	***360***	
	Informático Generalista	8	15,00	120,00
	Experto en Desarrollo de Proyectos	8	20,00	160,00
	Técnico de Organización	3,2	25,00	80,00
Herramientas		***30,4***	***552,00***	
	Técnico de Sistemas	16	15,00	240,00
	Experto en BD y su Administración	4,8	20,00	96,00
	Experto en Software de Comunicaciones	4,8	20,00	96,00
	Experto en Explotación	4,8	25,00	120,00
Otros		***31,2***	***588,00***	
	Informático Generalista	19,2	15,00	288,00
	Experto en Explotación	6,72	25,00	168,00
	Técnico de Organización	5,28	25,00	132,00
Informe Final		**33,56**		**719,20 €**
Realización del Informe Final		***33,56***	***719,20***	
	Informático Generalista	9,6	15,00	144,00
	Experto en Desarrollo de Proyectos	2,38	20,00	47,60
	Experto en BD y su Administración	2,38	20,00	47,60
	Técnico de Organización	9,6	25,00	240,00
	Técnico de Evaluación de Costes	9,6	25,00	240,00
Carta de Introducción o Presentación del Informe Final		**24**		**520,00 €**
Informe Final		***24***	***520,00***	
	Informático Generalista	8	15,00	120,00
	Técnico de Organización	8	25,00	200,00
	Técnico de Evaluación de Costes	8	25,00	200,00

COSTES INDIRECTOS

OTROS COSTES			
Cantidad	**Recurso**	**Categoría**	**Coste**
1	Material	Uso de material de oficina	20,00
1	Material	Herramientas de redes y comunicaciones	30,00
1	Soporte	Paquete de 5h de consultoría	400,00

SUBTOTAL B	**450,00 €**

COSTE BASICO (DIRECTOS + INDIRECTOS)	**7.201,70 €**
IVA (21%)	1.512,36 €
COSTE TOTAL DEL PROYECTO	**8.714,06 €**

Tabla 39. Presupuesto_2

17. Anexo II. Controles Detallados y Políticas

17.1. Política de Activos

Existe un documento actualizable permanentemente en el que se detalla el identificador del activo, su naturaleza, departamento y a qué recurso está asignado. A su vez, también tendrá referenciada la fecha de alta y baja, así como el estado de amortización. Este documento sólo será accesible por la persona responsable de RRHH y será regularmente comprobado por una auditoría externa de inventario.

Para solicitar cualquier cambio de activo, se rellenará un formulario que deberá tener todos los datos indicados anteriormente y que deberá ser firmado y aprobado por el *Responsable de Seguridad*, responsable de RRHH y el controller.

Cuando solicitemos una retirada de soporte o activo, deberemos crear una solicitud indicando si el activo es un cambio, sustitución o destrucción. Si el activo debe ser destruido, deberemos acompañar la solicitud de baja del activo con un certificado que nos asegure que ese activo ha sido destruido.

17.2. Política de Backup

Siguiendo con la información explicada en el punto 8.7.15, comentar que el proceso de backup se realizará en horario nocturno o periodo de baja actividad.

Para la realización del backup usaremos 2 juegos cintas de lunes a jueves, etiquetadas como lunes1 o lunes2 según corresponda y que rotarán cada 2 semanas. Para las cintas de fin de semana, usaremos un juego diferente para cada semana del mes, usando hasta 5 juegos el mes que tenga 5 semanas.

La retirada de cintas se realiza como sigue: cada martes de la semana, una empresa externa se encargará de recoger las cintas correspondientes al fin de semana y nos suministrará el siguiente juego de fin de semana. En nuestro poder quedarán los 2 juegos de lunes-jueves. Dicha empresa se encargará de salvaguardar la información y proteger su contenido, bajo firma de la pertinente política de confidencialidad entre ambas partes.

Cada mes vencido, la copia referida a ese fin de semana, se etiquetará correspondientemente y no se sobrescribirá, se almacenará de forma perpetua en la empresa de custodia.

En cada copia realizada a fin de mes, se procederá a su comprobación restaurando datos aleatorios.

17.3. Herramientas de Control

Para asegurar el correcto tránsito de información a través de la red, usaremos varias aplicaciones o servicios que nos permitan tener el control de la red.

En cuanto a los accesos que tienen los usuarios a Internet, sólo podrán usar los puertos 80 y 443, y accederán por medio de un proxy. El resto de puertos estarán bloqueados por el firewall de la organización, como el 21, 22 u otros que se utilicen. Sólo en caso de necesidad de uso y con los correspondientes permisos por parte de los responsables se permitirá el tráfico.

Y para asegurar un correcto funcionamiento de la red interna, establecemos un control de los switches a través de su monitorización y replicación.

17.4. Política Cloud

En *EMPRESA_X*, existe una política que prohíbe el uso de sistemas cuya información no esté alojada en nuestra propia empresa, ya que necesitamos tener un control absoluto de la información. Dichos sistemas serán, por ejemplo, Dropbox, WeTransfer, YouSendIt,... así como otros servicios web o de otro tipo.

Como excepción se permite el uso del sistema antivirus en la nube, previa firma de la política de confidencialidad y seguridad.

17.5. Política de Control

Para controlar el uso de los sistemas de los técnicos, en cada sistema de guardarán los logs tanto de acceso como de instalación de aplicaciones y otros eventos, a fin de tener un control exhaustivo sobre qué tareas hace cada cual.

Es deseable que dicho repositorio de logs esté centralizado en una única instancia para un mejor control y aseguramiento.

17.6. Procedimientos

Para la realización de cualquier tipo de petición a recursos humanos existirá una solicitud que se deberá rellenar. Estos procedimientos son por ejemplo: hoja de vacaciones, hoja de gastos, solicitud de compra de activo, solicitud de permisos a recursos de la red,...

Cada solicitud deberá ser presentada al responsable superior y firmada por los correspondientes controladores de la petición.

17.7. Política de Contraseñas

Cada usuario tiene varias contraseñas que usa regularmente:

- usuario de Novell: Este usuario da acceso a las unidades de red y recursos compartidos. Cada cambio de contraseña se produce a los 3 meses y debe ser una contraseña compleja.

- usuario de Active Directory: Este usuario permite autenticarse en el sistema a la vez que en Novell, y permite ejecutar las políticas asociadas que tenga. Se cambia a los 3 meses y debe ser una contraseña compleja.

- usuario proxy: es el usuario que permite el acceso a Internet. Dicha contraseña no se suele cambiar y permite ser una contraseña fácil.

- acceso a las impresoras: cada usuario tiene un código que le permite tener acceso o no a la impresora, escáner o copiadora.

- acceso Wifi: los usuarios tendrán acceso a cada uno de los 3 puntos de acceso:

  - Interno: acceso a la red interna corporativa securizada por filtro MAC
  - Hardware: acceso permitido al exterior libre para prueba de hardware
  - Invitados: acceso al exterior para personal de visita externo, accesible mediante ticket que será creado con sus datos identificativos.

17.8. Permisos de Usuario

Cada usuario tiene determinados permisos, tanto para acceder físicamente a ciertos lugares de la oficina, como acceder a impresoras o ciertos recursos de red. El acceso físicamente tanto a la oficina como a las diferentes salas que existen se realizará mediante el uso de una tarjeta magnética.

Dichos permisos deben ser solicitados por medio un documento firmado por el jefe de departamento, responsable de RRHH y controller.

17.9. Política de Acceso Remoto

Para el acceso remoto fuera de la oficina, el usuario se conectará a una página o aplicación instalada en su equipo en el que deberá introducir un usuario y una contraseña.

La contraseña deberá constar de un pin de entre 4 y 8 cifras más una clave que vendrá en un dispositivo llamado token. Dicho token será individualizado por usuario y que generará una clave aleatoria cada minuto mediante el algoritmo RSA.

Así pues, es una contraseña segura dado que tiene una contraseña conjunta que sólo la sabe el usuario y deberá de llevar su token que generará la otra parte. El token tiene un vida limitada, cuando se agote este deberá de solicitarse otro nuevo.

El acceso que se produce es una conexión VPN contra la red interna de la empresa. Una vez dentro, se conectará contra un servidor Terminal Server, para añadir un grado más de seguridad.

17.10. Control de Red por Usuario

Cada usuario está identificado en la red por la dirección IP asociada a su equipo. Cada equipo está identificado por una dirección MAC, y en función de esa MAC una IP. La IP se entrega por DHCP desde los servidores correspondientes usando reserva de MAC.

Una vez identificada una IP por usuario, en el firewall corporativo tendremos una entrada por cada IP y sus permisos pertinentes.

Por norma general, los permisos de acceso de cada usuario están denegados, y en función de las necesidades se van habilitando.

17.11. Seguridad en Dispositivos Móviles

Los dos tipos de dispositivos que los usuarios pueden usar fuera de la oficina son: ordenador portátil y dispositivo móvil BlackBerry.

El ordenador portátil tendrá restringido el acceso a la BIOS y lleva una contraseña habilitada en el disco duro, de forma que si se extraviase, la información estaría a salvo.

Para los dispositivos móviles, tendremos un servidor BES que se encargará del control, tanto de la confidencialidad de la transmisión de los datos como de la seguridad física. Cada dispositivo tendrá aparte del código PIN, un código de dispositivo que bloqueará el dispositivo a los 5 minutos de inactividad. En caso de introducir mal dicho código un número definido de veces, el dispositivo de formateará. También tenemos la posibilidad de resetear el dispositivo en remoto en caso de pérdida o robo.

17.12. Alta de Incidencias

El proceso para notificar una incidencia informática se realizará por medio de una aplicación llamada ServiceDesk. El usuario podrá dar el alta el ticket desde el portal web o mediante el envío de un correo electrónico. Todas las incidencias se almacenarán y asignarán a cada uno de los técnicos, pudiendo realizar un seguimiento de la misma a través de un SLA configurado previamente.

En esta aplicación se darán de alta los activos para establecer costes y periodos de garantía, y así tener toda la información en caso de avería.

Cada fin de mes, se generará un informe sobre las incidencias producidas, así como su clasificación y resolución. Dicho informe se remitirá a la dirección para su conocimiento.

18. Anexo III. Aplicación Cuestionario

Para mejorar la realización de la auditoría hemos creado una aplicación para realizar cuestionarios al diferente personal de la empresa. Dicho cuestionario es orientativo si bien, es posible modificar tanto las preguntas como los valores adjudicados a dichas preguntas para su aprobación.

Hemos creado 5 tipos de cuestionarios con varias preguntas en cada uno. La auditoría será correcta si se aprueban cada uno de los test por separado. Para aprobar cada test, se deberá sacar una valoración por encima del 70% de respuestas correctas, en cuyo caso se reflejará el texto "Valores Correctos". En caso de sacar una puntuación por debajo de 30% se mostrará el texto "Valores Deficientes", y en caso de que sea menor de 70%, "Valores Revisables". En nuestro programa hemos otorgado un valor equitativo a cada una de las preguntas.

Tanto los valores de las preguntas como la ponderación sobre éstos son orientativos, así como los valores de aprobación de la auditoría, los cuales podrían ser cambiados. En nuestro caso, evaluaremos 100 puntos en cada test, aunque se debería de ponderar el valor de cada test en función de su importancia.

(Anónimo, 2009)
(Auditoría Informática y de Sistemas, 2012)

A continuación mostraremos algunas capturas de ejemplo:

Caso de test con valores deficientes (<40%)

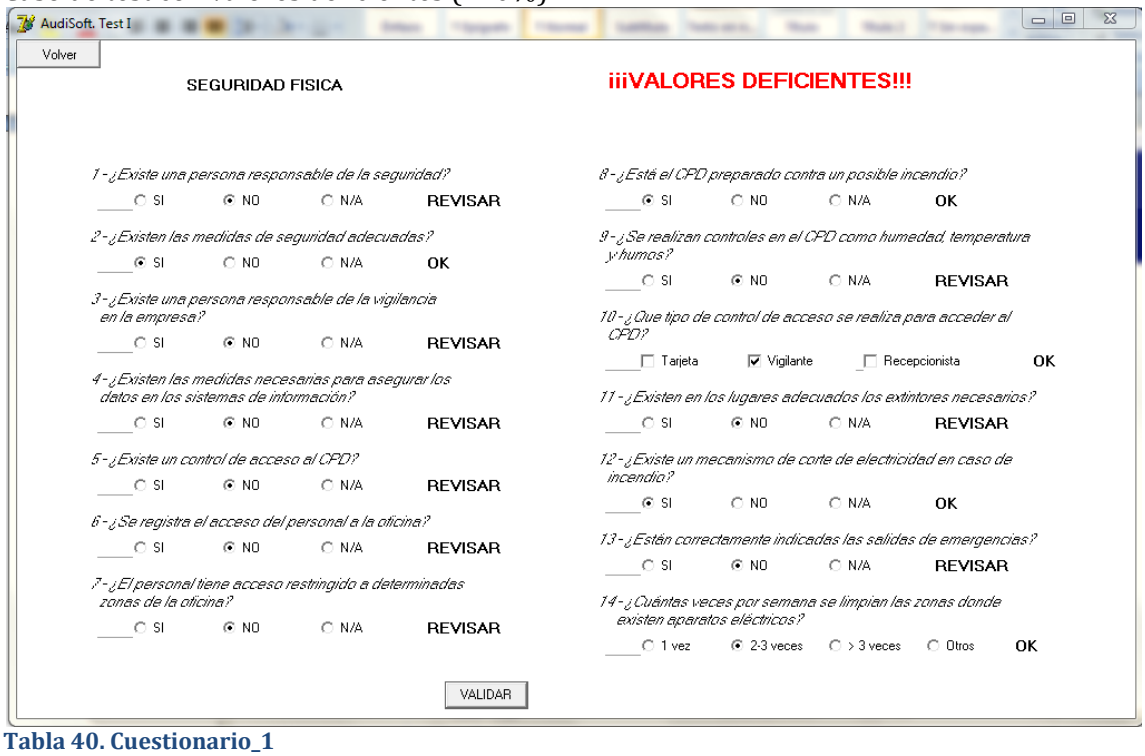

Tabla 40. Cuestionario_1

Caso de test con valores correctos (>70%)

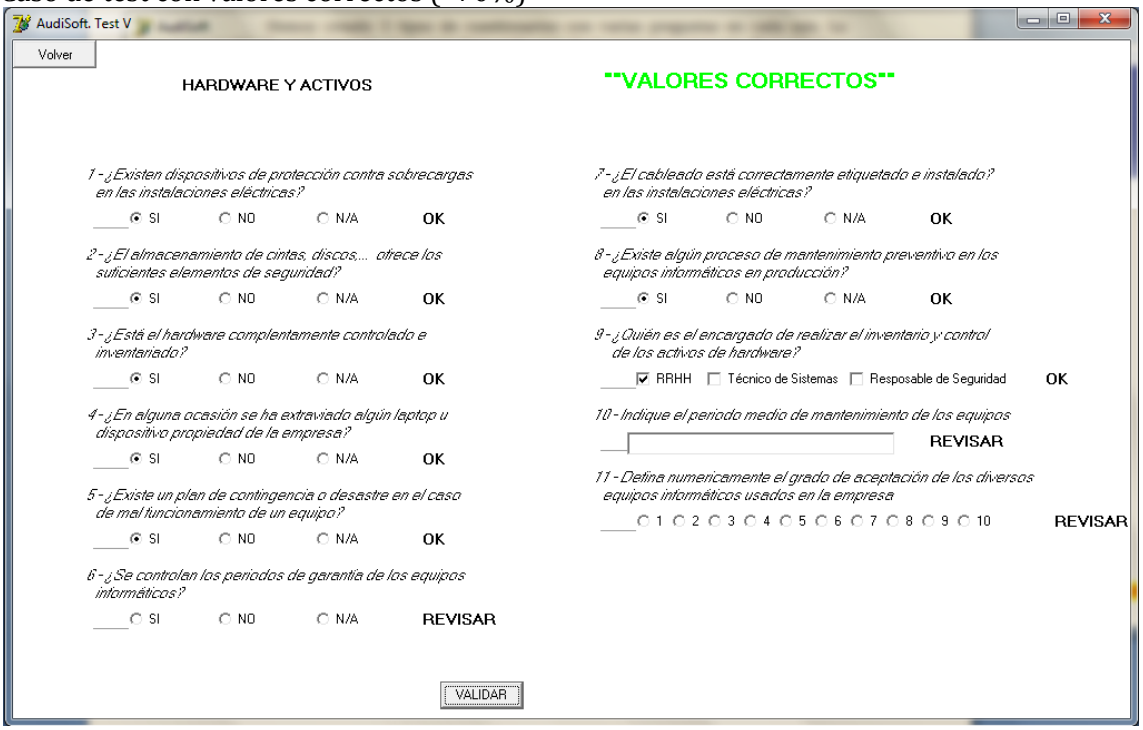

Tabla 41. Cuestionario_2

Caso de test con valores revisables (>40% y <70%)

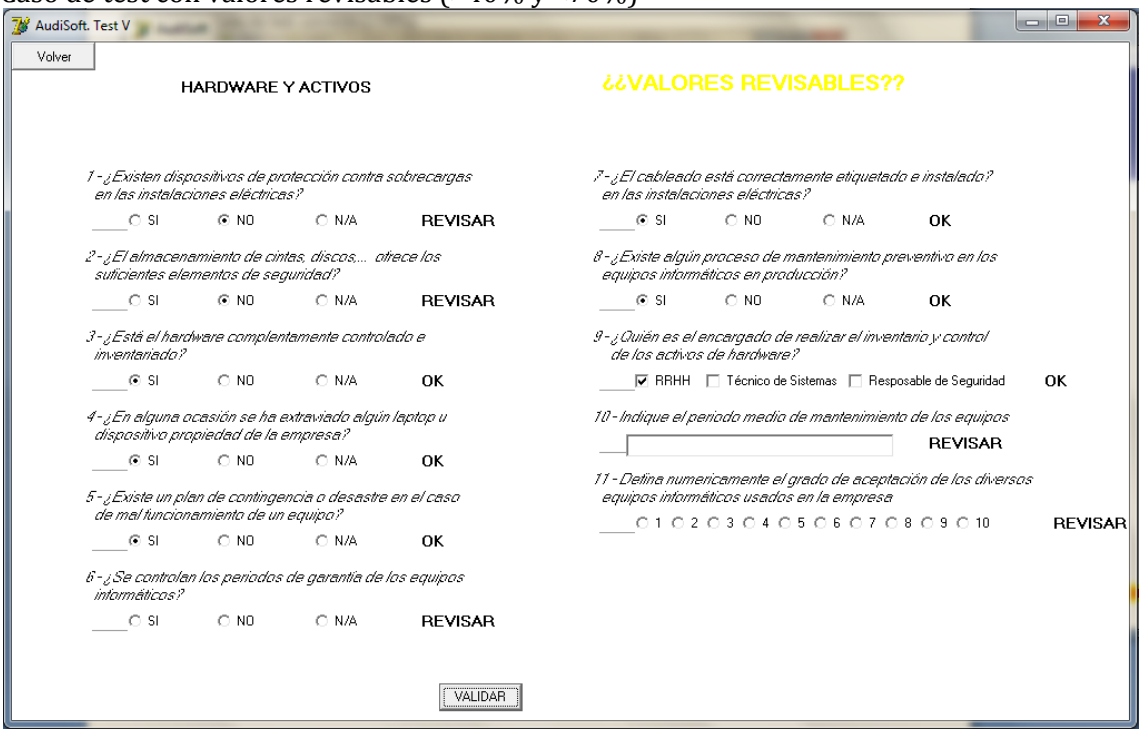

Tabla 42. Cuestionario_3

Caso de auditoría incorrecta

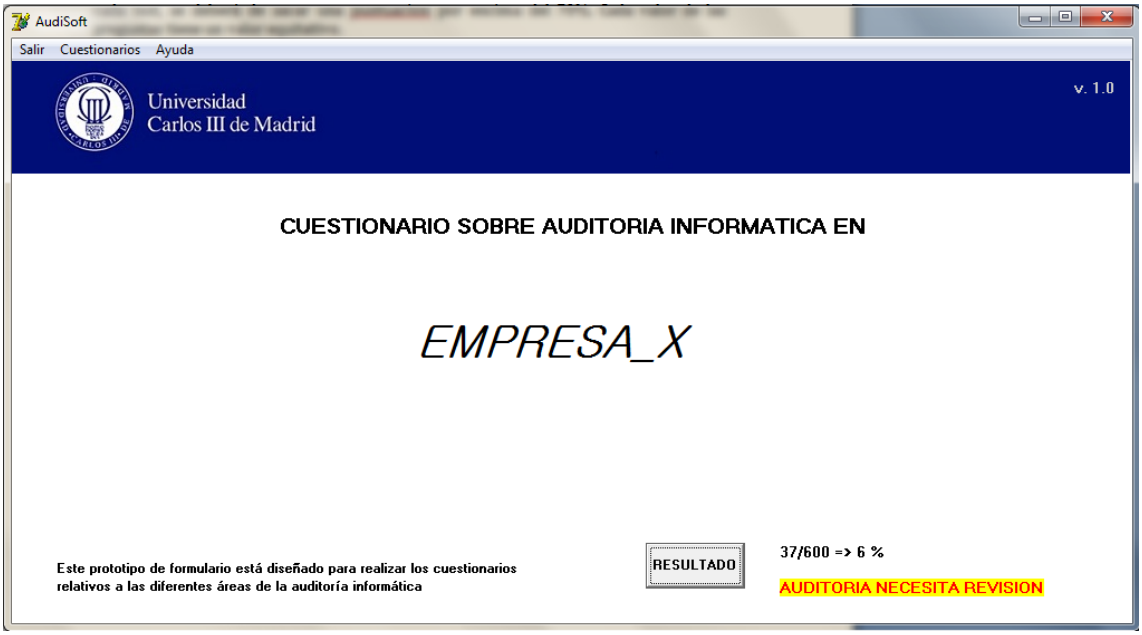

Tabla 43. Cuestionario_4

Caso de auditoría correcta

Tabla 44. Cuestionario_5

19. Anexo IV. Reportes con herramientas de detección de vulnerabilidades

19.1. Análisis con MBSA

A continuación detallaremos diversos controles que haremos a los servidores que tienen instalada alguna versión de Windows con la herramienta MBSA.

MBSA es un software que evalúa el software Microsoft y busca posibles deficiencias y recomendaciones sobre seguridad del sistema operativo. La versión que usaremos es la última disponible (2.3). La evaluación de cada punto analizado podrá tener varios resultados:

Resultado	Valor	Recomendación
☑	Ok	Valores correctos
☒	Error	Errores encontrados, necesaria revisión.
⦸	Warning	Errores menores encontrados, necesaria revisión
✳	Notificación	Sólo informativo

ESACD		
		Resultado
SECURITY UPDATES		
· *SQL Server Security Updates*	⦸	Falta o no aprobada: KB2463332
· *Windows Security Updates*	☒	No actualizado
· *Office Security Updates*	☒	Faltan o no aprobadas: KB974556, KB955440 y Office 2002 SP3
· *Developer Tools, Runtimes, and Redistributables Security Updates*	☒	Falta o no aprobada: KB2538242
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	⦸	Algunos usuarios (5/7) no la tienen habilitada
· *Administrators*	⦸	Existen más de 2 usuarios "administrador" (2)
· *Incomplete Updates*	⦸	Requiere reinicio para completar actualizaciones
· *Windows Firewall*	☒	No configurado
· *Automatic Updates*	☒	No configurado
· *File System*	☑	Todas configuradas en NTFS (3)
· *Guest Account*	☒	No deshabilitado
· *Autologon*	☒	Configurado
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	☒	Algunos usuarios (1/7) tienen contraseña simple o en blanco
Additional System Information		
· *Windows Version*	✳	Microsoft Windows 2008 SP1
· *Shares*	✳	C$, D$, E$ y F$ y Tiphone
· *Services*	✳	Algunos innecesarios: FTP (Stop) y WWW (Arrancado)
INTERNET INFORMATION SERVICES (IIS) SCAN RESULT		
Administrative Vulnerabilities		
· *IIS Status*	⦸	IIS Common Files no están instaladas en el equipo
· *IIS Lockdown Tool*	☑	No necesario para IIS 6.0 en adelante

SQL SERVER SCAN RESULT: INSTANCE (default)		
Administrative Vulnerabilities		
· *Service Accounts*	✳	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent no deberían ser miembro del grupo Administrador local o arrancado con una cuenta de sistema
· *Folder Permissions*	☒	Algunos permisos no están bien configurados
· *SQL Server/MSDE Security Mode*	⊘	Autenticación SQL Server and/or MSDE configurada en modo Windows Mixto
· *Domain Controller Test*	☑	SQL Server and/or MSDE no está cargado en un Domain Controller
· *CmdExec role*	☑	Restringido sólo al rol sysadmin
· *Registry Permissions*	☑	El grupo Everyone tiene solo acceso lectura al SQL Server and/or MSDE claves de registro
· *Sysadmin role members*	☑	BUILTIN\Administrator no forma parte del rol sysadmin
· *Guest Account*	☑	La cuenta Guest no está habilitada en ninguna base de datos
· *Sysadmins*	⊘	Existen más de 2 miembros del rol sysadmin
· *Password Policy*	☒	Habilitar expiración de password para la cuenta SQL Server
· *SSIS Roles*	☑	BUILTIN\Admin no pertenece a ningún rol SSIS
· *Sysdtslog*	✳	Recomendable crear logins diferentes en cada bases de datos
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· *IE Zones*	☑	Todos los usuarios tienen zonas securizadas
· *IE Enhanced Security Configuration for Administrators*	☑	El uso de Internet Explorer está restringido para los administradores
· *IE Enhanced Security Configuration for Non-Administrators*	☑	El uso de Internet Explorer está restringido para los no administradores
· *Macro Security*	☑	Excel, Word, y PowerPoint 2002 instalado. Sin problemas de seguridad.

Tabla 45. MBSA_ESACD

ESEDI		
		Resultado
SECURITY UPDATES		
· *SQL Server Security Updates*	⊘	Falta o no aprobada: KB2494113 y KB2463332
· *Windows Security Updates*	☒	No actualizado
· *Office Security Updates*	☒	No actualizado
· *Developer Tools, Runtimes, and Redistributables Security Updates*	☒	Falta o no aprobada: KB2538242
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	⊘	Ningún usuario (5) la tienen habilitada
· *Administrators*	⊘	Existen más de 2 usuarios "administrador" (4)
· *Incomplete Updates*	⊘	Requiere reinicio para completar actualizaciones
· *Windows Firewall*	☒	No configurado
· *Automatic Updates*	☒	No configurado
· *File System*	☑	Todas configuradas en NTFS (1)
· *Guest Account*	☑	Deshabilitado
· *Autologon*	☑	No Configurado
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	☒	Algunos usuarios (2/5) tienen contraseña simple o en blanco

Additional System Information		
· Windows Version	✳	Microsoft Windows 2008 R2 SP1
· Shares	✳	C$, $ADMIN y Users
· Services	✳	Ninguno innecesario encontrado
SQL SERVER SCAN RESULT: INSTANCE (default) (32b)		
Administrative Vulnerabilities		
· Service Accounts	⦸	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent no deberían ser miembro del grupo Administrador local o arrancado con una cuenta de sistema
· Folder Permissions	☒	Algunos permisos no están bien configurados
· SQL Server/MSDE Security Mode	☑	Autenticación SQL Server and/or MSDE configurada en modo Windows Only
· CmdExec role	☑	Restringido sólo al rol sysadmin
· Registry Permissions	☑	El grupo Everyone tiene solo acceso lectura al SQL Server and/or MSDE claves de registro
· Sysadmin role members	☑	BUILTIN\Administrator no forma parte del rol sysadmin
· Guest Account	☑	La cuenta Guest no está habilitada en ninguna base de datos
· Sysadmins	⦸	Existen más de 2 miembros del rol sysadmin
· Password Policy	☒	Habilitar expiración de password para la cuenta SQL Server
· SSIS Roles	☑	BUILTIN\Admin no pertenece a ningún rol SSIS
· Sysdtslog	✳	Recomendable crear logins diferentes en cada bases de datos
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· IE Zones	☑	Todos los usuarios tienen zonas securizadas

Tabla 46. MBSA_ESEDI

CONTROL		
		Resultado
SECURITY UPDATES		
· SQL Server Security Updates	☑	Actualizado
· Windows Security Updates	☒	Falta o no aprobada: KB976002
· Office Security Updates	☒	Faltan o no aprobadas: KB974556 y KB955440
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· Password Expiration	✳	No chequeado, el equipo forma parte del dominio
· Administrators	⦸	Existen más de 2 usuarios "administrador" (5)
· Incomplete Updates	☑	Ninguna
· Windows Firewall	☑	Configurado por GPO
· Automatic Updates	☑	Configurado por GPO
· File System	☑	Todas configuradas en NTFS (1)
· Guest Account	☑	Deshabilitado
· Autologon	✳	No chequeado, el equipo no forma parte del dominio
· Restrict Anonymous	☑	Activado
· Local Account Password Test	☒	Algunos usuarios (1/10) tienen contraseña simple o en blanco
Additional System Information		
· Windows Version	✳	Microsoft Windows XP SP3
· Shares	✳	C$ y $ADMIN
· Services	✳	Alguno innecesario: Telnet (Stop)
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		

· *IE Zones*	☑	Todos los usuarios tienen zonas securizadas
· *Macro Security*	☑	Excel, Word, y PowerPoint 2002 instalado. Sin problemas de seguridad.

Tabla 47. MBSA_CONTROL

NETXUS		
		Resultado
SECURITY UPDATES		
· *Windows Security Updates*	☒	Ya no soportado
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	⦸	Algunos usuarios (5/8) no la tienen habilitada
· *Administrators*	⦸	Existen más de 2 usuarios "administrador" (3)
· *Incomplete Updates*	☑	Ninguna
· *Windows Firewall*	☒	No disponible
· *Automatic Updates*	☑	Configurado por GPO
· *File System*	☑	Todas configuradas en NTFS (1)
· *Guest Account*	☑	Deshabilitado
· *Autologon*	☑	No Configurado
· *Restrict Anonymous*	☒	Desactivado
· *Local Account Password Test*	☒	Algunos usuarios (3/8) tienen contraseña simple o en blanco
Additional System Information		
· *Windows Version*	✳	Microsoft Windows 2000 SP4
· *Shares*	✳	C$, $ADMIN y Disco_C
· *Services*	✳	Algunos innecesarios: FTP (Arrancado), SMTP (Arrancado), Telnet (Stop) y WWW (Arrancado)
INTERNET INFORMATION SERVICES (IIS) SCAN RESULT		
Administrative Vulnerabilities		
· *IIS Status*	⦸	IIS Common Files no está instalado en el local computer
· *IIS Lockdown Tool*	☒	No arrancado
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· *IE Zones*	☒	Algunos usuarios (1) contienen zonas no securizadas

Tabla 48. MBSA_NETXUS

ESMIS		
		Resultado
SECURITY UPDATES		
· *SQL Server Security Updates*	☑	Actualizado
· *Windows Security Updates*	☑	Actualizado
· *Office Security Updates*	☒	Falta o no aprobada: KB974556 y KB955440
· *Developer Tools, Runtimes, and Redistributables Security Updates*	☒	Falta o no aprobada: KB2538243

WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· Password Expiration	⦸	Algunos usuarios (8/16) no la tienen habilitada
· Administrators	⦸	Existen más de 2 usuarios "administrador" (7)
· Incomplete Updates	☑	Ninguna
· Windows Firewall	☑	Configurado por GPO
· Automatic Updates	☑	Configurado por GPO
· File System	☑	Todas configuradas en NTFS (1)
· Guest Account	☑	Deshabilitado
· Autologon	☑	No Configurado
· Restrict Anonymous	☑	Activado
· Local Account Password Test	☒	Algunos usuarios (3/16) tienen contraseña simple o en blanco
Additional System Information		
· Windows Version	✳	Microsoft Windows 2003 SP2
· Shares	✳	C$, $ADMIN y carpetas de datos
· Services	✳	Algunos innecesarios: FTP (Stop) y WWW (Arrancado)
INTERNET INFORMATION SERVICES (IIS) SCAN RESULT		
Administrative Vulnerabilities		
· IIS Status	⦸	IIS Common Files no está instalado en el local computer
· IIS Lockdown Tool	☑	No necesario para IIS 6.0 en adelante
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· IE Zones	☒	Algunos usuarios (2) contienen zonas no securizadas
· IE Enhanced Security Configuration for Administrators	☑	El uso de Internet Explorer está restringido para los administradores
· IE Enhanced Security Configuration for Non-Administrators	☑	El uso de Internet Explorer está restringido para los no administradores
· Macro Security	☑	Excel y Word 2002 instalado. Sin problemas de seguridad.

Tabla 49. MBSA_MIS

ESTS1		
		Resultado
SECURITY UPDATES		
· SQL Server Security Updates	☑	Actualizado
· Windows Security Updates	☑	Actualizado
· Office Security Updates	☑	Actualizado
· Developer Tools, Runtimes, and Redistributables Security Updates	☒	Falta o no aprobada: KB2538243
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· Password Expiration	⦸	Algunos usuarios (3/4) no la tienen habilitada
· Administrators	☑	No más de 2 usuarios "administrador" (2)
· Incomplete Updates	☑	Ninguna

· *Windows Firewall*	☑	Activado
· *Automatic Updates*	☑	Configurado por GPO
· *File System*	☑	Todas configuradas en NTFS (1)
· *Guest Account*	☑	Deshabilitado
· *Autologon*	☑	No Configurado
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	☑	Algunos usuarios (1/4) tienen contraseña simple o en blanco
Additional System Information		
· *Windows Version*	✳	Microsoft Windows 2003 R2 SP2
· *Shares*	✳	C$ y $ADMIN
· *Services*	✳	Alguno innecesario: Telnet (Stop)
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· *IE Zones*	☑	Todos los usuarios tienen zonas securizadas
· *IE Enhanced Security Configuration for Administrators*	☒	El uso de Internet Explorer no está restringido para los administradores
· *IE Enhanced Security Configuration for Non-Administrators*	⦸	El uso de Internet Explorer no está restringido para los no administradores

Tabla 50. MBSA_ESTS1

ESTS3		
		Resultado
SECURITY UPDATES		
· *SQL Server Security Updates*	☑	Actualizado
· *Windows Security Updates*	☑	Actualizado
· *Office Security Updates*	☒	Falta o no aprobado: Office 2002 SP3
· *SDK Components Security Updates*	☑	Actualizado
· *Developer Tools, Runtimes, and Redistributables Security Updates*	☒	Falta o no aprobada: KB2538243
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	⦸	Algunos usuarios (23/26) no la tienen habilitada
· *Administrators*	⦸	Existen más de 2 usuarios "administrador" (4)
· *Incomplete Updates*	☑	Ninguna
· *Windows Firewall*	☑	Activado
· *Automatic Updates*	☑	Configurado por GPO
· *File System*	☑	Todas configuradas en NTFS (1)
· *Guest Account*	☑	Deshabilitado
· *Autologon*	☑	No Configurado
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	☑	Algunos usuarios (1/26) tienen contraseña simple o en blanco
Additional System Information		
· *Windows Version*	✳	Microsoft Windows 2003 R2 SP2
· *Shares*	✳	C$ y $ADMIN
· *Services*	✳	Alguno innecesario: Telnet (Stop)

DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· IE Zones	☑	Todos los usuarios tienen zonas securizadas
· IE Enhanced Security Configuration for Administrators	☒	El uso de Internet Explorer no está restringido para los administradores
· IE Enhanced Security Configuration for Non-Administrators	⦸	El uso de Internet Explorer no está restringido para los no administradores

Tabla 51. MBSA_ESTS3

ESTS4		
		Resultado
SECURITY UPDATES		
· SQL Server Security Updates	☑	Actualizado
· Windows Security Updates	☑	Actualizado
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· Password Expiration	⦸	Algunos usuarios (12/31) no la tienen habilitada
· Administrators	⦸	Existen más de 2 usuarios "administrador" (4)
· Incomplete Updates	☑	Ninguna
· Windows Firewall	☑	Activado
· Automatic Updates	☑	Configurado
· File System	☑	Todas configuradas en NTFS (1)
· Guest Account	☑	Deshabilitado
· Autologon	☑	No Configurado
· Restrict Anonymous	☑	Activado
· Local Account Password Test	☒	Algunos usuarios (2/31) tienen contraseña simple o en blanco
Additional System Information		
· Windows Version	✳	Microsoft Windows 2003 R2 SP2
· Shares	✳	C$ y $ADMIN
· Services	✳	Alguno innecesario: Telnet (Stop)
SQL SERVER SCAN RESULT: INSTANCE (default)		
Administrative Vulnerabilities		
· Service Accounts	✳	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent no deberían ser miembro del grupo Administrador local o arrancado con una cuenta de sistema
· Folder Permissions	☑	Los permisos están bien configurados
· SQL Server/MSDE Security Mode	☑	Autenticación SQL Server and/or MSDE configurada en modo Windows Only
· Exposed SQL Server/MSDE Password	☑	'sa' password y SQL server Account no están en texto claro
· CmdExec role	☑	Restringido sólo al rol sysadmin
· Registry Permissions	☑	El grupo Everyone tiene solo acceso lectura al SQL Server and/or MSDE claves de registro
· Sysadmin role members	✳	BUILTIN\Administrator no forma parte del rol sysadmin
· Guest Account	☑	La cuenta Guest no está habilitada en ninguna base de datos
· Sysadmins	☑	No más de 2 miembros del rol sysadmin
· Domain Controller Test	☑	SQL Server y/o MSDE no está cargado en un Domain Controller
DESKTOP APPLICATION SCAN RESULTS		

Administrative Vulnerabilities		
· IE Zones	☑	Todos los usuarios tienen zonas securizadas
· IE Enhanced Security Configuration for Administrators	☒	El uso de Internet Explorer no está restringido para los administradores
· IE Enhanced Security Configuration for Non-Administrators	⦸	El uso de Internet Explorer no está restringido para los no administradores

Tabla 52. MBSA_ESTS4

ESTS5		
		Resultado
SECURITY UPDATES		
· SQL Server Security Updates	☑	Actualizado
· Windows Security Updates	☑	Actualizado
· Office Security Updates	☑	Actualizado
· Developer Tools, Runtimes, and Redistributables Security Updates	☒	Falta o no aprobada: KB2538243
· Silverlight Security Updates	☒	Falta o no aprobada: KB2890788
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· Password Expiration	⦸	Algunos usuarios (18/24) no la tienen habilitada
· Administrators	⦸	Existen más de 2 usuarios "administrador" (5)
· Incomplete Updates	☑	Ninguna
· Windows Firewall	☑	Activado
· Automatic Updates	☑	Configurado por GPO
· File System	☑	Todas configuradas en NTFS (1)
· Guest Account	☑	Deshabilitado
· Autologon	☑	No Configurado
· Restrict Anonymous	☑	Activado
· Local Account Password Test	☑	Algunos usuarios (1/24) tienen contraseña simple o en blanco
Additional System Information		
· Windows Version	✳	Microsoft Windows 2003 R2 SP2
· Shares	✳	C$ y $ADMIN
· Services	✳	Alguno innecesario: Telnet (Stop)
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· IE Zones	☒	Algunos usuarios (1) contienen zonas no securizadas.
· IE Enhanced Security Configuration for Administrators	☒	El uso de Internet Explorer no está restringido para los administradores
· IE Enhanced Security Configuration for Non-Administrators	⦸	El uso de Internet Explorer no está restringido para los no administradores

Tabla 53. MBSA_ESTS5

ESTS8		
		Resultado
SECURITY UPDATES		
· Windows Security Updates	☑	Actualizado
· Office Security Updates	☑	Actualizado
· Developer Tools, Runtimes, and Redistributables Security Updates	☑	Actualizado
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· Password Expiration	⊘	Algunos usuarios (15/89) no la tienen habilitada
· Administrators	⊘	Existen más de 2 usuarios "administrador" (7)
· Incomplete Updates	☑	Ninguna
· Windows Firewall	☑	Configurado por GPO
· Automatic Updates	☑	Configurado por GPO
· File System	☑	Todas configuradas en NTFS (1)
· Guest Account	☑	Deshabilitado
· Autologon	☑	No configurado
· Restrict Anonymous	☑	Activado
· Local Account Password Test	✳	No realizado en Domain Controller
Additional System Information		
· Windows Version	✳	Microsoft Windows 2008 R2 SP1
· Shares	✳	Impresoras compartidas y carpetas de software. C$, ADMIN$, SYSVOL y NETLOGON
· Services	✳	Ninguno innecesario encontrado
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· IE Zones	☒	Algunos usuarios (3) contienen zonas no securizadas.

Tabla 54. MBSA_ESTS8

ESBES		
		Resultado
SECURITY UPDATES		
· Windows Security Updates	☑	Actualizado
· Office Security Updates	☑	Actualizado
· Developer Tools, Runtimes, and Redistributables Security Updates	☑	Actualizado
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· Password Expiration	⊘	Algunos usuarios (3/6) no la tienen habilitada
· Administrators	⊘	Existen más de 2 usuarios "administrador" (5)
· Incomplete Updates	☑	Ninguna
· Windows Firewall	☑	Configurado por GPO
· Automatic Updates	☑	Configurado por GPO
· File System	☑	Todas configuradas en NTFS (1)
· Guest Account	☑	Deshabilitado
· Autologon	☑	No configurado
· Restrict Anonymous	☑	Activado
· Local Account Password Test	☑	Algunos usuarios (1/6) tienen contraseña simple o en blanco
Additional System Information		

· *Windows Version*	✳	Microsoft Windows 2008 R2 SP1
· *Shares*	✳	C$, ADMIN$, Users, BES
· *Services*	✳	Ninguno innecesario encontrado
SQL SERVER SCAN RESULT: INSTANCE BLACKBERRY (32b)		
Administrative Vulnerabilities		
· *Service Accounts*	⦸	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent no deberían ser miembro del grupo Administrador local o arrancado con una cuenta de sistema
· *Folder Permissions*	☒	Algunos permisos no están bien configurados
· *SQL Server/MSDE Security Mode*	⦸	Autenticación SQL Server and/or MSDE configurada en modo Windows Mixto
· *Domain Controller Test*	☑	SQL Server and/or MSDE no está cargado en un Domain Controller
· *CmdExec role*	☑	Restringido sólo al rol sysadmin
· *Registry Permissions*	☑	El grupo Everyone tiene solo acceso lectura al SQL Server and/or MSDE claves de registro
· *Sysadmin role members*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· *Guest Account*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· *Sysadmins*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· *Password Policy*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· *SSIS Roles*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· *Sysdtslog*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· *IE Zones*	☒	Algunos usuarios (1) contienen zonas no securizadas.
· *IE Enhanced Security Configuration for Administrators*	☒	El uso de Internet Explorer no está restringido para los administradores
· *IE Enhanced Security Configuration for Non-Administrators*	☑	El uso de Internet Explorer está restringido para los no administradores

Tabla 55. MBSA_ESBES

ESSD		
		Resultado
SECURITY UPDATES		
· *SQL Server Security Updates*	☑	Actualizado
· *Windows Security Updates*	☑	Actualizado
· *Developer Tools, Runtimes, and Redistributables Security Updates*	☒	Falta o no aprobada: KB2538243
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	⦸	Algunos usuarios (5/7) no la tienen habilitada
· *Administrators*	☑	No más de 2 usuarios "administrador" (2)
· *Incomplete Updates*	☑	Ninguna
· *Windows Firewall*	☑	Activado
· *Automatic Updates*	☑	Configurado por GPO
· *File System*	☑	Todas configuradas en NTFS (2)

· *Guest Account*	☑	Deshabilitado
· *Autologon*	☑	No Configurado
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	☒	Algunos usuarios (2/7) tienen contraseña simple o en blanco
Additional System Information		
· *Windows Version*	✳	Microsoft Windows 2003 R2 SP2
· *Shares*	✳	C$, $ADMIN y carpetas de datos
· *Services*	✳	Algunos innecesarios: FTP (Stop) y WWW (Arrancado)
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· *IE Zones*	☒	Algunos usuarios (1) contienen zonas no securizadas
· *IE Enhanced Security Configuration for Administrators*	☑	El uso de Internet Explorer está restringido para los administradores
· *IE Enhanced Security Configuration for Non-Administrators*	☑	El uso de Internet Explorer está restringido para los no administradores

Tabla 56. MBSA_ESSD

ESBKP		
		Resultado
SECURITY UPDATES		
· *Windows Security Updates*	☒	Faltan IE10 e IE11
· *Developer Tools, Runtimes, and Redistributables Security Updates*	☒	Faltan o no aprobados: (KB2538242), (KB971117), (KB971118)
· *SDK Components Security Updates*	☑	Actualizado
· *SQL Server Security Updates*	☑	Actualizado
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	⦸	Algunos usuarios (7/10) no la tienen habilitada
· *Administrators*	⦸	Existen más de 2 usuarios "administrador" (4)
· *Incomplete Updates*	☑	Ninguna
· *Windows Firewall*	☑	Configurado por GPO
· *Automatic Updates*	☑	Configurado por GPO
· *File System*	☑	Todas configuradas en NTFS (2)
· *Guest Account*	☑	Deshabilitado
· *Autologon*	☑	No configurado
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	☒	Algunos usuarios (2/10) tienen contraseña simple o en blanco
Additional System Information		
· *Windows Version*	✳	Microsoft Windows 2008 R2 SP1
· *Shares*	✳	F$, C$, D$, ADMIN$, WSUS y carpetas de datos
· *Servicing*	✳	World Wide Web Publishing Service (Start)
INTERNET INFORMATION SERVICES (IIS) SCAN RESULT		
Administrative Vulnerabilities		
· *IIS Status*	⦸	IIS Common Files no está instalado en el local computer
· *IIS Lockdown Tool*	☑	No necesario para IIS 6.0 en adelante

SQL SERVER SCAN RESULT: INSTANCE MICROSOFT##SSEE		
Administrative Vulnerabilities		
· Service Accounts	⦸	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent no deberían ser miembro del grupo Administrador local o arrancado con una cuenta de sistema
· Folder Permissions	☒	Algunos permisos no están bien configurados
· Domain Controller Test	☑	SQL Server and/or MSDE no está cargado en un Domain Controller
· SQL Server/MSDE Security Mode	☑	Autenticación SQL Server and/or MSDE configurada en modo Windows Only
· CmdExec role	☑	Restringido sólo al rol sysadmin
· Registry Permission	☑	El grupo Everyone tiene solo acceso lectura al SQL Server and/or MSDE claves de registro
· Systemadmin role members	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· Guest Account	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· Sysadmins	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· Password Policy	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· SSIS Role	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· Sysdtslog	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
SQL SERVER SCAN RESULT: INSTANCE BKUPEXEC (32b)		
Administrative Vulnerabilities		
· Folder Permissions	☒	Algunos permisos no están bien configurados
· Password Policy	☒	Habilitar expiración de password para la cuenta SQL Server
· Sysadmins	⦸	Existen más de 2 miembros del rol sysadmin
· Sysadmin role members	✳	BUILTIN\Administrator no forma parte del rol sysadmin
· Service Accounts	✳	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent no deberían ser miembro del grupo Administrador local o arrancado con una cuenta de sistema
· Sysdtslog	✳	Recomendable crear logins diferentes en cada bases de datos
· Domain Controller Test	☑	SQL Server and/or MSDE no está cargado en un Domain Controller
· SQL Server/MSDE Security Mode	☑	Autenticación SQL Server and/or MSDE configurada en modo Windows Only
· CmdExec role	☑	Restringido sólo al rol sysadmin
· Registry Permission	☑	El grupo Everyone tiene solo acceso lectura al SQL Server and/or MSDE claves de registro
· Guest Account	☑	La cuenta Guest no está habilitada en ninguna base de datos
· SSIS Role	☑	BUILTIN\Admin no pertenece a ningún rol SSIS
DESKTOP APPLICACTION SCAN RESULT		
Administrative Vulnerabilities		
· IE Enhanced Security Configuration for Administrators	☒	El uso de Internet Explorer no está restringido para los administradores
· IE Enhanced Security Configuration for Non-Administrators	⦸	El uso de Internet Explorer no está restringido para los no administradores
· IE Zones	☑	Todos los usuarios tienen zonas securizadas

Tabla 57. MBSA_ESBKP

ES-DIVA		
		Resultado
SECURITY UPDATES		
· *Windows Security Updates*	☑	Actualizado
· *Office Security Updates*	⦸	Faltan o no aprobadas: KB974556 y KB955440
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	✳	No chequeado, el equipo no forma parte del dominio
· *Administrators*	⦸	Existen más de 2 usuarios "administrador" (3)
· *Incomplete Updates*	☑	Ninguna
· *Windows Firewall*	☑	Configurado por GPO
· *Automatic Updates*	☑	Configurado por GPO
· *File System*	☑	Todas configuradas en NTFS (1)
· *Guest Account*	☑	Deshabilitado
· *Autologon*	✳	No chequeado, el equipo no forma parte del dominio
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	☑	Ningún usuario tienen contraseña simple o en blanco
Additional System Information		
· *Windows Version*	✳	Microsoft Windows XP SP3
· *Shares*	✳	C$ y $ADMIN
· *Services*	✳	Alguno innecesario: Telnet (Stop)
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· *IE Zones*	☑	Todos los usuarios tienen zonas securizadas
· *Macro Security*	☑	Excel 2002 instalado. Sin problemas de seguridad.

Tabla 58. MBSA_ES-DIVA

PTTS		
		Resultado
SECURITY UPDATES		
· *SQL Server Security Updates*	☑	Actualizado
· *Windows Security Updates*	☑	Actualizado
· *Office Security Updates*	☑	Actualizado
· *SDK Components Security Updates*	☑	Actualizado
· *Developer Tools, Runtimes, and Redistributables Security Updates*	☒	Falta o no aprobada: KB2538243
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	⦸	Algunos usuarios (18/26) no la tienen habilitada
· *Administrators*	⦸	Existen más de 2 usuarios "administrador" (6)
· *Incomplete Updates*	☑	Ninguna
· *Windows Firewall*	☑	Activado
· *Automatic Updates*	☑	Configurado
· *File System*	☑	Todas configuradas en NTFS (1)
· *Guest Account*	☑	Deshabilitado
· *Autologon*	☑	No Configurado
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	☒	Algunos usuarios (2/26) tienen contraseña simple o en blanco

Additional System Information		
· Windows Version	✳	Microsoft Windows 2003 R2 SP2
· Shares	✳	C$, $ADMIN y carpetas de datos
· Services	✳	Alguno innecesario: Telnet (Stop)
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· IE Zones	☒	Algún usuario (1) contiene zonas no securizadas
· IE Enhanced Security Configuration for Administrators	☒	El uso de Internet Explorer no está restringido para los administradores
· IE Enhanced Security Configuration for Non-Administrators	⦸	El uso de Internet Explorer no está restringido para los no administradores

Tabla 59. MBSA_PTTS

ESVC		
		Resultado
SECURITY UPDATES		
· SQL Server Security Updates	☑	Actualizado
· Windows Security Updates	☑	Actualizado
· Developer Tools, Runtimes, and Redistributables Security Updates	☒	Falta o no aprobada: KB2538243
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· Password Expiration	⦸	Algunos usuarios (1/3) no la tienen habilitada
· Administrators	☑	No más de 2 usuarios "administrador" (2)
· Incomplete Updates	☑	Ninguna
· Windows Firewall	☑	Activado
· Automatic Updates	☑	Configurado por GPO
· File System	☑	Todas configuradas en NTFS (1)
· Guest Account	☑	Deshabilitado
· Autologon	☑	No Configurado
· Restrict Anonymous	☑	Activado
· Local Account Password Test	☑	Algunos usuarios (1/3) tienen contraseña simple o en blanco
Additional System Information		
· Windows Version	✳	Microsoft Windows 2008 R2 SP1
· Shares	✳	C$ y $ADMIN
· Services	✳	Ninguno
SQL SERVER SCAN RESULT: Instance MSSQL10_50.VIM_SQLEXP		
Administrative Vulnerabilities		
· Service Accounts	⦸	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent no deberían ser miembro del grupo Administrador local o arrancado con una cuenta de sistema
· Folder Permissions	☒	Algunos permisos no están bien configurados
· SQL Server/MSDE Security Mode	⦸	Autenticación SQL Server and/or MSDE configurada en modo Windows Mixto
· Exposed SQL Server/MSDE Password	☑	'sa' password y SQL server Account no están en texto claro
· CmdExec role	⦸	Inaccesible

· *Registry Permissions*	☑	El grupo Everyone tiene solo acceso lectura al SQL Server and/or MSDE claves de registro
· *Sysadmin role members*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· *Guest Account*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· *Sysadmins*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· *Domain Controller Test*	☑	SQL Server y/o MSDE no está cargado en un Domain Controller
· *Password Policy*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· *SSIS Role*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
· *Sysdtslog*	✳	ODBC (DBNETLIB) no existe el servidor SQL Server o se ha denegado el acceso
SQL SERVER SCAN RESULT: Instance VIM_SQLEXP		
Administrative Vulnerabilities		
· *Service Accounts*	⦸	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent no deberían ser miembro del grupo Administrador local o arrancado con una cuenta de sistema
· *Folder Permissions*	☑	Permisos bien configurados
· *SQL Server/MSDE Security Mode*	⦸	Autenticación SQL Server and/or MSDE configurada en modo Windows Mixto
· *Exposed SQL Server/MSDE Password*	☑	'sa' password y SQL server Account no están en texto claro
· *CmdExec role*	☑	Restringido sólo al rol sysadmin
· *Registry Permissions*	☑	El grupo Everyone tiene solo acceso lectura al SQL Server and/or MSDE claves de registro
· *Sysadmin role members*	✳	BUILTIN\Administrator no forma parte del rol sysadmin
· *Guest Account*	☑	La cuenta Guest no está habilitada en ninguna base de datos
· *Sysadmins*	⦸	Existen más de 2 miembros del rol sysadmin
· *Domain Controller Test*	☑	SQL Server y/o MSDE no está cargado en un Domain Controller
· *Password Policy*	☒	Habilitar expiración de password para la cuenta SQL Server
· *SSIS Role*	☑	BUILTIN\Admin no pertenece a ningún rol SSIS
· *Sysdtslog*	☑	No existe
SQL SERVER SCAN RESULT: Instance VIM_SQLEXP (32b)		
Administrative Vulnerabilities		
· *Service Accounts*	⦸	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent no deberían ser miembro del grupo Administrador local o arrancado con una cuenta de sistema
· *Folder Permissions*	☑	Permisos bien configurados
· *SQL Server/MSDE Security Mode*	⦸	Autenticación SQL Server and/or MSDE configurada en modo Windows Mixto
· *Exposed SQL Server/MSDE Password*	☑	'sa' password y SQL server Account no están en texto claro
· *CmdExec role*	☑	Restringido sólo al rol sysadmin
· *Registry Permissions*	☑	El grupo Everyone tiene solo acceso lectura al SQL Server and/or MSDE claves de registro
· *Sysadmin role members*	✳	BUILTIN\Administrator no forma parte del rol sysadmin
· *Guest Account*	☑	La cuenta Guest no está habilitada en ninguna base de datos
· *Sysadmins*	⦸	Existen más de 2 miembros del rol sysadmin
· *Domain Controller Test*	☑	SQL Server y/o MSDE no está cargado en un Domain Controller
· *Password Policy*	☒	Habilitar expiración de password para la cuenta SQL Server
· *SSIS Role*	☑	BUILTIN\Admin no pertenece a ningún rol SSIS
· *Sysdtslog*	☑	No existe

DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· IE Zones	☑	Todos los usuarios tienen zonas securizadas
· IE Enhanced Security Configuration for Administrators	☒	El uso de Internet Explorer no está restringido para los administradores
· IE Enhanced Security Configuration for Non-Administrators	⦸	El uso de Internet Explorer no está restringido para los no administradores

Tabla 60. MBSA_ESVC

ESRSA		
		Resultado
SECURITY UPDATES		
· SQL Server Security Updates	☑	Actualizado
· Windows Security Updates	☑	Actualizado
· Developer Tools, Runtimes, and Redistributables Security Updates	☒	Falta o no aprobada: KB2538243
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· Password Expiration	⦸	Algunos usuarios (4/5) no la tienen habilitada
· Administrators	☑	No más de 2 usuarios "administrador" (2)
· Incomplete Updates	☑	Ninguna
· Windows Firewall	☑	Activado
· Automatic Updates	☑	Configurado
· File System	☑	Todas configuradas en NTFS (1)
· Guest Account	☑	Deshabilitado
· Autologon	☑	No Configurado
· Restrict Anonymous	☑	Activado
· Local Account Password Test	☑	Algunos usuarios (1/5) tienen contraseña simple o en blanco
Additional System Information		
· Windows Version	✳	Microsoft Windows 2003 R2 SP2
· Shares	✳	C$ y $ADMIN
· Services	✳	Alguno innecesario: Telnet (Stop)
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· IE Zones	☑	Todos los usuarios tienen zonas securizadas
· IE Enhanced Security Configuration for Administrators	☒	El uso de Internet Explorer no está restringido para los administradores
· IE Enhanced Security Configuration for Non-Administrators	⦸	El uso de Internet Explorer no está restringido para los no administradores

Tabla 61. MBSA_ESRSA

ESBDSAC		
		Resultado
SECURITY UPDATES		
· *SQL Server Security Updates*	☑	Actualizado
· *Windows Security Updates*	☑	Actualizado
· *Developer Tools, Runtimes, and Redistributables Security Updates*	☑	Actualizado
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	⊘	Algunos usuarios (4/6) no la tienen habilitada
· *Administrators*	⊘	Existen más de 2 usuarios "administrador" (4)
· *Incomplete Updates*	☑	Ninguna
· *Windows Firewall*	☒	No configurado
· *Automatic Updates*	☑	Configurado por GPO
· *File System*	☑	Todas configuradas en NTFS (2)
· *Guest Account*	☑	Deshabilitado
· *Autologon*	☑	No Configurado
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	☑	Algunos usuarios (1/6) tienen contraseña simple o en blanco
Additional System Information		
· *Windows Version*	✳	Microsoft Windows 2008 R2 SP1
· *Shares*	✳	C$, E$ y $ADMIN
· *Services*	✳	World Wide Web Publishing Service (Start)
INTERNET INFORMATION SERVICES (IIS) SCAN RESULT		
Administrative Vulnerabilities		
· *IIS Status*	⊘	IIS Common Files no está instalado en el local computer
· *IIS Lockdown Tool*	☑	No necesario para IIS 6.0 en adelante
SQL SERVER SCAN RESULT: Instance (default)		
Administrative Vulnerabilities		
· *Service Accounts*	⊘	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent no deberían ser miembro del grupo Administrador local o arrancado con una cuenta de sistema
· *Folder Permissions*	☒	Algunos permisos no están bien configurados
· *SQL Server/MSDE Security Mode*	⊘	Autenticación SQL Server and/or MSDE configurada en modo Windows Mixto
· *CmdExec role*	☑	Restringido sólo al rol sysadmin
· *Registry Permissions*	☑	El grupo Everyone tiene solo acceso lectura al SQL Server and/or MSDE claves de registro
· *Sysadmin role members*	✳	BUILTIN\Administrator no forma parte del rol sysadmin
· *Guest Account*	☑	La cuenta Guest no está habilitada en ninguna base de datos
· *Sysadmins*	⊘	Existen más de 2 miembros del rol sysadmin
· *Domain Controller Test*	☑	SQL Server y/o MSDE no está cargado en un Domain Controller
· *Password Policy*	☒	Habilitar expiración de password para la cuenta SQL Server
· *SSIS Role*	☑	BUILTIN\Admin no pertenece a ningún rol SSIS
· *Sysdtslog*	✳	Recomendable crear logins diferentes en cada bases de datos
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· *IE Zones*	☒	Algún usuario (1) contiene zonas no securizadas
· *IE Enhanced Security Configuration for Administrators*	☑	El uso de Internet Explorer está restringido para los administradores
· *IE Enhanced Security*	☑	El uso de Internet Explorer está restringido para los no

Configuration for Non-Administrators		administradores

Tabla 62. MBSA_ESBDSAC

ESWWW		
		Resultado
SECURITY UPDATES		
· *SQL Server Security Updates*	☑	Actualizado
· *Windows Security Updates*	☑	Actualizado
WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	⊘	Ningún usuario (6) la tienen habilitada
· *Administrators*	⊘	Existen más de 2 usuarios "administrador" (4)
· *Incomplete Updates*	☑	Ninguna
· *Windows Firewall*	☒	No configurado
· *Automatic Updates*	☑	Configurado por GPO
· *File System*	☑	Todas configuradas en NTFS (2)
· *Guest Account*	☑	Deshabilitado
· *Autologon*	☑	No Configurado
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	☑	Algunos usuarios (1/6) tienen contraseña simple o en blanco
Additional System Information		
· *Windows Version*	✳	Microsoft Windows 2008 R2 SP1
· *Shares*	✳	C$, E$ y $ADMIN
· *Services*	✳	World Wide Web Publishing Service (Start)
INTERNET INFORMATION SERVICES (IIS) SCAN RESULT		
Administrative Vulnerabilities		
· *IIS Status*	⊘	IIS Common Files no está instalado en el local computer
· *IIS Lockdown Tool*	☑	No necesario para IIS 6.0 en adelante
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· *IE Zones*	☑	Todos los usuarios tienen zonas securizadas
· *IE Enhanced Security Configuration for Administrators*	☑	El uso de Internet Explorer está restringido para los administradores
· *IE Enhanced Security Configuration for Non-Administrators*	☑	El uso de Internet Explorer está restringido para los no administradores

Tabla 63. MBSA_ESWWW

ESDC		
		Resultado
SECURITY UPDATES		
· *SQL Server Security Updates*	☑	Actualizado
· *Windows Security Updates*	☑	Actualizado
· *Developer Tools, Runtimes, and Redistributables Security Updates*	☒	Falta o no aprobado: (KB2538243)

WINDOWS SCAN RESULTS		
Administrative Vulnerabilities		
· *Password Expiration*	⦸	Algunos usuarios (15/89) no la tienen habilitada
· *Administrators*	⦸	Existen más de 2 usuarios "administrador" (7)
· *Incomplete Updates*	☑	Ninguna
· *Windows Firewall*	☑	Configurado por GPO
· *Automatic Updates*	☑	Configurado por GPO
· *File System*	☑	Todas configuradas en NTFS (1)
· *Guest Account*	☑	Deshabilitado
· *Autologon*	☑	No configurado
· *Restrict Anonymous*	☑	Activado
· *Local Account Password Test*	✳	No realizado en Domain Controller
Additional System Information		
· *Windows Version*	✳	Microsoft Windows 2008 R2 SP1
· *Shares*	✳	Impresoras compartidas y carpetas de software. C$, SYSVOL y NETLOGON
· *Services*	✳	Ninguno innecesario encontrado
DESKTOP APPLICATION SCAN RESULTS		
Administrative Vulnerabilities		
· *IE Zones*	☑	Todos los usuarios tienen zonas securizadas

Tabla 64. MBSA_ESDC
* El análisis sobre los servidores está realizado a fecha de diciembre de 2013

19.2. Análisis con OpenVAS

OpenVAS (Open Vulnerability Assesment System) es una aplicación OpenSource que nos permite realizar análisis sobre los elementos de seguridad y posibles vulnerabilidades existentes en los equipos. Su uso más importante es el análisis de la comunicación del equipo a partir de puertos o servicios abiertos.

A continuación, detallaremos los reportes realizados a cada servidor indicando el factor de riesgo que conlleva. Analizaremos lo siguiente: el puerto de comunicación abierto o con conexión, la descripción de la vulnerabilidad, el nivel de riesgo que tiene y su posible solución. También indicamos información extra de los puertos gracias a los logs.

Este escáner pretende ser una guía para revisar todas las indicaciones que nos detecta y proceder a su ajuste y solución si fuese necesaria.

ESDTA

Most Severe Result(s)	High	Medium	Low
Severity: High	3	11	7

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
ajp13 (8009/tcp)	**High**	· Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability	· Set the 'secure' attribute for any cookies that are sent over an SSL connection
ntp (123/udp)	**High**	· NTP Stack Buffer Overflow Vulnerability	· Upgrade to NTP version 4.2.4p7-RC2 · CVE: CVE-2009-0159

			· BID: 34481
	High	· NTP 'ntpd' Autokey Stack Overflow Vulnerability	· Apply the security update according to the OS version · CVE: CVE-2009-1252 · BID: 35017
cncp (1636/tcp)	**Medium**	· Check for SSL Weak Ciphers	· Revisar cifrado débil
general /tcp	**Medium**	· TCP timestamps	· Revisar
general /udp	**Medium**	· NTP EVP_VerifyFinal() Security Bypass Vulnerability	· Upgrade to NTP version 4.2.4p6 or 4.2.5p151 · CVE: CVE-2009-0021 · BID: 33150
http (80/tcp)	**Medium**	· Apache Web Server ETag Header Information Disclosure Weakness	· OpenBSD has released a patch to address this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare · CVE: CVE-2003-1418 · BID: 6939
https (443/tcp)	**Medium**	· Apache Web Server ETag Header Information Disclosure Weakness	· OpenBSD has released a patch to address this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare · CVE: CVE-2003-1418 · BID: 6939
	Medium	· Check for SSL Weak Ciphers	· Revisar cifrado débil
ipp (631/tcp)	**Medium**	· Apache Web Server ETag Header Information Disclosure Weakness	· OpenBSD has released a patch to address this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare · CVE: CVE-2003-1418 · BID: 6939
ldap (389/tcp)	**Medium**	· LDAP allows null bases	· Disable NULL BASE queries on your LDAP server
ldaps (636/tcp)	**Medium**	· Check for SSL Weak Ciphers	· Revisar cifrado débil
ssh (22/tcp)	**Medium**	· openssh-server Forced Command Handling Information Disclosure Vulnerability. The version of OpenSSH installed on the remote host is older than 5.7: ssh-1.99-openssh_5.1	· Updates are available · CVE: CVE-2012-0814 · BID: 51702
vnc-1 (5901/tcp)	**Medium**	· VNC security types	· Comunicación permitida
ajp13 (8009/tcp)	**Low**	· No 404 check	· Parece desconfigurado
ntp (123/udp)	**Low**	· NTP read variables	· Set NTP to restrict default access to ignore all info packets: restrict default ignore
ldap (389/tcp)	**Low**	· LDAP Detection	· Comunicación permitida
domain (53/tcp)	**Low**	· Determine which version of BIND name daemon is running. The remote bind version is: 9.6-ESV-R5-P1	· Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts
http-alt (8008/tcp)	**Low**	· No 404 check	· Parece desconfigurado
vnc (5900/tcp)	**Low**	· Check for VNC	· Asegurar que el software es utilizado acorde con la política de seguridad · Filtrar tráfico entrante en este puerto

vnc-http-1 (5801/tcp)	**Low**	· No 404 check	· Parece desconfigurado
general /tcp	**Log**	· Checks for open udp port: o domain (53/udp) o ntp (123/udp) · Traceroute: a través de firewall · Checks for open tcp ports: o https (443/tcp) o http-alt (8008/tcp) o cncp (1636/tcp) o vnc (5900/tcp) o ajp13 (8009/tcp) o vnc-1 (5901/tcp) o ssh (22/tcp) o ldaps (636/tcp) o svrloc (427/tcp) o msn-messenger-voice-chat (6901/tcp) o iclpv-dm (1389/tcp) o vnc-http-1 (5801/tcp) o wbem-https (5989/tcp) o ldap (389/tcp) o ndmp (10000/tcp) o domain (53/tcp) o ncp (524/tcp) o http (80/tcp) o ipp (631/tcp)	
ajp13 (8009/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: NetWare HTTP Stack	
cncp (1636/tcp)	**Log**	· A TLSv1 server answered on this port	
http (80/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Apache/2.2.3 (Linux/SUSE)	
https (443/tcp)	**Log**	· A web server is running on this port through SSL · The remote web server type is: Apache/2.2.3 (Linux/SUSE)	
ipp (631/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Apache/2.2.3 (Linux/SUSE)	
ldaps (636/tcp)	**Log**	· A TLSv1 server answered on this port	
ssh (22/tcp)	**Log**	· An ssh server is running on this port · Detected SSH server version: SSH-1.99-OpenSSH_5.1	
domain (53/tcp)	**Log**	· A DNS Server is running at this Host	
http-alt (8008/tcp)	**Log**	· A web server is running on this port · The remote web server type is: NetWare HTTP Stack	
vnc-http-1 (5801/tcp)	**Log**	· A web server is running on this port	
domain (53/udp)	**Log**	· A DNS Server is running at this Host	
wbem-https (5989/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: openwbem/3.2.0 (CIMOM)	

Tabla 65. OpenVAS_ESDTA

ESACD

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	1

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
general/tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
		· TCP timestamps	· Revisar
ms-sql-s (1433/tcp)	**Low**	· Microsoft SQL TCP/IP listener is running	· Bloquear este puerto de la comunicación externa
general /tcp	**Log**	· Checks for open udp port: None · Traceroute: a través de firewall · Checks for open tcp ports: ○ ms-sql-s (1433/tcp) ○ entextnetwk (12001/tcp) ○ mailbox (2004/tcp) ○ sd (9876/tcp) ○ ms-wbt-server (3389/tcp) ○ rtsserv (2500/tcp) ○ incommand (9400/tcp)	
ms-sql-s (1433/tcp)	**Log**	· MS SQL can be accessed by remote attackers	
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port	

Tabla 66. OpenVAS_ESACD

ESGW

Most Severe Result(s)	High	Medium	Low
Severity: High	3	6	6

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
nfs (2049/udp)	**High**	· NFS export. Please check the permissions of this exports	· CVE: CVE-1999-0554, CVE-1999-0548
ntp (123/udp)	**High**	· NTP Stack Buffer Overflow Vulnerability	· Upgrade to NTP version 4.2.4p7-RC2 · CVE: CVE-2009-0159 · BID: 34481
		· NTP 'ntpd' Autokey Stack Overflow Vulnerability	· Apply the security update according to the OS version · CVE: CVE-2009-1252 · BID: 35017
general /tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 1018
	Medium	· TCP timestamps	· Revisar
general /udp	**Medium**	· NTP EVP_VerifyFinal() Security Bypass Vulnerability	· Upgrade to NTP version 4.2.4p6 or 4.2.5p151 · CVE: CVE-2009-0021 · BID: 33150
netbios-ssn (139/tcp)	**Medium**	· Samba 'client/mount.cifs.c' Remote Denial of Service Vulnerability	· CVE: CVE-2010-0547 · BID: 38326
ssh (22/tcp)	**Medium**	· openssh-server Forced Command Handling Information Disclosure Vulnerability. the version of OpenSSH installed on the remote host is older than 5.7: ssh-1.99-openssh_5.1	· Updates are available · CVE: CVE-2012-0814 · BID: 51702
vnc-1 (5901/tcp)	**Medium**	· VNC security types	· Comunicación permitida
ntp	**Low**	· NTP read variables	· Set NTP to restrict default

(123/udp)			access to ignore all info packets: restrict default ignore
vnc-1 (5901/tcp)	**Low**	· Check for VNC	· Asegurar que el software es utilizado acorde con la política de seguridad · Filtrar tráfico entrante en este puerto
domain (53/tcp)	**Low**	· Determine which version of BIND name daemon is running. The remote bind version is : 9.6-ESV-R5-P1	· Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts
vnc (5900/tcp)	**Low**	· VNC security types	· Comunicación permitida
	Low	· Check for VNC	· Asegurar que el software es utilizado acorde con la política de seguridad · Filtrar tráfico entrante en este puerto
vnc-http-1 (5801/tcp)	**Low**	· No 404 check	· Parece desconfigurado
general /tcp	**Log**	· Checks for open udp port: ○ domain (53/udp) ○ nfs (2049/udp) ○ ntp (123/udp) ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ groupwise (1677/tcp) ○ pop3 (110/tcp) ○ microsoft-ds (445/tcp) ○ vnc (5900/tcp) ○ sunrpc (111/tcp) ○ vpp (677/tcp) ○ vnc-1 (5901/tcp) ○ ssh (22/tcp) ○ font-service (7100/tcp) ○ nfs (2049/tcp) ○ smtp (25/tcp) ○ vnc-http-1 (5801/tcp) ○ netbios-ssn (139/tcp) ○ domain (53/tcp) ○ imap (143/tcp) ○ swat (901/tcp)	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	
ssh (22/tcp)	**Log**	· An ssh server is running on this port · Detected SSH server version: SSH-1.99-OpenSSH_5.1	
domain (53/tcp)	**Log**	· A DNS Server is running at this Host.	
vnc-http-1 (5801/tcp)	**Log**	· A web server is running on this port	
domain (53/udp)	**Log**	· A DNS Server is running at this Host.	
imap (143/tcp)	**Log**	· An IMAP server is running on this port	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
pop3 (110/tcp)	**Log**	· A pop3 server is running on this port	
smtp (25/tcp)	**Log**	· An SMTP server is running on this port. GroupWise Internet Agent 8.0.2	
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port	

Tabla 67. OpenVAS_ESGW

ESIMG

Most Severe Result(s)	High	Medium	Low
Severity: High	11	18	6

Resultado por HOST

Service (Port)	*Threat Level*	*Description*	*Solution*
ajp13 (8009/tcp)	**High**	· Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability	· Set the 'secure' attribute for any cookies that are sent over an SSL connection
http (80/tcp)	**High**	· Apache httpd Web Server Range Header Denial of Service Vulnerability	· Revisar (3) · CVE: CVE-2011-3192 · BID: 49303
		· http TRACE XSS attack	· CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604
https (443/tcp)	**High**	· Apache httpd Web Server Range Header Denial of Service Vulnerability	· Revisar (3) · CVE: CVE-2011-3192 · BID: 49303
	High	· http TRACE XSS attack	· CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604
ici (2200/tcp)	**High**	· Apache httpd Web Server Range Header Denial of Service Vulnerability	· Revisar (3) · CVE: CVE-2011-3192 · BID: 49303
	High	· http TRACE XSS attack	· CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604
ldap (389/tcp)	**High**	· Novell eDirectory Multiple Security Vulnerabilities	· An update is available · CVE: CVE-2012-0428, CVE-2012-0429, CVE-2012-0430, CVE-2012-0432 · BID: 57038
	High	· Novell eDirectory '/dhost/modules?I:' Buffer Overflow Vulnerability	· CVE: CVE-2009-4653 · BID: 37009
	High	· Novell eDirectory Multiple Remote Vulnerabilities	· CVE: CVE-2009-4653 · BID: 40541
	High	· Novell eDirectory 'DHOST' Cookie Hijack Vulnerability	· CVE: CVE-2009-4655
http (80/tcp)	**Medium**	· Apache Web Server ETag Header Information Disclosure Weakness	· OpenBSD has released a patch to address this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare · CVE: CVE-2003-1418 · BID: 6939
	Medium	· Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	· Upgrade to Apache HTTP Server version 2.2.22 or later · CVE: CVE-2012-0053 · BID: 51706
	Medium	· Apache Tomcat mod_jk Information Disclosure Vulnerability	· Upgrade to mod_jk 1.2.27 or later · CVE: CVE-2008-5519 · BID: 34412
https (443/tcp)	**Medium**	· Apache Web Server ETag Header Information Disclosure Weakness	· OpenBSD has released a patch to address this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare · CVE: CVE-2003-1418 · BID: 6939
	Medium	· Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	· Upgrade to Apache HTTP Server version 2.2.22 or later · CVE: CVE-2012-0053 · BID: 51706
	Medium	· Apache Tomcat mod_jk Information Disclosure Vulnerability	· Upgrade to mod_jk 1.2.27 or later · CVE: CVE-2008-5519 · BID: 34412

ici (2200/tcp)	**Medium**	· Apache Web Server ETag Header Information Disclosure Weakness	· OpenBSD has released a patch to address this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare · CVE: CVE-2003-1418 · BID: 6939
	Medium	· Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	· Upgrade to Apache HTTP Server version 2.2.22 or later · CVE: CVE-2012-0053 · BID: 51706
	Medium	· Apache Tomcat mod_jk Information Disclosure Vulnerability	· Upgrade to mod_jk 1.2.27 or later · CVE: CVE-2008-5519 · BID: 34412
ldap (389/tcp)	**Medium**	· Novell eDirectory NULL Base DN Denial Of Service Vulnerability	· Updates are available · CVE: CVE-2009-3862 · BID: 36902
	Medium	· Novell eDirectory eMBox SOAP Request Denial Of Service Vulnerability	· Updates are available · CVE: CVE-2010-0666 · BID: 38157
	Medium	· Novell eDirectory Server Malformed Index Denial Of Service Vulnerability	· Updates are available · BID: 43662
	Medium	· LDAP allows null bases	· Disable NULL BASE queries on your LDAP server
general /tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
ldaps (636/tcp)	**Medium**	· Check for SSL Weak Ciphers	· Revisar
ncp (524/tcp)	**Medium**	· Netware NDS Object Enumeration	· The NDS object PUBLIC should not have Browse rights the tree should be restricted to authenticated users only
wbem-https (5989/tcp)	**Medium**	· Check for SSL Weak Ciphers	· Revisar cifrado débil
	Medium	· SSL Certificate Expiry	· Revisar
http (80/tcp)	**Low**	· Apache mod_jk Module Version Detection	· Mod JK version 1.2.21 was detected on the host
https (443/tcp)	**Low**	· Apache mod_jk Module Version Detection	· Mod JK version 1.2.21 was detected on the host
ici (2200/tcp)	**Low**	· Apache mod_jk Module Version Detection	· Mod JK version 1.2.21 was detected on the host
ldap (389/tcp)	**Low**	· LDAP Detection	· Conexión permitida
afpovertcp (548/tcp)	**Low**	· AppleShare IP Server status query. Machine type: Novell NetWare 5.70.07	· Conexión permitida
ntp (123/udp)	**Low**	· NTP read variables	· Comunicación permitida
general /tcp	**Log**	· Checks for open udp port: ○ snmp (161/udp) ○ ntp (123/udp) ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ hosts2-ns (81/tcp) ○ https (443/tcp) ○ afpovertcp (548/tcp) ○ http-alt (8008/tcp) ○ ajp13 (8009/tcp) ○ sunrpc (111/tcp) ○ ldaps (636/tcp) ○ pichat (9009/tcp) ○ pichat (9009/tcp) ○ msn-messenger-voice-chat (6901/tcp) ○ ici (2200/tcp)	

		○ wbem-https (5989/tcp) ○ ldap (389/tcp) ○ netbios-ssn (139/tcp) ○ btrieve (3351/tcp) ○ ncp (524/tcp) ○ http (80/tcp)
ajp13 (8009/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: NetWare HTTP Stack
http (80/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Apache/2.0.59 (NETWARE) mod_jk/1.2.21
https (443/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: Apache/2.0.59 (NETWARE) mod_jk/1.2.21
ici (2200/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: Apache/2.0.59 (NETWARE) mod_jk/1.2.21
ldap (389/tcp)	**Log**	· Detected Novell eDirectory version: 8.8 SP3 (20216.80)
ldaps (636/tcp)	**Log**	· A TLSv1 server answered on this port
wbem-https (5989/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: openwbem/3.1.0 (CIMOM)
hosts2-ns (81/tcp)	**Log**	· A web server is running on this port · The remote web server type is: NetWare HTTP Stack
http-alt (8008/tcp)	**Log**	· A web server is running on this port · The remote web server type is: NetWare HTTP Stack
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered
snmp (161/udp)	**Log**	· A SNMP server is running on this host

Tabla 68. OpenVAS_ESIMG

ESPING

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	3	0

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
general /tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
		· TCP timestamps	· Revisar
ssh (22/tcp)	**Medium**	· openssh-server Forced Command Handling Information Disclosure Vulnerability. the version of OpenSSH installed on the remote host is older than 5.7: ssh-1.99-openssh_4.1	· Updates are available · CVE: CVE-2012-0814 · BID: 51702
general /tcp	**Log**	· Checks for open udp ports: None · Traceroute: directly · Checks for open tcp ports: ○ sunrpc (111/tcp) ○ ssh (22/tcp) ○ ipp (631/tcp)	
ssh (22/tcp)	**Log**	· An ssh server is running on this port · Detected SSH server version: SSH-1.99-OpenSSH_4.1	
ipp (631/tcp)	**Log**	· A web server is running on this port. · The remote web server type is: CUPS/1.1	

Tabla 69. OpenVAS_ESPING

ESEDI

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	5	6

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
compaq-https (2381/tcp)	**Medium**	· Remote Compaq HTTP server detection: 9.9 HP System Management Homepage	· Revisar utilidad web
cpq-wbem (2301/tcp)	**Medium**	· Remote Compaq HTTP server detection: 9.9 HP System Management Homepage	· Revisar utilidad web
epmap (135/tcp)	**Medium**	· DCE services running on the remote host · DCE services running Ports: 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, 49183/tcp, 49186/tcp	· Filtrar tráfico entrante en este puerto · También usada para la aplicación Panda EndPoint
general /tcp	**Medium**	TCP timestamps	· Revisar
compaq-https (2381/tcp)	**Low**	· No 404 check	· Parece desconfigurado
cpq-wbem (2301/tcp)	**Low**	· No 404 check	· Parece desconfigurado
ms-sql-m (1434/udp)	**Low**	· Microsoft SQL UDP Info Query	· Filtrar tráfico entrante en este puerto
ms-sql-s (1433/tcp)	**Low**	· Microsoft SQL TCP/IP listener is running	· Bloquear este puerto de la comunicación externa
vnc (5900/tcp)	**Low**	· VNC security types · Check for VNC	· Comunicación permitida · Asegurar que el software es utilizado acorde con la política de seguridad
general /tcp	**Log**	· Checks for open udp ports: o netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: o compaq-https (2381/tcp) o microsoft-ds (445/tcp) o vnc (5900/tcp) o cpq-wbem (2301/tcp) o epmap (135/tcp) o ms-sql-s (1433/tcp) o ndmp (10000/tcp) o netbios-ssn (139/tcp) o ms-wbt-server (3389/tcp)	
compaq--https (2381/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port	
cpq-wbem (2301/tcp)	**Log**	· A web server is running on this port	
ms-sql-s (1433/tcp)	**Log**	· MS SQL can be accessed by remote attackers	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port	
ndmp (tcp/10000)	**Log**	· Symantec Backup Exec 13.0.5204.127	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	

Tabla 70. OpenVAS_ESEDI

CONTROL

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	4

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
epmap (135/tcp)	**Medium**	· DCE (2) services running on the remote host · DCE services running · Port: 1030/tcp	· Filtrar tráfico entrante en este puerto
ntp (123/udp)	**Low**	· NTP read variables	· Comunicación permitida
vnc (5900/tcp)	**Low**	· VNC security types · Check for VNC	· Comunicación permitida · Asegurar que el software es utilizado acorde con la política de seguridad · Filtrar tráfico entrante en este puerto
vnc-http (5800/tcp)	**Low**	· No 404 check	· Parece desconfigurado
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp) ○ ntp (123/udp) · Traceroute: directly · Checks for open tcp ports: ○ microsoft-ds (445/tcp) ○ ndmp (10000/tcp) ○ netbios-ssn (139/tcp) ○ qencp (2120/tcp) ○ svrloc (427/tcp) ○ iad1 (1030/tcp) ○ vnc (5900/tcp) ○ vnc-http (5800/tcp) ○ epmap (135/tcp)	
vnc-http (5800/tcp)	**Log**	· A web server is running on this port	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	

Tabla 71. OpenVAS_CONTROL

NETXUS

Most Severe Result(s)	High	Medium	Low
Severity: High	7	5	9

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
ftp (21/tcp)	**High**	· Microsoft IIS FTPd NLST stack overflow	· Filtrar tráfico entrante en este puerto · CVE: CVE-2009-3023
http (80/tcp)	**High**	· IIS .IDA ISAPI filter applied	· unmap the .IDA extension · CVE: CVE-2001-0500 · BID: 2880
	High	· http TRACE XSS attack	· Disable these methods. · CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604

microsoft-ds (445/tcp)	**High**	· Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote	· Revisar (5) · CVE: CVE-2008-4114, CVE-2008-4834, CVE-2008-4835 · BID:31179
	High	· Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	· Revisar (6) · CVE: CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231
ms-wbt-server (3389/tcp)	**High**	· Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)	· Revisar (7) · CVE: CVE-2012-0002, CVE-2012-0152 · BID: 52353, 52354
smtp (25/tcp)	**High**	· Microsoft Windows SMTP Server DNS spoofing vulnerability	· CVE: CVE-2010-1690, CVE-2010-1689 · BID: 39910, 39908
http (80/tcp)	**Medium**	· Microsoft IIS IP Address/Internal Network Name Disclosure Vulnerability	· (8) · BID: 3159
smtp (25/tcp)	**Medium**	· Microsoft Windows SMTP Server MX Record Denial of Service Vulnerability	· CVE: CVE-2010-0024, CVE-2010-0025 · BID: 39308, 39381
epmap (135/tcp)	**Medium**	· DCE services running on the remote host	· Filtrar tráfico entrante en este puerto
		· DCE services running · Port: 1025/tcp, 1026/tcp, 1027/tcp, 1029/tcp, 1030/tcp	
general/tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
ftp (21/tcp)	**Low**	· FTP Server type and version 5.0	· Revisar
http (80/tcp)	**Low**	· Windows SharePoint Services detection	· Comunicación permitida
	Low	· HTTP TRACE	
ms-wbt-server (3389/tcp)	**Low**	· Microsoft Remote Desktop Protocol Detection	· Comunicación permitida
smtp (25/tcp)	**Low**	· SMTP Server type and version	· Revisar
nntp (119/tcp)	**Low**	· News Server type and version	· Comunicación permitida
	Low	· Misc information on News server	
vnc (5900/tcp)	**Low**	· VNC security types	· Comunicación permitida · Asegurar que el software es utilizado acorde con la política de seguridad · Filtrar tráfico entrante en este puerto
		· Check for VNC	
general /tcp	**Log**	· Checks for open udp ports: o netbios-ns (137/udp) · Traceroute: a través de Firewall · Checks for open tcp ports: o https (443/tcp) o blackjack (1025/tcp) o cap (1026/tcp) o microsoft-ds (445/tcp) o exosee (1027/tcp) o vnc (5900/tcp) o ftp (21/tcp) o ms-lsa (1029/tcp) o epmap (135/tcp) o vnc-http (5800/tcp) o smtp (25/tcp) o netbios-ssn (139/tcp) o ms-wbt-server (3389/tcp) o nntp (119/tcp) o nntps (563/tcp) o tip2 (3372/tcp) o http (80/tcp)	
ftp (21/tcp)	**Log**	· An FTP server is running on this port	
http (80/tcp)	**Log**	· A web server is running on this port	

		· The remote web server type is: Microsoft-IIS/5.0
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port
smtp (25/tcp)	**Log**	· An SMTP server is running on this port
nntp (119/tcp)	**Log**	· An NNTP server is running on this port
https (443/tcp)	**Log**	· An unknown service is running on this port.
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port
nntps (563/tcp)	**Log**	· An unknown service is running on this port.
tip2 (3372/tcp)	**Log**	· A MSDTC server is running on this port
vnc-http (5800/tcp)	**Log**	· A web server is running on this port

Tabla 72. OpenVAS_NETXUS

PROXY

Most Severe Result(s)	High	Medium	Low
Severity: High	1	6	2

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
http-alt (8080/tcp)	**High**	· Squid information-disclosure vulnerability	· CVE: CVE-2009-1211 · BID: 33858
medium http-alt (8080/tcp)	**Medium**	· Squid Proxy String Processing NULL Pointer Dereference Denial Of Service Vulnerability	· Updates are available · CVE: CVE-2010-3072 · BID: 42982
	Medium	· Squid Header-Only Packets Remote Denial of Service Vulnerability	· CVE: CVE-2010-0308 · BID: 37522
general /tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
	Medium	· TCP timestamps	· Revisar
ssh (22/tcp)	**Medium**	· openssh-server Forced Command Handling Information Disclosure Vulnerability. The version of OpenSSH installed on the remote host is older than 5.7: ssh-2.0-openssh_5.4	· Updates are available · CVE: CVE-2012-0814 · BID: 51702
xdmcp (177/udp)	**Medium**	· X Display Manager Control Protocol (XDMCP)	· Disable XDMCP
http-alt (8080/tcp)	**Low**	· HTTP TRACE	· Revisar
vnc-http-1 (5801/tcp)	**Low**	· No 404 check	· Parece desconfigurado
general /tcp	**Log**	· Checks for open udp ports: o xdmcp (177/udp) · Traceroute: directly · Checks for open tcp ports: o sunrpc (111/tcp) o ssh (22/tcp) o http-alt (8080/tcp) o vnc-http-1 (5801/tcp)	
http-alt (8080/tcp)	**Log**	· A web server is running on this port · An HTTP proxy is running on this port · The remote web server type is: squid/3.0.STABLE25	
ssh (22/tcp)	**Log**	· An ssh server is running on this port · Detected SSH server version: SSH-2.0-OpenSSH_5.4	
vnc-http-1 (5801/tcp)	**Log**	· A web server is running on this port	

Tabla 73. OpenVAS_PROXY

ESMIS

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	3	5

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
epmap (135/tcp)	**Medium**	· DCE services running on the remote host · DCE services running · Ports: 1025/tcp	· Filtrar tráfico entrante en este puerto
http (80/tcp)	**Medium**	· Microsoft IIS Tilde Character Information Disclosure Vulnerability	· BID: 54251
http (80/tcp)	**Low**	· The remote IIS server seems to be Microsoft IIS 6.0. Build 3790 · Windows SharePoint Services detection. X-AspNet-Version: 1.1.4322	· Actualizar la versión
m2ua (2904/tcp)	**Low**	· Check open ports	· Revisar
m3ua (2905/tcp)	**Low**	· Check open ports	
vnc (5900/tcp)	**Low**	· VNC security types	· Comunicación permitida
general /tcp	**Log**	· Checks for open udp ports: o netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: o blackjack (1025/tcp) o m2ua (2904/tcp) o m3ua (2905/tcp) o microsoft-ds (445/tcp) o vnc (5900/tcp) o epmap (135/tcp) o vnc-http (5800/tcp) o ndmp (10000/tcp) o netbios-ssn (139/tcp) o http (80/tcp) o naap (1340/tcp)	
http (80/tcp)	**Log**	· A web server is running on this port · File/Folder name found on server starting with :aspnet · The remote web server is: Microsoft-IIS/6.0	BID: 54251
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	
vnc-http (5800/tcp)	**Log**	· A web server is running on this port	

Tabla 74. OpenVAS_ESMIS

ESTS1

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	3

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
epmap (135/tcp)	**Medium**	· DCE services running on the remote host · DCE services running	· Filtrar tráfico entrante en este puerto

		· Ports: 1035/tcp, 1047/tcp	
ms-wbt-server (3389/tcp)	**Low**	· Microsoft Remote Desktop Protocol Detection	· Comunicación permitida
vnc (5900/tcp)	**Low**	· VNC security types	· Comunicación permitida
		· Check for VNC	· Asegurar que el software es utilizado acorde con la política de seguridad · Filtrar tráfico entrante en este puerto
general /tcp	**Log**	· Checks for open udp ports: o netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: o autocuelog (3104/tcp) o neod1 (1047/tcp) o microsoft-ds (445/tcp) o vnc (5900/tcp) o svrloc (427/tcp) o amanda (10080/tcp) o epmap (135/tcp) o vnc-http (5800/tcp) o mxxrlogin (1035/tcp) o netbios-ssn (139/tcp) o ms-wbt-server (3389/tcp)	
amanda (10080/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Apache-Coyote/1.1	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	

Tabla 75. OpenVAS_ESTS1

ESTS3

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	1

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
epmap (135/tcp)	**Medium**	· DCE services running on the remote host	· Filtrar tráfico entrante en este puerto
		· DCE services running · Ports: 1036/tcp	
ms-wbt-server (3389/tcp)	**Low**	· Microsoft Remote Desktop Protocol Detection	· Comunicación permitida
general /tcp	**Log**	· Checks for open udp ports: o netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: o openvpn (1194/tcp) o microsoft-ds (445/tcp) o svrloc (427/tcp) o epmap (135/tcp) o pcg-radar (1036/tcp) o ndmp (10000/tcp) o netbios-ssn (139/tcp) o ms-wbt-server (3389/tcp)	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	

netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port

Tabla 76. OpenVAS_ESTS3

ESTS4

Most Severe Result(s)	High	Medium	Low
Severity: High	3	7	6

Resultado por HOST			
Service (Port)	***Threat Level***	***Description***	***Solution***
compaq-https (2381/tcp)	**High**	· Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability	· Set the 'secure' attribute for any cookies that are sent over an SSL connection
cpq-wbem (2301/tcp)	**High**	· HP System Management Homepage Multiple Vulnerabilities (July 2012)	· Upgrade to HP System Management Homepage version 7.1.1 or later · CVE: CVE-2012-2012, CVE-2012-2013, CVE-2012-2014, CVE-2012-2015, CVE-2012-2016 · BID: 54218
		· HP System Management Homepage Multiple Vulnerabilities (July 2013)	· CVE: CVE-2013-3576 · BID: 60471
cpq-wbem (2301/tcp)	**Medium**	· HP System Management Homepage Multiple Vulnerabilities (July 2013)	· Upgrade to version 7.2.1 or later · CVE: CVE-2012-5217, CVE-2013-2355, CVE-2013-2356, CVE-2013-2357, CVE-2013-2358, CVE-2013-2359, CVE-2013-2360, CVE-2013-2361, CVE-2013-2362, CVE-2013-2363, CVE-2013-2364, CVE-2013-4821 · BID: 61340, 61338, 61333, 61332, 61339, 61342, 61343, 61336, 61337, 61335, 61341
		· HP System Management Homepage Cross-site scripting Vulnerability	· Upgrade to HP SMH version 6.0.0.96 (for windows), 6.0.0-95 (for linux) · CVE: CVE-2009-4185 · BID: 38081
		· HP System Management Homepage Unspecified XSS Vulnerability	· Update to version 2.1.15.210 or later · CVE: CVE-2008-4411 · BID: 31663
		· HP System Management Homepage Unspecified XSS Vulnerability	· Upgrade to version 3.0.1.73 or later · CVE: CVE-2009-1418 · BID: 35031
		· HP System Management Homepage Multiple Vulnerabilities	· Upgrade to HP System Management Homepage 6.2 or later · CVE: CVE-2010-3284, CVE-2010-3283
epmap (135/tcp)	**Medium**	· DCE services running on the remote host	· Filtrar tráfico entrante en este puerto
		· DCE services running · Ports: 1026/tcp, 1032/tcp	
compaq-https (2381/tcp)	**Low**	· No 404 check	· Parece desconfigurado
cpq-wbem (2301/tcp)	**Low**	· No 404 check	· Parece desconfigurado
ms-sql-m (1434/udp)	**Low**	· Microsoft SQL UDP Info Query	· Filtrar tráfico entrante en este puerto
ms-sql-s	**Low**	· Microsoft SQL TCP/IP	· Bloquear este puerto de la comunicación externa

(1433/tcp)		listener is running	
ms-wbt-server (3389/tcp)	**Low**	· Microsoft Remote Desktop Protocol Detection	· Comunicación permitida
wbem-https (5989/tcp)	**Low**	· No 404 check	· Parece desconfigurado
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ compaq-https (2981/tcp) ○ cap (1026/tcp) ○ microsoft-ds (445/tcp) ○ cpq-wbem (2301/tcp) ○ svrloc (427/tcp) ○ iad3 (1032/tcp) ○ emap (135/tcp) ○ ms-sql-s (1433/tcp) ○ wbem-https (5989/tcp) ○ ndmp (10000/tcp) ○ netbios-ssn (139/tcp) ○ ms-wbt-server (3389/tcp) ○ advant-lm (2295/tcp)	
compaq-https (2381/tcp)	**Log**	· A web server is running on this port through SSL · TLSv1 is answered on this port	
cpq-wbem (2301/tcp)	**Log**	· A web server is running on this port	
ms-sql-s (1433/tcp)	**Log**	· MS SQL can be accessed by remote attackers	
wbem-https (5989/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	

Tabla 77. OpenVAS_ESTS4

ESTS5

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	1

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
epmap (135/tcp)	**Medium**	· DCE services running on the remote host · DCE services running · Ports: 1036/tcp, 1056/tcp	· Filtrar tráfico entrante en este puerto
ms-wbt-server (3389/tcp)	**Low**	· Microsoft Remote Desktop Protocol Detection	· Comunicación permitida
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ vfo (1056/tcp) ○ microsoft-ds (445/tcp) ○ svrloc (427/tcp) ○ epmap (135/tcp)	

		○ pcg-radar (1036/tcp) ○ ndmp (10000/tcp) ○ netbios-ssn (139/tcp) ○ ms-wbt-server (3389/tcp)
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port

Tabla 78. OpenVAS_ESTS5

ESTS8

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	5	4

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
epmap (135/tcp)	**Medium**	· DCE services running on the remote host · DCE services running · Ports: 5722/tcp, 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, 49158/tcp, 49159/tcp, 51053/tcp, 61674/tcp, 62713/tcp, 62719/tcp, 64393/tcp	· Filtrar tráfico entrante en este puerto
general/tcp	**Medium**	· TCP timestamps	· Revisar
ldap (389/tcp)	**Medium**	· LDAP allows null bases	· Disable NULL BASE queries on your LDAP server
		· Use LDAP search request to retrieve information from NT Directory Services	· execute the command: net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete
ldap (389/tcp)	**Low**	· LDAP Detection	· Comunicación permitida
domain (53/tcp)	**Low**	· Microsoft DNS server internal hostname disclosure detection 0.in-addr.arpa/SOA/IN, 255.in-addr.arpa/SOA/IN	· Comunicación permitida
ntp (123/udp)	**Low**	· NTP read variables	· Comunicación permitida
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp) ○ kerberos (88/udp) ○ ntp (123/udp) ○ domain (53/udp) · Traceroute: directly · Checks for open tcp ports: ○ kpasswd (464/tcp) ○ microsoft-ds (445/tcp) ○ http-rpc-epmap (593/tcp) ○ ldaps (636/tcp) ○ epmap (135/tcp) ○ kerberos (88/tcp) ○ ldap (389/tcp) ○ ndmp (10000/tcp) ○ netbios-ssn (139/tcp) ○ ms-wbt-server (3389/tcp) ○ domain (53/tcp) ○ msft-gc (3268/tcp) ○ msft-gc-ssl (3269/tcp)	
dns (53/tcp)	**Log**	· A DNS Server is running at this Host	
dns (53/udp)	**Log**	· A DNS Server is running at this Host	
kerberos (88/tcp)	**Log**	· A Kerberos Server is running at this port	

kerberos (88/udp)	**Log**	· A Kerberos Server is running at this port
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port

Tabla 79. OpenVAS_ESTS8

ESCTL

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	0

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
general /tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
	Medium	· TCP timestamps	· Revisar
general /tcp	**Log**	· Checks for open udp ports: None · Traceroute: a través de firewall · Checks for open tcp ports: ○ smtp (25/tcp)	
smtp (25/tcp)	**Log**	· An SMTP server is running on this port	

Tabla 80. OpenVAS_ESCTL

ESBES

Most Severe Result(s)	High	Medium	Low
Severity: High	2	4	3

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
cslistener (9000/tcp)	**High**	· Trojan horses. It is sometimes opened by this/these Trojan horse(s): DevilRobber.A, Netministrator, W32.Randex, W32.Mytob, W32.Esbot	· Verificar con antivirus un posible troyano alojado
https (443/tcp)	**High**	· JBoss Enterprise Application Platform Multiple Remote Vulnerabilities	· Actualizar la versión · CVE: CVE-2010-3708, CVE-2010-3862, CVE-2010-3878 · BID: 45148
https (443/tcp)	**Medium**	· JBoss Enterprise Application Platform Multiple Vulnerabilities	· Actualizar la versión · CVE: CVE-2010-0738, CVE-2010-1428, CVE-2010-1429 · BID: 39710
epmap (135/tcp)	**Medium**	· DCE services running on the remote host	· Filtrar tráfico entrante en este puerto
	Medium	· DCE services running · Ports: 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, 49210/tcp	
general /tcp	**Medium**	· TCP timestamps	· Revisar
https (443/tcp)	**Low**	· SSL Certificate Expiry	· Revisar

vnc (5900/tcp)	**Low**	· VNC security types	· Comunicación permitida
		· Check for VNC	· Asegurar que el software es utilizado acorde con la política de seguridad · Filtrar tráfico entrante en este puerto
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ https (443/tcp) ○ microsoft-ds (445/tcp) ○ vnc (5900/tcp) ○ epmap (135/tcp) ○ vnc-http (5800/tcp) ○ netbios-ssn (139/tcp) ○ ms-wbt-server (3389/tcp) ○ cslistener (9000/tcp)	
https (443/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: Apache-Coyote/1.1	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	
vnc-http (5800/tcp)	**Log**	· A web server is running on this port	

Tabla 81. OpenVAS_ESBES

ESSD

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	2

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
epmap (135/tcp)	**Medium**	· DCE services running on the remote host	· Filtrar tráfico entrante en este puerto
	Medium	· DCE services running · Ports: 1037/tcp	
http_alt (8080/tcp)	**Low**	· ManageEngine ServiceDesk Plus Detection	· Comunicación permitida
ms-wbt-server (3389/tcp)	**Low**	· Microsoft Remote Desktop Protocol Detection	· Comunicación permitida
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ microsoft-ds (445/tcp) ○ svrloc (427/tcp) ○ epmap (135/tcp) ○ http-alt (8080/tcp) ○ LiebDevMgmt_A (3029/tcp) ○ startron (1057/tcp) ○ ndmp (10000/tcp) ○ netbios-ssn (139/tcp) ○ nim (1058/tcp)	

		○ ms-wbt-server (3389/tcp) ○ kiosk (1061/tcp)
http_alt (8080/tcp)	**Log**	· A web server is running on this port through SSL · The remote web server type is: Apache-Coyote/1.1
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port

Tabla 82. OpenVAS_ESSD

ESBKP

Most Severe Result(s)	High	Medium	Low
Severity: High	10	16	6

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
hosts2-ns (81/tcp)	**High**	· Apache Tomcat Windows Installer Privilege Escalation Vulnerability	· Revisar (1) · CVE: CVE-2009-3548 · BID: 36954
	High	· Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service Vulnerabilities	· Actualizar la versión · CVE: CVE-2010-2227 · BID: 41544
	High	· Apache Tomcat Multiple Vulnerabilities January 2010	· Actualizar la versión · CVE: CVE-2009-2901, CVE-2009-2902, CVE-2009-2693 · BID: 37945, 37942, 37944
http-alt (8080/tcp)	**High**	· Trojan horses. It is sometimes opened by this/these Trojan horse(s): Brown Orifice, Generic backdoor, RemoConChubo, Reverse WWW, Tunnel Backdoor, RingZero, MyDoom, Nemog, Webus, W32.Spybot, Feutel, W32.Mytob, W32.Picrate, W32.Kelvir, W32.Opanki, Haxdoor, W32.Zotob, Tjserv, W32.Botter, W32.Looksky, Ryknos, Naninf, Hesive	· Verificar con antivirus un posible troyano alojado
https (443/tcp)	**High**	· Multiple SonicWALL Products Authentication Bypass Vulnerability	· Actualizar la versión · CVE: CVE-2013-1359, CVE-2013-1360 · BID: 57445
	High	· Apache Tomcat Windows Installer Privilege Escalation Vulnerability	· Revisar (1) · CVE: CVE-2009-3548 · BID: 36954
	High	· Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service Vulnerabilities	· Actualizar la versión · CVE: CVE-2010-2227 · BID: 41544
	High	· Apache Tomcat Multiple Vulnerabilities January 2010	· Actualizar la versión · CVE: CVE-2009-2901, CVE-2009-2902, CVE-2009-2693 · BID: 37945, 37942, 37944
remoteware-cl (3000/tcp)	**High**	· Trojan horses. It is sometimes opened by this/these Trojan horse(s): FirstClass, InetSpy, Remote Shut, Kutex, W32.Mimail	· Verificar con antivirus un posible troyano alojado
	High	· Trojan horses. It is sometimes opened by this/these Trojan horse(s): FirstClass, InetSpy, Remote Shut, Kutex, W32.Mimail	
hosts2-ns (81/tcp)	**Medium**	· Apache Tomcat Multiple Security Bypass Vulnerabilities (Windows)	· Apply patch or upgrade Apache Tomcat to 5.5.36, 6.0.36, 7.0.30 or later · CVE: CVE-2012-5887, CVE-2012-5886, CVE-2012-5885 · BID: 56403

	Medium	· Apache Tomcat HTTP NIO Denial Of Service Vulnerability (Windows)	· Apply patch or upgrade Apache Tomcat to 6.0.36, 7.0.28 or later · CVE: CVE-2012-2733 · BID: 56402
	Medium	· Apache Tomcat NIO Connector Denial of Service Vulnerability	· Upgrade Apache Tomcat version to 6.0.32, 7.0.8 or later · CVE: CVE-2011-0534 · BID: 46164
	Medium	· Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilities	· Actualizar la versión · CVE: CVE-2010-4172 · BID: 45015
	Medium	· Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability	· Actualizar la versión · CVE: CVE-2010-1157 · BID: 39635
	Medium	· Apache Tomcat Security bypass vulnerability	· Upgrade to the latest version of Apache Tomcat 5.5.30 or 6.0.27 or later · CVE: CVE-2010-1157 · BID: 39635
https (443/tcp)	**Medium**	· Apache Tomcat Multiple Security Bypass Vulnerabilities (Windows)	· Apply patch or upgrade Apache Tomcat to 5.5.36, 6.0.36, 7.0.30 or later · CVE: CVE-2012-5887, CVE-2012-5886, CVE-2012-5885 · BID: 56403
	Medium	Apache Tomcat HTTP NIO Denial Of Service Vulnerability (Windows)	· Apply patch or upgrade Apache Tomcat to 6.0.36, 7.0.28 or later · CVE: CVE-2012-2733 · BID: 56402
	Medium	· Apache Tomcat NIO Connector Denial of Service Vulnerability	· Upgrade Apache Tomcat version to 6.0.32, 7.0.8 or later · CVE: CVE-2011-0534 · BID: 46164
	Medium	· Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilities	· Actualizar la versión · CVE: CVE-2010-4172 · BID: 45015
	Medium	· Check for SSL Weak Ciphers	· Revisar cifrados débiles
	Medium	· Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability	· Actualizar la versión · CVE: CVE-2010-1157 · BID: 39635
	Medium	· Apache Tomcat Security bypass vulnerability	· Upgrade to the latest version of Apache Tomcat 5.5.30 or 6.0.27 or later · CVE: CVE-2010-1157 · BID: 39635
epmap (135/tcp)	**Medium**	· DCE services running on the remote host	· Filtrar tráfico entrante en este puerto
	Medium	· DCE services running · Ports: 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, 57900/tcp, 57907/tcp	
general /tcp	**Medium**	TCP timestamps	· Revisar
hosts2-ns (81/tcp)	**Low**	· Apache Tomcat SecurityManager Security Bypass Vulnerability	· Upgrade Apache Tomcat version to 5.5.33, 6.0.30, 7.0.4 or later · CVE: CVE-2010-3718 · BID: 46177
https (443/tcp)	**Low**	· Apache Tomcat SecurityManager Security Bypass Vulnerability	· Upgrade Apache Tomcat version to 5.5.33, 6.0.30, 7.0.4 or later CVE: CVE-2010-3718 BID: 46177
general /tcp	**Low**	· FileZilla Server Version Detection	· Actualizar la versión

ftp (21/tcp)	**Low**	· FTP Server type and version 0.9.40	· Actualizar la versión
http (80/tcp)	**Low**	· Windows SharePoint Services detection. Microsoft-IIS/7.5. X-AspNet-Version: 2.0.50727	· Revisar
ms-sql-m (1434/udp)	**Low**	· Microsoft's SQL UDP Info Query	· Filtrar tráfico entrante en este puerto
general /tcp	**Log**	· Checks for open udp ports: o netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: o hosts2-ns (81/tcp) o https (443/tcp) o remoteware-cl (3000/tcp) o neod1 (1047/tcp) o microsoft-ds (445/tcp) o csdm (1048/tcp) o neod2 (1468/tcp) o remoteware-srv (3002/tcp) o ajp13 (8009/tcp) o ftp (21/tcp) o sunrpc (111/tcp) o synchronet-rtc (6101/tcp) o nfs (2049/tcp) o epmap (135/tcp) o http-alt (8080/tcp) o mpsserver (6106/tcp) o remoteware-un (2999/tcp) o ndmp (10000/tcp) o netbios-ssn (139/tcp) o ms-wbt-server (3389/tcp) o gauntlet-admin (21000/tcp) o personal-agent (5555/tcp) o http (80/tcp)	
hosts2-ns (81/tcp)	**Log**	· A web server is running on this port through SSL · The remote web server type is: Apache-Coyote/1.1 (Apache Tomcat version: 6.0.20)	
http-alt (8080/tcp)	**Log**	· An unknown service is running on this port	
https (443/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: Apache-Coyote/1.1. Detected Apache Tomcat version: 6.0.20	
ftp (21/tcp)	**Log**	· An FTP server is running on this port	
http (80/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Microsoft-IIS/7.5	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port	
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	
personal-agent (5555/tcp)	**Log**	· A TLSv1 server answered on this port	

Tabla 83. OpenVAS_ESBKP

NAGIOS

Most Severe Result(s)	High	Medium	Low
Severity: High	1	3	2

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
http (80/tcp)	**High**	· http TRACE XSS attack	· CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604
general /tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
	Medium	· TCP timestamps	· Revisar
xdmcp (177/udp)	**Medium**	· X Display Manager Control Protocol (XDMCP)	· Disable XDMCP
ntp (123/udp)	**Low**	· NTP read variables	· Set NTP to restrict default access to ignore all info packets: restrict default ignore
vnc-http-1 (5801/tcp)	**Low**	· No 404 check	· Parece desconfigurado
general /tcp	**Log**	· Checks for open udp ports: ○ xdmcp (177/udp) ○ ntp (123/udp) · Traceroute: directly · Checks for open tcp ports: ○ (5900/tcp) ○ (111/tcp) ○ (22/tcp) ○ (6001/tcp) ○ (5801/tcp) ○ (80/tcp)	
http (80/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Apache/2.2.17 (Linux/SUSE)	
vnc-http-1 (5801/tcp)	**Log**	· A web server is running on this port	
ssh (22/tcp)	**Log**	· An ssh server is running on this port · Detected SSH server version: SSH-2.0-OpenSSH_5.8	

Tabla 84. OpenVAS_NAGIOS

ES-DIVA

Most Severe Result(s)	High	Medium	Low
Severity: High	1	0	1

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
ms-wbt-server (3389/tcp)	**High**	· Microsoft RDP Server Private Key Information Disclosure Vulnerability	· CVE: CVE-2005-1794 · BID: 13818
ms-wbt-server (3389/tcp)	**Low**	· Microsoft Remote Desktop Protocol Detection	· Comunicación permitida
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ microsoft-ds (445/tcp) ○ netbios-ssn (139/tcp) ○ ms-wbt-server (3389/tcp)	
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port	

microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port

Tabla 85. OpenVAS_ES-DIVA

SpareLoad

Most Severe Result(s)	High	Medium	Low
Severity: High	1	5	2

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
nfs (2049/udp)	**High**	· NFS export. Please check the permissions of this exports.	· CVE: CVE-1999-0554, CVE-1999-0548
general /tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
	Medium	· TCP timestamps	· Revisar
personal-agent (5555/tcp)	**Medium**	· Web Server Cross Site Scripting	· Revisar
ssh (22/tcp)	**Medium**	· openssh-server Forced Command Handling Information Disclosure Vulnerability. The version of OpenSSH installed on the remote host is older than 5.7: ssh-2.0-openssh_5.4	· Updates are available · CVE: CVE-2012-0814 · BID: 51702
vnc-1 (5901/tcp)	**Medium**	· VNC security types	· Comunicación permitida
ntp (123/udp)	**Low**	· NTP read variables	· Set NTP to restrict default access to ignore all info packets: restrict default ignore
vnc-http-1 (5801/tcp)	**Low**	· No 404 check	· Parece desconfigurado
general /tcp	**Log**	· Checks for open udp ports: o ntp (123/udp) o nfs (2049/udp) · Traceroute: directly · Checks for open tcp ports: o (1677/tcp) o (111/tcp) o (5901/tcp) o (22/tcp) o (2049/tcp) o (5801/tcp) o (10000/tcp) o (5555/tcp)	
personal-agent (5555/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Reload 4.0.0 Web Interface	
ssh (22/tcp)	**Log**	· An ssh server is running on this port · Detected SSH server version: SSH-2.0-OpenSSH_5.4	
vnc-http-1 (5801/tcp)	**Log**	· A web server is running on this port	

Tabla 86. OpenVAS_SpareLoad

PTTS

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	1

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
epmap (135/tcp)	**Medium**	· DCE services running on the remote host · DCE services running · Ports: 1026/tcp, 1029 /tcp	· Filtrar tráfico entrante en este puerto
ms-wbt-server (3389/tcp)	**Low**	· Microsoft Remote Desktop Protocol Detection	· Comunicación permitida
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ cap (1026/tcp) ○ microsoft-ds (445/tcp) ○ ms-lsa (1029/tcp) ○ svrloc (427/tcp) ○ epmap (135/tcp) ○ ndmp (10000/tcp) ○ netbios-ssn (139/tcp) ○ ms-wbt-server (3389/tcp) ○ isns (3205/tcp)	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	

Tabla 87. OpenVAS_PTTS

PTFS

Most Severe Result(s)	High	Medium	Low
Severity: High	34	23	6

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
ajp13 (8009/tcp)	**High**	· Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability	· Set the 'secure' attribute for any cookies that are sent over an SSL connection
domain (53/tcp)	**High**	· Trojan horses. It is sometimes opened by this/these Trojan horse(s): ADM worm, Civcat, Esteems, Lion, W32.Spybot, W32.Dasher	· Verificar con antivirus un posible troyano alojado
http (80/tcp)	**High**	· Apache httpd Web Server Range Header Denial of Service Vulnerability	· Revisar (3) · CVE: CVE-2011-3192 · BID: 49303
	High	· http TRACE XSS attack	· CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604
https (443/tcp)	**High**	· Apache httpd Web Server Range Header Denial of Service Vulnerability	· Revisar (3) · CVE: CVE-2011-3192 · BID: 49303
	High	· http TRACE XSS attack	· CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604
ici (2200/tcp)	**High**	· PHP version smaller than 5.2.7	· Update PHP to version 5.2.7 or later · CVE: CVE-2008-2371, CVE-2008-2665, CVE-

			2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658 · BID: 29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948
	High	· PHP version smaller than 5.2.0	· Update PHP to version 5.2.0 or later · CVE: CVE-2006-1015, CVE-2006-1549, CVE-2006-2660, CVE-2006-4486, CVE-2006-4625, CVE-2006-4812, CVE-2006-5465, CVE-2006-5706, CVE-2006-7205, CVE-2007-0448, CVE-2007-1381, CVE-2007-1584, CVE-2007-1888, CVE-2007-2844, CVE-2007-5424 · BID: 20349, 20879, 49634
	High	· PHP version smaller than 5.2.1	· Update PHP to version 5.2.1 or later · CVE: CVE-2006-6383, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1376, CVE-2007-1380, CVE-2007-1383, CVE-2007-1452, CVE-2007-1453, CVE-2007-1454, CVE-2007-1700, CVE-2007-1701, CVE-2007-1824, CVE-2007-1825, CVE-2007-1835, CVE-2007-1884, CVE-2007-1885, CVE-2007-1886, CVE-2007-1887, CVE-2007-1889, CVE-2007-1890, CVE-2007-4441, CVE-2007-4586 · BID: 21508, 22496, 22805, 22806, 22862, 22922, 23119, 23120, 23219, 23233, 23234, 23235, 23236, 23237, 23238
	High	· PHP version smaller than 5.2.6	· Update PHP to version 5.2.6 or later · CVE: CVE-2007-4850, CVE-2007-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, CVE-2008-2051 · BID: 27413, 28392, 29009
	High	· PHP ' php stream scandir()' Buffer Overflow Vulnerability (Windows)	· Upgrade to PHP 5.4.5 or 5.3.15 or later · CVE: CVE-2012-2688 · BID: 54638
	High	· PHP version smaller than 5.2.14	· Update PHP to version 5.2.14 or later · CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3065 · BID: 38708, 40948, 41991
	High	· PHP version smaller than 5.1.2	· Update PHP to version 5.1.2 or later · CVE: CVE-2006-0200, CVE-2006-0207, CVE-2006-0208 · BID: 16220, 16803
	High	· PHP version smaller than 5.2.5	· Update PHP to version 5.2.5 or later · CVE: CVE-2007-3996, CVE-2007-4782, CVE-2007-4783, CVE-2007-4784, CVE-2007-4825, CVE-2007-4840, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE-2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2008-2107, CVE-2008-2108, CVE-2008-4107 · BID: 26403
	High	· PHP version smaller than 5.3.3	· Update PHP to version 5.3.3 or later · CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-1917, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3062, CVE-2010-

			3063, CVE-2010-3064, CVE-2010-3065 · BID: 38708, 40461, 40948, 41991
	High	· PHP version smaller than 5.2.2	· Update PHP to version 5.2.2 or later · CVE: CVE-2007-1649 · BID:23105
	High	· Apache httpd Web Server Range Header Denial of Service Vulnerability	· Revisar (3) · CVE: CVE-2011-3192 · BID: 49303
	High	· PHP version smaller than 5.2.11	· Update PHP to version 5.2.11 or later · CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018, CVE-2009-5016 · BID: 36449, 44889
	High	· PHP version smaller than 5.3.1	· Update PHP to version 5.3.1 or later · CVE: CVE-2009-3557, CVE-2009-3559, CVE-2009-4017, CVE-2009-4018, CVE-2010-1128 · BID: 36554, 36555, 37079, 37138
	High	· PHP version smaller than 5.2.8	· Update PHP to version 5.2.8 or later · CVE: CVE-2008-5814, CVE-2008-5844 · BID: 32673
	High	· PHP version smaller than 5.2.4	· Update PHP to version 5.2.4 or later · CVE: CVE-2007-1413, CVE-2007-2872, CVE-2007-3294, CVE-2007-3378, CVE-2007-3790, CVE-2007-3799, CVE-2007-3806, CVE-2007-4010, CVE-2007-4033, CVE-2007-4255, CVE-2007-4507, CVE-2007-4652, CVE-2007-4658, CVE-2007-4659, CVE-2007-4660, CVE-2007-4661, CVE-2007-4662, CVE-2007-4663 · BID: 24661, 24261, 24922, 25498
	High	· PHP Multiple Vulnerabilities -March 2013 (Windows)	· Upgrade to PHP 5.4.13 or 5.3.23, which will be available soon · CVE: CVE-2013-1635, CVE-2013-1643 · BID: 58224
	High	· PHP 'phar/tar.c' Heap Buffer Overflow Vulnerability (Windows)	· Upgrade to PHP 5.4.4 or 5.3.14 or later · CVE: CVE-2012-2386 · BID: 47545
	High	· PHP Remote Code Execution and Denial of Service Vulnerabilities Dec13	· Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later · CVE: CVE-2013-6420
	High	· PHP version smaller than 5.3.4	· CVE: CVE-2006-7243, CVE-2010-2094, CVE-2010-2950, CVE-2010-3436, CVE-2010-3709, CVE-2010-3710, CVE-2010-3870, CVE-2010-4150, CVE-2010-4156, CVE-2010-4409, CVE-2010-4697, CVE-2010-4698, CVE-2010-4699, CVE-2010-4700, CVE-2011-0753, CVE-2011-0754, CVE-2011-0755 · BID: 40173, 43926, 44605, 44718, 44723, 44951, 44980, 45119, 45335, 45338, 45339, 45952, 45954, 46056, 46168
	High	· PHP version smaller than 5.2.3	· Update PHP to version 5.2.3 or later · CVE: CVE-2007-1900, CVE-2007-2756, CVE-2007-2872, CVE-2007-3007 · BID: 23359, 24089, 24259, 24261
	High	· PHP Sessions Subsystem Session Fixation Vulnerability-Aug13 (Windows)	· Upgrade to PHP version 5.5.2 or later · CVE: CVE-2011-4718
	High	· http TRACE XSS attack	· CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604
	High	· PHP Multiple Vulnerabilities -01 March13 (Windows)	· Upgrade to PHP 5.4.0 or later · CVE: CVE-2012-1172 · BID: 53403
ldap (389/tcp)	**High**	· Novell eDirectory Multiple Security Vulnerabilities	· An update is available · CVE: CVE-2012-0428, CVE-2012-0429, CVE-2012-0430, CVE-2012-0432

			· BID: 57038
	High	· Novell eDirectory '/dhost/modules?I:' Buffer Overflow Vulnerability	· CVE: CVE-2009-4653 · BID: 37009
	High	· Novell eDirectory Multiple Remote Vulnerabilities	· CVE: CVE-2009-4653 · BID: 40541
	High	· Novell eDirectory 'DHOST' Cookie Hijack Vulnerability	· CVE: CVE-2009-4655
nfs (2049/udp)	**High**	· NFS export. Please check the permissions of this exports	· CVE: CVE-1999-0554, CVE-1999-0548
http (80/tcp)	**Medium**	· Apache Web Server ETag Header Information Disclosure Weakness	· CVE: CVE-2003-1418 · BID: 6939
	Medium	· Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	· Upgrade to Apache HTTP Server version 2.2.22 or later · CVE: CVE-2012-0053 · BID: 51706
	Medium	· Apache Tomcat mod_jk Information Disclosure Vulnerability	· Upgrade to mod_jk 1.2.27 or later · CVE: CVE-2008-5519 · BID: 34412
https (443/tcp)	**Medium**	· Apache Web Server ETag Header Information Disclosure Weakness	· OpenBSD has released a patch to address this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare · CVE: CVE-2003-1418 · BID: 6939
	Medium	· Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	· Upgrade to Apache HTTP Server version 2.2.22 or later · CVE: CVE-2012-0053 · BID: 51706
	Medium	· Apache Tomcat mod_jk Information Disclosure Vulnerability	· Upgrade to mod_jk 1.2.27 or later · CVE: CVE-2008-5519 · BID: 34412
ici (2200/tcp)	**Medium**	· PHP version smaller than 5.1.0	· Update PHP to version 5.1.0 or later · CVE: CVE-2005-3319, CVE-2005-3883 · BID: 15177, 15571
	Medium	· PHP version smaller than 5.2.9	· Update PHP to version 5.2.9 or later · CVE: CVE-2008-5498, CVE-2009-1271, CVE-2009-1272 · BID: 33002, 33927
	Medium	· PHP 'open basedir' Security Bypass Vulnerability (Windows)	· Upgrade to PHP 5.3.15 or later · CVE: CVE-2012-3365 · BID: 54612
	Medium	· PHP Multiple Vulnerabilities - June13 (Windows)	· Upgrade to PHP 5.4.16 or 5.3.26 or later · CVE: CVE-2013-4635, CVE-2013-2110 · BID: 60731, 60411
	Medium	· Apache Web Server ETag Header Information Disclosure Weakness	· OpenBSD has released a patch to address this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare · CVE: CVE-2003-1418 · BID: 6939
	Medium	· PHP SSL Certificate Validation Security Bypass Vulnerability (Windows)	· Upgrade to PHP version 5.4.18 or 5.5.2 or later · CVE: CVE-2013-4248 · BID: 61776
	Medium	· PHP SOAP Parser Multiple Information Disclosure Vulnerabilities	· Upgrade to PHP 5.3.22 or 5.4.12 or later · CVE: CVE-2013-1824 · BID: 62373
	Medium	· Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	· Upgrade to Apache HTTP Server version 2.2.22 or later · CVE: CVE-2012-0053 · BID: 51706
	Medium	· Apache Tomcat mod_jk	· Upgrade to mod_jk 1.2.27 or later.

		Information Disclosure Vulnerability	· CVE: CVE-2008-5519 · BID: 34412
ldap (389/tcp)	**Medium**	· Novell eDirectory NULL Base DN Denial Of Service Vulnerability	· Updates are available · CVE: CVE-2009-3862 · BID: 36902
	Medium	· Novell eDirectory eMBox SOAP Request Denial Of Service Vulnerability	· Updates are available · CVE: CVE-2010-0666 · BID: 38157
	Medium	· Novell eDirectory Server Malformed Index Denial Of Service Vulnerability	· Updates are available · BID: 43662
	Medium	· LDAP allows null bases	· Disable NULL BASE queries on your LDAP server
general /tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
ldaps (636/tcp)	**Medium**	· Check for SSL Weak Ciphers	· Revisar cifrado débil
ncp (524/tcp)	**Medium**	· Netware NDS Object Enumeration	· The NDS object PUBLIC should not have Browse rights the tree should be restricted to authenticated users only
wbem-https (5989/tcp)	**Medium**	SSL Certificate Expiry	· Revisar
http (80/tcp)	**Low**	· Apache mod_jk Module Version Detection	· Mod JK version 1.2.23 was detected on the host
https (443/tcp)	**Low**	· Apache mod_jk Module Version Detection	· Mod JK version 1.2.23 was detected on the host
ici (2200/tcp)	**Low**	· Apache mod_jk Module Version Detection	· Mod JK version 1.2.23 was detected on the host
ldap (389/tcp)	**Low**	· LDAP Detection	· Comunicación permitida
ftp (21/tcp)	**Low**	· FTP Server type and version	· Comunicación permitida
ntp (123/udp)	**Low**	· NTP read variables	· Comunicación permitida
general /tcp	**Log**	· Checks for open udp ports: o nfs (2049/udp) o ntp (123/udp) o netbios-ns (137/udp) o snmp (161/udp) · Traceroute: directly · Checks for open tcp ports: o hosts2-ns (81/tcp) o https (443/tcp) o groupwise (1677/tcp) o http-alt (8008/tcp) o ajp13 (8009/tcp) o ftp (21/tcp) o sunrpc (111/tcp) o ldaps (636/tcp) o font-service (7100/tcp) o svrloc (427/tcp) o dhcp-failover2 (847/tcp) o nfs (2049/tcp) o msn-messenger-voice-chat (6901/tcp) o smtp (25/tcp) o ici (2200/tcp) o wbem-https (5989/tcp) o ldap (389/tcp) o netbios-ssn (139/tcp) o domain (53/tcp) o netviewdm3 (731/tcp) o btrieve (3351/tcp) o sometimes-rpc19 (32778/tcp) o ncp (524/tcp) o sometimes-rpc21 (32779/tcp)	

		○ callbook (2000/tcp) ○ http (80/tcp) ○ search-agent (1234/tcp)
ajp13 (8009/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: NetWare HTTP Stack
http (80/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Apache/2.0.63 (NETWARE) mod_jk/1.2.23
https (443/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: Apache/2.0.63 (NETWARE) mod_jk/1.2.23
ici (2200/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: Apache/2.0.63 (NETWARE) mod_jk/1.2.23 PHP/5.0.5
ldaps (636/tcp)	**Log**	· A TLSv1 server answered on this port
wbem-https (5989/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: openwbem/3.1.0 (CIMOM)
ftp (21/tcp)	**Log**	· An FTP server is running on this port
hosts2-ns (81/tcp)	**Log**	· A web server is running on this port · The remote web server type is: NetWare HTTP Stack
http-alt (8008/tcp)	**Log**	· A web server is running on this port · The remote web server type is: NetWare HTTP Stack
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port
smtp (25/tcp)	**Log**	· An SMTP server is running on this port
snmp (161/udp)	**Log**	· A SNMP server is running on this host

Tabla 88. OpenVAS_PTFS

PTIMG

Most Severe Result(s)	High	Medium	Low
Severity: High	33	23	6

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
ajp13 (8009/tcp)	**High**	· Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability	· Set the 'secure' attribute for any cookies that are sent over an SSL connection
http (80/tcp)	**High**	· Apache httpd Web Server Range Header Denial of Service Vulnerability	· Revisar (3) · CVE: CVE-2011-3192 · BID: 49303
	High	· http TRACE XSS attack	· CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604
https (443/tcp)	**High**	· Apache httpd Web Server Range Header Denial of Service Vulnerability	· Revisar (3) · CVE: CVE-2011-3192 · BID: 49303
	High	· http TRACE XSS attack	· CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604
ici (2200/tcp)	**High**	· PHP version smaller than 5.2.7	· Update PHP to version 5.2.7 or later · CVE: CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658 · BID: 29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948

	High	· PHP version smaller than 5.2.0	· Update PHP to version 5.2.0 or later · CVE: CVE-2006-1015, CVE-2006-1549, CVE-2006-2660, CVE-2006-4486, CVE-2006-4625, CVE-2006-4812, CVE-2006-5465, CVE-2006-5706, CVE-2006-7205, CVE-2007-0448, CVE-2007-1381, CVE-2007-1584, CVE-2007-1888, CVE-2007-2844, CVE-2007-5424 · BID: 20349, 20879, 49634
	High	· PHP version smaller than 5.2.1	· Update PHP to version 5.2.1 or later · CVE: CVE-2006-6383, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1376, CVE-2007-1380, CVE-2007-1383, CVE-2007-1452, CVE-2007-1453, CVE-2007-1454, CVE-2007-1700, CVE-2007-1701, CVE-2007-1824, CVE-2007-1825, CVE-2007-1835, CVE-2007-1884, CVE-2007-1885, CVE-2007-1886, CVE-2007-1887, CVE-2007-1889, CVE-2007-1890, CVE-2007-4441, CVE-2007-4586 · BID: 21508, 22496, 22805, 22806, 22862, 22922, 23119, 23120, 23219, 23233, 23234, 23235, 23236, 23237, 23238
	High	· PHP version smaller than 5.2.6	· Update PHP to version 5.2.6 or later · CVE: CVE-2007-4850, CVE-2007-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, CVE-2008-2051 · BID: 27413, 28392, 29009
	High	· PHP ' php stream scandir()' Buffer Overflow Vulnerability (Windows)	· Upgrade to PHP 5.4.5 or 5.3.15 or later · CVE: CVE-2012-2688 · BID: 54638
	High	· PHP version smaller than 5.2.14	· Update PHP to version 5.2.14 or later · CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3065 · BID: 38708, 40948, 41991
	High	· PHP version smaller than 5.1.2	· Update PHP to version 5.1.2 or later · CVE: CVE-2006-0200, CVE-2006-0207, CVE-2006-0208 · BID: 16220, 16803
	High	· PHP version smaller than 5.2.5	· Update PHP to version 5.2.5 or later · CVE: CVE-2007-3996, CVE-2007-4782, CVE-2007-4783, CVE-2007-4784, CVE-2007-4825, CVE-2007-4840, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE-2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2008-2107, CVE-2008-2108, CVE-2008-4107 · BID: 26403
	High	· PHP version smaller than 5.3.3	· Update PHP to version 5.3.3 or later · CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-1917, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3062, CVE-2010-3063, CVE-2010-3064, CVE-2010-3065 · BID: 38708, 40461, 40948, 41991
	High	· PHP version smaller than 5.2.2	· Update PHP to version 5.2.2 or later · CVE: CVE-2007-1649 · BID: 23105
	High	· Apache httpd Web Server Range Header Denial of Service	· Revisar (3) · CVE: CVE-2011-3192 · BID: 49303

		Vulnerability	
	High	· PHP version smaller than 5.2.11	· Update PHP to version 5.2.11 or later · CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018, CVE-2009-5016 · BID: 36449, 44889
	High	· PHP version smaller than 5.3.1	· Update PHP to version 5.3.1 or later · CVE: CVE-2009-3557, CVE-2009-3559, CVE-2009-4017, CVE-2009-4018, CVE-2010-1128 · BID: 36554, 36555, 37079, 37138
	High	· PHP version smaller than 5.2.8	· Update PHP to version 5.2.8 or later · CVE: CVE-2008-5814, CVE-2008-5844 · BID: 32673
	High	· PHP version smaller than 5.2.4	· Update PHP to version 5.2.4 or later · CVE: CVE-2007-1413, CVE-2007-2872, CVE-2007-3294, CVE-2007-3378, CVE-2007-3790, CVE-2007-3799, CVE-2007-3806, CVE-2007-4010, CVE-2007-4033, CVE-2007-4255, CVE-2007-4507, CVE-2007-4652, CVE-2007-4658, CVE-2007-4659, CVE-2007-4660, CVE-2007-4661, CVE-2007-4662, CVE-2007-4663 · BID: 24661, 24261, 24922, 25498
	High	· PHP Multiple Vulnerabilities -March 2013 (Windows)	· Upgrade to PHP 5.4.13 or 5.3.23, which will be available soon · CVE: CVE-2013-1635, CVE-2013-1643 · BID: 58224
	High	· PHP 'phar/tar.c' Heap Buffer Overflow Vulnerability (Windows)	· Upgrade to PHP 5.4.4 or 5.3.14 or later · CVE: CVE-2012-2386 · BID: 47545
	High	· PHP Remote Code Execution and Denial of Service Vulnerabilities Dec13	· Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later · CVE: CVE-2013-6420
	High	· PHP version smaller than 5.3.4	· CVE: CVE-2006-7243, CVE-2010-2094, CVE-2010-2950, CVE-2010-3436, CVE-2010-3709, CVE-2010-3710, CVE-2010-3870, CVE-2010-4150, CVE-2010-4156, CVE-2010-4409, CVE-2010-4697, CVE-2010-4698, CVE-2010-4699, CVE-2010-4700, CVE-2011-0753, CVE-2011-0754, CVE-2011-0755 · BID: 40173, 43926, 44605, 44718, 44723, 44951, 44980, 45119, 45335, 45338, 45339, 45952, 45954, 46056, 46168
	High	· PHP version smaller than 5.2.3	· Update PHP to version 5.2.3 or later · CVE: CVE-2007-1900, CVE-2007-2756, CVE-2007-2872, CVE-2007-3007 · BID: 23359, 24089, 24259, 24261
	High	· PHP Sessions Subsystem Session Fixation Vulnerability-Aug13 (Windows)	· Upgrade to PHP version 5.5.2 or later · CVE: CVE-2011-4718
	High	· http TRACE XSS attack	· CVE: CVE-2004-2320, CVE-2003-1567 · BID: 9506, 9561, 11604
	High	· PHP Multiple Vulnerabilities -01 March13 (Windows)	· Upgrade to PHP 5.4.0 or later · CVE: CVE-2012-1172 · BID: 53403
ldap (389/tcp)	**High**	· Novell eDirectory Multiple Security Vulnerabilities	· An update is available · CVE: CVE-2012-0428, CVE-2012-0429, CVE-2012-0430, CVE-2012-0432 · BID: 57038
	High	Novell eDirectory '/dhost/modules?I:' Buffer Overflow Vulnerability	· CVE: CVE-2009-4653 · BID: 37009
	High	· Novell eDirectory Multiple Remote	· Revisar (4) · CVE: CVE-2009-4653

		Vulnerabilities	· BID: 40541
	High	· Novell eDirectory 'DHOST' Cookie Hijack Vulnerability	· CVE: CVE-2009-4655
nfs (2049/udp)	**High**	· NFS export. Running a superfluous NFS daemon. You should consider removing it	· CVE: CVE-1999-0554, CVE-1999-0548
http (80/tcp)	**Medium**	· Apache Web Server ETag Header Information Disclosure Weakness	· CVE: CVE-2003-1418 · BID: 6939
	Medium	· Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	· Upgrade to Apache HTTP Server version 2.2.22 or later · CVE: CVE-2012-0053 · BID: 51706
	Medium	· Apache Tomcat mod_jk Information Disclosure Vulnerability	· Upgrade to mod_jk 1.2.27 or later · CVE: CVE-2008-5519 · BID: 34412
https (443/tcp)	**Medium**	· Apache Web Server ETag Header Information Disclosure Weakness	· OpenBSD has released a patch to address this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare · CVE: CVE-2003-1418 · BID: 6939
	Medium	· Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	· Upgrade to Apache HTTP Server version 2.2.22 or later · CVE: CVE-2012-0053 · BID: 51706
	Medium	· Apache Tomcat mod_jk Information Disclosure Vulnerability	· Upgrade to mod_jk 1.2.27 or later · CVE: CVE-2008-5519 · BID: 34412
ici (2200/tcp)	**Medium**	· PHP version smaller than 5.1.0	· Update PHP to version 5.1.0 or later · CVE: CVE-2005-3319, CVE-2005-3883 · BID: 15177, 15571
	Medium	· PHP version smaller than 5.2.9	· Update PHP to version 5.2.9 or later · CVE: CVE-2008-5498, CVE-2009-1271, CVE-2009-1272 · BID: 33002, 33927
	Medium	· PHP 'open basedir' Secuirity Bypass Vulnerability (Windows)	· Upgrade to PHP 5.3.15 or later · CVE: CVE-2012-3365 · BID: 54612
	Medium	· PHP Multiple Vulnerabilities - June13 (Windows)	· Upgrade to PHP 5.4.16 or 5.3.26 or later · CVE: CVE-2013-4635, CVE-2013-2110 · BID: 60731, 60411
	Medium	· Apache Web Server ETag Header Information Disclosure Weakness	· OpenBSD has released a patch to address this issue. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare · CVE: CVE-2003-1418 · BID: 6939
	Medium	· PHP SSL Certificate Validation Security Bypass Vulnerability (Windows)	· Upgrade to PHP version 5.4.18 or 5.5.2 or later · CVE: CVE-2013-4248 · BID: 61776
	Medium	· PHP SOAP Parser Multiple Information Disclosure Vulnerabilities	· Upgrade to PHP 5.3.22 or 5.4.12 or later · CVE: CVE-2013-1824 · BID: 62373
	Medium	· Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	· Upgrade to Apache HTTP Server version 2.2.22 or later · CVE: CVE-2012-0053 · BID: 51706
	Medium	· Apache Tomcat mod_jk Information Disclosure	· Upgrade to mod_jk 1.2.27 or later · CVE: CVE-2008-5519

		Vulnerability	· BID: 34412
ldap (389/tcp)	**Medium**	· Novell eDirectory NULL Base DN Denial Of Service Vulnerability	· Updates are available · CVE: CVE-2009-3862 · BID: 36902
	Medium	· Novell eDirectory eMBox SOAP Request Denial Of Service Vulnerability	· Updates are available · CVE: CVE-2010-0666 · BID: 38157
	Medium	· Novell eDirectory Server Malformed Index Denial Of Service Vulnerability	· Updates are available · BID: 43662
	Medium	· LDAP allows null bases	· Disable NULL BASE queries on your LDAP server
general /tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
ldaps (636/tcp)	**Medium**	· Check for SSL Weak Ciphers	· Revisar cifrado débil
ncp (524/tcp)	**Medium**	· Netware NDS Object Enumeration	· The NDS object PUBLIC should not have Browse rights the tree should be restricted to authenticated users only
wbem-https (5989/tcp)	**Medium**	SSL Certificate Expiry	· Revisar
http (80/tcp)	**Low**	· Apache mod_jk Module Version Detection	· Mod JK version 1.2.23 was detected on the host
https (443/tcp)	**Low**	· Apache mod_jk Module Version Detection	· Mod JK version 1.2.23 was detected on the host
ici (2200/tcp)	**Low**	· Apache mod_jk Module Version Detection	· Mod JK version 1.2.23 was detected on the host
ldap (389/tcp)	**Low**	· LDAP Detection	· Comunicación permitida
ftp (21/tcp)	**Low**	· FTP Server type and version	· Comunicación permitida
ntp (123/udp)	**Low**	· NTP read variables	· Comunicación permitida
general /tcp	**Log**	· Checks for open udp ports: o nfs (2049/udp) o ntp (123/udp) o netbios-ns (137/udp) o snmp (161/udp) · Traceroute: directly · Checks for open tcp ports: o hosts2-ns (81/tcp) o https (443/tcp) o http-alt (8008/tcp) o ajp13 (8009/tcp) o ftp (21/tcp) o sunrpc (111/tcp) o ldaps (636/tcp) o pichat (9009/tcp) o svrloc (427/tcp) o dhcp-failover2 (847/tcp) o nfs (2049/tcp) o msn-messenger-voice-chat (6901/tcp) o ici (2200/tcp) o wbem-https (5989/tcp) o ldap (389/tcp) o netbios-ssn (139/tcp) o domain (53/tcp) o netviewdm3 (731/tcp) o btrieve (3351/tcp) o sometimes-rpc19 (32778/tcp) o ncp (524/tcp) o sometimes-rpc21 (32779/tcp) o callbook (2000/tcp)	

		○ http (80/tcp) ○ search-agent (1234/tcp)
ajp13 (8009/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: NetWare HTTP Stack
http (80/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Apache/2.0.63 (NETWARE) mod_jk/1.2.23
https (443/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: Apache/2.0.63 (NETWARE) mod_jk/1.2.23
ici (2200/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: Apache/2.0.63 (NETWARE) mod_jk/1.2.23 PHP/5.0.5
ldaps (636/tcp)	**Log**	· A TLSv1 server answered on this port
wbem-https (5989/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: openwbem/3.1.0 (CIMOM)
ftp (21/tcp)	**Log**	· An FTP server is running on this port
hosts2-ns (81/tcp)	**Log**	· A web server is running on this port · The remote web server type is: NetWare HTTP Stack
http-alt (8008/tcp)	**Log**	· A web server is running on this port · The remote web server type is: NetWare HTTP Stack
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port
snmp (161/udp)	**Log**	· A SNMP server is running on this host

Tabla 89. OpenVAS_PTIMG

ESXi1

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	3

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
general/ tcp	**Medium**	· VMSA-2013-0011 VMware ESX and ESXi updates to third party libraries (remote check). ESXi Version: 5.1.0. Detected Build: 1065491	· Fixed Build: 1142907 · CVE: CVE-2013-1661
	Medium	· TCP timestamps	· Revisar
http (80/tcp)	**Low**	· No 404 check	· Parece desconfigurado
ideafarm-chat (902/tcp)	**Low**	· VMware ESX/GSX Server detection	· Conexión permitida
xprint-server (8100/tcp)	**Low**	· Check open ports	· Revisar
general /tcp	**Log**	· Checks for open udp ports: None · Traceroute: directly · Checks for open tcp ports: ○ https (443/tcp) ○ homepage (8182/tcp) ○ svrloc (427/tcp) ○ xprint-server (8100/tcp) ○ wbem-https (5989/tcp) ○ irdmi (8000/tcp) ○ ideafarm-chat (902/tcp) ○ http (80/tcp)	
http (80/tcp)	**Log**	· A web server is running on this port	
https (443/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port	

		· Detected VMware ESXi Version: 5.1.0 Build 1065491
wbem-https (5989/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: sfcHttpd

Tabla 90. OpenVAS_ESXi1

ESXi2

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	3

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
general/ tcp	**Medium**	· VMSA-2013-0011 VMware ESX and ESXi updates to third party libraries (remote check). ESXi Version: 5.1.0. Detected Build: 1065491	· Fixed Build: 1142907 · CVE: CVE-2013-1661
	Medium	· TCP timestamps	· Revisar
http (80/tcp)	**Low**	· No 404 check	· Parece desconfigurado
ideafarm-chat (902/tcp)	**Low**	· VMware ESX/GSX Server detection	· Conexión permitida
xprint-server (8100/tcp)	**Low**	· Check open ports	· Revisar
general /tcp	**Log**	· Checks for open udp ports: None · Traceroute: directly · Checks for open tcp ports: ○ https (443/tcp) ○ homepage (8182/tcp) ○ svrloc (427/tcp) ○ xprint-server (8100/tcp) ○ wbem-https (5989/tcp) ○ irdmi (8000/tcp) ○ ideafarm-chat (902/tcp) ○ http (80/tcp)	
http (80/tcp)	**Log**	· A web server is running on this port	
https (443/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · Detected VMware ESXi Version: 5.1.0 Build 1065491	
wbem-https (5989/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: sfcHttpd	

Tabla 91. OpenVAS_ESXi2

ESXi3

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	2	3

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
general/ tcp	**Medium**	· VMSA-2013-0011 VMware ESX and ESXi updates to third party libraries (remote check). ESXi Version: 5.1.0. Detected Build: 1065491	· Fixed Build: 1142907 · CVE: CVE-2013-1661
	Medium	· TCP timestamps	· Revisar
http (80/tcp)	**Low**	· No 404 check	· Parece desconfigurado
ideafarm-chat	**Low**	· VMware ESX/GSX Server detection	· Conexión

(902/tcp)			permitida
xprint-server (8100/tcp)	**Low**	· Check open ports	· Revisar
general /tcp	**Log**	· Checks for open udp ports: None · Traceroute: directly · Checks for open tcp ports: ○ https (443/tcp) ○ homepage (8182/tcp) ○ svrloc (427/tcp) ○ xprint-server (8100/tcp) ○ wbem-https (5989/tcp) ○ irdmi (8000/tcp) ○ ideafarm-chat (902/tcp) ○ http (80/tcp)	
http (80/tcp)	**Log**	· A web server is running on this port	
https (443/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · Detected VMware ESXi Version: 5.1.0 Build 1065491	
wbem-https (5989/tcp)	**Log**	· A web server is running on this port through SSL · The remote web server type is: sfcHttpd · A TLSv1 server answered on this port	

Tabla 92. OpenVAS_ESXi3

ESVC

Most Severe Result(s)	High	Medium	Low
Severity: High	1	11	4

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
websm (9090/tcp)	**High**	· Apache Tomcat Session Fixation Vulnerability (Windows)	· Apply patch or upgrade Apache Tomcat to 7.0.33 or 6.0.37 or later · CVE: CVE-2013-2067 · BID: 59799
websm (9090/tcp)	**Medium**	· WEB-INF folder accessible	· CVE: CVE-2002-1855, CVE-2002-1856, CVE-2002-1857, CVE-2002-1858, CVE-2002-1859, CVE-2002-1860, CVE-2002-1861 · BID: 5119
	Medium	· Apache Tomcat Multiple Security Bypass Vulnerabilities (Windows)	· Apply patch or upgrade Apache Tomcat to 5.5.36, 6.0.36, 7.0.30 or later · CVE: CVE-2012-5887, CVE-2012-5886, CVE-2012-5885 · BID: 56403
	Medium	· Apache Tomcat HTTP NIO Denial Of Service Vulnerability (Windows)	· Apply patch or upgrade Apache Tomcat to 6.0.36, 7.0.28 or later · CVE: CVE-2012-2733 · BID: 56402
	Medium	· Apache Tomcat Partial HTTP Requests DoS Vulnerability (Windows)	· CVE: CVE-2012-5568 · BID: 56686
	Medium	· Apache Tomcat Denial Of Service Vulnerability (Windows)	· Apply patch or upgrade Apache Tomcat to 7.0.30 or 6.0.37 or later · CVE: CVE-2012-3544 · BID: 59797
	Medium	· Apache Tomcat Information Disclosure Vulnerability (Windows)	· Apply patch or upgrade Apache Tomcat to 7.0.40 or later · CVE: CVE-2013-2071 · BID: 59798
epmap (135/tcp)	**Medium**	· DCE services running on the remote host · DCE services running	· Filtrar tráfico entrante en este puerto

		· Ports: 49152/tcp, 49153/tcp, 49154/tcp, 49171/tcp, 49175/tcp, 49205/tcp	
general /tcp	**Medium**	· TCP timestamps	· Revisar
ldap (389/tcp)	**Medium**	· LDAP allows null bases	· Disable NULL BASE queries on your LDAP server
	Medium	· Use LDAP search request to retrieve information from NT Directory Services	· Disable NULL BASE queries on your LDAP server
websm (9090/tcp)	**Low**	· robot(s).txt exists on the Web Server	· Revisar
ldap (389/tcp)	**Low**	· LDAP Detection	· Revisar
http (80/tcp)	**Low**	· No 404 check	· Parece desconfigurado
ms-sql-m (1434/udp)	**Low**	· Microsoft's SQL UDP Info Query	· Filtrar tráfico entrante en este puerto
general /tcp	**Log**	· Checks for open udp ports: o ms-sql-m (1434/udp) o netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: o https (443/tcp) o afs3-rmtsys (7009/tcp) o microsoft-ds (445/tcp) o ajp13 (8009/tcp) o pichat (9009/tcp) o amanda (10080/tcp) o epmap (135/tcp) o http-alt (8080/tcp) o sapv1 (9875/tcp) o ldap (389/tcp) o netbios-ssn (139/tcp) o ms-wbt-server (3389/tcp) o pcsync-https (8443/tcp) o http (80/tcp) o websm (9090/tcp)	
websm (9090/tcp)	**Log**	· A web server is running on this port. Detected Apache Tomcat version: 7.0.26 · The remote web server type is: Apache-Coyote/1.1	
http (80/tcp)	**Log**	· A web server is running on this port	
amanda (10080/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Apache	
http-alt (8080/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Apache-Coyote/1.1	
https (443/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	
pcsync-https (8443/tcp)	**Log**	· A web server is running on this port through SSL · A TLSv1 server answered on this port · The remote web server type is: Apache-Coyote/1.1	

Tabla 93. OpenVAS_ESVC

ESRSA

Most Severe Result(s)	High	Medium	Low
Severity: High	1	3	9

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
remotewatch (5556/tcp)	**High**	· Trojan horses. It is sometimes opened by this/these Trojan horse(s): BO Facil	· Verificar con antivirus un posible troyano alojado
epmap (135/tcp)	**Medium**	· DCE services running on the remote host · DCE services running · Ports: 1025/tcp, 1026 /tcp	· Filtrar tráfico entrante en este puerto
radius-acct (1813/tcp)	**Medium**	· The SSL certificate of the remote service can't be parsed!	· Revisar
remotewatch (5556/tcp)	**Low**	· Unknown services banners	· Revisar
afs3-errors (7006/tcp)	**Low**	· The SSL certificate of the remote service is valid for more than 15 years	· Revisar
afs3-kaserver (7004/tcp)	**Low**	· The SSL certificate of the remote service is valid for more than 15 years	· Revisar
afs3-prserver (7002/tcp)	**Low**	· The SSL certificate of the remote service is valid for more than 15 years	· Revisar
afs3-update (7008/tcp)	**Low**	· The SSL certificate of the remote service is valid for more than 15 years	· Revisar
domain (53/tcp)	**Low**	· Microsoft DNS server seems to be running on this port 0.in-addr.arpa/SOA/IN, 255.in-addr.arpa/SOA/IN	· Comunicación permitida
ms-wbt-server (3389/tcp)	**Low**	· Microsoft Remote Desktop Protocol Detection	· Comunicación permitida
talon-engine (7012/tcp)	**Low**	· The SSL certificate of the remote service is valid for more than 15 years	· Revisar
general /tcp	**Log**	· Checks for open udp ports: ○ domain (53/udp) ○ kerberos (88/udp) ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ kpasswd (464/tcp) ○ http-rpc-epmap (593/tcp) ○ ldaps (636/tcp) ○ kerberos (88/tcp) ○ ldap (389/tcp) ○ domain (53/tcp) ○ msft-gc (3268/tcp) ○ msft-gc-ssl (3269/tcp) ○ microsoft-ds (445/tcp) ○ epmap (135/tcp) ○ ndmp (10000/tcp) ○ netbios-ssn (139/tcp) ○ ms-wbt-server (3389/tcp)	
domain (53/tcp)	**Log**	· A DNS Server is running at this Host	
domain (53/udp)	**Log**	· A DNS Server is running at this Host	
kerberos (88/tcp)	**Log**	· A Kerberos Server is running at this port	
kerberos (88/udp)	**Log**	· A Kerberos Server is running at this port	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port	
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	

netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port

Tabla 94. OpenVAS_ESRSA

ESBDSAC

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	3	2

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
epmap (135/tcp)	**Medium**	· DCE services running on the remote host · DCE services running · Ports: 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, 49163/tcp, 49165/tcp, 49178/tcp	· Filtrar tráfico entrante en este puerto
general /tcp	**Medium**	· TCP timestamps	· Revisar
http-alt (8080/tcp)	**Low**	· Windows SharePoint Services detection. X-AspNet-Version: 2.0.50727	· Comunicación permitida
ms-sql-s (1433/tcp)	**Low**	· Microsoft SQL TCP/IP listener is running	· Bloquear este puerto de la comunicación externa
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ microsoft-ds (445/tcp) ○ epmap (135/tcp) ○ http-alt (8080/tcp) ○ ms-sql-s (1433/tcp) ○ ndmp (10000/tcp) ○ netbios-ssn (139/tcp) ○ nsjtp-data (1688/tcp) ○ ms-wbt-server (3389/tcp)	
http-alt (8080/tcp)	**Log**	· A web server is running on this port · The remote web server type is: Microsoft-IIS/7.5	
ms-sql-s (1433/tcp)	**Log**	· MS SQL can be accessed by remote attackers	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port	
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	

Tabla 95. OpenVAS_ESBDSAC

ESWWW

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	4	1

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
epmap (135/tcp)	**Medium**	· DCE services running on the remote host · DCE services running · Ports: 49152/tcp, 49153/tcp, 49154/tcp,	· Filtrar tráfico entrante en este puerto

		49155/tcp, 49161/tcp, 49163/tcp	
general /tcp	**Medium**	· TCP Sequence Number Approximation Reset Denial of Service Vulnerability	· CVE: CVE-2004-0230 · BID: 10183
	Medium	· TCP timestamps	· Revisar
ftp (21/tcp)	**Low**	· FTP Server type and version	· Actualizar la versión
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp) · Traceroute: directly · Checks for open tcp ports: ○ microsoft-ds (445/tcp) ○ ftp (21/tcp) ○ epmap (135/tcp) ○ ndmp (10000/tcp) ○ netbios-ssn (139/tcp) ○ nsjtp-data (1688/tcp) ○ ms-wbt-server (3389/tcp)	
ftp (21/tcp)	**Log**	· An FTP server is running on this port.	
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port	
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port	
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225	
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered	
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port	

Tabla 96. OpenVAS_ESWWW

ESDC

Most Severe Result(s)	High	Medium	Low
Severity: Medium	0	5	7

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
epmap (135/tcp)	**Medium**	· DCE services running on the remote host	· Filtrar tráfico entrante en este puerto
		· DCE services running · Ports: 5722/tcp, 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, 49158/tcp, 49159/tcp, 54795/tcp, 54851/tcp, 54856/tcp, 63184/tcp	
general/tcp	**Medium**	· TCP timestamps	· Revisar
ldap (389/tcp)	**Medium**	· LDAP allows null bases	· Disable NULL BASE queries on your LDAP server
		· Use LDAP search request to retrieve information from NT Directory Services	· execute the command: net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete
ldap (389/tcp)	**Low**	· LDAP Detection	· Comunicación permitida
domain (53/tcp)	**Low**	· Microsoft DNS server internal hostname disclosure detection	· Comunicación permitida
		0.in-addr.arpa/SOA/IN, 255.in-addr.arpa/SOA/IN	
msft-gc-ssl (3269/tcp)	**Low**	· Check open ports	· Revisar
ntp (123/udp)	**Low**	· NTP read variables	· Comunicación permitida
vnc (5900/tcp)	**Low**	· VNC security types	· Comunicación permitida
vnc-http (5800/tcp)	**Low**	· No 404 check	· Parece desconfigurado
general /tcp	**Log**	· Checks for open udp ports: ○ netbios-ns (137/udp)	

		○ kerberos (88/udp) ○ ntp (123/udp) ○ domain (53/udp) · Traceroute: directly · Checks for open tcp ports: ○ kpasswd (464/tcp) ○ microsoft-ds (445/tcp) ○ http-rpc-epmap (593/tcp) ○ vnc (5900/tcp) ○ ldaps (636/tcp) ○ epmap (135/tcp) ○ vnc (5800/tcp) ○ kerberos (88/tcp) ○ ldap (389/tcp) ○ ndmp (10000/tcp) ○ netbios-ssn (139/tcp) ○ nsjtp-data (1688/tcp) ○ ms-wbt-server (3389/tcp) ○ domain (53/tcp) ○ msft-gc (3268/tcp) ○ msft-gc-ssl (3269/tcp)
domain (53/tcp)	**Log**	· A DNS Server is running at this Host
domain (53/udp)	**Log**	· A web server is running on this port
vnc (5800/tcp)	**Log**	· A web server is running on this port
kerberos (88/tcp)	**Log**	· A Kerberos Server is running at this port
kerberos (88/udp)	**Log**	· A Kerberos Server is running at this port
microsoft-ds (445/tcp)	**Log**	· A CIFS server is running on this port
ms-wbt-server (3389/tcp)	**Log**	· A TLSv1 server answered on this port
ndmp (10000/tcp)	**Log**	· Symantec Backup Exec 13.0.5204.1225
netbios-ns (137/udp)	**Log**	· Netbios names has been gathered
netbios-ssn (139/tcp)	**Log**	· An SMB server is running on this port

Tabla 97. OpenVAS_ESDC

(1) http://svn.apache.org/viewvc?view=revision&revision=834047
(2) DCE -> (Distributed Computing Environmet)
(3) http://marc.info/?l=apache-httpd-dev&m=131420013520206&w=2
(4) http://www.novell.com/support/viewContent.do?externalId=3426981
(5) http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx
(6) http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx
(7) http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Auditoría sobre los switches

SWXX

Most Severe Result(s)	High	Medium
Severity: Medium	0	3

Resultado por HOST			
Service (Port)	**Threat Level**	**Description**	**Solution**
general /tcp	**Medium**	· TCP timestamps	· Revisar

https (443/tcp)	**Medium**	· SSL Certificate Expiry	· Revisar
ssh (22/tcp)	**Medium**	· openssh-server Forced Command Handling Information Disclosure Vulnerability. The version of OpenSSH installed on the remote host is older than 5.7: ssh-2.0-openssh_ 3.7.1p2	· Actualizar versión · CVE: CVE-2012-0814 · BID:51702
tftp (69/udp)	Low	· TFTP detection	· Revisar
general /tcp	Log	· Checks for open udp ports: ○ tftp (69/tcp) · Checks for open tcp ports: ○ https (443/tcp) ○ ssh (22/tcp)	
https (443/tcp)	Log	· The remote web server type is: eHTTP v2.0 · A TLSv1 server answered on this port · A web server is running on this port through SSL	
ssh (22/tcp)	Log	· Detected SSH server version: SSH-2.0-OpenSSH_3.7.1p2 · An ssh server is running on this port	

Tabla 98. OpenVAS_Switches
* El análisis sobre los servidores está realizado a fecha de enero de 2014

Las soluciones a los problemas vienen definidos con estas dos referencias:

CVE (Common Vulnerabilities and Exposures): Es una lista sobre vulnerabilidades conocidas mantenido por el National Vulnerability Database (http://cve.mitre.org/). Sigue el siguiente formato: año-nº de vulnerabilidad.

BID: Es un código equivalente al CVE. Mantenido en http://www.securityfocus.com/

20. Anexo V. Casos prácticos

En el siguiente punto mostraremos con casos prácticos la necesidad de cumplir los estándares de seguridad como la ISO 27001 y LOPD. Gracias a estos ejemplos, comprenderemos la importancia de estar completamente concienciados en seguir dichas pautas, tanto por las consecuencias que tengan referentes a la seguridad así como posibles sanciones a recibir.

- **ISO 27001**

Ejemplo 1. Existencia de un Plan de Desastre y Contingencia

Un claro caso de un sistema de contingencia ante desastres lo supuso el incendio de la torre Windsor en Madrid (2005). Una de estas empresas afectadas fue DELOITTE:

DEFICIENCIAS

- Fallo de las medidas elementales de mecanismos de prevención y detección contra incendios, que provoca que el edificio en cuestión en poco tiempo se vea inutilizado por el fuego.

PREVISION

- A pesar de esto, DELOITTE disponía de un plan para responder automáticamente y asegurar la continuidad de negocio.
    - Existencia de una buena política de seguridad que asegura un backup de todos los datos importantes en diferentes localizaciones
    - Previsión de reubicación física inmediata en otras oficinas cercanas (Torre Picasso)

RESULTADO

A pesar de un resultado a priori catastrófico desde todo punto de vista, gracias a que se disponía de un plan de contingencia se minimizan:

- A pesar de las enormes pérdidas económicas se atenuaron en gran medida las consecuencias. De no adoptar estas medidas según qué tipo de empresa podría verse obligada a cerrar
- Se pudo restablecer el trabajo de la empresa en poco tiempo

Ejemplo 2. Contraseñas débiles

La mala concienciacion de los usuarios al establecer contraseñas en los sistemas es un hecho, y por tanto, una mala práctica. Esto hace que cualquier persona malintencionada en la búsqueda de acceso pruebe contraseñas típicas.

En la págna http://splashdata.com/press/worstpasswords2013.htm podemos ver un estudio realizado a empresas sobre las contraseñas más utilizadas por los usuarios en diferentes sistemas:

Rank	Password
1	123456
2	Password
3	12345678
4	qwerty
5	abc123
6	123456789
7	111111
8	1234567
9	iloveyou
10	adobe123

Tabla 99. Caso_1

➢ Con los actuales potentes equipos, basta poco tiempo para reventar una contraseña. Por una **contraseña aleatoria de 6 caracteres** se tardan unos **5 minutos** en descifrarla y si se **combinan las mayúsculas y las minúsculas** se amplía el tiempo a **> 8 días**.

➢ Por ello es importante seguir las recomendaciones de las buenas prácticas para elegir una contraseña adecuada al tipo de información sensible que manejemos.

Ejemplo 3. Phishing

En enero de 2014, tanto *Banco Santander* como *Caja España* sufren una campaña de phishing. Esta técnica busca mediante el envío de emails con la apariencia visual de dichas empresas, obtener datos relativos a cuentas bancarias y datos personales.

Tabla 100. Caso_2

Ante estas prácticas, sólo se puede ser precavido y sospechar de cualquier información en la que se nos pidan datos desde cualquier entidad bancaria. Mediante el instituto INTECO se alerta de estas prácticas a los internautas.

Para tratar de identificar un posible phishing, hay que fijarse en varios elementos:

· La existencia de faltas de ortografía o caracteres extraños puede dar pistas sobre una suplantación de página.

· El formato o las imágenes de la página que no cuadren o el tamaño sea inadecuado puede ser también un motivo para desconfiar.

· El acceso a la página mediante un protocolo no seguro sin un certificado firmado por una entidad reconocida es un caso claro. Sobretodo entidades importantes donde haya que intercambiar información importante, se accederá mediante el protocolo https con un certificado firmado o autofirmado.

Hay que recordar además que ninguna entidad financiera solicitará por correo electrónico algún tipo de acceso o contraseña a sus clientes.

Ejemplo 4. Nadie está a salvo

Es muy importante concienciarse de que cuanto más inseguro sea nuestro sistema más fácil será para los hackers un intento de intrusión. Aún teniendo un sistema securizado y siguiendo las buenas prácticas relativas a seguridad, podemos sufrir algún tipo de ataque. Mostramos debajo un timeline sobre algunos ataques llamativos a diferentes personas o empresas relevantes:

Date	Author	Target	Description	Attack	Target Category	Attack Category	Country
23-Oct			Anonymous claim to have breached the systems of Mossos d'Esquadra, the police force of Spanish community of Catalonia and leak the details of **431** individuals.	SQLi	Law Enforcement	Hacktivism	ES
30-Oct	Misafir	Google	A Turkish hacker called Misafir hacks and defaces the official Google Bolivia domain 2013 along with 7 other Google domains such as Google Translator, Maps, SMS, News, ID, Labs and Google Images domain.	DNS Hijacking	Online Services	Cyber Crime	BO
18-Sep			In name of #OpToroDeLaVega, hackers from the Anonymous collective defaces the web page of Tordesillas, a Spanish Town famous for "el Toro de la Vega", a festival in which a bull is slaughtered.	Defacement	Gov	Hacktivism	ES
16-Aug	?		The official Twitter account of famous German footballer Mario Götze, @MarioGoetze, is hacked and posts bogus messages in favor of Marouane Chamakh, a Moroccan footballer.	Account Hijacking	Single Individual	Cyber Crime	DE
8-Jul	?	club. nintendo	Almost **24,000** user accounts on Nintendo's main fan site Club Nintendo have been hijacked in a sustained mass-login attack that began early last month. Personal information was exposed including users' real names, addresses, phone numbers and e-mail	Account Hijacking	Industry: Video Games	Cyber Crime	JP

Tabla 101. Caso_3

*Datos recogidos de la web http://hackmageddon.com/

- **LOPD**

Ejemplo 1. Sanciones por incumplimiento de LOPD

En diciembre de 2013, Google es multado por la AEPD con 900000€ por infracciones sobre la LOPD. La multa se justifica en que Google recopila información personal sin indicar en muchas ocasiones qué datos se recogen y a qué se destinan, así como la ausencia de consentimiento al recogerlos.

Las empresas deben concienciarse de cumplir con la LOPD, no solo para cumplir con los deberes que se definen en la ley, sino porque la AEPD es muy estricta en la vigilancia de su cumplimiento y establece grandes sanciones en el caso de su incumplimiento.

Podemos encontrar en la página www.agpd.es muchos procedimientos sancionadores a empresas por incumplimiento de la LOPD. Podemos destacar algunos como:

- envío de correos publicitarios no solicitados (infracción leve)

- contratación de suministro de gas sin consentimiento del interesado (infracción grave)
- inclusión indebida en ficheros de morosidad (infracción grave)
- videovigilancia en vestuario y falta de inscripción del fichero (infracción grave)
- recogida de datos de menores sin consentimiento paterno en sitio web (infracción grave)

Ejemplo 2. Ejemplo de incidente de seguridad

Este caso ocurrió en junio de 2011. Hubo una intrusión en el portal web de INTECO (organismo público). Datos personales de muchos usuarios incluidos el *mío* fueron comprometidos.

En caso de que el incidente de seguridad sea problema por una mala securización de los sistemas de INTECO, podría ser responsable y propensa a sufrir algún tipo de sanción o denuncia por la AEPD o por los propios usuarios afectados.

formacion-online@inteco.es 06/06/11

para mí

Estimado/a usuario/a:

Nos ponemos en contacto con usted para comunicarle que INTECO ha sufrido un incidente de seguridad que ha provocado una sustracción de datos de información personal de la base de datos de usuarios de nuestra plataforma de formación en línea. Los datos que han sido robados son aquellos que nos facilitó usted durante el proceso de registro, entre los que pueden estar:

- Nombre y apellidos.
- Número de teléfono.
- DNI.
- Correo electrónico.

Hemos procedido a bloquear el acceso a la plataforma de formación hasta que el problema haya sido resuelto y se pueda garantizar su seguridad. Le informaremos tan pronto se reanude el servicio de modo que pueda continuar con su actividad formativa.

Existe el riesgo de que la información sustraída pudiera ser empleada con fines maliciosos. Por ese motivo, le recomendamos que siga los siguientes consejos de seguridad:

1. Desde INTECO nunca se le solicitará información de carácter personal por correo electrónico o teléfono. No responda a ninguna petición de información de estas características.
2. No haga clic en enlaces incluidos en mensajes de correo electrónico, mensajes SMS o MMS cuyo origen no sea confiable.
3. Mantenga su equipo adecuadamente protegido con aplicaciones de seguridad y debidamente actualizado con los parches recomendados por el fabricante.
4. Ante cualquier duda, póngase en contacto con INTECO en la dirección de correo incidencias@cert.inteco.es

Desde INTECO queremos pedirle disculpas por los inconvenientes causados y nos ponemos a su disposición para resolver cualquier duda que pueda surgirle.

Reciba un cordial saludo.

Tabla 102. Caso_4

Este es un caso que puede ocurrir en cualquier empresa, por lo cual habrá que adoptar las máximas medidas de seguridad para que no ocurra.