Universidad De Valladolid.

E.T.S. DE INGENIERÍA INFORMÁTICA (SEGOVIA)

Grado en Ingeniería Informática de Servicios y Aplicaciones.

Título: Metodología para Auditorías de Ciberseguridad

Alumno: Jaime Mejías Macías.

Universidad De Valladolid.

E.T.S. DE INGENIERÍA INFORMÁTICA (SEGOVIA)

Grado en Ingeniería Informática de Servicios y Aplicaciones.

Título: Metodología para Auditorías de Ciberseguridad

Alumno: Jaime Mejías Macías.

Tutor: Juan José Álvarez Sánchez.

ÍNDICE

1. INTRODUCCIÓN

1.1 Motivación

En las **auditorías de ciberseguridad** se analizan los riesgos relativos a la seguridad con un enfoque acorde a la nueva realidad de las tecnologías de la información.

Este enfoque consiste en realizar un mayor énfasis en las amenazas procedentes de redes de comunicación externas a la unidad auditada y en los nuevos tipos de **ataques y fraudes** basados en dichas redes, sin obviar los ataques e intentos de fraude tradicionales o que se pueden producir internamente (originados por personal de la propia organización).

A estas redes de comunicaciones externas al grupo, las denominaremos **ciberespacio**.

Toda organización que opera en internet tiene clientes en el ciberespacio. Esta operativa implica que la entidad se encuentra expuesta a sufrir lo que denominamos **ciberataques** (ataques maliciosos procedentes de las redes de comunicación externas y cuyo objetivo es recabar información, evitar que se presten servicios en el ciberespacio o cometer fraude en la entidad).

Los principales tipos de ciberataque existentes que buscan explotar las **vulnerabilidades** de los sistemas son los siguientes:

a. Ataques que evitan prestar el servicio en el ciberespacio (DDoS).
b. Ataques dirigidos a alterar la información, robarla o cometer fraude. (virus, troyanos, etc).

Debido a los continuos y crecientes ataques de ciberseguridad que se producen en las grandes empresas (casos conocidos como Sony, Apple, etc.), algunas empresas han tenido pérdidas multimillonarias y, por consiguiente, hay una tendencia para invertir importantes cantidades en los presupuestos de las empresas en ciberseguridad y ésta es cada vez más protagonista en los planes estratégicos de las empresas.

A continuación podemos ver algún ejemplo de grandes compañías afectadas gravemente por ciberataques en algún momento.

TECNOLOGÍA

La Voz de Galicia

Sony alcanza un acuerdo económico con las víctimas del ciberataque que sufrió en el 2014

• *Pagará 8 millones de dólares por permitir que su información personal quedara expuesta a los piratas informáticos*

EFE. 20 de octubre de 2015. Actualizado a las 22:39 h.

0 votos

FOTO: KEVORK DJANSEZIAN | REUTERS.

Sony Pictures Entertainment (SPE) ha alcanzado **un acuerdo económico con víctimas del ciberataque que sufrió el año pasado**, a las que pagará hasta 8 millones de dólares por permitir que su información personal quedara expuesta a los piratas informáticos.

Según recoge este martes la prensa local, el acuerdo con extrabajadores y miembros actuales de la compañía ha sido depositado en uno de los juzgados de Los Ángeles (EE.UU.) y debe ser aún ratificado por el juez. En un mensaje enviado a la plantilla, el director ejecutivo de la empresa, Michael Lynton, **califica el acuerdo como «un paso adelante importante y positivo para dejar atrás de forma firme el ciberataque»**.

TEMAS RELACIONADOS

Sony | Cine | Corea del Norte | EE.UU.

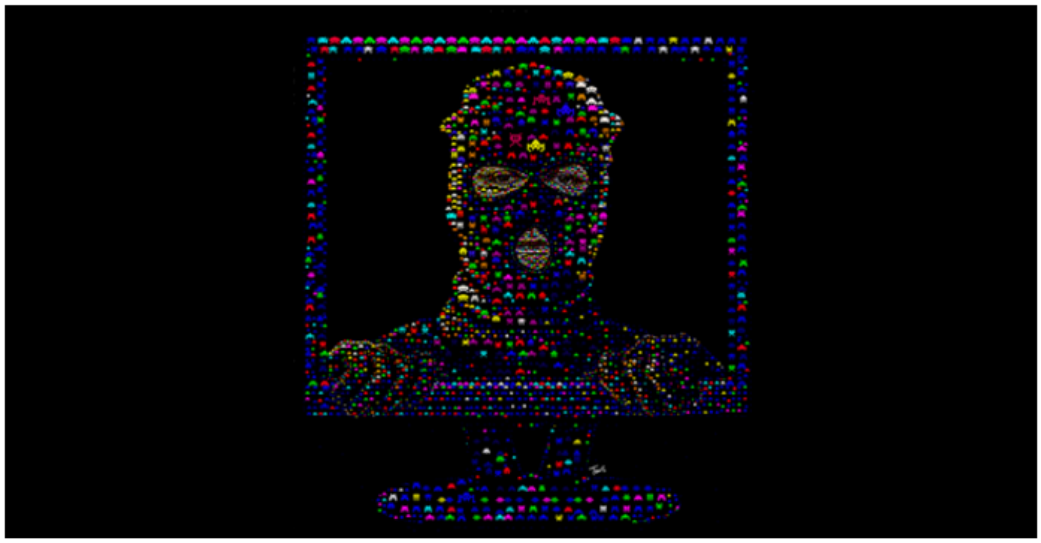
MÁS NOTICIAS DE SONY

- Coches y realidad virtual, protagonistas de la feria CES de Las Vegas
- La montaña rusa de la realidad virtual
- El gurú del videojuego Hideo Kojima deja Konami y negocia fichar por Sony
- El «VdeValarés» ya tiene imagen

Ciberataque Sony Pictures Entertaiment

Un ciberataque a bancos rusos roba un botín de más 20 millones de euros

Seguridad 23 diciembre, 2014



COMPARTIR

Twitter 0

Facebook 0

Google + 5

Linkedin 0

Pinterest 0

Flip Meneame

Parece que el de Sony Pictures no ha sido el último gran ciberataque del año. **Un grupo de cibercriminales rusos se habría hecho con más de 20 millones de euros en su país y las antiguas repúblicas soviéticas que lo rodean** a través de un sofisticado ataque a bancos y entidades financieras.

El objetivo de estos atacantes, a los que se vincula con la organización cibercriminal Anunak, no son los clientes de estos bancos, como en otras ocasiones, sino **las propias entidades y su infraestructura**. Y, según informa Computer World, sus ambiciones no terminan ahí, sino que se extienden a **cadenas de tiendas y establecimientos norteamericanos y europeos**, en los que intentan infiltrarse *hackeando* sus TPV. Al menos 12 firmas norteamericanas, en tres de las cuales ya ha sido confirmado el robo de números de tarjetas de crédito, podrían haberse visto comprometidas

Ciberataque a bancos rusos

Ante lo comentado anteriormente, las empresas realizan cada vez auditorías más intensas sobre ciberseguridad. Por ello, puede ser de **utilidad para el auditor** de ciberseguridad la creación de una metodología que sirva como referencia o manual a quien se disponga a realizar una auditoría de Ciberseguridad en una empresa de cierto tamaño. Con esta metodología **se analizarán los distintos elementos, hardware y software**, a los que pueda afectar un ataque de ciberseguridad y se podrá establecer un rating del **risk assesment(riesgo potencial)** que indique hasta qué punto la unidad auditada es robusta o no.

Además, dispondremos de una **aplicación de ayuda para la generación del informe final de auditoría** donde se pueda observar el resultado de todos los puntos analizados. Este informe ha de servir como **soporte** a la hora de establecer las conclusiones en el **informe final de Auditoría** realizado y, con ello, ayude a la determinación del rating del Riesgo Potencial de la entidad auditada (Risk assesment).

Aplicando lo contenido en el manual y en el aplicativo, se debe dar respuesta preguntas como las siguientes. ¿La unidad auditada es resistente? ¿La política de privacidad de la unidad auditada es correcta? ¿Son seguros los sitios web y las aplicaciones que se utilizan? ¿Se están gestionando eficientemente las amenazas? etc.

1.2 Objetivos

La revisión se centra en las **plataformas y redes de comunicación** que albergan los sistemas de la organización, siendo los principales puntos de revisión los siguientes:

- **Modelo de Gobierno**. En este apartado procederemos al análisis de la implicación de la alta dirección en los aspectos relativos a la seguridad de los sistemas y redes de comunicación de la entidad, las medidas adoptadas para prevenir incidentes de seguridad y las acciones que se toman cuando se detectan y reportan incidencias, eventos o vulnerabilidades en los sistemas.

Dentro de este apartado analizaremos con mayor profundidad los siguientes aspectos:

- **Organización y estrategia.** Se analizará la suficiencia de la estructura organizativa del área de control del riesgo tecnológico para desempeñar las tareas de control, seguimiento y reporte a los diversos departamentos y comités involucrados en garantizar la ciberseguridad de la entidad.

- **Análisis y evaluación.** Se verificará la existencia y suficiencia del riesgo potencial de ciberseguridad de la unidad, así como la adecuación de las medidas e indicadores que se elaboren en base a dicho análisis.

- **Políticas y procedimientos.** Se comprobará que las políticas, procedimientos y acciones que tome la unidad auditada en base a los mismos son adecuados.

- **Gestión y Control.** El objetivo de este apartado es analizar la adecuación del modelo de gestión del riesgo tecnológico relativo a la ciberseguridad, así como verificar la suficiencia de los controles establecidos para mitigar los riesgos.

Analizaremos con mayor detenimiento los siguientes aspectos:

- **Inventario de activos críticos.** Identificaremos y revisaremos que los activos e inventarios de la entidad se encuentran adecuadamente gestionados.

- **Monitorización y herramientas.** Verificaremos que se realiza una adecuada monitorización y seguimiento de los eventos de seguridad, así como la existencia de medidas proactivas por parte de la entidad para evitar incidentes.

- **Gestión y resolución de incidentes.** Analizaremos la suficiencia de los procedimientos y medidas adoptadas para resolver las incidencias de seguridad y el reporting de las mismas.

- **Seguridad perimetral y en Internet.** Revisaremos si las medidas de prevención de ciberataques son adecuadas, si la configuración de los servidores de prevención de intrusos (IDS) y los filtros implementados en la navegación web y en el correo electrónico son suficientes y las adecuación de las plataformas antivirus, anti malware, etc.

- **Seguridad de las comunicaciones.** Analizaremos la arquitectura de red y los dispositivos que la componen, la adecuación de la administración de los dispositivos de seguridad de la red y las reglas implementadas en ellos, el empleo de protocolos de red seguros, la suficiencia en los controles de acceso a las redes existentes y la seguridad en las conexiones con terceros (reguladores, otras entidades, etc.).

- **Seguridad de datos y sistemas.** Comprobaremos que existen políticas, procedimientos y medidas implementadas en los sistemas que garanticen un adecuado control de acceso a los sistemas y que protegen la información contenida en los repositorios de datos.

- Igualmente y con objeto de mitigar las vulnerabilidades reportadas por los fabricantes de hardware y software, se revisara que existen tanto **procedimientos periódicos**, como un nivel razonable de actualizaciones de seguridad en la plataforma de la entidad.

- **Seguridad de los usuarios.** Se verificará que los usuarios no disponen de privilegios en sus equipos de trabajo que les permitan realizar acciones maliciosas o sustraer información de la plataforma tecnológica de la entidad.

Por otro lado, se va a realizar una **aplicación que recorra todos los apartados de la auditoría** y que indique si el resultado de cada uno de los puntos revisados en la auditoría ha sido satisfactorio o no.

Tras rellenar los distintos apartados de la interfaz, se generará un archivo PDF automáticamente con un informe de la auditoría, el cual podrá ser personalizado con comentarios adicionales realizados por el auditor y nos **podrá servir como informe final de auditoría o como soporte a la hora de generar el informe final de auditoría.**

1.3 Resultados

El principal resultado del trabajo será un informe (memoria) con los siguientes contenidos:

- Una descripción de todos los procedimientos llevados a cabo para auditar los objetivos descritos.
- Ejemplos prácticos de las pruebas y el trabajo de campo a realizar en los distintos pasos.
- Generación de conclusiones con la elaboración de un Informe de Auditoría.
- Documentación técnica y evidencias del desarrollo de la aplicación de generación automática de informes.

1.4 Metodología

Para llevar a cabo este trabajo, se ha realizado un **enfoque cuantitativo** en el cual se parte de datos e información para demostrar si las hipótesis planteadas previamente a la realización de pruebas son o no son verdaderas.

Por otro lado, se aplicará **investigación documental** para recabar información sobre los procedimientos adecuados para realizar auditorías de ciberseguridad.

1.5 Recursos

Para la realización del proyecto se precisará del siguiente equipo informático:

Hardware: se necesitará un computador personal con una impresora láser, acceso a Internet de alta velocidad debido a la gran cantidad de datos que se deberán buscar, preferiblemente el procesador deberá ser de alta velocidad.

Software:

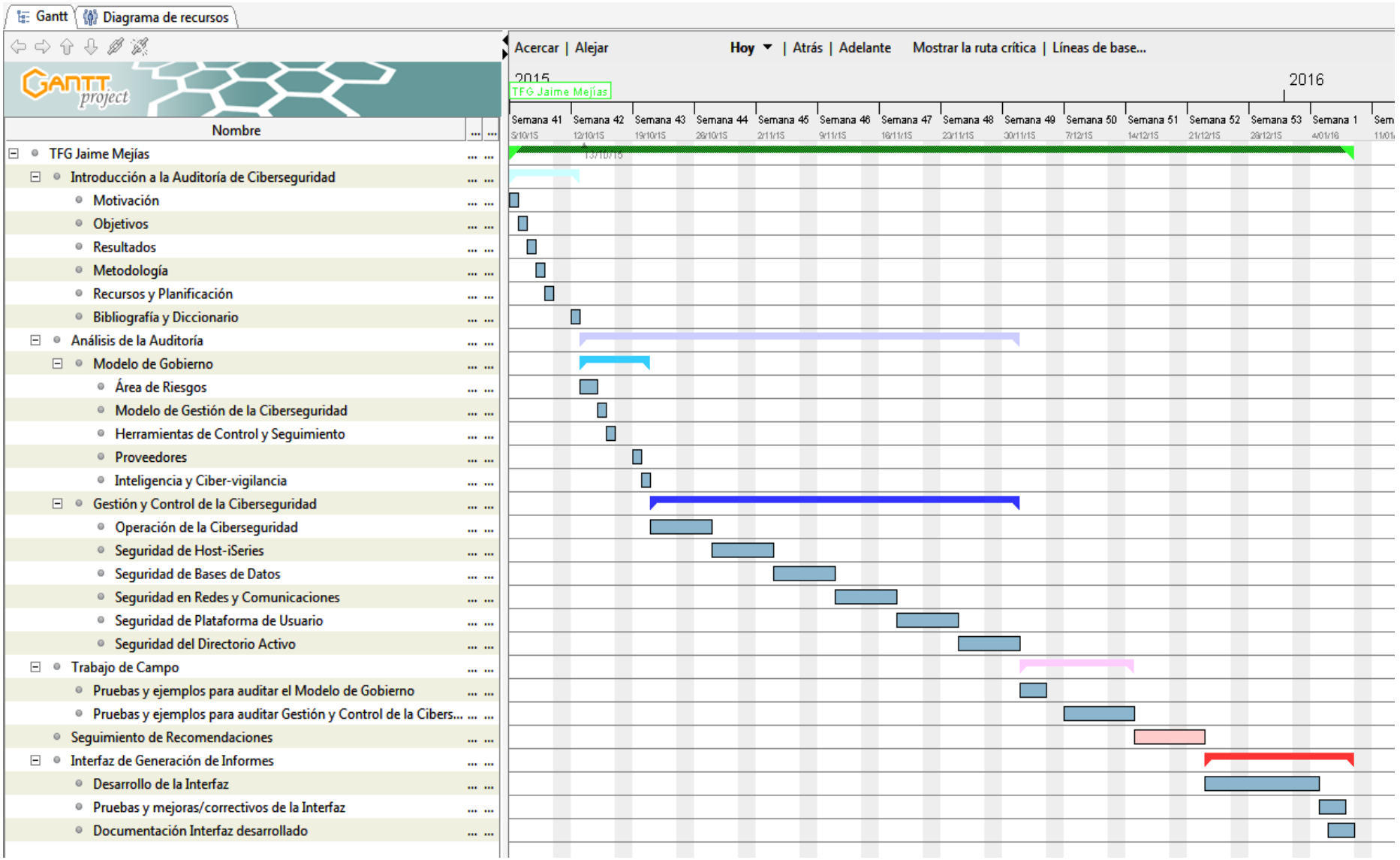
- Se utilizará **Microsoft Word** para la realización de la memoria.
- Por otro lado, se instalará el paquete **WAMP**, que es gratuito y nos permitirá el desarrollo de la aplicación en un servidor Apache y el uso de las tecnologías Mysql para base de datos y PHP para la programación web.
- Procesador de textos **Notepad ++**: lo utilizaré para la generación de código para la programación web de la Interfaz.
- **Gantt Project**: para estructurar la planificación del proyecto y realizar los diagramas de Gantt.

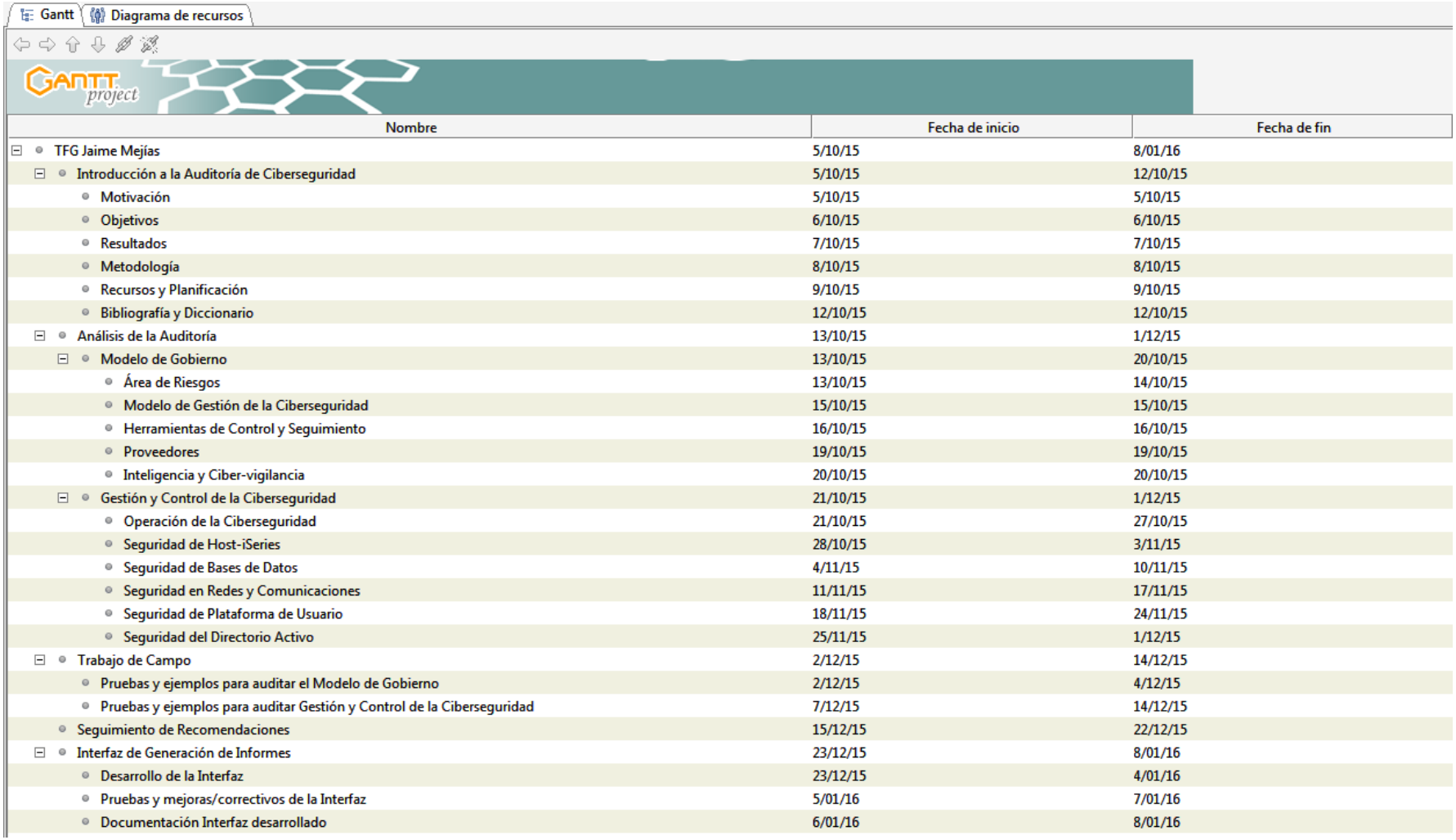
1.6 Planificación

La estimación de costes la he realizado basándome en el modelo de productividad. En este modelo, la productividad es definida como una función tanto del valor como de costo. En donde el valor incluye factores de calidad como de cantidad, los costos incluyen factores de recursos, complejidad y de personal.

A continuación se muestran los diagramas de Gantt donde se puede apreciar que el Trabajo de Fin de Grado llevará consigo un coste total de 70 jornadas repartidas de la siguiente manera:

- Introducción a la Auditoría: 6 días
- Análisis de la Auditoría: 36 días
  - Análisis del Modelo de Gobierno de la unidad auditada: 6 días
  - Análisis Gestión y control de la ciberseguridad: 30 días
- Trabajo de campo: 9 días
  - Pruebas y ejemplos para auditar Modelo de Gobierno: 3 días
  - Pruebas y ejemplos para auditar Gestión y control de la ciberseguridad: 6 días
- Seguimiento de recomendaciones: 6 días
- Interfaz Generación de Informes: 13 días
  - Desarrollo Interfaz: 9 días
  - Pruebas interfaz y mejoras/correctivos: 2 días
  - Documentación: 2 días


Gantt
Diagrama de recursos
Acercar | Alejar
Hoy | Atrás | Adelante
Mostrar la ruta crítica | Líneas de base...
2015
2016
TFG Jaime Mejías
Nombre
TFG Jaime Mejías
Introducción a la Auditoría de Ciberseguridad
Motivación
Objetivos
Resultados
Metodología
Recursos y Planificación
Bibliografía y Diccionario
Análisis de la Auditoría
Modelo de Gobierno
Área de Riesgos
Modelo de Gestión de la Ciberseguridad
Herramientas de Control y Seguimiento
Proveedores
Inteligencia y Ciber-vigilancia
Gestión y Control de la Ciberseguridad
Operación de la Ciberseguridad
Seguridad de Host-iSeries
Seguridad de Bases de Datos
Seguridad en Redes y Comunicaciones
Seguridad de Plataforma de Usuario
Seguridad del Directorio Activo
Trabajo de Campo
Pruebas y ejemplos para auditar el Modelo de Gobierno
Pruebas y ejemplos para auditar Gestión y Control de la Cibers...
Seguimiento de Recomendaciones
Interfaz de Generación de Informes
Desarrollo de la Interfaz
Pruebas y mejoras/correctivos de la Interfaz
Documentación Interfaz desarrollado


Gantt | Diagrama de recursos

GANTT project

Nombre	Fecha de inicio	Fecha de fin
TFG Jaime Mejías	5/10/15	8/01/16
Introducción a la Auditoría de Ciberseguridad	5/10/15	12/10/15
Motivación	5/10/15	5/10/15
Objetivos	6/10/15	6/10/15
Resultados	7/10/15	7/10/15
Metodología	8/10/15	8/10/15
Recursos y Planificación	9/10/15	9/10/15
Bibliografía y Diccionario	12/10/15	12/10/15
Análisis de la Auditoría	13/10/15	1/12/15
Modelo de Gobierno	13/10/15	20/10/15
Área de Riesgos	13/10/15	14/10/15
Modelo de Gestión de la Ciberseguridad	15/10/15	15/10/15
Herramientas de Control y Seguimiento	16/10/15	16/10/15
Proveedores	19/10/15	19/10/15
Inteligencia y Ciber-vigilancia	20/10/15	20/10/15
Gestión y Control de la Ciberseguridad	21/10/15	1/12/15
Operación de la Ciberseguridad	21/10/15	27/10/15
Seguridad de Host-iSeries	28/10/15	3/11/15
Seguridad de Bases de Datos	4/11/15	10/11/15
Seguridad en Redes y Comunicaciones	11/11/15	17/11/15
Seguridad de Plataforma de Usuario	18/11/15	24/11/15
Seguridad del Directorio Activo	25/11/15	1/12/15
Trabajo de Campo	2/12/15	14/12/15
Pruebas y ejemplos para auditar el Modelo de Gobierno	2/12/15	4/12/15
Pruebas y ejemplos para auditar Gestión y Control de la Ciberseguridad	7/12/15	14/12/15
Seguimiento de Recomendaciones	15/12/15	22/12/15
Interfaz de Generación de Informes	23/12/15	8/01/16
Desarrollo de la Interfaz	23/12/15	4/01/16
Pruebas y mejoras/correctivos de la Interfaz	5/01/16	7/01/16
Documentación Interfaz desarrollado	6/01/16	8/01/16

1.7 Bibliografía

- COBIT
- ISO 27001
- ISO 27002
- Expansión, *Control Interno, Auditoría y Seguridad Informática.*
- Piattini, M., E. Del Peso, *Auditoría Informática: un enfoque práctico.*

1.8 Diccionario

- **SLA**: Un **acuerdo de nivel de servicio** (en inglés *Service Level Agreement* o *SLA*), es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.
- **Segregación de funciones**: es un método que usan las organizaciones para separar las responsabilidades de las diversas actividades.
- **Waivers**: son permisos otorgados como excepción a una política de ciberseguridad.
- **SOC (centro de operaciones de seguridad)**: es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet.
- **Ddos (ataque de denegación de servicio:** es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.
- **Parche de seguridad:** un parche consta de cambios que se aplican a un programa, para corregir errores, agregarle funcionalidad, actualizarlo, etc.

- **CMDB:** listado con todos los elementos que componen la infraestructura de red.

- **VPN (Red Privada Virtual):** es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.

- **PKI (Infraestructura de Clave Pública):** es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

- **Hacking ético:** Hacking ético es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

- **Firewall:** es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

- **IDS (Sistema de Detección de Intrusiones):** es un programa de detección de accesos no autorizados a un computador o a una red.

- **Proxy:** es un punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo.

- **MDM:** es un tipo de software que permite asegurar, monitorear y administrar dispositivos móviles sin importar el operador de telefonía o proveedor de servicios.

- **Bastionado de servidores:** se refiere a la configuración de seguridad de los servidores.

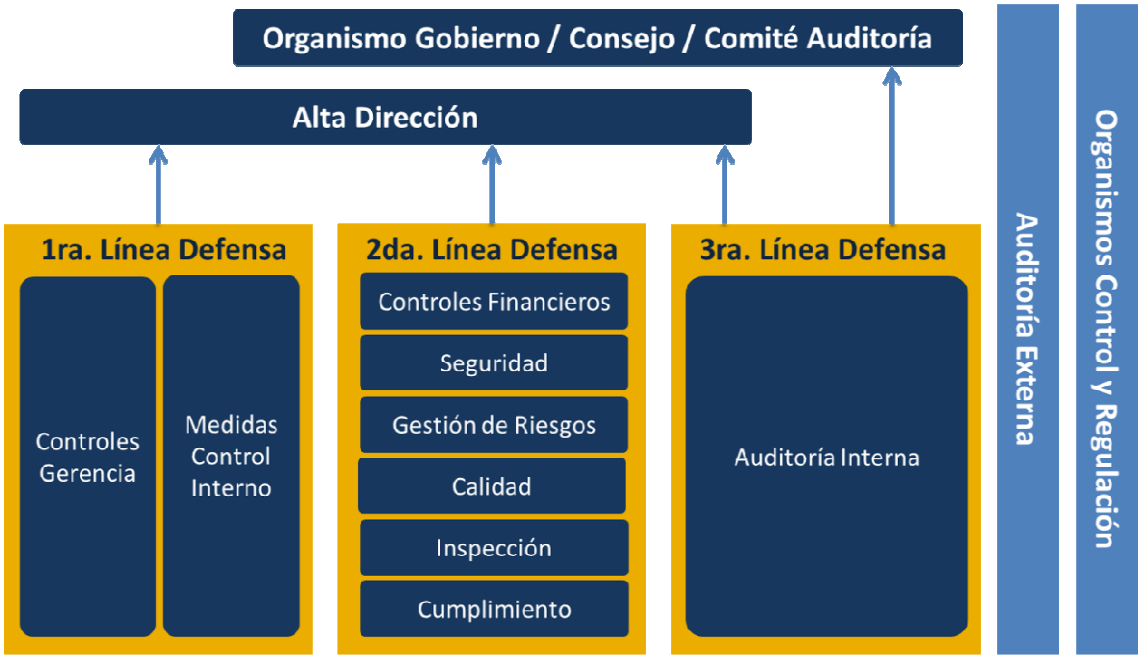
- **Compliance:** es una serie de normas o buenas prácticas a seguir en una organización.

2. MODELO DE GOBIERNO

2.1 ÁREA DE RIESGOS.

2.1.1 Organigrama del área.

Deberemos verificar que el control y la gestión de la tecnología se encuentran segregados conforme al **modelo de ciberseguridad**, por ejemplo el modelo Tres líneas de defensa:



2.1.2 Funciones y responsabilidades.

Para la gestión de la ciberseguridad en una compañía, el área o áreas encargadas de esta función han de dar cobertura a las siguientes funcionalidades:

- Desarrollar, elaborar y proponer a aplicar las normas y metodologías de seguridad de TI, asegurando el cumplimiento del nivel de información de seguridad de los sistemas, de acuerdo con las definiciones de la política de seguridad informática.

- Colaborar para la definición de los requisitos para garantizar la seguridad, integridad y control de las áreas en las que operan con la tecnología.

- Proponer un calendario y realizar pruebas periódicas de seguridad lógica con el fin de verificar la eficacia de los controles instalados, identificar brechas de seguridad y proponer medidas correctoras; y, en coordinación con el área de Recursos Humanos, ocuparse de la formación técnica en seguridad informática.

- Analizar las fuentes de exposición de Riesgo Tecnológico a través de indicadores de riesgo y cuestionarios de autoevaluación y seguir las recomendaciones y/o sugerencias para mejorar la calidad de la primera línea.

- El seguimiento de los proyectos de mitigación definidos a nivel tecnológico por parte de las distintas áreas.

2.1.3 Personal que compone el área (externo e interno)

Es necesario identificar el personal y que éste tenga una correcta segregación funcional para verificar que todos y cada uno de los empleados pertenecientes al área, tienen un adecuado acceso a la información.

2.1.4 Relaciones jerárquicas y funcionales del área

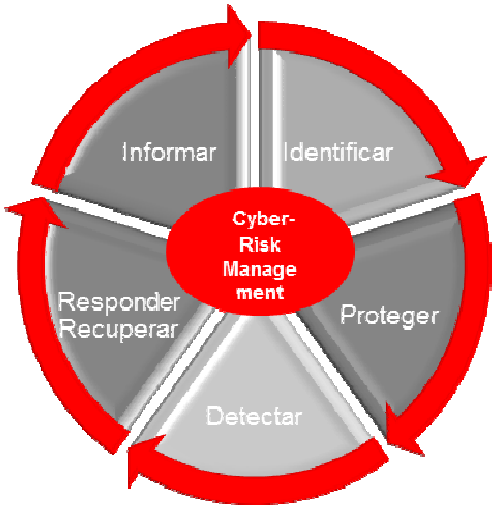
Con ello, analizaremos la responsabilidad que recae en cada una de las partes importantes del área.

Para ello, deberemos analizar la estructura de comités, pidiendo evidencias de la celebración de éstos, analizando en todo caso la adecuación de los asistentes, los reportes realizados, la planificación, seguimiento y aprobación de medidas y planes, análisis de nivel de servicio ofrecido por proveedores, resolución de incidencias, etc.

Además, el área de Seguridad deberá estar en constante comunicación en caso de que pueda haber cambios normativos o regulatorios.

2.2 MODELO DE GESTIÓN DE LA CIBERSEGURIDAD

El Modelo de Gestión de la Ciberseguridad ha de estar alineado con los **estándares definidos en esta materia (NIST, COBIT e ISO)** y las directrices de los reguladores, tanto internacionales como nacionales. A continuación, podemos ver el ejemplo de lo que debe de ser un Modelo de Gestión de la Ciberseguridad adecuado. Se basa en las siguientes tareas que se ejecutan de manera cíclica y se realimentan:



- **Identificar**: analizando los riesgos, midiendo la exposición, reconociendo los activos y las aplicaciones más críticas y sus vulnerabilidades…

- **Proteger**: asegurando una adecuada configuración de la seguridad (control de accesos, bastionado de dispositivos, etc.), disponiendo de herramientas adecuadas (plataformas antiDDoS, antimalware, antivirus, ect.), teniendo procedimientos completos y una apropiada formación a los empleados.

- **Detectar**: monitorizando la infraestructura, manteniendo colaboración con las autoridades, contratando servicios de hacking-ético…

- **Responder / Recuperar**: con protocolos adecuados de comunicación de incidencias y un Centro de Respuesta a Incidencias (SOC), desarrollando planes de mejora y de recuperación…

- **Informar**: reportando ciberindicadores y ciberincidentes, haciendo seguimientos y control de proyectos relacionados.

2.3 MECANISMOS PARA CONTROL DE CIBERSEGURIDAD

Se debe analizar la existencia de herramientas y/o **mecanismos para la supervisión de la actividad de la 1ª línea de defensa** y que la unidad analiza que estas medidas son suficientes y cubren todos los dominios del riesgo tecnológico (Seguridad de la información, Producción, Desarrollo y Gestión de la tecnología).

La unidad auditada ha de disponer de herramientas y procedimientos a incidentes de **phishing** (fraude mediante webs o emails falsos que imitan los sitios oficiales), **vishing** (fraude telefónico realizando pagos u operaciones a nombre de la víctima) y **smishing** (similar al phishing con origen a través de mensajes de texto telefónicos).

Además se debe dar seguimiento a las incidencias de seguridad en los diferentes niveles:

- Evolución de las incidencias de ciberseguridad.

- Seguimiento del estado actual de la seguridad en la unidad: las vulnerabilidades activas, calendario de tests de seguridad, clasificación de sus webs por nivel de seguridad, modelo de gestión de la ciberseguridad, estado del plan de ciberseguridad, etc.

- Seguimiento de los fraudes, alertas y vulnerabilidades detectadas.

2.4 PROVEEDORES.

Identificar los proveedores que tiene la unidad, quien nos proporcionará contratos y **SLAS** vigentes en la fecha de la auditoría.

En especial debemos recabar información de aquellos proveedores que se encarguen de temas de ciberseguridad (antivirus, SOC, etc.).

La unidad debe realizar Risks Assesment estableciendo un rating de los proveedores contemplando aspectos relativos a la seguridad como:

- Normativa de Seguridad de información.
- Organización de Seguridad de información.
- Seguridad de los Recursos Humanos.
- Seguridad Física y Ambiental.
- Amenazas de transferencias de datos.
- Información CPD's

2.5 INTELIGENCIA Y CIBER-VIGILANCIA

Las labores principales de análisis e inteligencia que se realizan han de consistir en:

- Observatorio en foros, chats, Facebook, etc. de posibles ataques o temas que pudieran afectar a la actividad de la unidad analizando la información relevante.

- Canal de comunicación con las autoridades locales.

- Informar a los empleados de posibles riesgos que podrían afectarles.

3. GESTIÓN Y CONTROL

3.1 OPERACIÓN DE LA SEGURIDAD

El objetivo de este apartado es obtener la estructura organizativa del departamento de seguridad, verificando que se cumplen los siguientes aspectos:

a) Las **áreas de seguridad se encuentran convenientemente identificadas**.

b) La descripción funcional de los puestos y la relación entre los mismos se encuentran correctamente definidas. (ref. ISO/IEC 27001:2013)

c) Existe una adecuada **segregación funcional** entre las áreas que componen el departamento, como por ejemplo: (ref. ISO/IEC 27001:2013)

- Los encargados de la gestión de usuarios administradores son independientes de los autorizadores.

- Los responsables de la implantación de las políticas de seguridad no son los encargados de definirlas.

- Existe distinción entre los operadores de seguridad y el personal encargado de revisar la actividad de los mismos.

- Existe un departamento que analiza todas las amenazas de seguridad IT que se producen (Advanced Persistent Threats, Malware, Botnets, DDoS, 0-Day, Identity Theft, Data Loss Prevention, phising y fraude interno) y que coordina su resolución y mantiene contacto con los organismos de alerta temprana (CERT). (ref. ISO/IEC 27001:2013)

Comprobar que se han implementado procedimientos de seguridad y que existen mecanismos para garantizar la implantación de las políticas de seguridad, así como la aprobación y registro de las excepciones a su implantación (**waivers**).

Tomar especial atención en aquellos procedimientos que permiten comprobar que la **actividad de los operadores se encuentra regulada** recogiéndose las principales tareas que realicen (ref. ISO/IEC 27001:2013):

a) Gestión de usuarios y claves (alta, baja, modificación y desbloqueo)

b) Utilización de usuarios de emergencia

c) Gestión de claves criptográficas

d) Gestión de accesos desde el exterior

e) Configuración de sistemas y dispositivos de seguridad.

En el siguiente cuadro se muestra un resumen con algunos de los procedimientos y normativas que la unidad debería aplicar:

Procedimientos y normas	Descipción
Políticas y Normas de utilización del correo electrónico e internet, Email y las políticas de uso de internet y regulaciones.	Instrucciones generales
	AVISO LEGAL a incluir en los correos electrónicos
Control y gestión de los accesos a los sistemas informáticos, objetivos e índice	Nomenclatura, identificación y definición de USERID
	Competencias para el control y gestión de acceso de los sistemas
	Procedimientos de control y administración de acceso a sistemas
	Cuadro resumen de las competencias y funciones
	Cuadro con información de empresas externas
Normas de seguridad de información	Organización de la seguridad de la Información. Estándar
	Utilización del material informático, Internet, E-mail
	Gestión de Incidentes de Seguridad
	Terceros
	Gestión de Activos
	Clasificación de Seguridad de la información
	Adquisición y Mantenimiento de Software
	Control de accesos.

Control y gestión de incidentes de Seguridad	Procedimientos de comunicación y distintos departamentos implicados en la gestión de incidentes
	Comunicación de incidentes
	Flujograma
	Matriz de incidentes de seguridad
Respuesta a Incidentes de Phishing, Vishing e SMiShing	Procedimientos ante la respuesta de incidentes
Política de Escritorio Limpio	Política y Procedimiento para mantener el Clean Desk

En cuanto a **ciberincidentes**, se deberá contar con un procedimiento correctamente definido dónde se detalle la categorización de los mismos. A continuación, se muestra un listado con lo que podría ser una correcta categorización de ciberincidentes:

CATEGORÍA	DESCRIPCIÓN
Acceso externo no autorizado	Ataques externos no autorizados que permitan acceder, modificar datos o interrumpir un servicio utilizando técnicas de hacking como SQL Injection, Cross-Site, ataques de ingenieria social, etc
Acceso interno no autorizado	Acceso interno no auttorizado a los sistemas que comprometan la integridad, confidenciadlidad y accesibilidad o disponibilidad de los negocios críticos utilizando técnicas como hacking o ingenieria social.
Robos	Robos de dispositivos no cifrados quje contengan información condifencial como PC, laptops, tablets, smartphones, pendrives, etc..
Incumplimientos	Incumplimientos de regulación y legales relacionados con la seguridad de la información causadas por un acto deliberado y que tengan consecuencias directas en las operaciones de negocio.
Malware	Indisponibilidad de funciones críticas de negocio debido a programas malware (virus, troyanos) con posibilidad de afectar a otras entidades del grupo
DoS	Ataques de denegación de servicio que causen indisponibilidad de servicios crítcos o que puedan repercutir en la imagen de la compañía.
Otros	Cualquier otro tipo de incidentes relacionado con la seguridad y que no estén incluidos en los anteriores.

Por otro lado, sería aconsejable contar con algún **manual de buenas prácticas** cuyo objetivo es inculcar las medidas de seguridad para garantizar la protección de los activos e información general de los clientes. En él, se incluye información para ayudar a evitar situaciones en los que la seguridad de la información se puede poner en riesgo, así como los mecanismos más eficaces para cumplir con el compromiso de garantizar la seguridad y la eficiencia del entorno de trabajo.

Verificar que el departamento de seguridad implementa medidas suficientes para garantizar la adecuada **formación del personal** dedicado a la gestión de la seguridad.

Contrastar que se realizan **revisiones periódicas de las políticas y procedimientos**. (ref. ISO/IEC 27001:2013)

Comprobar que los operadores de seguridad cuentan con herramientas suficientes para el desarrollo de sus funciones, siendo preferible el uso de herramientas centralizadas.

Verificar que las herramientas utilizadas registran la actividad de los usuarios administradores:

a) Marca temporal (fecha y hora en la que se realiza la acción) y que el tiempo se obtenga de una fuente validada.

b) Registro de altas, bajas y modificaciones de usuarios

c) Pistas de auditoría, que incluyan traza de acceso a datos sensibles y eventos de seguridad (intentos de acceso fallido al sistema y a los datos, modificaciones en los parámetros de seguridad de los usuarios, conexiones remotas, etc.

d) Mecanismos que permitan identificar al personal que realiza cada una de las operaciones

Comprobar si las herramientas generan **alarmas ante los cambios** en las cuentas de usuarios de administradores. (ref. ISO/IEC 27001:2013)

Verificar que los **logs de seguridad** se almacenan durante un tiempo razonable, principalmente si existen requerimientos legales al respecto, y que esta información se encuentra convenientemente respaldada. Comprobar igualmente que estos registros son analizados periódicamente por responsables. (ref. ISO/IEC 27001:2013)

Verificar que la unidad realiza tareas de revisión sobre los usuarios administradores de sistemas:

a) Revisiones periódicas de usuarios con el fin de comprobar que se eliminan aquellos que no estén vigentes, que no existen usuarios genéricos (salvo excepciones debidamente autorizadas) y que se respetan los procedimientos de gestión de usuarios. (ref. ISO/IEC 27001:2013)

b) Identificación y evaluación de **perfiles y privilegios de acceso** asignados a los usuarios. Verificar que dichos perfiles/privilegios se corresponden con las responsabilidades y funciones asociadas a los roles que desempeñan. (ref. ISO/IEC 27001:2013)

Realizar una revisión de los usuarios administradores sobre una muestra de sistemas (físicos y virtuales) y/o dispositivos de seguridad, tomando como base: el listado de usuarios proporcionado por la unidad, los logs de actividad, y el fichero de RRHH.

Para la detección y el análisis de vulnerabilidades, sería conveniente revisar si se realiza la **gestión centralizada de los incidentes de seguridad**. Para ello, algunas empresas cuentan con un **SOC** (Security Operation Center), donde se cuantifican y se intentan minimizar las incidencias que se puedan producir, entre las que destacarían las siguientes:

- **Malware**: Malicious software
- **Corporate Security**: Gestión de parches, Spam, Pérdida de información, sondas y escaneos, intentos de acceso no autorizados, **exploits**.
- **DDoS**: **Ataques de denegación de servicio** distribuidos
- **End User Security**: Amenazas de password, violación de políticas corporativas.

Para que el SOC pueda realizar su trabajo adecuadamente, debe contar con algún tipo de **herramienta que registre todos los eventos** que se puedan producir en los sistemas e infraestructura. Además, la herramienta debe categorizar las incidencias que se produzcan según su criticidad.

Revisar si los dispositivos de la **infraestructura** (servidores de autentificación, componentes de red, firewalls, IDS/IPS, antivirus, etc) están siendo monitorizados por la herramienta de registro de eventos.

3.2 GESTIÓN Y CONTROL

3.2.1 Seguridad del Host - iSeries

El sistema iSeries o AS/400 es un equipo de IBM de gama media y alta, para todo tipo de empresas y grandes departamentos.

Se trata de un sistema multiusuario, con una interfaz controlada mediante menús y comandos CL (Control Language) intuitivos que utiliza terminales y un sistema operativo basado en objetos y bibliotecas, denominado OS/400. Un punto fuerte del OS/400 es su integración con la base de datos DB2/400, siendo los objetos del sistema miembros de la citada base de datos. Ésta también da soporte para los datos de las aplicaciones, dando como resultado un sistema integrado potente y estable.

Soporta otros sistemas operativos tales como GNU/Linux, AIX o incluso Windows en una placa Intel integrada, soportando también de forma nativa múltiples aplicaciones antes reservadas a Windows.

La capacidad de supervivencia de la máquina es debida a su capa de MI o Machine Interface, que aísla el hardware y permite, mediante el uso de APIs, que el sistema operativo y los programas de aplicaciones se aprovechen de los avances en hardware sin tener que recompilarlo y de su adaptación al entorno empresarial crítico, en donde la estabilidad y fiabilidad del sistema son fundamentales.

Los objetivos de una auditoría de seguridad Host para servidores **iSeries** son los siguientes:

- Identificar y obtener las políticas y procedimientos relativos a la configuración de la seguridad de la plataforma zSeries/iSeries. (ref. ISO/IEC 27001:2013)

- Comprobar que dichos procedimientos han sido construidos teniendo en cuenta los requerimientos de las políticas corporativas, regulatorias, y las mejores prácticas de la industria, ya sean del fabricante, o de organismos dedicados a la publicación de estándares de seguridad (NIST, FIPS, ANSI, IEEE, ISO, IEC, ISACA, etc). (ref. ISO/IEC 27001:2013)

- Contrastar si la **configuración de los sistemas** (físicos y virtualizados) es conocida y aprobada por Seguridad Informática y está alineada con los procedimientos o estándares mantenidos por el área.

- Analizar si la unidad utiliza alguna herramienta automática de **compliance**. (ref. ISO/IEC 27001:2013)

- Comprobar que los sistemas cuentan con un **nivel de actualización** suficiente, mediante la instalación de **parches de seguridad**. Verificar que el departamento de seguridad es partícipe de estas actualizaciones y mantiene una política de gestión de los mismos (prioridad de instalación de los parches para solucionar vulnerabilidades, periodicidad de revisión, etc).

- En el caso de la plataforma zSeries e iSeries comprobar:

  a) Que tanto el sistema operativo, como el sistema CICS y las bases de datos DB2 están contempladas en el proceso.

  b) Que las versiones están soportadas en los diferentes programas de gestión del ciclo de vida del fabricante y que el número de licencias instaladas se adecua a los contratos de software.

  c) El porcentaje de parches denominados PTFs (Program Temporary Fixes) o RSU (Recommended Service Updates) no aplicados y su justificación.

d) Si para la gestión del parcheado se utilizan entornos diferenciados y herramientas de IBM o de terceros que permitan conocer el estado de actualización como por ejemplo:

- System Modification Program/Extended – SMP/E para zSeries.
- IBM Systems Director Update Manager para iSeries.

- Verificar que existen **mecanismos que regulan y limitan el acceso de los usuarios** a los sistemas:

  a) Los accesos a los datos se efectúan siempre mediante la utilización de un usuario y una contraseña que identifica de forma inequívoca a la persona que está accediendo

  b) Longitud mínima y composición de la clave acorde a las definidas en las políticas de seguridad de la unidad

  c) Vigencia adecuada de la contraseña

  d) Controles para no repetir las últimas contraseñas de un usuario

  e) Número de intentos de acceso fallido permitidos y mecanismos para el bloqueo y desbloqueo de usuarios

  f) Las contraseñas se almacenan cifradas, comprobando bajo qué sistema y con qué cifrado se encuentran, verificando que no se muestran en claro en las pantallas, listados, mensajes de comunicaciones, etc. (ref. ISO/IEC 27001:2013)

- Inventariar y analizar los **usuarios con privilegios especiales** (técnicos/administradores) en los sistemas iSeries en el alcance de la revisión. (ref. ISO/IEC 27001:2013)

- Determinar si los accesos de administración a los servidores se realiza mediante el uso de **protocolos seguros** (evitando servicios como FTP, telnet, snmp v2, HTTP) y a través de interfaces o redes dedicadas a la administración y segregadas de las redes de servicio (trafico tradicional de las aplicaciones). (ref. ISO/IEC 27001:2013)

- Comprobar la implementación de medidas de seguridad y control y gestión de **claves criptográficas** utilizadas por los sistemas iSeries para el funcionamiento de sus procesos (p. ej para la generación de los PINs de sistemas de tarjeta, certificados de servidor, etc, utilizando los módulos HSM – Hardware Security Modules y sistemas de PKI). (ref. ISO/IEC 27001:2013)

- Comprobar que los sistemas en el alcance de la revisión generan trazas de seguridad suficientes (logs), así como alarmas e informes de eventos de seguridad que son revisados por Seguridad Informática. (ref. ISO/IEC 27001:2013)

- Comprobar que estos logs son almacenados y custodiados de manera segura (ya sea localmente o en repositorios externos como un SIEM/SIM o un servidor Syslog) analizando que el personal de Seguridad no tiene acceso a su modificación y/o eliminación. (ref. ISO/IEC 27001:2013)

- Evaluar si se efectúan **pruebas de seguridad de forma periódica** sobre los sistemas iSeries, que permitan detectar vulnerabilidades ocasionadas por: una deficiente configuración, existencia de usuarios sin la adecuada protección, sistemas desactualizados, etc.

- Comprobar que estas revisiones:

  a) Se documentan formalmente

  b) Los resultados obtenidos se presentan al nivel adecuado, así como las acciones recomendadas para solventar las deficiencias obtenidas

  c) Permiten detectar deficiencias en el cumplimiento de las políticas y procedimientos de seguridad. (ref. ISO/IEC 27001:2013).

A continuación, explicamos alguna de las pruebas que puede hacer el auditor:

- **Prueba básica de caja blanca** para detectar los puertos abiertos potencialmente peligrosos y que deberían estar cerrados o tener una justificación para estar abiertos.

  Para realizar la prueba podemos partir de la **CMDB** (listado con todos los elementos que componen la infraestructura de red). Normalmente escogeremos aquellos elementos que sean más críticos (entorno de producción, estado activo, etc).

  La prueba consiste en ver qué servicios respondían a un ping. Según el puerto que tengan abierto podemos saber qué servicio tienen asociado, por ejemplo:

  - FTP de control (Puerto 21 TCP).
  - Telnet (Puerto 23 TCP).
  - HTTP (Puerto 80 TCP).

  Para realizar la prueba se puede ejecutar un script donde indiquemos aquellas IP's de entrada a analizar.

- **Prueba de control de usuarios administradores de iSeries** donde verificaremos que los usuarios correctos tienen los privilegios adecuados de administración de los equipos. Si se encuentran usuarios con permisos que no han de tener, se comunicará a la unidad el borrado o modificación de las cuentas.

3.2.2 Seguridad de Bases de Datos

Los objetivos de una auditoría de seguridad de Bases de Datos son los siguientes:

- Identificar y obtener las políticas y procedimientos relativos a la configuración de la seguridad de los **sistemas gestores de bases de datos** (DB2 – Host, DB2 – LUW, Oracle, Sybase, Microsoft SQL Server, PostgreSQL, MySQL). (ref. ISO/IEC 27001:2013)

- Comprobar que dichos procedimientos han sido construidos teniendo en cuenta los requerimientos de las políticas corporativas, locales, regulatorias que afecten a la entidad, y las mejores prácticas de la industria, ya sean del fabricante, o de organismos dedicados a la publicación de estándares de seguridad (NIST, FIPS, ANSI, IEEE, ISO, IEC, ISACA, etc).

- Contrastar si la configuración de los sistemas gestores de bases de datos es conocida y aprobada por Seguridad Informática y está alineada con los procedimientos o estándares mantenidos por el área.

- Analizar si la unidad utiliza alguna herramienta automática de compliance. (ref.

- Comprobar que los sistemas cuentan con un nivel de actualización suficiente, mediante la instalación de parches de seguridad. Verificar que el departamento de seguridad es partícipe de estas actualizaciones y mantiene una política de gestión de los mismos (prioridad de instalación de los parches para solucionar vulnerabilidades, periodicidad de revisión, etc).

- Comprobar:

    a) El nivel de parcheado del sistema gestor de bases de datos.

    b) Que las versiones están soportadas en los diferentes programas de gestión del ciclo de vida del fabricante y que el número de licencias instaladas se adecua a los contratos de software.

    c) Si para la gestión del parcheado se utilizan entornos de prueba diferenciados y herramientas automáticas de gestión de parches.

- Verificar que existen mecanismos que regulan y limitan el acceso de los usuarios a los sistemas gestores de bases de datos:

    a) Los accesos a los datos se efectúan siempre mediante la utilización de un usuario y una contraseña que identifica de forma inequívoca a la persona que está accediendo

    b) Longitud mínima y composición de la clave acorde a las definidas en las políticas de seguridad de la unidad y corporativas

    c) Vigencia adecuada de la contraseña

    d) Controles para no repetir las últimas contraseñas de un usuario

    e) Número de intentos de acceso fallido permitidos y mecanismos para el bloqueo y desbloqueo de usuarios

    f) Las contraseñas se almacenan cifradas, comprobando bajo qué sistema y con qué cifrado se encuentran, verificando que no se muestran en claro en las pantallas, listados, mensajes de comunicaciones, etc.

- Inventariar y analizar los usuarios con privilegios especiales (técnicos/administradores) en los sistemas gestores de bases de datos en el alcance de la revisión.

- Determinar si los accesos de administración a las bases de datos se realiza mediante el uso de protocolos seguros y a través de interfaces o redes dedicadas a la administración y segregadas de las redes de servicio (trafico tradicional de las aplicaciones).

- Comprobar que los sistemas gestores de bases de datos en el alcance de la revisión generan trazas de seguridad suficientes (logs), así como alarmas e informes de eventos de seguridad que son revisados por Seguridad Informática.

- Comprobar que estos logs son almacenados y custodiados de manera segura (ya sea localmente o en repositorios externos como un SIEM/SIM o un servidor Syslog) analizando que el personal de Seguridad no tiene acceso a su modificación y/o eliminación.

- Analizar si los sistemas gestores de bases de datos se encuentran bajo el perímetro de revisión de herramientas específicas de monitorización de la actividad (DAM) como Guardium de IBM o Imperva.

- Evaluar si se efectúan pruebas de seguridad de forma periódica sobre los sistemas gestores de bases de datos, que permitan detectar vulnerabilidades ocasionadas por: una deficiente configuración, existencia de usuarios sin la adecuada protección, sistemas desactualizados, etc.

- Comprobar que estas revisiones:

    a) Se documentan formalmente

    b) Los resultados obtenidos se presentan al nivel adecuado, así como las acciones recomendadas para solventar las deficiencias obtenidas

    c) Permiten detectar deficiencias en el cumplimiento de las políticas y procedimientos de seguridad.

Para verificar una correcta implementación de las bases de datos habría que analizar las configuraciones aplicadas sobre una muestra de bases de datos.

En la elección de una correcta muestra, deberemos seleccionar aquellas que prestan servicios críticos a la unidad.

Para cada base de datos, la información solicitada a la unidad es la siguiente:

- Fichero de configuración .ora
- Tablas:
    - DBA_USERS
    - DBA_PROFILES
    - DBA_TABLES
    - DBA_SYS_PRIVS
    - DBA_ROLE_PRIVS
    - DBA_TAB_PRIVS
    - DBA_COL_PRIVS

Con el análisis de la información solicitada deberemos poder identificar usuarios con permisos o accesos incorrectos, caducados, complejidad de contraseñas, etc.

En el caso de detectar alguna anomalía en la configuración de las bases de datos, se comunicará inmediatamente a la unidad auditada.

3.2.3 Seguridad en Redes y Comunicaciones

Los objetivos a revisar en una auditoría de seguridad en redes son los siguientes:

- Identificar y obtener las políticas y procedimientos relativos a la configuración de la seguridad de los **dispositivos de red** (Firewalls, IDS/IPS, enrutadores y switches y appliances de seguridad en red como proxies, email o VPN).

- Comprobar que dichos procedimientos han sido construido teniendo en cuenta los requerimientos de las políticas corporativas, regulatorias que afecten a la entidad, y las mejores prácticas de la industria, ya sean del fabricante, o de organismos dedicados a la publicación de estándares de seguridad (NIST, FIPS, ANSI, IEEE, ISO, IEC, ISACA, etc)

- Obtener el mapa de red del ámbito de análisis, además del mapa de red global, para verificar la existencia de mecanismos de seguridad:

    a) Dispositivos para el filtrado de las conexiones (firewalls).

    b) Dispositivos para la segmentación de la red (switches)

    c) Dispositivos de detección de intrusos y ataques.

    d) Sistemas de análisis de correo, antivirus, proxies, Network Access Control Appliances y Data Loss Prevention agents.

    e) Dispositivos de conexión como VPN

- Contrastar si la configuración de los dispositivos de red es conocida y aprobada por Seguridad Informática y está alineada con los procedimientos o estándares mantenidos por el área.

- Verificar que el departamento de seguridad gestiona los dispositivos de seguridad de la red, analizando que:

a) El procedimiento para el mantenimiento o creación de las reglas firewall e IDS/IPS incluye la intervención del departamento de seguridad.

b) Cualquier modificación sobre las reglas existentes es aprobada por esta área la cuál efectúa revisiones periódicas que aseguran que no se han producido modificaciones sin su consentimiento.

c) Los dispositivos que se conectan a la red son los autorizados y existe una segregación física/lógica entre las redes de administración de dispositivos y de servicio o aplicaciones.

- Comprobar que los dispositivos cuentan con un nivel de actualización suficiente, mediante la instalación de parches de seguridad. Verificar que el departamento de seguridad es partícipe de estas actualizaciones y mantiene una política de gestión de los mismos (prioridad de instalación de los parches para solucionar vulnerabilidades, periodicidad de revisión, etc).

- Comprobar para una muestra de dispositivos de red:

  a) Las versiones del software o firmware instalado.

  b) El nivel de parcheado si existe de cada dispositivo

  c) Que las versiones están soportadas en los diferentes programas de gestión del ciclo de vida del fabricante y que el número de licencias instaladas se adecua a los contratos de software.

  d) Si para la gestión del parcheado se utilizan entornos de prueba diferenciados y herramientas automáticas de gestión de parches.

- Verificar que existen mecanismos que regulan y limitan el acceso de los usuarios a los dispositivos de red:

  a) Los dispositivos delegan las funciones de AAA (Authentication, Authorization and Accounting) en servicios centralizados como por ejemplo RADIUS O TACACS+.

  b) Los accesos a los datos se efectúan siempre mediante la utilización de un usuario y una contraseña que identifica de forma inequívoca al técnico o usuario administrador que está accediendo.

  c) Longitud mínima y composición de la clave acorde a las definidas en las políticas de seguridad de la unidad y corporativas

  d) Vigencia adecuada de la contraseña

  e) Controles para no repetir las últimas contraseñas de un usuario

  f) Número de intentos de acceso fallido permitidos y mecanismos para el bloqueo y desbloqueo de usuarios

  g) Las contraseñas se almacenan cifradas, comprobando bajo qué sistema y con qué cifrado se encuentran, verificando que no se muestran en claro en las pantallas, listados, mensajes de comunicaciones, etc. (tanto en los servicios centralizados como en los usuarios administrativos locales de contingencia).

- Inventariar y analizar los usuarios con privilegios especiales (técnicos/administradores) en los dispositivos de red y en los servicios de AAA.

- Determinar si los accesos de administración a los dispositivos de red se realiza mediante el uso de protocolos seguros (evitando servicios como FTP, telnet, snmp v2, HTTP) y a través de interfaces o redes dedicadas a la administración y segregadas de las redes de servicio (trafico tradicional de las aplicaciones).

- Analizar los tipos de redes inalámbricas existentes. Asegurar la existencia de redes diferenciadas para empleados e invitados, así como los mecanismos de seguridad implementados para controlar el acceso a los medios (WPA2, 802.1x, portal cautivo, etc).

- Identificar y analizar los mecanismos de acceso desde redes externas existentes a la red de la entidad. Inventariar los accesos mediante **VPN**, servidores Web o conexiones dedicadas, comprobando que los mecanismos de acceso son seguros, los usuarios con acceso conocido y las trazas de seguridad activadas.

- Determinar si existen procedimientos y herramientas para detectar software no autorizado en la red.

- Comprobar la implementación de medidas de seguridad y control y gestión de claves criptográficas utilizadas por los dispositivos de red para el funcionamiento de sus procesos (p. ej para la generación de los PINs de sistemas de tarjeta, certificados de servidor, etc, utilizando los módulos HSM – Hardware Security Modules y sistemas de **PKI**).

- Comprobar que los sistemas en el alcance de la revisión generan trazas de seguridad suficientes (logs), así como alarmas e informes de eventos de seguridad que son revisados por Seguridad Informática. Tener en cuenta que estos logs pueden ser gestionados por la herramienta de AAA.

- Comprobar que estos logs son almacenados y custodiados de manera segura (ya sea localmente o en repositorios externos como un SIEM/SIM o un servidor Syslog) analizando que el personal de Seguridad no tiene acceso a su modificación y/o eliminación.

- Evaluar si se efectúan pruebas de seguridad de forma periódica sobre los dispositivos de red, que permitan detectar vulnerabilidades ocasionadas por: una deficiente configuración, existencia de usuarios sin la adecuada protección, sistemas desactualizados, etc.

- Comprobar que estas revisiones:

  a) Se documentan formalmente.

  b) Los resultados obtenidos se presentan al nivel adecuado, así como las acciones recomendadas para solventar las deficiencias obtenidas

  c) Permiten detectar deficiencias en el cumplimiento de las políticas y procedimientos de seguridad.

- Contrastar que el departamento de seguridad contempla dentro del alcance de las pruebas de intrusión (pruebas de **hacking ético**), los dispositivos de red más expuestos. Si estos sistemas han sido incluidos en las pruebas a realizar ya sea por una empresa externa o por el departamento de seguridad, comprobar:

  a) Planificación de pruebas con el alcance (servicios e IP), descripción, hitos y entregables

  b) Tipo de pruebas que se realizan: de caja negra (pre/post autenticación) y caja blanca.

  c) Cláusulas de confidencialidad sobre los informes generados.

  d) Plan de acción para las vulnerabilidades encontradas; verificar que se atienden las vulnerabilidades según su criticidad, facilidad de explotación, impacto en el cliente, etc.

  e) Actividades realizadas por el departamento de seguridad para asegurar una adecuada cobertura de los sistemas de su unidad:

  - Inventario de servicios críticos.

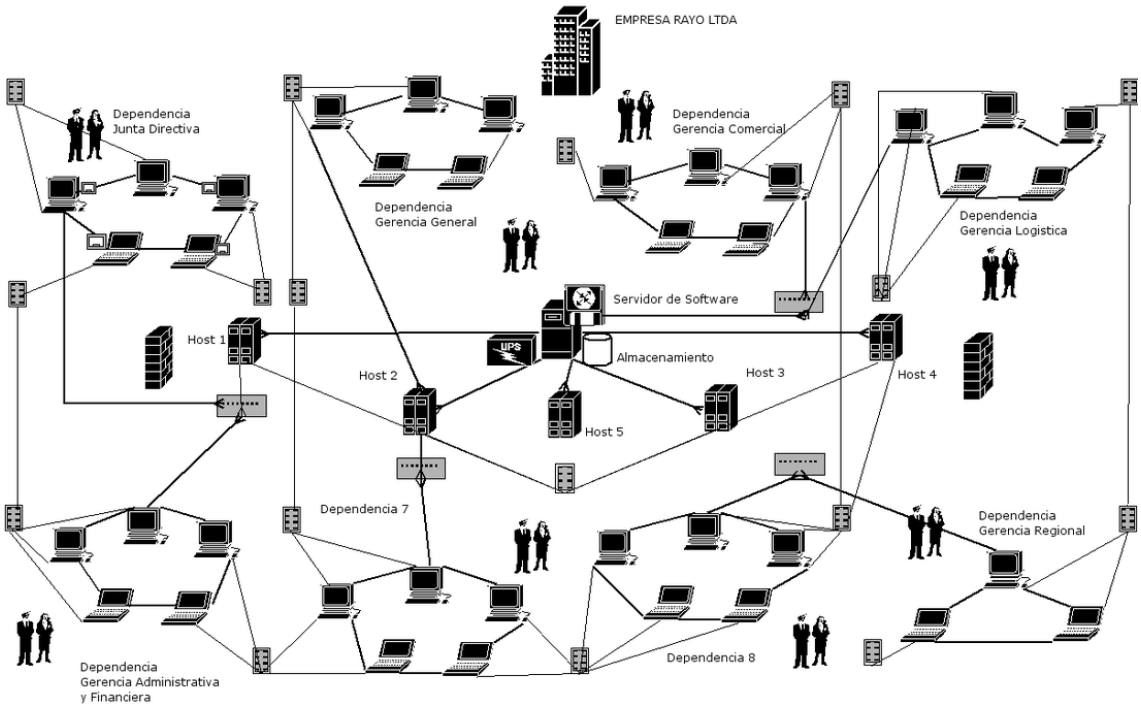
  - Fecha de última revisión de cada servicio y resultado.

  - Planes para asegurar que todos los servicios se revisan periódicamente.

Tras desarrollar los objetivos de revisión en redes, vamos a detallar algunos de los documentos a recibir o pruebas a realizar más importantes:

3.2.3.1 Mapas de Red

La unidad debe remitir a Auditoría el mapa de red global de su infraestructura. A continuación, podemos observar un ejemplo del contenido de un mapa de red en una empresa:



Los mapas han de contar con dispositivos de seguridad de red tales como **firewalls**, **IDS**, **proxys**, etc. permitiendo en todo momento que las conexiones con el exterior se realicen de forma segura.

3.2.3.2 Gestión de Dispositivos de Red

Se debe comprobar que se realizan revisiones periódicas de las reglas de firewall para ver si hay reglas que se pueden eliminar, mantenerse o crear algunas nuevas.

Uno de los riesgos que aplica al trabajo de ciberseguridad es el acceso de los empleados de los proveedores externos a la red interna del banco. Para controlarlo, se ha de realizar revisión sobre el acceso de los usuarios externos.

Por su parte, se ha de realizar la petición del inventario de usuarios con privilegios en los dispositivos de red y se ha de comprobar que se realiza una revisión periódica de los mismos.

3.2.3.3 Hacking Ético

Se ha de verificar si se realizan por parte de la unidad pruebas periódicas de intrusión en los sistemas. Entre las pruebas más importantes, destacamos tres categorías:

- **Pruebas de caja negra**: consisten en el lanzamiento de intentos de intrusión para la detección de vulnerabilidades sin conocimiento previo de los detalles de la infraestructura tecnológica. Este tipo de pruebas se lanzan típicamente desde Internet.

- **Pruebas de Post Autenticación**: son una variante de las anteriores, pero previamente el cliente ha facilitado unas credenciales de acceso y autorizado al auditor para iniciar sesión y realizar pruebas pertinentes una vez autenticado.

- **Pruebas de caja blanca**: consisten en el lanzamiento de intentos de intrusión para la detección de vulnerabilidades con conocimiento precio de los detalles de la infraestructura tecnológica auditada, bien desde la red interna o porque se facilitan ficheros de configuración, tablas de rutas o reglas de firewall, documentación sobre la arquitectura, cuentas de usuario de pruebas o cualquier otro dato del que no dispondría, a priori, un usuario malicioso.

3.2.4 Seguridad en Plataforma de Usuarios

Los objetivos a revisar en una auditoría de plataforma de usuarios son los siguientes:

- Identificar y obtener las políticas y procedimientos relativos a la configuración de la seguridad de los dispositivos de plataforma de usuario, como por ejemplo workstations, notebooks, tablets o teléfonos inteligentes. (ref. ISO/IEC 27001:2013)

- Comprobar que dichos procedimientos han sido construidos teniendo en cuenta los requerimientos de las políticas corporativas, regulatorias que afecten a la entidad, y las mejores prácticas de la industria, ya sean del fabricante, o de organismos dedicados a la publicación de estándares de seguridad (NIST, FIPS, ANSI, IEEE, ISO, IEC, ISACA, etc) (ref. ISO/IEC 27001:2013)

- Verificar que las políticas relativas a los usuarios finales contemplan entre otros los siguientes aspectos:

  a) Verificación de los posibles antecedentes de los candidatos. (ref. ISO/IEC 27001:2013)

  b) Clausulas en materia de concienciación y aceptación de responsabilidades sobre la seguridad de la información en la organización. (ref. ISO/IEC 27001:2013)

  c) Exista un proceso disciplinario para aquellos casos en los que se determine la responsabilidad del empleado en la materialización de alguna brecha de seguridad informática. (ref. ISO/IEC 27001:2013)

  d) Procedimiento para la comunicación y revisión de las responsabilidades en materia de seguridad, cuando se extinga o modifique la relación contractual con el empleado, incluyendo cambios de funciones. (ref. ISO/IEC 27001:2013)

  e) Controles para mitigar los riesgos derivados de un mal uso de los sistemas, tales como dejar el equipo desatendido o información confidencial en el escritorio. (ref. ISO/IEC 27001:2013)

- Contrastar si la configuración de los dispositivos de plataforma de usuario es conocida y aprobada por Seguridad Informática y está alineada con los procedimientos o estándares mantenidos por el área.

  Analizar si la unidad utiliza alguna herramienta automática de compliance y de gestión de dispositivos móviles (MDM).

- Comprobar que los sistemas cuentan con un nivel de actualización suficiente, mediante la instalación de parches de seguridad. Verificar que el departamento de seguridad es partícipe de estas actualizaciones y mantiene una política de gestión de los mismos (prioridad de instalación de los parches para solucionar vulnerabilidades, periodicidad de revisión, etc).

  Comprobar:

  a) Que tanto el sistema operativo, como las principales aplicaciones que tenga instaladas el dispositivo (navegador, antivirus, etc) están contemplados en el proceso. (ref. ISO/IEC 27001:2013)

  b) Que las versiones están soportadas en los diferentes programas de gestión del ciclo de vida del fabricante y que el número de licencias instaladas se adecua a los contratos de software.

  c) El porcentaje de parches no aplicados y su justificación.

  d) Si para la gestión del parcheado se utilizan plataformas de prueba y herramientas automáticas de gestión de parches como por ejemplo System Center Configuration Manager o Windows Server Update Services para plataformas Windows.

- Verificar que existen mecanismos que regulan y limitan el acceso de los usuarios a los sistemas:

  a) Los accesos a los datos se efectúan siempre mediante la utilización de un usuario y una contraseña que identifica de forma inequívoca a la persona que está accediendo

  b) Longitud mínima y composición de la clave acorde a las definidas en las políticas de seguridad de la unidad y corporativas

  c) Vigencia adecuada de la contraseña

  d) Controles para no repetir las últimas contraseñas de un usuario

  e) Número de intentos de acceso fallido permitidos y mecanismos para el bloqueo y desbloqueo de usuarios

  f) Las contraseñas se almacenan cifradas, comprobando bajo qué sistema y con qué cifrado se encuentran, verificando que no se muestran en claro en las pantallas, listados, mensajes de comunicaciones, etc. (ref. ISO/IEC 27001:2013)

- Verificar para aquellas situaciones en las que se permita el acceso a los datos de la unidad con dispositivos móviles, o externos propiedad de los empleados (Bring Your Own Device - BYOD), que se contempla la existencia de:

  a) Un acuerdo de confidencialidad y uso de dispositivos firmado entre el empleado y la organización, incluyendo una política de uso razonable de los dispositivos y la información almacenada en ellos y un procedimiento de retorno una vez finalizada la relación entre el empleado y la sociedad. (ref. ISO/IEC 27001:2013)

  b) Una política de seguridad específica. (ref. ISO/IEC 27001:2013)

c) Herramientas para la gestión remota de la seguridad y aplicación de políticas y configuraciones en los dispositivos (Mobile Device Management – MDM). Estas herramientas han de permitir al menos:

- Protección de datos sensibles y de propiedad intelectual (p. ej, mediante la aplicación de una política específica de contraseñas o de bloqueo del dispositivo, cifrado de datos, política de bloqueo y borrado remoto del dispositivo en caso de pérdida). Esto será de aplicabilidad, con las limitaciones pertinentes, también en el caso de medios extraíbles (discos, USB, etc). (ref. ISO/IEC 27001:2013)

- Registro del dispositivo y protección de las redes corporativas a las que se conectan. (p. ej, mediante la existencia de listas de dispositivos permitidos y denegados a tener acceso a la red).

- Backup de los dispositivos.

- Borrado de los datos de la organización una vez terminada la relación entre el empleado y la misma.

- Protección contra malware, e instalación de aplicaciones no permitidas (jail breaking o rooting.

- Inventariar y analizar los usuarios con privilegios especiales en las aplicaciones **MDM**.

- Confirmar que los sistemas se encuentran protegidos por **software antivirus actualizado** y asegurar que éste no puede ser desactivado por el usuario.

- Analizar la existencia de software no autorizado en los sistemas, ya sea instalado por los propios usuarios por disponer de un exceso de privilegios, o por ser instalado por los usuarios técnicos sin contar con las licencias adecuadas.

- Verificar si los accesos de administración por parte de los técnicos a los dispositivos en caso de asistencia remota (remote hands) se realiza utilizando protocolos seguros.

- Comprobar que los sistemas en el alcance de la revisión generan trazas de seguridad suficientes (logs), así como alarmas e informes de eventos de seguridad que son revisados por Seguridad Informática. Tener en cuenta que el volumen de dispositivos puede hacer inviable su revisión o almacenamiento en dispositivos externos.

- Comprobar que estos logs son almacenados y custodiados de manera segura (ya sea localmente o en repositorios externos como un SIEM/SIM o un servidor Syslog) analizando que el personal de Seguridad no tiene acceso a su modificación y/o eliminación.

- Evaluar si se efectúan pruebas de seguridad de forma periódica sobre los dispositivos, que permitan detectar vulnerabilidades ocasionadas por: una deficiente configuración, existencia de usuarios sin la adecuada protección, sistemas desactualizados, etc.

  Comprobar que estas revisiones:

  a) Se documentan formalmente

  b) Los resultados obtenidos se presentan al nivel adecuado, así como las acciones recomendadas para solventar las deficiencias obtenidas

  c) Permiten detectar deficiencias en el cumplimiento de las políticas y procedimientos de seguridad.

Vamos a analizar alguna de las pruebas más importantes a realizar:

3.2.4.1 Antivirus y Software no autorizado

Auditoría ha de comprobar si se dispone de alguna solución corporativa de antivirus que pueda ser, a su vez, configurado para realizar el bloqueo y borrado automático de software potencialmente peligroso o dañino (Ej: herramientas de hacking)

Por su parte, Auditoría ha de analizar cómo se realiza la gestión para la instalación y actualización del antivirus en los servidores y ordenadores personales de los usuarios.

En la revisión del antivirus, se debe verificar si se cuenta a parte con mecanismos y herramientas específicas de protección antimalware y/o amenazas avanzadas (APTs). En ocasiones el mismo antivirus da cobertura a esta parte.

Una prueba interesante a realizar por el auditor puede ser constatar si para el total o para una muestra de servidores críticos (pueden ser descargados de la CMDB) se dispone de antivirus instalado.

Adicionalmente, para aquellos equipos que tienen instalado antivirus, se debe comprobar que se realizan revisiones periódicas con el fin de comprobar si hay firmas desactualizadas. Como resultado del análisis, podemos generar un documento desglosando las siguientes tipologías:

- % Servidores sin antivirus sobre el total
- % PC’s sin antivirus sobre el total.
- % Servidores con firmas anti-virus desactualizadas

3.2.4.2 Dispositivos Móviles

Se debe verificar si se dispone de procedimientos específicos de seguridad para dispositivos móviles. El objetivo de estos procedimientos es definir las reglas de entrega de los medios móviles entre los empleados de la Unidad auditada y cómo deben ser las conexiones de acceso a los sistemas de información cuando se conectan remotamente.

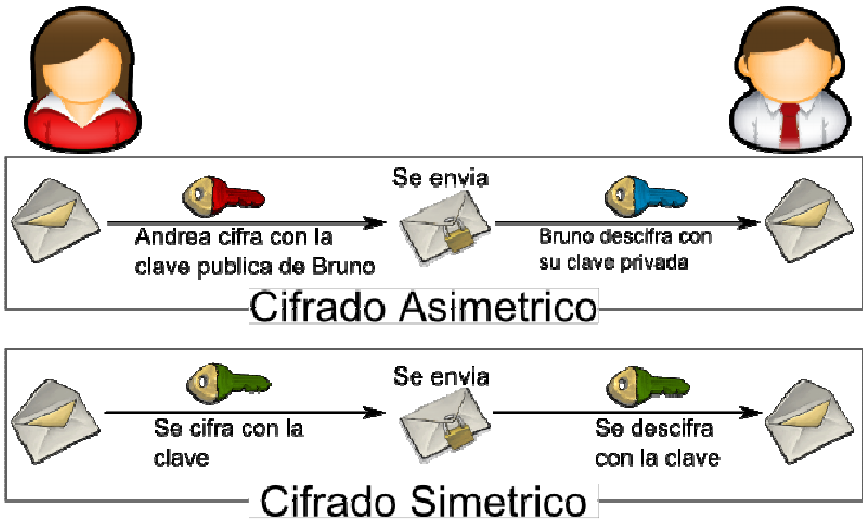
Es importante comprobar la existencia de alguna herramienta para la gestión centralizada de la seguridad en los dispositivos móviles.

Mediante esta herramienta se pretende establecer una guía de **bastionado** y configuración que cumplan los estándares de seguridad y se pueda desplegar en todos los dispositivos de una manera centralizada.

La unidad ha de tener un listado de SW autorizado para todas las plataformas de software que se utilicen.

3.2.4.3 Cifrado de la Información

Todos los datos intercambiados por la unidad han de llevar consigo un correcto cifrado. Por ello, se debe comprobar que se dispone de mecanismos o medidas de cifrado de información para los dispositivos portátiles, ya sea un PC o un dispositivo de almacenamiento USB por ejemplo.



3.2.4.4 Actualización de software

Se ha de comprobar que el nivel de actualización del software en los ordenadores de los usuarios es adecuado. Además, se deben recibir evidencias sobre la realización periódica de distribuciones automáticas de los parches de seguridad y actualizaciones críticas del sistema Microsoft Windows para su instalación en dichos equipos.

Para observar la obsolescencia del sistema operativo, el auditor puede realizar una prueba partiendo de los servidores esenciales del sistema, verificando, uno a uno, si el sistema operativo que tienen instalado tiene, a fecha de auditoría, algún soporte del fabricante o llevan instalada la versión más actualizada.

3.2.5 Seguridad en el Directorio Activo

El Directorio activo es un servicio establecido en uno o varios servidores donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.

Los objetivos a revisar en una auditoría de seguridad en el directorio activo son los siguientes:

- Identificar y obtener las políticas y procedimientos relativos a la configuración de la seguridad de los servicios de directorio tales como Microsoft Active Directory u otros compatibles con LDAP.

- Comprobar que dichos procedimientos han sido construidos teniendo en cuenta los requerimientos de las políticas corporativas, regulatorias que afecten a la entidad, y las mejores prácticas de la industria, ya sean del fabricante, o de organismos dedicados a la publicación de estándares de seguridad (NIST, FIPS, ANSI, IEEE, ISO, IEC, ISACA, etc)

- Contrastar si la configuración de los servicios de directorio es conocida y aprobada por Seguridad Informática y está alineada con los procedimientos o estándares mantenidos por el área.

a) Describir la estructura lógica del servicio de directorio, objetos, bosques, árboles y dominios.

b) Determinar si se contempla una segregación entre los administradores de servicio (responsable del diseño del servicio de directorio y de la administración del mismo a alto nivel) de los administradores de datos (responsables de las credenciales de usuario y derechos de acceso)

- Verificar que existen mecanismos que regulan y limitan el acceso de los usuarios a los sistemas.

Para ello obtener la configuración del servicio de directorio y comprobar que:

a) Los accesos a los datos se efectúan siempre mediante la utilización de un usuario y una contraseña que identifica de forma inequívoca a la persona que está accediendo

b) Longitud mínima y composición de la clave acorde a las definidas en las políticas de seguridad de la unidad y corporativas

c) Vigencia adecuada de la contraseña

d) Controles para no repetir las últimas contraseñas de un usuario

e) Número de intentos de acceso fallido permitidos y mecanismos para el bloqueo y desbloqueo de usuarios

- Duración del bloqueo de cuenta: 0 (requiere administrador para volver a habilitar la cuenta después del bloqueo)

- Umbral de bloqueos de la cuenta: tres de cinco (número de intentos antes de que la cuenta está bloqueada y no se requiere la intervención del administrador)

- Restablecer la cuenta por bloqueos: establecer este número en cuestión de minutos, considera que la cuenta se vuelve a activar después del número de minutos que se introduzca aquí.

f) Las contraseñas se almacenan cifradas, comprobando bajo qué sistema y con qué cifrado se encuentran, verificando que no se muestran en claro en las pantallas, listados, mensajes de comunicaciones, etc.

- Inventariar y analizar los usuarios con privilegios especiales (técnicos/administradores) en los servicios de directorio en el alcance de la revisión.

- Determinar si los accesos de administración a los servicios de directorio se realiza mediante el uso de protocolos seguros (evitando servicios como FTP, telnet, snmp v2, HTTP) y a través de interfaces o redes dedicadas a la administración y segregadas de las redes de servicio (trafico tradicional de las aplicaciones).

- Comprobar que las directivas de auditoría en los servicios de directorio en el alcance de la revisión generan trazas de seguridad suficientes (logs), así como alarmas e informes de eventos de seguridad que son revisados por Seguridad Informática.

- Comprobar que estos logs son almacenados y custodiados de manera segura (ya sea localmente o en repositorios externos como un SIEM/SIM o un servidor Syslog) analizando que el personal de Seguridad no tiene acceso a su modificación y/o eliminación.

Vamos a analizar alguna de las pruebas más importantes a realizar:

3.2.5.1 Políticas de dominio

La unidad nos ha de proporcionar los valores de los atributos de los directorios activos y de los controladores de dominio. Tras recibir estos atributos, hemos de verificar que están acorde con unas políticas de gestión de seguridad adecuadas, en concreto con la parte donde se describen las políticas de contraseñas y de bloqueo de cuentas para todo el directorio activo y la política de Auditoría para los controladores de dominio.

A continuación, se muestran algunos de los atributos que pueden venir definidos en las políticas de dominio y que el auditor debería comprobar si se cumplen:

Políticas de dominio
Historial de contraseñas: 10
Tiempo de vida máximo de contraseña: 45 días para los usuarios personales.
Tiempo de vida mínimo de contraseña: 1 día (en DAs será aceptable configurar este parámetro a 0).
Longitud mínima: 8 caracteres
Almacenar contraseñas utilizando un algoritmo de cifrado reversible: deshabilitado.
Habilitar complejidad de contraseñas en servidores que lo soporten
Duración del bloqueo: 0 minutos
Umbral de contraseñas fallidas: 5 intentos
Reinicio del contador de contraseñas: 1440 minutos
Renombrar usuario Administrador o Administrator

3.2.5.2 Control de Acceso

Además de comprobar la seguridad en los distintos directorios activos de la unidad, se ha de analizar el acceso a las distintas aplicaciones.

Para ello, se deberá hacer una prueba verificando que se cumplen los distintos requisitos de acceso definidos en las políticas. Estos requisitos pueden ser la longitud o complejidad de la contraseña, caducidad, intentos fallidos, almacenamiento de histórico de contraseñas, revocación por inactividad, etc.

4. SEGUIMIENTO DE RECOMENDACIONES

4.1 Introducción al Seguimiento de Recomendaciones

Las auditorías no finalizan con la emisión del informe. En éste, el auditor plasma una serie de recomendaciones para **corregir la problemática detectada.**

Es por ello que hay que realizar un seguimiento de las recomendaciones que fueron emitidas en la anterior auditoría, si es que hubo una.

Gracias al seguimiento de las recomendaciones se genera valor a las actuaciones realizadas por auditoría, ya que se **multiplica el impacto** que las recomendaciones tienen en la unidad auditada y favorece su difusión.

Para realizar un adecuado seguimiento de recomendaciones, el auditor recopilará datos y evidencias para posteriormente analizar la información y evaluar los resultados. Además, se aplicarán procedimientos de auditoría para sustentar las conclusiones finales sobre la implantación o no de las recomendaciones.

4.2 Objetivos del Seguimiento de Recomendaciones

- Verificar el grado de cumplimiento de las recomendaciones o de aceptación del riesgo de no implantarlas.
- Evaluación del impacto obtenido tras implantación de las recomendaciones observando posibles mejoras producidas o deficiencias.
- Favorecer el control interno en la unidad auditada.
- Mejorar la eficacia de las auditorías.

4.3 Implantación de las recomendaciones

El auditor ha de hacer seguimiento, pidiendo a la unidad la información que crea que pueda serle útil para posteriormente analizarla.

Se investigará y se realizarán pruebas de datos para convertir los datos obtenidos en evidencias, ya sean para su implantación a para su no implantación.

Para realizar el seguimiento debe ser de utilidad tener una plantilla o documento donde seamos capaces de reflejar la siguiente información:

- **Número identificador** de la recomendación.
- **Descripción con texto explícito de la recomendación** que se emitió en el Informe de la auditoría anterior. En algunos casos, una sola recomendación puede llevar consigo varias incidencias que solventar. Cuando esto se da, se pueden considerar las recomendaciones como parcialmente implantadas siempre y cuando se hayan resuelto parte de los puntos a los que hace referencia la recomendación.
- **Evidencias enviadas por la unidad** al equipo de auditoría hasta el momento sobre la recomendación.
- **Responsable:** persona encargada del área en el cual se ha emitido la recomendación.
- **Situación actual**: No implantada dentro de plazo, No implantada fuera de plazo, implantada o parcialmente implantada.
- **Fecha de recomendación**: fecha en la que se emitió la recomendación y, por lo tanto, la unidad auditada firmó.
- **Fecha de implantación**: fechas límite en la que la recomendación ha de haberse implantado y, por lo tanto, que las incidencias y debilidades, hayan sido resueltas.

A continuación, un ejemplo de cómo podría ser esta plantilla:

Id Reco	Texto Recomendación	Evidencias obtenidas	Jefe área	Situación actual	Fecha Reco	Fecha Implant. Reco
1	Acceso de los usuarios incorrecto debido a no estar alineado con las políticas de acceso.			Implantada		
2	Servidores con sistema operativo obsoleto y sin soporte actual.			No Implantada		
3	* No se realiza cifrado en transferencia de datos de los dispositivos móviles * Dispositivos móviles sin antivirus instalado			Parcialmente Implantada		

Por último, se sacarían porcentajes para determinar el **grado de cumplimiento** de implantación de las recomendaciones que se emitieron en la anterior auditoría.

Las recomendaciones que no se den por implantadas y cuya fecha límite haya sido rebasada, serán motivo de reformulación en la presente auditoría.

5. INTERFAZ PARA GENERACIÓN DE INFORMES

5.1 Introducción

La última parte a realizar en toda auditoría de ciberseguridad, es la **emisión del informe final de auditoría** por parte de responsable asignado. Evidentemente, recibirá el apoyo del resto del equipo de auditores para contar con la mayor cantidad de datos posibles.

El mínimo contenido que debería incluirse en el informe de una auditoría de ciberseguridad debería ser el siguiente:

1) Objetivo de la auditoría
2) Alcance de la auditoría (incluyendo procesos, departamentos, delegaciones, etc)
3) Criterios de auditoría: Normas y Sistema de gestión ante los que comparamos los hallazgos de auditoría.
4) Equipo auditor, con nombres, apellidos y figura que ocupa en el equipo.
5) Fechas y lugares en las que se realizó la auditoría
6) Hallazgos y evidencias de la auditoría: Es muy **recomendable** que la **exposición** de los hallazgos y evidencias se hagan siguiendo el **orden del Sistema de Gestión y / o de las normas de aplicación**, de forma que permita una fácil identificación de los requisitos cumplidos / incumplidos.
7) Conclusiones sobre el Sistema auditado
8) Declaración del grado de cumplimiento del sistema auditado sobre los criterios de auditoría

En este sentido, he incluido en mi Trabajo de Fin de Grado una interfaz que nos sirva como referencia a la hora de generar el informe final.

Según el grado de completitud del auditor en los distintos campos de la aplicación, se podrá generar desde un informe que nos sirva como soporte y ayuda en la auditoría hasta un informe completo que cubra los apartados esenciales que debe contener un Informe de Auditoría.

5.2 Antecedentes

No se han encontrado otras aplicaciones que estén destinadas a este propósito. No obstante, esta interfaz está enfocada como una herramienta interna para plantilla de la propia empresa auditada (auditores internos) o para que cualquier auditor, interno o no, pueda identificar de una manera fácil, los elementos indispensables que revisar en una auditoría de ciberseguridad.

Existen aplicaciones parecidas pero en otros ámbitos, como por ejemplo las utilizadas por los centros de ITV, donde el propietario del vehículo revisado obtiene un documento final con un resumen de los parámetros analizados y con sus respectivas incidencias en caso de encontrarlas, emitiendo un resultado (rating) que puede ser favorable o desfavorable.

Dirección General de Industria, Energía y Minas
CONSEJERÍA DE ECONOMÍA Y HACIENDA
Comunidad de Madrid

itv

INFORME DE INSPECCIÓN TÉCNICA

Clasificación	Tipo	Marca/Modelo	Nº bastidor	Fecha 1ª matrícula	Matrícula
1000	B5	AUDI A4 1.8 5V	[redacted]	07/05/1998	[redacted]

Tipo de inspección	Kilómetros	Contraseña de homologación	Fecha inspección	Informe Nº
PERIODICA	203.927	E1*93/81*0013	26/05/2014	[redacted]

Elementos inspeccionados

Informe correspondiente a la factura nº: 2865/ 12.270

01 IDENTIFICACIÓN	A 03.02 CINT.SEG.Y ANCLAJES		A 06.15 TUBOS RIGIDOS	A 09.03 SISTEMA DE ESCAPE
A 01.01 DOCUMENTACION			A 06.16 TUBOS FLEXIBLES	A 09.04 TRANSMISION
A 01.02 NUMERO DE BASTIDOR	A 03.04 ANTIHIELO Y ANTIVAHO		A 06.17 FORROS	
A 01.03 PLACAS DE MATRICULA	A 03.05 ANTIRROBO Y ALARMA	**05 EMIS. CONTAMINANTES**	A 06.18 TAMBORES Y DISCOS	**10 OTROS**
A 01.04 SEGURO OBLIGATORIO	A 03.06 CAMPO VISION	A 05.01 RUIDO	A 06.19 CABLES,VARILLAS,PAL.	
02 ACONDIC. EXTERIOR, CARROCERÍA Y CHASIS		A 05.02 VEH.MOTOR ENC.	A 06.20 CILINDR.DIST.FRENADO	
	A 03.08 INDICADOR			
	A 03.09 SALIENTES INTERIORES	**06 FRENOS**	A 06.22 AJUST.TENSION AUTOM.	
A 02.02 CARROCERIA Y CHASIS		A 06.01 FRENO DE SERVICIO	**07 DIRECCIÓN**	
	04 ALUMBR.Y SEÑALIZACIÓN		A 07.01 DESVIACION DE RUEDAS	A 10.06 REFORMAS NO
A 02.04 GUARDAB.Y DISP.ANTIP	A 04.01 LUCES CRUCE Y	A 06.03 FRENO	A 07.02 VOLANTE, COL.DIREGC.	
A 02.05 LIMPIA Y LAVAPARABR.	A 04.02 LUZ DE MARCHA		A 07.03 CAJA DE DIRECCION	
	A 04.03 LUCES IND.DIRECCION	A 06.05 DISP.ANTIBLOQUEO	A 07.04 TIMONERIA Y ROTULAS	
A 02.07 PROTECCION TRASERA	A 04.04 SEÑAL DE EMERGENCIA		A 07.05 SERVODIRECCION	
A 02.08 PUERTAS Y PELDAÑOS	A 04.05 LUCES DE FRENADO	A 06.07 PEDAL DISP.FRENADO	**08 EJES,RUEDAS,NEUMÁT.**	
A 02.09 RETROVISORES	A 04.06 LUZ PLACA MAT.		A 08.01 EJES	
	A 04.07 LUCES DE POSICION		A 08.02 RUEDAS	
	A 04.08 LUCES ANTINIEBLA		A 08.03 NEUMATICOS	
A 02.12 VIDRIOS DE			A 08.04 SUSPENSION	
	A 04.10 CATADIOPTRICOS		**09 MOTOR Y TRANSMISIÓN**	
03 ACONDIC. INTERIOR			A 09.01 ESTAD.GENERAL MOTOR	
A 03.01 ASIENTOS Y ANCLAJES	A 04.12 AVISADOR ACUSTICO	A 06.14 SERVOFRENO CIL.IN.MA.	A 09.02 SISTEMA ALIMENTACION	

Mediciones efectuadas durante la inspección:

FRENADO (KN) Equipo nº 023	1ºeje izq/dcha	2ºeje izq/dcha	3ºeje izq/dcha	4ºeje izq/dcha
Freno Servicio	3,04 3,01	1,91 1,68	--- ---	--- ---
Freno Socorro	--- ---	--- ---	--- ---	--- ---
Freno Estacionamiento	--- ---	2,12 2,02	--- ---	--- ---
Ovalidad	12,6 13,8	18,9 19,0	--- ---	--- ---
DECELERÓMETRO (m/s²) Equipo nº	**BÁSCULA (kg)** Equipo nº	---		

EMISIONES Equipo nº 005	
Opacidad (m^{-1}) K	---
CO Ralentí (%)	0,00
CO Acelerado (%)	0,00
Factor λ	1,012
RUIDO dB(A) Equipo nº	---

ALINEACIÓN (m/Km) Equipo nº 013	
1º Eje	0,70
2º Eje	---
VEL.ACT.LIM. Equipo nº	---
DINAMÓMETRO (N) Equipo nº	--- ---

CÓDIGO	DESCRIPCIÓN DE DEFECTOS ENCONTRADOS DURANTE LA INSPECCIÓN	CALIFICACIÓN
02.02.01	Defectos de estado (oxidos, perforaciones, desperfectos, etc.)	LEVE
09.01.01	Perdidas de aceite sin goteo	LEVE
09.03.01	Defectos de estado del sistema de escape (TRAMO INTERMEDIO)	LEVE
09.04.02	Defectos de estado de los guardapolvos (EJE 1 IZQUIERDA/O)	LEVE

Los elementos indicados con A han sido inspeccionados en La línea 02 por el inspector 417
Los elementos indicados con B han sido inspeccionados en ..... por el inspector .....
Los elementos indicados con C han sido inspeccionados en ..... por el inspector .....

RESULTADO DE LA INSPECCIÓN: FAVORABLE CON DEF. LEVES
FECHA PRÓXIMA INSPECCIÓN: 26/05/2015

Observaciones

Vº Bº Estación

Firma y sello

Inspección regulada por el R.D.2042/94 de 14 de Octubre, el RD 711/2006 de 9 de Junio y el RD 224/2008 de 15 de Febrero

Página 1 de 1

5.3 Resultados

El resultado obtenido por la aplicación será un informe en PDF donde podremos observar las vulnerabilidades de los apartados revisados en una auditoría de ciberseguridad, así como aquellos que resultaron favorables tras la revisión de auditoría.

A pesar de que esta interfaz automatiza en cierto modo la generación del informe, una auditoría de ciberseguridad ha de tener siempre participación manual por parte del auditor. En este sentido, la aplicación ha sido diseñada para que el auditor pueda añadir la información que considere necesaria en cada uno de los puntos analizados, por lo que el informe PDF puede ser utilizado como un mero resumen de la auditoría y también como un documento final para ser emitido.

5.4 Características

En esta parte vamos a analizar las características y funcionalidades de la interfaz creada informando en todos los campos de la aplicación y generando el informe final.

La primera pantalla únicamente tiene la función de hacer de portada.

Generación de Informe de Auditoría

5.4.1 Introducción de datos de la auditoría

Como puede observarse, nos obliga a introducir por lo menos al auditor jefe y el nombre de la auditoría.

Generación de Informe de Auditoría

Nombre del auditor jefe (requerido):

Completa este campo

Nombre del auditor 2: Juan Sanchez Perez

Nombre del auditor 3: María Fernandez Garcia

Nombre de la auditoria (requerido):

Introduccion de la auditoria:

Objetivos Objetivos Objetivos Objetivos Objetivos

Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance
Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance

En esta primera pantalla, el auditor podrá escribir la introducción, objetivos o alcance de la auditoría.

Una vez rellenados los datos mínimos, pulsamos en el botón que indica “siguiente”:

Generación de Informe de Auditoría

Nombre del auditor jefe (requerido): Jaime Mejias Macias

Nombre del auditor 2: Juan Sanchez Perez

Nombre del auditor 3: María Fernandez Garcia

Nombre de la auditoria (requerido): Ciberseguridad de la UVA

Introduccion de la auditoria:

Objetivos Objetivos Objetivos Objetivos Objetivos

Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance
Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance Alcance

Borrar Siguiente

5.4.2 Acceso al formulario con apartados de auditoría de ciberseguridad

En este formulario, podemos observar todos los puntos que contiene nuestro manual para auditorías de ciberseguridad. En ellos podemos indicar los siguientes resultados:

- OK: El análisis de auditoría para el punto al que hace referencia ha resultado satisfactorio.
- KO: Se han encontrado incidencias en el análisis de auditoría para el punto al que hace referencia.
- No revisado: El punto al que hace referencia no ha sido revisado en esta auditoría.

Se ha establecido la lógica necesaria para la generación del informe en PDF en cada uno de los apartados. Según el resultado que indiquemos en el formulario la aplicación actuará de la siguiente manera:

- OK: El documento final contendrá un texto fijo que indique los aspectos revisados en ese punto por auditoría y que éstos han sido favorables.
- KO: El documento final contendrá un texto fijo que indique los aspectos revisados en ese punto por auditoría y que éstos han sido desfavorables.
- No revisado: El punto al que hace referencia no se incluirá en el informe.

Además, en cada uno de los apartados, el auditor dispondrá de un área de texto donde podrá incluir una descripción del trabajo realizado (pruebas de datos, evidencias obtenidas de la unidad, etc) y quedará reflejado en el documento final.

Generación de Informe de Auditoría

A.1.1 MODELO DE GOBIERNO - Área de Riesgos - Organigrama

OK

KO

No revisado

Comentarios Informe Organigrama

B.2.1 GESTION Y CONTROL - Seguridad Host iSeries

OK

KO

No revisado

Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas

B.2.2 GESTION Y CONTROL - Seguridad de BBDD

OK

KO

No revisado

Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas

B.2.5 GESTION Y CONTROL - Seguridad en Directorio Activo

OK

KO

No revisado

Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas

C Seguimiento de Recomendaciones

OK

KO

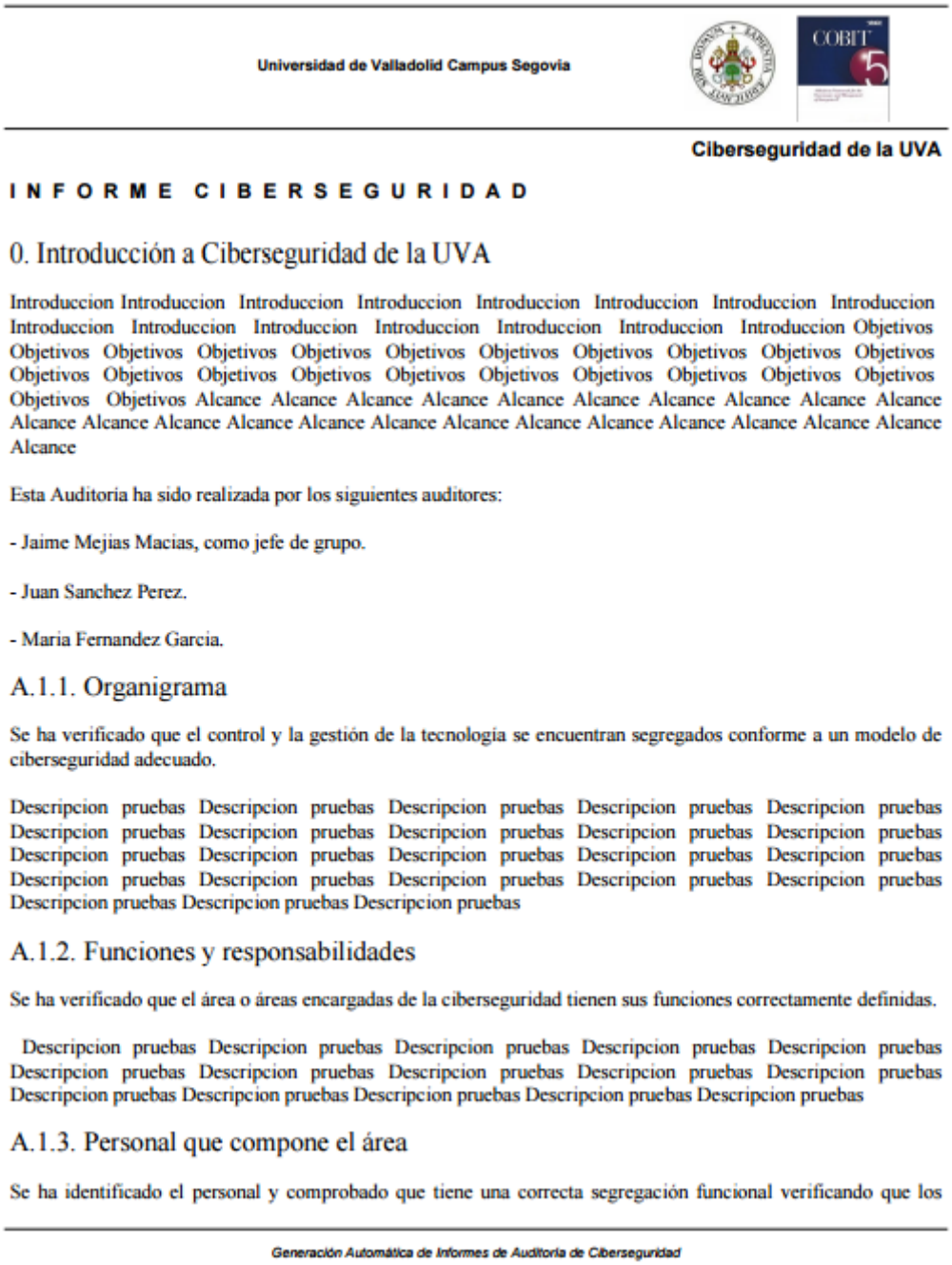
No revisado

Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas

Borrar Generar PDF

5.4.3 Informe en PDF

Como se puede ver a continuación, se crea un informe donde podremos imprimir en papel los resultados obtenidos en la auditoría. Este informe podrá ser más o menos detallado según el criterio del auditor y del fin con el que éste vaya a ser utilizado.



Universidad de Valladolid Campus Segovia

Ciberseguridad de la UVA

INFORME CIBERSEGURIDAD

0. Introducción a Ciberseguridad de la UVA

Introduccion Introduccion Introduccion Introduccion Introduccion Introduccion Introduccion Introduccion Introduccion Introduccion Introduccion Introduccion Introduccion Introduccion Introduccion Objetivos Alcance

Esta Auditoria ha sido realizada por los siguientes auditores:

- Jaime Mejias Macias, como jefe de grupo.

- Juan Sanchez Perez.

- Maria Fernandez Garcia.

A.1.1. Organigrama

Se ha verificado que el control y la gestión de la tecnología se encuentran segregados conforme a un modelo de ciberseguridad adecuado.

Descripcion pruebas Descripcion pruebas

A.1.2. Funciones y responsabilidades

Se ha verificado que el área o áreas encargadas de la ciberseguridad tienen sus funciones correctamente definidas.

Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas Descripcion pruebas

A.1.3. Personal que compone el área

Se ha identificado el personal y comprobado que tiene una correcta segregación funcional verificando que los

Generación Automática de Informes de Auditoría de Ciberseguridad

5.4.4 Código generado para el desarrollo

Para la creación de la interfaz de generación de informes ha sido necesario programar en los lenguajes de programación web PHP y HTML.

A continuación se explican los archivos PHP más importantes en el desarrollo de la interfaz y que se incluirán dentro del software de la entrega del proyecto:

- Formulario_ciber_1: código referente al formulario de introducción de datos de la auditoría, introducción y auditores.

```
<!DOCTYPE html>
<html lang="es">
    <head>
        <title>Audit. Ciberseguridad</title>
        <meta charset="utf-8"/>

        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" href="../css/misestilos2.css"/>
        <script type="text/javascript" src="../js/jquery-1.10.2.min.js"></script>
    </head>

    <body>
        <div class="wrap">
            <header>
                <a href="../index.php"><img src="../img/logociber.jpg"/> </a><br></br>
                <h1>Generación de Informe de Auditoría</h1>
            </header>

            <section id="formulario">
                <form  method="post" ACTION="../php/formulario_ciber_2.php">
                        <div id="div_bloque_1">

                            <label for="txt_auditorjefe" style="color:black">Nombre del auditor jefe <span>(requerido):  </span></label>
                            <input type="text" name="txt_auditorjefe" required/><br><br>
                            <label for="txt_auditor2" style="color:black">Nombre del auditor 2:  </label>
                            <input type="text" name="txt_auditor2"><br><br>
                            <label for="txt_auditor3" style="color:black">Nombre del auditor 3:  </label>
                            <input type="text" name="txt_auditor3"><br><br>
                        </div>
                        <div id="div_bloque_2">
                            <label for="txt_auditoria" style="color:black">Nombre de la auditoria <span>(requerido):  </span> </label>
                            <input type="text" name="txt_auditoria" required/><br><br>
                    </div>
                        <div id="div_bloque_3">
                            <label for="txta_descaudit" style="color:black">Introduccion de la auditoria:  </label>
                            <textarea rows="3" class="textbox" placeholder="Breve descripción de la auditoria realizada" name="txta_descaudit" maxlength="25000"></textarea><
                        </div>
                        <input type="reset" value="Borrar">
                        <input type="submit" value="Siguiente" >

                </form>
            </section>
        </div>
    </body>
</html>
```

- Formulario_ciber_2: código referente al formulario de introducción de datos de los resultados obtenidos en la auditoría y creación del informe.

```php
<?php
//Recibimos parámetros introducidos en el formulario anterior
    $txt_auditorjefe = $_POST['txt_auditorjefe'];
    $txt_auditor2 = $_POST['txt_auditor2'];
    $txt_auditor3 = $_POST['txt_auditor3'];
    $txt_auditoria = $_POST['txt_auditoria'];
    $txta_descaudit = $_POST['txta_descaudit'];
?>
<!DOCTYPE html>
<html lang="es">
    <head>
        <title>Audit. Ciberseguridad</title>
        <meta charset="utf-8"/>

        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" href="../css/misestilos2.css"/>
        <script type="text/javascript" src="../js/jquery-1.10.2.min.js"></script>
    </head>

    <body>
        <div class="wrap">
            <header>
                <a href="../index.php"><img src="../img/logociber.jpg"/> </a><br></br>
                <h1>Generación de Informe de Auditoría</h1>
            </header>

            <section id="formulario">
                <form  method="post" ACTION="creaPDF.php?txt_auditorjefe=<?php echo $txt_auditorjefe?>&txt_auditor2=<?php echo $txt_auditor2?>&txt_auditor3=<?php echo $
                    <div id="div_bloque_1">
                    <p style="color:green;text-decoration: underline">A.1.1 MODELO DE GOBIERNO - Área de Riesgos - Organigrama</p><br></br>
                    <input type="radio" class="radiobutton" name="rb_a11" value="OK" checked><label style="color:black">OK</label><br></br>
                    <input type="radio" class="radiobutton" name="rb_a11" value="KO"><label style="color:black">KO</label><br></br>
                    <input type="radio" class="radiobutton" name="rb_a11" value="NR"><label style="color:black">No revisado</label><br></br>
                    <textarea rows="3" class="textbox" placeholder="Comentarios Informe Organigrama" name="txta_a11" maxlength="25000"></textarea><br></br>

                    </div>

                    <div id="div_bloque_2">
                    <p style="color:green;text-decoration: underline">A.1.2 MODELO DE GOBIERNO - Área de Riesgos - Funciones y responsabilidades</p><br></br>
                    <input type="radio" class="radiobutton" name="rb_a12" value="OK" checked><label style="color:black">OK</label><br></br>
                    <input type="radio" class="radiobutton" name="rb_a12" value="KO"><label style="color:black">KO</label><br></br>
                    <input type="radio" class="radiobutton" name="rb_a12" value="NR"><label style="color:black">No revisado</label><br></br>
                    <textarea rows="3" class="textbox" placeholder="Comentarios Informe Funciones y responsabilidades" name="txta_a12" maxlength="25000"></textarea>
                    </div>
```

- FPDF: es una clase desarrollada en PHP para poder realizar documentos en PDF, dinámicamente a partir de nuestros scripts PHP. Esta clase trabaja de manera totalmente autónoma, por lo que no requiere utilizar la librería PDFlib ni cualquier otro producto similar.

- PDF: es una extensión de la clase genérica FPDF en la cual se han añadido funciones para creación de encabezamiento, pie de página, estilos del texto, títulos, etc.

```php
<?php
include_once('fpdf.php');
class PDF extends FPDF
{
    function Footer()
    {
        $this->SetY(-15);
        $this->SetFont('Arial','I',8);
        $this->Cell(0,10,'Generación Automática de Informes de Auditoría de Ciberseguridad','T',0,'C');
    }
    function Header()
    {
        $this->SetFont('Arial','B',9);

        $this->Line(10,10,206,10);
        $this->Line(10,35.5,206,35.5);

        $this->Cell(30,25,'',0,0,'C',$this->Image('../img/logouva.jpg', 152,12, 19));
        $this->Cell(111,25,'Universidad de Valladolid Campus Segovia ',0,0,'C');
        $this->Cell(40,25,'',0,0,'C',$this->Image('../img/logocobit1.jpg', 175, 12, 19));

        $this->Ln(25);
    }
    function ImprimirTexto($text)
    {
        //$txt = file_get_contents($file);

        $this->SetFont('Times','',12);
        $this->MultiCell(0,5,$text);
        $this->MultiCell(0,5,"");

    }
    function ImprimirTitulo($text)
    {
        //$txt = file_get_contents($file);

        $this->SetFont('Times','',16);
        $this->MultiCell(0,5,$text);
        $this->MultiCell(0,5,"");

    }
    function cabecera($cabecera){
        $this->SetXY(50,105);
        $this->SetFont('Arial','B',15);
        foreach($cabecera as $columna)
        {
            $this->Cell(40,7,$columna,1, 2 , 'L' ) ;
        }
    }
}//fin clase PDF
?>
```

- CreaPDF: en este fichero PHP recogemos los datos introducidos por el auditor para invocar a las funciones de creación de PDF.

```
    $txta_a2 = $_POST['txta_a2'];
    $txta_a3 = $_POST['txta_a3'];
    $txta_a4 = $_POST['txta_a4'];
    $txta_a5 = $_POST['txta_a5'];
    $txta_b1 = $_POST['txta_b1'];
    $txta_b21 = $_POST['txta_b21'];
    $txta_b22 = $_POST['txta_b22'];
    $txta_b23 = $_POST['txta_b23'];
    $txta_b24 = $_POST['txta_b24'];
    $txta_b25 = $_POST['txta_b25'];
    $txta_c = $_POST['txta_c'];




    //Recibimos dentro de una cadena el nombre de la auditoría
    $nombreaudit=$txt_auditoria;
    //Se crea un objeto de PDF
    //Para hacer uso de los métodos
    $pdf = new PDF();
    $pdf->AddPage('P', 'Letter');
    $pdf->SetFont('Arial','B',12);
    $pdf->Cell(0,10,$nombreaudit,0,1,'R');

    $pdf->Cell(40,7,'I  N  F  O  R  M  E     C  I  B  E  R  S  E  G  U  R  I  D  A  D',0, 1 , ' L ');
    $pdf->Ln();

if ($txta_descaudit != ""){
    $pdf->ImprimirTitulo('0. Introducción a '.$txt_auditoria); //Texto fijo
    $pdf->ImprimirTexto($txta_descaudit);}
    $textoinic="Esta Auditoría ha sido realizada por: ".$txt_auditorjefe;
    $pdf->ImprimirTexto("Esta Auditoría ha sido realizada por los siguientes auditores: ");
    $txtinicjefe="- ".$txt_auditorjefe.", como jefe de grupo. ";

    $pdf->ImprimirTexto($txtinicjefe);
    if ($txt_auditor2 != ""){
    $txtinicaudit2="- ".$txt_auditor2.".";
    $pdf->ImprimirTexto($txtinicaudit2);}
    if ($txt_auditor3 != ""){
    $txtinicaudit3="- ".$txt_auditor3.".";
    $pdf->ImprimirTexto($txtinicaudit3);}

if ($rb_a11 != 'NR'){
$pdf->ImprimirTitulo('A.1.1. Organigrama'); //Texto fijo
if ($rb_a11 == 'OK'){
    $pdf->ImprimirTexto('Se ha verificado que el control y la gestión de la tecnología se encuentran segregados conforme a un modelo de ciberseguridad adecuado.');
}
    else{
```

6. CONCLUSIONES DEL TFG

La Metodología para Auditorías de Ciberseguridad realizada en mi Trabajo de Fin de Grado puede servir de mucha utilidad tanto a aquellas personas que se inician en el mundo de la ciberseguridad como los que ya tienen cierta experiencia.

De esta manera, el auditor puede identificar los procedimientos y puntos más importantes a la hora de realizar una auditoría. Todos los puntos están basados en los estándares fijados por **COBIT** y los estándares de **ISO 27001**.

Además, en la Metodología para Auditorías de Ciberseguridad no me he detenido en lo puramente teórico, ya que algunas de las pruebas realizadas en el trabajo de campo más corrientes en las auditorías de ciberseguridad han sido explicadas con ejemplos prácticos.

Con la creación de la Interfaz de generación de informes, se facilita la creación del informe de auditoría, sirviendo como soporte a éste o pasando a ser directamente el informe final de auditoría.

Debido a que normalmente en las auditorías participan distintos auditores que revisan diversos puntos, la interfaz puede servir para aglutinar los resultados obtenidos en las pruebas de los auditores.

La idea principal es que sirva como uso interno dentro de la entidad a la que pertenezca el auditor, y de esta manera adaptar el diseño del informe final a las normas y procedimientos de la organización en cuanto a estilos, encabezamiento de las hojas, etc.

Por su parte, los auditores externos también pueden encontrar la interfaz de utilidad para disponer de un documento de ayuda para la generación de su informe final.

El mundo de la ciberseguridad está en constante evolución ya que cada vez hay más atacantes dispuestos a realizar algún acto malicioso. Las personas estamos expuestas a este tipo de actos, ya que confiamos nuestros datos personales, financieros, etc. a muchas organizaciones que pueden estar no cumpliendo con su deber de garantizar una adecuada ciberseguridad.

Es por ello que creo necesario darle más importancia a este tipo de auditorías ya que, aunque la ciberseguridad absoluta no existe, hay que minimizar el riesgo al máximo.