UNIVERSIDAD
DE BURGOS

PLAN DE AUDITORIA PARA EL SISTEMA DE INFORMACIÓN DE UNA EMPRESA DEDICADA A LA DOCENCIA.

EDUARDO MORA GONZÁLEZ

CONTENIDO

1. INTRODUCCIÓN

Toda institución o empresa está sometida a diferentes auditorías imprescindibles para su funcionamiento. Una de estas auditorías son las referentes a la seguridad, amparadas por la normativa vigente, la Ley 5/2014, de 4 de abril de Seguridad Privada. Esta seguridad incluye la revisión y mejora de, por ejemplo, el estado de la seguridad de un edificio, entre otros.

Para comprender el funcionamiento de las auditorías de seguridad es importante ir al origen. Y es que una auditoría se define como **[R1]** "Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse". Por otro lado, encontramos la palabra seguridad que tiene interesantes acepciones:

1. "Certeza, garantía de que algo va a cumplirse".
2. "Mecanismo que previene algún riesgo o asegura el buen funcionamiento de alguna cosa, precaviendo que falle".

Por lo tanto, la seguridad es un mecanismo interno que permite que el sistema funcione, y la seguridad se refleja a través del sistema de seguridad. En el caso de una auditoría, analizará el funcionamiento de todo el sistema en lugar de analizar las medidas técnicas de forma aislada. Estas medidas incluyen detección de intrusos, barreras físicas, circuito cerrado de televisión, equipos de control de acceso, centralización, etc.

"Las auditorías de seguridad se centran en el funcionamiento del engranaje en su total, y no en el cada rueda o unidad independiente del sistema" **[R2]**

2. AUDITORÍA TÉCNICA DE SEGURIDAD

En este documento se va a realizar una auditoria de seguridad para el sistema de información de una empresa dedicada a la docencia, para ello se va a analizar tanto el aspecto de gestión administrativa como la propia docencia.

2.1. DEFINICIÓN DEL PLAN DE AUDITORÍA

La auditoría en la organización se llevará a cabo durante la primera quincena del mes de mayo como se ha acordado con la empresa.

2.1.1. OBJETIVOS

El objetivo general es realizar el estudio, revisión, verificación y evaluación de los sistemas de información relacionado con la docencia impartida en la empresa, observando el cumplimiento de las diferentes normas mediante la auditoria a la seguridad física, seguridad lógica, infraestructura tecnológica y software.

Entre los objetivos específicos se encuentran los siguientes:

- Obtener una evaluación real y efectiva sobre los posibles riesgos presente en sistemas de información dedicados a la docencia.
- Identificar y analizar las diferentes vulnerabilidades que se pueden presentar en cada uno de los componentes del sistema de información.
- Verificar la aplicación de barreras y procedimientos que resguarden el acceso a los datos.
- Comprobar el tipo de docencia, comprobando si está al mismo nivel de calidad que exigente.

2.1.2. ALCANCE

La auditoria pretende identificar las condiciones actuales del sistema de información de la empresa dedicada a la docencia en los siguientes ítems:

- **Seguridad física:** Se verificarán las condiciones ambientales para permitir la protección a través de varios elementos que se combinan para ayudar a integrar una serie de medidas preventivo-disuasivas o represivas contra eventualidades de carácter ilícito.

- **Seguridad lógica:** Verificar los diferentes controles de acceso a la información y diferentes roles que los clientes internos usan el sistema de información, y verifique los límites de los servicios que estos usuarios tienen.
- **Infraestructura tecnológica:** Se evaluará el tipo de mantenimiento y el historial de cada terminal, y sus respectivos usos se verificarán de acuerdo con los usuarios.
- **Software:** Verificar las licencias de funcionamiento de los diferentes programas instalados en la empresa.

2.2. EJECUCIÓN DE LA AUDITORÍA

Una vez identificado los objetivos y el alcance de la auditoria se va a realizar la auditoría.

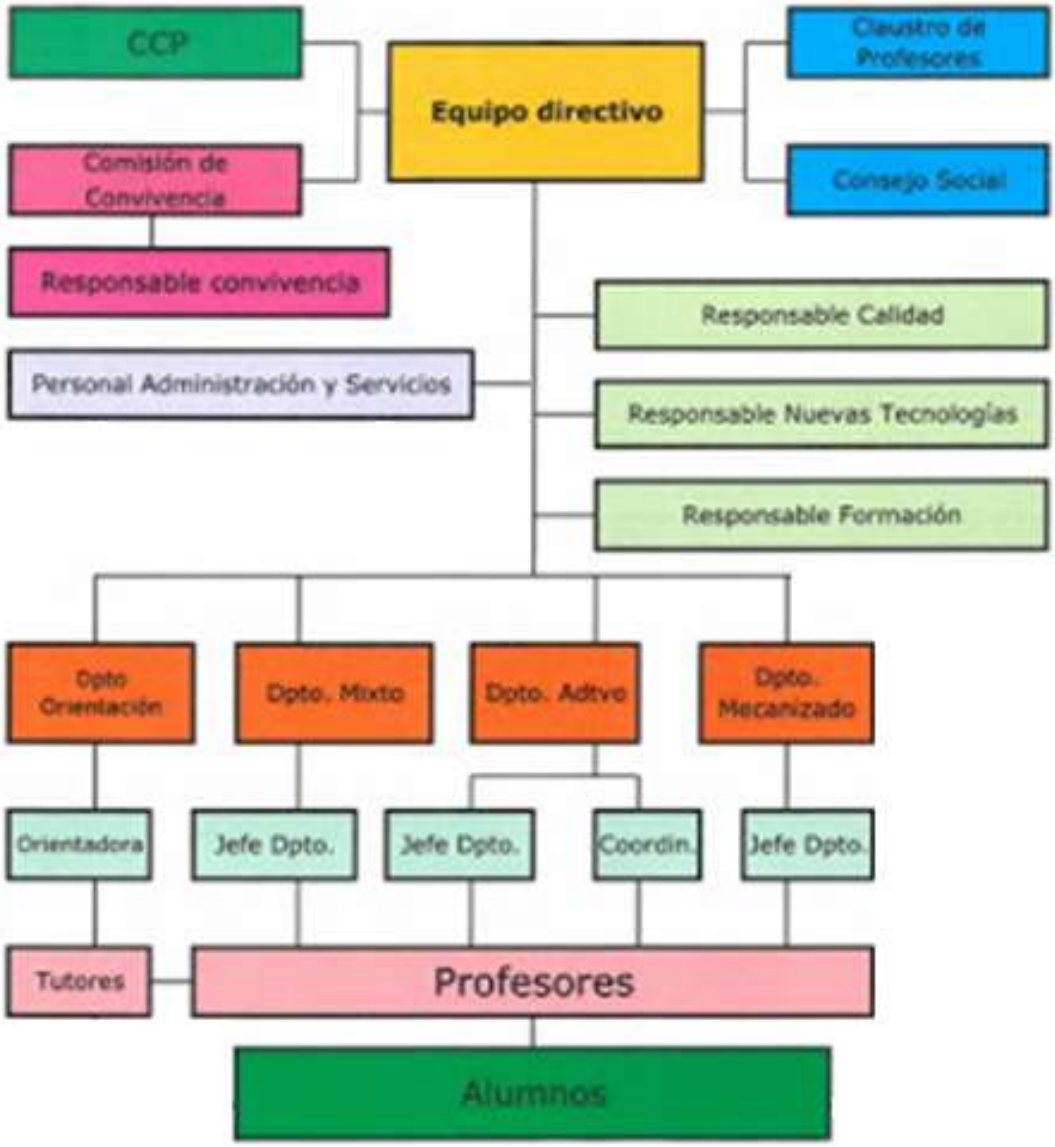
2.2.1. RECOLECCIÓN DE INFORMACIÓN PREVIA

El objetivo principal de la compañía es ofrecer una docencia de calidad al mayor numero de personas, para ello los valores de la empresa son: Disponibilidad, Eficacia y Compromiso.

Respecto a las leyes que la empresa debe tener en concordancia con el propósito que pretende son:

- Ley Orgánica 2/2006, de 3 de mayo, de Educación.
- Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por otro lado, debemos conocer la estructura de la empresa para saber como esta organizada, en el siguiente organigrama se muestra dicha estructura:



Para finalizar, se ha obtenido una copia de los siguientes documentos para que sirvan de ayuda para la realización de la auditoria:

- Políticas y procedimientos de la empresa.
- Descripción de los entornos, tantos físicos como digitales en los que trabaja la empresa, de tratamiento de información.
- Documento de nombramiento y estudio de las vulnerabilidades.
- Curriculum Vitae de todos los profesionales.
- Listado de licencias.

Una vez obtenida toda la información, se va a proceder a la siguiente etapa del proceso de Auditoria.

2.2.2. EJECUCIÓN DE LA PRUEBAS DE AUDITORÍA

Para realizar las pruebas se ha desarrollado un formulario que servirá como apoyo para realizar las pruebas.

PAGINA			PRUEBAS DE ANALISIS DE AUDITORIA	REF
1	DE			

ENTIDAD AUDITADA			%
DOMINIO AUDITADO			
RESPONSABLE		AUDITOR RESPONSABLE	
MATERIAL DE SOPORTE			

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANALISIS	DE EJECUCION

Este formulario dará como salida un porcentaje de riesgo, que hace referencia a la probabilidad de que el proceso de vea afectado por las acciones de las cuales se ha indagado. El porcentaje de riesgo se calculará de con la siguiente formula:

P-Riesgo = 100 – (TOTAL SI * 100) / TOTAL

Para determinar el nivel de riesgo se ha usado la siguiente categorización:

PORCENTAJE	RIESGO
< 30%	BAJO
30 - 70%	MEDIO
>70%	ALTO

Una vez definido el formulario y la estimación porcentual de como se evaluará el riesgo se va a proceder ahora a ejecución de las pruebas, empezando con la revisión de la documentación, siguiendo con una entrevista a todos los empleados y terminando con una comprobación técnica y visita a la oficina para comprobar in situ los sistemas.

2.2.2.1. REVISIÓN DE LA DOCUMENTACIÓN

Toda la documentación revisada ha sido validada y comprobada de que todo esta conforme a lo previsto excepto el documento de políticas y procedimiento de la empresa, en el cual, tras su análisis se ha sacado las siguientes conclusiones:

- Las políticas de seguridad no están adaptadas a la LOPD actual.
- Falta una descripción detallada de los procedimientos que usa la empresa para impartir su docencia.

2.2.2.2. REALIZACIÓN DE ENTREVISTAS

Dentro de la documentación solicitada se encontraba los curriculum vitae de los empleados para poder tener una entrevista con ellos y constatar la veracidad de ellos además de hacer un cuestionario sobre la empresa.

La conclusión obtenida ha sido buena, todos los entrevistados han tenido una actitud participativa y todos han demostrado tanto su profesionalidad como conocimiento de la empresa.

2.2.2.3. EJECUCIÓN DE PRUEBAS TÉCNICAS

Terminada la revisión de los documentos y de las entrevistas, se ha realizado las pruebas técnicas. En estas pruebas se han comprobado el funcionamiento del sistema, sus comunicaciones y el contenido de sus cursos para ver también la calidad docente.

Tras el análisis se ha descubierto una vulnerabilidad en la seguridad de la información de todo el material usado en la docencia, esta vulnerabilidad ha provocado un riesgo bastante alto.

2.2.2.4. REALIZACIÓN DE VISITAS

Entrando en la ultima fase de las pruebas, se ha realizado varias visitas a las instalaciones de la empresa para comprobar el estado físico de los dispositivos, servidores, redes…

En estas visitas no se ha detectado nada relevante que ponga el riesgo la seguridad.

2.2.3. ANÁLISIS DE LA INFORMACIÓN

Una vez concluida las pruebas se ha procedido a una reunión con la empresa donde se ha leído el documento de petición de la auditoria y el informe de auditoría.

En esta etapa de la auditoria se ha usado la técnica de análisis de riesgo para evaluar la importancia relativa o el riesgo de una" no conformidad" detectada. Esta técnica usa el siguiente diagrama **[**R3**]**:

La información obtenida de las pruebas ha supuesto el hallazgo de los siguientes riesgos:

- No actualización de la LPOD.
- Vulnerabilidad de seguridad en la información relativa a la docencia.

Esta información ha sido mencionada en la reunión y discutida.

Por ultimo se ha revisado las políticas contestando a las siguientes preguntas:

- **¿Existen y están al alcance personal que se encuentra afectado por ellas?**
  Si, las políticas están disponibles para todo el personal y la empresa pone mucho interés a través de cursos y formaciones que están lleguen a todos.

- **¿Es bueno su contenido?**
  El contenido de las políticas es calificado de decente como se va a poder comprobar en las siguientes preguntas. Se ha dado unas pautas a la empresa para poder tener unas políticas mejores.

- **¿Cuál es la temática de la política y cuál es el activo de información que se pretende proteger?**
  La temática de la política es la calidad de la docencia y se pretende proteger la impartición de esta docencia.

- **¿Quién es el responsable de emitir la política y quién se encuentra afectado por ella?**
  Una persona del equipo directivo y afecta a toda la empresa.

- **¿A qué partes de la organización afecta la política?**
  A todas las partes.

No todas las preguntas han sido contestadas de una forma clara y concisa, por lo que la calificación de las políticas no ha sido tan buenas como lo esperado, por eso a la pregunta de si es bueno su contenido se le ha calificado como decente.

2.3. REPORTING DE LA AUDITORÍA

El informe creado de la auditoria y que ha sido enviado a la empresa auditada, en donde se encuentra una visión general de la empresa, las conclusiones obtenidas y las recomendaciones, es el siguiente:

INTRODUCION

La empresa auditada durante la primera quincena del mes de mayo se dedica a la docencia online.

Dicha empresa tiene varios departamentos bien diferenciados y disponen de todo el material necesario para impartir una docencia de calidad.

METODOLOGÍA EMPLEADA

La metodología usada ha sido propia al equipo de auditoria, en la cual se usan una serie de informes para asignar un porcentaje de riesgo que tiene un activo auditado.

Para la realización de la entrevista se ha usado un cuestionario de conocimiento de los trabajadores de la empresa y sus propios curriculum vitae para comprobar la veracidad de estos.

En las pruebas técnicas, se han realizado pruebas de rendimiento (intentando llevar los sistemas a limite), de seguridad (intentando hacer un hacking ético al sistema), de integridad (comprobando la veracidad de los datos impartido en la docencia).

En las visitas a las instalaciones se han hecho unas pruebas estructurales y comprobación de los puestos de trabajo, dispositivos, servidores…

CONCLUSIONES

La empresa en general cumple con lo esperado a excepción de:

- No actualización de la LOPD actual.
- Vulnerabilidad de seguridad encontrada.

La primera tiene un nivel importante, pero la segunda es crítica por lo que la empresa deberá subsanarlo de una manera rápida y eficaz.

RECOMENDACIONES

Respecto a la seguridad, es conveniente que periódicamente se contrate la presencia de una persona que detecte las vulnerabilidades de los sistemas.

2.4. SEGUIMIENTO DE LA AUDITORÍA

La empresa ha llegado al acuerdo de que una vez cada 2 años se realizara una autoría para comprobar el estado de la organización y así comprobar si las medidas correctoras solicitadas han sido aplicadas.

3. CONCLUSION

El trabajo de crear un plan de auditoria me ha ayudado a tener una visión más amplia y detallada de las auditorias.

Hacer una simulación de un caso real, hace ponerte en la piel de la empresa y de los auditores para saber el rol que tiene cada uno.

Gracias a estos conocimientos adquiridos, tengo mas conciencia de lo importante que es tener todo controlado para que no pueda pasar ningún incidente.

REFERENCIAS

R1: https://dle.rae.es/auditor%C3%ADa

R2: https://www.auditoresseguridad.es/single-post/que-es-auditoria-seguridad

R3: MATERIAL DE LA ASIGNATURA.

BIBLIOGRAFIA

- **https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/502-ccn-stic-802-auditoria-del-ens/file.html**
- MATERIAL DE LA ASIGNATURA.
- **https://debitoor.es/glosario/definicion-auditoria**
- **https://www.fimax.es/sirve-una-auditoria-empresa/**
- **https://www.isecauditors.com/auditoria-tecnica-de-seguridad**
- **http://openaccess.uoc.edu/webapps/o2/bitstream/10609/53506/10/ipenatTFM0616presentaci%C3%B3n.pdf**