

# **AUDITORÍA DE SISTEMAS**

## GUIA DE CLASE N° 01

### **Docente**

Riascos Armas Juan Orlando

### **Estudiante**

Junior Cercado Vasquez

Semestre 2022 II

## **AUDITORÍA INFORMÁTICA Y APLICACIÓN A UN CASO EN UNA EMPRESA REAL**

Es impensable conocer el funcionamiento de una empresa sin el uso de la nueva tecnología integrada con los sistemas de información, desde que las diversas entidades de negocio de una empresa se fueran apoyando conjuntamente en la informática.

En la actualidad, casi todas las empresas de medio-gran tamaño realiza sus propias auditorías externas, internas o ambas, facilitando cumplir todos sus requerimientos legales. Estas auditorías resultan un punto control muy importante sobre el funcionamiento interno de la empresa.

Es importante llevar un control sobre la seguridad física y sobre los sistemas de información. A veces suele ocurrir que estos procesos sobre la seguridad son esquivadas o se buscan soluciones parche para salir del proceso. Esto ocurre por prisas o por desconocimiento y se llega adoptar malas prácticas.

La auditoría informática es un elemento que, aunque sea o parezca poco importante es esencial para determinar vulnerabilidades, básicamente consiste en recoger, agrupar y evaluar las evidencias.

Todos los sistemas de información pueden tener debilidades de seguridad ya que la tecnología avanza a pasos agigantados y al gran número de desarrollos a nivel de software que se van creando. Entonces el objetivo de una auditoría no es detectar fallos para encontrar un culpable, sino para que haya una mejora de rendimiento en todos los procesos.

### **TIPOS DE AUDITORÍA INFORMÁTICA: INTERNA Y EXTERNA**

#### **INTERNA**

Esto se lleva a cabo dentro de la empresa, realizado por el personal que pertenece la empresa auditada. Los miembros que realicen la auditoria deben de cumplir algunos requisitos como tales:

- Dependencia del orden superior
- Conocimiento de los auditores
- Relación entre auditores
- No realizar otras funciones
- Contratación del personal externo

- Conocimiento sobre la propia empresa

### **EXTERNA**

Tiene por objetivo realizar un estudio más en profundidad teniendo en cuenta que los encargos de realizar esta auditoria no tendrán contacto previo con ningún trabajador de la empresa auditada. Las características más importantes:

- Elección de la empres
- Proceso de contratación
- Plan de trabajo previo

### **EL AUDITOR INFORMÁTICO**

Es el encargado que va a revisar la seguridad, el control interno, la efectividad, la gestión del cambio y la integridad de la información.

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

### **ETAPAS DE LA METODOLOGÍA**

El buen análisis y estructuración de las etapas en el inicio de la auditoría hará que realicemos una auditoría lo más eficientemente posible.

- **FASE I:** Definición de alcance y objetivos
- **FASE II:** Estudio inicial
- **FASE III:** Entorno operacional
- **FASE IV:** Determinación de recursos de la auditoria informática
- **FASE V:** Actividades de la auditoria informática.
- **FASE VI:** Informe final
- **FASE VII:** Carta de introducción o presentación del informe final

## MARCOS Y REFERENCIAS PARA LA ADUITORÍA INFORMÁTICA

**LOPD:** Ley orgánica de Protección de Datos de Carácter Personal. Contiene lo siguiente:

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

**ISO 27001:2005:** Es un estándar internacional para la seguridad de la información. Es parte de un conjunto de estándares definidos por la serie 27000 que engloba a más normas especializadas

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

Un sistema de Gestión de la seguridad de la información tiene como fin la protección de la información de una organización. Teniendo sus características:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad y no repudio.
- Audibilidad
- Protección frente a la duplicación
- Legalidad
- Confiabilidad de la información

La política de seguridad es un conjunto de normas que explican las directrices principales de seguridad de la información y de las comunicaciones por todos los usuarios. Cada usuario tiene determinados permisos, tanto por acceder físicamente a ciertos lugares de la oficina.

Para realización de cualquier tipo de petición a recursos humanos existirá una solicitud que se deberá rellenar. Cada solicitud deberá ser presentada al responsable superior y firmada por los correspondientes controladores de la petición.

Lo más importante para no cometer errores en el futuro es establecer las funciones de las que se encargará cada miembro de la organización en general. Es fundamental que cada miembro que tenga algún tipo de responsabilidad en alguna materia sea consciente de las normas que debe de cumplir.