1. INTRODUCCIÓN

Las organizaciones hoy en día, con la sofisticación tecnológica y la complejidad en el manejo de información, enfrentan distintas amenazas que muchas veces explotan sus vulnerabilidades. La confidencialidad, integridad y disponibilidad de la información en la empresa, es fundamental para el aumento de la competitividad de la firma. Las organizaciones están obligadas si desean continuar operando, a instaurar sistemas de gestión de seguridad que permitan asegurar que tienen identificados sus activos vitales, controlados los riesgos potenciales y puedan con precisión instituir los controles pertinentes.

El ataque a los sistemas puede ser por fines económicos, por obtener cierto tipo de información, para sabotear las operaciones de la empresa, para desmeritar su prestigio, por revanchismo o simplemente por curiosidad, entre otras muchas causas. En cualquier caso, el riesgo e impacto son altos para la empresa. La pérdida de información sensitiva, fraude, paro de operaciones además de las pérdidas en imagen por el impacto publicitario que genere el ataque, representan altos costos para una empresa.

La existencia de amenazas que afectan la disponibilidad, integridad y confidencialidad (la llamada tríada de seguridad) de los datos es real. Es crítico para las organizaciones poder identificar esas amenazas y adoptar recomendaciones que permitan prevenir, detectar y protegerse de ellas. La diversidad y la heterogeneidad de los sistemas de información que requieren las organizaciones actuales, sumado a la globalización a la que se enfrentan al conectar esos sistemas al mundo de Internet, genera un sinfín de incertidumbres en lo referente a la Seguridad de la Información.

El riesgo está siempre presente, es algo inherente y aunque no se puede eliminar en su totalidad, si se puede mitigar. La cuestión clave está en saber qué nivel de riesgo hay y cuál estamos dispuestos a admitir antes de tomar medidas. La definición de riesgo aceptable, así como el enfoque para administrar el riesgo, varía de una organización a otra. No hay una respuesta acertada o errónea; existen numerosos modelos de administración de riesgos en uso actualmente. Cada modelo ofrece un equilibrio entre precisión, recursos, tiempo, complejidad y **subjetividad**.

Por tanto, para poder decidir si un tipo de riesgos es admisible, se requiere estimar su magnitud, por lo que se hace necesario realizar un análisis sistemático y lo más completo posible de todos los aspectos que implica para los activos la presencia de una amenaza.

El **análisis de riesgos** es por tanto una herramienta de gestión que permite tomar decisiones. Las decisiones pueden tomarse antes de desplegar un servicio o con éste funcionando. Es muy deseable hacerlo antes, de forma que las medidas que haya que tomar se incorporen en el diseño del servicio, en la elección de componentes, en el desarrollo de las aplicaciones y en los manuales de usuario. Todo lo que sea corregir riesgos imprevistos es costoso en tiempo propio y ajeno, lo que puede ir en detrimento de la imagen prestada por la Organización y puede suponer, en último extremo, la pérdida de confianza en su capacidad. Siempre se ha dicho que es mejor prevenir que curar y aquí se aplica: no espere a que un servicio haga agua; hay que prever y estar prevenido.

Para tener una idea de cual es el estado de riesgo del sistema se han de realizar cálculos complejos ya que hay que tener en cuenta múltiples factores. Hay cuatro procesos a seguir cuando tratamos con los riesgos: el análisis, la valoración, la evaluación y el tratamiento del riesgo. La interrelación entre los recursos, los posibles ataques y las posibles defensas de las que se disponen llevan a una serie de resultados. Éstos nos indicarán el nivel de vulnerabilidad del sistema y remarcará los puntos débiles que requieren especial protección.

El análisis de riesgos es un proceso dinámico, ya que aparecen nuevos activos, hay que contemplar distintas amenazas y los controles pueden ser suplantados por otros más efectivos; es decir, ha de soportar los cambios futuros de la organización. Tanto el análisis como la gestión encajan por tanto en la actividad continua de gestión de la seguridad.

La doble problemática de complejidad y dinamismo llevan a la necesidad de implantar una herramienta que agilice los cálculos, arroje resultados y contemple fácilmente la evolución de la organización.

Esta herramienta arrojará una serie de datos y proporciona una serie de claves a partir de las cuales se iniciará la **gestión de los riesgos**, donde se decide si se asume, mitiga (implantando las contramedidas necesarias) o transfiere el riesgo resultante del análisis. Aquí entra en juego el equilibrio entre costo y efectividad. Será un equipo de seguridad experto el encargado de realizar esta labor.

La inversión en un proceso de administración de riesgos, con un marco sólido y funciones y responsabilidades bien definidas, prepara la organización para articular prioridades, planear la mitigación de amenazas y afrontar la siguiente amenaza o vulnerabilidad de la empresa. Además, un programa de administración de riesgos eficaz ayudará a la empresa a realizar un progreso importante hacia el cumplimiento de los nuevos requisitos legislativos.

1.1. Problemática y Objetivos

Este proyecto surge debido a la necesidad de tener una herramienta que permita la realización de un análisis de riesgos como paso previo para la redacción de una documentación de seguridad durante el proceso de acreditación de un Sistema de Información y Comunicaciones (SIC o CIS), o para verificar el estado de riesgo a que está sometido un sistema de SIC como paso previo a la implantación de salvaguardas.

La utilización de esta herramienta nos aporta precisión y rapidez, permitiendo simular fácilmente distintos entornos y evaluar cual es el óptimo tras analizar los resultados obtenidos.

Así podremos deducir como mejorar y proteger un sistema ya implantado o que aun se encuentre en vías de desarrollo.

Es un tema recurrente la inquietud por la seguridad de los sistemas de información. Lo ideal es que los sistemas no fallen. Pero lo cierto es que se acepta convivir con sistemas que fallan. La seguridad absoluta no existe, siempre hay que aceptar un riesgo. El asunto no es tanto la ausencia de incidentes como la confianza en que están bajo

control: se sabe qué puede pasar y se sabe qué hacer cuando pasa. El temor a lo desconocido es el principal origen de la desconfianza y , en consecuencia, aquí se busca conocer para confiar: conocer los riesgos para poder afrontarlos y controlarlos.

En ocasiones el análisis de riesgos no se hace por capricho, sino que puede venir requerido por precepto legal. Por poner algunos ejemplos tenemos el caso del Real Decreto 263/1996, o la Ley Orgánica 15/1999.

En conclusión, se procederá a analizar y gestionar los riesgos cuando directa o indirectamente lo establezca un precepto legal y siempre que lo requiera la protección responsable de los activos de una organización.

1.2. Plan de Trabajo

La realización del Proyecto se abordó realizando la división en las siguientes tareas:

0.- Planificación general del proyecto

Es imprescindible un buen esquema global del proyecto para delimitar de alguna forma los hitos por los que se deberá ir pasando.

1.- Documentación

Se realizaría una labor de investigación, documentación e iniciación acerca de las tecnologías básicas que van a estar necesariamente implicadas en la realización del proyecto (SQL, OpenOffice, StarOffice Basic...), con la que obtener una visión global que ayudará a realizar el análisis de la aplicación. En este apartado también se incluye un estudio inicial de la base teórica.

2. - Análisis Estadístico

Se profundiza en la base teórica para tener claros los retos matemáticos que tenemos que implementar.

3.- Análisis Completo

A continuación se realizaría un estudio de los requisitos y especificaciones de la aplicación. En esta fase se deberían delimitar claramente los diferentes módulos de los que constaría la aplicación, así como una enumeración detallada de las funcionalidades necesarias en cada uno de ellos.

Se diseñaría el modelo de datos de la aplicación, elaborándose un prototipo del Diagrama Entidad Relación (ERD), éste sufrirá ligeras modificaciones conforme avance el proyecto, debido a la conveniencia de añadir o suprimir determinados campos, cambiar nombres de tablas, incluir relaciones...

También se generarán los scripts necesarios para la creación del esquema de la propia base de datos.

4.- Inicio de la programación

Como cabe suponerse, la fase más extensa del proceso. En esta fase se procedería a la codificación de los diferentes módulos de la aplicación. Éstos se describirán en sucesivos apartados.

5.- Estética de la aplicación

Esta fase se centraría en el desarrollo de la presentación de la aplicación.

6.- Pruebas sucesivas

Paralelamente a la fase de programación se llevaría a cabo una fase de pruebas. El desarrollo se ejecutaría de forma muy modular, y realizando continuas pruebas de cada pequeño módulo funcional que se fuera creando. Se pueden dividir en dos grupos:

- Pruebas de validación de módulos: se realizarán en el contexto de proyectos que corresponden al modelo de desarrollo modular.

- Pruebas de integración: comprueba la integración conjunta de los distintos módulos o elementos del software que componen la aplicación.

7.- Batería definitiva de pruebas

La aplicación se sometería a un conjunto de pruebas destinadas a determinar y afinar su robustez en el entorno de producción.

8.- Elaboración de los manuales de usuario

Se elaborarán y entregarán los manuales necesarios en los que se especificarán y describirán de forma clara y detallada las instrucciones necesarias para que los usuarios finales puedan instalar y utilizar de forma efectiva la aplicación, de acuerdo con los requisitos de funcionalidad establecidos.

9.- Formación de los usuarios finales

En esta actividad se establecen las necesidades de formación del usuario final, con el objetivo de conseguir la explotación eficaz de la aplicación

10.- Redacción de la memoria

Desde fases tempranas de desarrollo se irían redactando pequeños informes, que en esta fase final serían agrupados, homogeneizados y extendidos para dar lugar a la presente memoria.