

## Análisis y Gestión de Riesgos

### Situación Actual

Para la mayoría de las empresas e instituciones, sus sistemas de información son los activos por excelencia, imprescindibles para su propia existencia y supervivencia.

Tanto las pymes como las multinacionales, reconocen el grado de criticidad que los sistemas de información representan para su funcionamiento y supervivencia y el alto grado de vulnerabilidad inherente a la propia naturaleza de estos sistemas. Y lo que es más grave, la insuficiencia de las políticas y normas de seguridad implantadas a la fecha.

Con frecuencia somos testigos y/o víctimas de ataques de virus, de hackers, e incluso de empleados o usuarios maliciosos que acceden a información confidencial y la utilizan de forma perjudicial para la empresa. En muchas ocasiones somos conscientes de los daños causados cuando es demasiado tarde o quizá nunca.

Otras situaciones reflejan retrasos o ineficiencias en los caos de fallos de aplicaciones, ausencias de personal cualificado, sistemas de respaldo incompletos o ineficientes que repercuten

en un menor nivel de servicio, costes excesivos o baja rentabilidad.

### Situación Deseada

La situación deseada es aquella que nos da la confianza de que el negocio funciona con suavidad, sin mayores sorpresas, sin interrupciones y sin la aparición de emergencias.

En este caso, el esfuerzo se orienta a resolver los asuntos propios del negocio y no a apagar fuegos con prisas y a cualquier coste.

El Análisis y la Gestión de Riesgos es la pieza fundamental para llegar a esta situación deseada.

### El Análisis de Riesgos (A.R.)

El Análisis de Riesgos del negocio en lo relativo a los Sistemas de Información es la piedra angular sobre la que se apoyan las acciones para la selección de controles a aplicar e incluso la base para elaborar Planes Directores o Parciales de Seguridad o un Plan de Continuidad del Negocio.

El proceso de Análisis de Riesgos, a grandes rasgos, se basa en:

- Creación de un inventario de activos
- Simplificación de activos en Dominios

• Detección de vulnerabilidades y amenazas asociadas. Se utilizan complementariamente los servicios de Hacking Ético si así se solicita.

• Evaluación de probabilidades e impactos.

• Análisis de controles ISO implantados.

• Obtención del riesgo.

Se analiza en qué grado y medida actúan cada uno de los controles que el negocio tenga implantado para proteger sus sistemas de información de acuerdo con la Norma ISO 27002 (también denominada ISO 17799:2005), que es el Código de Buenas Prácticas en materia de seguridad. Esta norma nos permite conocer el estado actual de la seguridad de la compañía desde todas las perspectivas (política de seguridad, gestión, seguridad física, etc.)

Los resultados del Análisis de Riesgos nos proporcionan tanto una valoración económica como los rangos de riesgos de otros valores más intangibles. En definitiva, nos dice de forma clara y concluyente cuáles son los riesgos a los que estamos expuestos en la situación actual de acuerdo con una norma universal aceptada.

## La Gestión de los Riesgos

Una vez obtenida la fotografía exacta de estos riesgos se recomienda la aplicación de las medidas de salvaguarda con el objetivo de reducirlos al nivel deseado. Este proceso se denomina Gestión de Riesgos.

En general, las medidas relativas a la gestión son más eficaces, en términos de rentabilidad, que las medidas puramente tecnológicas (como antivirus, firewalls, IDS's, etc.), si bien se hace necesario trabajar en ambos frentes de forma coordinada.

Este trabajo requiere una participación estrecha de los mandos intermedios y el apoyo de la Dirección General. De no ser así, es mejor no iniciar un Análisis y Gestión de Riesgos, pues probablemente estará abocado al fracaso. Si la decisión es a favor de realizarlo, recomendamos empezar por un sector de la empresa y no por la empresa en su totalidad.

## Beneficios

- Conocimiento preciso del nivel de riesgo al que está expuesta la información de la compañía para poder tomar decisiones ajustadas y reducir el riesgo con un coste razonable.
- Reducción de aquellos riesgos que, en caso de materializarse las amenazas que les originan, pueden representar pérdidas ingentes de capital, bien por facturación fallida, por reposición de los daños causados, por pérdida de oportunidades de negocio, por reclamación de clientes, por sanciones legales etc.
- Ahorro de tiempo y dinero al afrontar y corregir situaciones nefastas antes de que ocurran y nos obliguen a resolverlas con prisas y a cualquier precio.
- Mejora de la imagen y revalorización de la confianza en la empresa de los accionistas, inversores, empleados, proveedores y clientes al mostrarles que se toman medidas diarias para garantizar la continuidad del negocio.

## Sobre ESA Security

**ESA Security** es una consultora especializada únicamente en la Seguridad de la Información que ha realizado con éxito la preparación de empresas para que consigan su Certificación ISO 27001, además de haber obtenido su propia certificación en gestión de Seguridad de la Información.

Sus profesionales están altamente cualificados, incluyendo certificaciones CISA y CISM, y lo más importante: con la experiencia práctica de haber conseguido Certificaciones ISO y haber realizado en múltiples ocasiones Planes Directores de Seguridad, Planes de Continuidad de Negocio, Análisis y Gestión de Riesgos, Proyectos de Hacking Ético, Formación en Seguridad, Adecuaciones y Auditorías LOPD y servicios relativos a la Seguridad de la Información en general.