Análisis de riesgos & SOA

ITAPP

Gestión de seguridad - POPBL

MONDRAGON UNIBERTSITATEA | MACC

Hoja de control

Organismo	**Equipo de desarrollo del producto ITAPP**		
Proyecto	ITAPP		
Entregable	Análisis de riesgos & SOA		
Autor	Haritz Saiz, Xabier Gandiaga, Álvaro Huarte, Xabier Etxezarreta, Onintza Ugarte y Ander Bolumburu		
Versión/Edición	0001	**Fecha Versión**	30/05/20
Aprobado por		**Fecha Aprobación**	08/06/20
		Nº Total de Páginas	

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
0100	Versión inicial	Ander Bolumburu	25/05/20

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos
Ander Bolumburu Casado

Contenido

1. Introducción

Teniendo en cuenta que vivimos en un mundo globalizado y competitivo en el que las compañías se encuentran diariamente con nuevos desafíos, cada vez es más importante gestionar la seguridad de la información en la empresa y así evitar la pérdida de su activo más valioso hoy en día: los datos.

Tanto los Sistemas de Gestión de Seguridad de la Información como las redes de trabajo de cualquier organización se ven constantemente afectados por amenazas de seguridad, por ciberataques y por fraudes informáticos. Además, se enfrentan continuamente a sabotajes o virus con el consiguiente riesgo de eliminación y pérdida de la información.

La clave está en que la organización invierta recursos en aplicar herramientas que mejoren la seguridad.

En lo que a seguridad de la información se refiere, algunos de los aspectos fundamentales que deben ser analizados y medidos, son:

- La disponibilidad de los datos
- La confidencialidad de los documentos
- La integridad de la información

¿Por lo tanto, como se pueden minimizar los incidentes? Entre otras cosas, elaborando un inventario de activos, en el que se tenga identificada y localizada toda la información de la que se dispone en la empresa.

Por otro lado, esos activos deben ser valorados con el fin de evitar posibles fallos y finalmente se deben analizar los riesgos que pueden enfrentar estos activos y establecer un protocolo para enfrentarse a esos riesgos.

Finalmente, a través de este documento se van a intentar cubrir diferentes aspectos de la gestión de la seguridad explicados en la certificación ISO 27000 la cual reúne unas buenas prácticas para el establecimiento, implantación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información.

Dentro de la serie de artículos sobre ISO 27001 analizaremos diferentes pasos para implantar la norma. Primero realizaremos un análisis de riesgos, el cual nos permite determinar el ámbito de aplicación de la norma también denominada «declaración de aplicabilidad».

2. Análisis de riesgos & SOA

En este apartado, se deben identificar cada uno de los riesgos estableciendo los controles apropiados para gestionar el riesgo de manera sistemática de forma que consideremos todos los aspectos importantes para la empresa.

Nos encontramos ante la parte más compleja de la norma; pero al mismo tiempo la evaluación del riesgo y su tratamiento es el paso más importante en su proyecto de seguridad de la información. Aquí se establecen las bases para la seguridad de la información en la empresa.

Si nos preguntamos acerca del motivo de la importancia de este paso podemos afirmar que la filosofía de la norma ISO 270001 es:

> *Identificar las consecuencias de los posibles incidentes, o lo que es equivalente: «evaluar los riesgos». De esta forma, podremos determinar las formas más adecuadas para evitar este tipo de incidentes, es decir: el tratamiento de los riesgos.*

Sin embargo, esto no es suficiente, ya que debemos no solo identificar los riesgos, si no que debemos valorar la importancia de estos de forma que nos centremos en los más importantes y demos el tratamiento de forma ponderada a la importancia de cada uno.

2.1 Selección de metodología

El primer paso es determinar una metodología de evaluación de riesgos adecuada para cada empresa. En general podemos decir que deberíamos tener en cuenta para ello:

- Integración: Elegir una metodología aplicable a toda la empresa, o lo que es lo mismo que pueda ser aplicada a todas las partes de la organización.
- Determinar una metodología centrada en aspectos cualitativos del riesgo y cuantitativos (Escalas de medición)
- Definir los criterios de niveles aceptables de riesgos

Existen multitud de metodologías que permiten realizar todos estos procesos del análisis de riesgos. En nuestro caso hemos optado por seleccionar la metodología que propone INCIBE con un enfoque acorde a los servicios de nuestra empresa.

Esta metodología propone principalmente lo siguiente:

- Realizar un inventario de activos donde se recojan todos aquellos recursos de la empresa.
- Detallas las amenazas y vulnerabilidades que pueden poner en riesgo a los activos tomando en consideración la probabilidad y el impacto que puedan tener sobre dichos activos.

- Una vez tenemos identificados tanto los activos como sus principales amenazas y vulnerabilidades debemos evaluar los principales riesgos de la empresa y optar por tratarlo aplicando controles o aceptarlo en caso de que el coste de mitigar dicho riesgo supera el coste del daño causado por el riesgo.

2.2 Identificación de activos

Como Control de la norma ISO 27001 2017 se exige la realización de un inventario de activos, que es además la mejor manera de comenzar a trabajar. Si no sabemos lo que tenemos, nos será muy complicado gestionarlo o controlarlo correctamente. Este inventario se deberá mantener actualizado a lo largo del tiempo, por lo que se deberán realizar revisiones periódicas y comunicar los cambios.

En este caso se ha optado por dividir los activos en diferentes grupos quedando organizado de la siguiente forma:

- Personas: Product Owner y desarrolladores
- Aplicaciones y bases de datos: Conjuntos de datos, accesos a las APIs, código fuente, modelo de inteligencia artificial, aplicación web, email y sistemas de almacenamiento.
- Documentación: Digital y física.
- TI, comunicaciones y demás equipamiento: Ordenadores y dominio web
- Infraestructura física: Lugar de desarrollo del producto
- Infraestructura lógica: Cuenta en AWS y Google Cloud
- Servicios tercerizados: Suministro de energía eléctrica, mantenimiento de equipo de TIC, mantenimiento de sistemas de información y servicios de correo

2.3 Identificación de amenazas

Otro aspecto clave a la hora de realizar un análisis de riesgos según INCIBE es la identificación de amenazas. Por este motivo procedemos a listar en diferentes categorías algunas de las muchas amenazas que pueden suceder a nuestra empresa:

- Desastres naturales: Fuego, daños por agua, contaminación electromagnética, desastres naturales, pandemias…
- Fallos de sistemas informáticos: Con estos nos referimos a errores que afecten al hardware de los distintos servidores o equipos de la empresa, como pueden ser los ataques externos
- Errores humanos: Fallos accidentales o provocados por las personas que trabajan con la infraestructura de la organización.

Cabe destacar, que el listado detallado se encuentra en la tercera hoja del fichero xlsx adjunto a este documento.

2.4 Identificación de vulnerabilidades

Tras identificar tanto los activos como las amenazas es hora de analizar las posibles vulnerabilidades o puntos débiles de nuestra empresa. En las siguientes líneas se procederá a listar algunas de las vulnerabilidades encontradas en nuestra empresa:

- Relacionadas con los trabajadores: Descargas de internet sin control, uso de contraseñas inseguras, conexiones a la red sin protección…
- En los sistemas informáticos y comunicaciones: Uso de versiones del sistema operativo desactualizadas y con vulnerabilidades públicas o incluso uso de software con errores de configuración.
- Errores humanos: Baja o nula formación en las herramientas utilizadas en la organización.

Nos parece interesante destacar que el listado detallado de las vulnerabilidades se encuentra en la cuarta hoja del fichero xlsx adjunto a este documento.

2.5 Identificación de controles

Con el fin de identificar los controles necesarios se ha recurrido al anexo A de la norma ISO 27000. El Anexo A de la Norma ISO 27001 es probablemente el anexo más famoso de todas las normas ISO porque provee una herramienta esencial para la gestión de la seguridad: una lista de los controles (o medidas) de seguridad que pueden ser usados para mejorar la seguridad de la información.

Estos controles serán aplicados (o no) dependiendo del riesgo que suponga para la empresa.

Cabe destacar, que el listado detallado se encuentra en la sexta hoja del fichero xlsx adjunto a este documento.

2.6 Definición de escalas de impacto – probabilidad

La definición de probabilidad – impacto es una herramienta de análisis cualitativo de riesgos que nos permite establecer prioridades en cuanto a los posibles riesgos de un proyecto en función tanto de la probabilidad de que ocurran como de las repercusiones que podrían tener sobre nuestro proyecto en caso de que ocurrieran.

Estas han sido definidas en la última hoja del fichero adjunto.

2.7 Evaluación de riesgos

Tras definir es hora de realizar una evaluación de los riesgos, en este apartado únicamente destacaremos los riesgos más "interesantes", para una visión general, por favor, recurrid al análisis detallado.

Los activos que mayor riesgo presentaban han sido por un lado el servidor de dominio ya que este es vulnerable a la amenaza de la denegación del servicio, lo que provocaría una interrupción del servicio. Esto provocaría pérdidas económicas para la empresa.

Por otro lado, otro de los activos que mayor riesgo tenían en la empresa era el Router ya que corría con el riesgo de que gente externa a la organización accediera a la red, pudiendo robar información confidencial.

2.8 Declaración de aplicabilidad (SOA)

La declaración de aplicabilidad es el documento central que define cómo implementará una gran parte de la seguridad de la información de la empresa.

De hecho, la declaración de aplicabilidad es el nexo principal entre la evaluación y el tratamiento del riesgo y la implementación de su sistema de seguridad de la información.

El objetivo de este documento es definir cuáles de los controles (medidas de seguridad) sugeridos en el Anexo A de la norma ISO 27001 son los que se implementarán y, para los controles que correspondan, cómo se realizará su implementación.

Estos son unos de los motivos por los que este documento es importante:

- Durante el análisis de riesgos se han identificado los controles que debían implementarse porque primero identificaron los riesgos que era necesario disminuir. Sin embargo, en la declaración de la aplicabilidad también se identifican los controles necesarios por otras razones; por ejemplo, por motivos legales, por requisitos contractuales, por otros procesos, etc.
- Por otro lado, el Informe sobre la evaluación de riesgos puede resultar bastante largo: algunas organizaciones pueden identificar algunos riesgos. Por eso, un documento de estas características no resulta realmente útil en el uso diario. En cambio, la declaración de aplicabilidad es bastante breve ya que tiene 133 filas (cada una representa un control); esto permite que pueda ser presentada ante la gerencia y que pueda ser actualizada.

- Por último, y más importante, la declaración de aplicabilidad debe documentar si cada control aplicable ya está implementado o no. Una estrategia efectiva, y que la mayoría de los auditores buscará, también es describir cómo se implementa cada control aplicable; por ejemplo, haciendo referencia a un documento (política, procedimiento, instrucciones de funcionamiento, etc.) o detallando brevemente el procedimiento vigente o el equipo que se utiliza.

De hecho, si solicita la certificación ISO 27001, el auditor tomará la declaración de aplicabilidad y recorrerá la empresa verificando si ha implementado los controles de la forma detallada en el documento. Es el principal documento que utilizan para realizar la auditoría presencial.

Dicho esto, comentemos unos aspectos remarcables de nuestra declaración de aplicabilidad:

- Por un lado, la modalidad de teletrabajo se encuentra parcialmente implementada debido a que ha sido una medida adoptada recientemente debido a la pandemia que se está sufriendo actualmente. En este caso podemos decir que el entorno nos ha hecho adaptarnos y adoptar medidas que en un momento no estaban contempladas y estas medidas se ven claramente reflejadas en la declaración de aplicabilidad.
- Por otro lado, la devolución de los activos no está contemplada, pero si planificada ya que actualmente en la organización no existe ninguna política definida de transferencia y borrado de datos de los equipos devueltos por los trabajadores que dejan de hacer uso de estos activos.