UNIVERSIDAD REY JUAN CARLOS

ESCUELA SUPERIOR DE INGENIERÍA INFORMÁTICA

INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN

Curso Académico 2009/2010

Proyecto de Fin de Carrera

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Autor: LAURA MARTÍN IGLESIAS

Tutor: JAVIER MARTINEZ MOGUERZA

1. RESUMEN

El proyecto consiste en realizar un Diseño de un Sistema de Seguridad de la Información (SGSI) de acuerdo con la norma ISO 27001 para una empresa de Servicios de gestión y almacenamiento de volcado de datos.

El objetivo principal es obtener un SGSI que permita garantizar el nivel de seguridad en el manejo de la información requerido para este tipo de servicios y que esté listo para obtener la certificación ISO/IEC 27001 2005, 6 meses después de su implantación mediante una auditoria externa a desarrollar por su compañía como BSI o DNV.

Primeramente se realizará una descripción general del SGSI cuyos puntos principales serán: la definición del escenario y el desarrollo del modelo Plan-Do-Check-Act (PDCA). A continuación, se definirá el estado de aplicabilidad del SGSI con la fijación de los controles para los puntos de la norma aplicables.

Posteriormente, realizaremos el proceso de gestión de riesgos y el consiguiente plan de acción con los controles asociados.

Tras plantear una visión global del proyecto, se realizará el plan de continuidad del negocio para garantizar la fiabilidad adecuada a los clientes en cualquier circunstancia y el plan de implantación para asegurar la certificación en el tiempo previsto.

2.ÍNDICE

1. RESUMEN.....2

2. ÍNDICE..... 3

3. INTRODUCCIÓN.....6

3.1. LA SEGURIDAD DE LA INFORMACIÓN.....6

3.2. LA CONTINUIDAD DEL NEGOCIO.....7

4. ESCENARIO.....8

4.1. RADIOGRAFÍA DE LA EMPRESA.....8

4.1.1. PERFIL.....8

4.1.2. SERVICIOS.....9

4.1.3. ESCENARIO.....11

4.1.3.1. ENTORNO FÍSICO.....11

4.1.3.2. ENTORNO DE APLICACIONES.....13

4.1.4. ESTRUCTURA.....14

4.1.4.1. DIAGRAMA EMPRESARIAL.....14

4.2. METODOLOGÍA EMPLEADA.....16

4.2.1. DEFINICIÓN DE SGSI.....16

4.2.2. LA NORMA ISO 27001.....18

5. PROCESO DE DISEÑO.....20

5.1 DESCRIPCIÓN GENERAL DEL SGSI.....21

5.1.1. DEFINICIÓN GENERAL DEL SGSI.....21

5.1.2. POLÍTICA DEL SGSI.....21

5.1.3. GESTIÓN DE RIESGOS.....22

5.1.4. AUTORIZACIÓN DE LA DIRECCIÇON Y ESTABLECIMIENTO DE OBJETIVOS.....22

5.1.5. ESTADO DE APLICABILIDAD.....23

5.1.6. IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI.....23

5.1.7. MONITORIZACIÓN Y REVISIÓN DEL SGSI.....24

5.1.8. REQUISITOS DE LA DOCUMENTACIÓN DEL SGSI..25

5.1.9. COMPROMISO DE LA DIRECCIÓN.....26

5.1.10. PLANIFICACIÓN DE AUDITORÍAS.....26

5.1.11. REVISIÓN DEL SGSI.....27

5.1.12. MEJORAMIENTO DEL SGSI.....27

5.2. GESTIÓN DE RIESGOS.....28

5.2.1. PROPÓSITO.....28

5.2.2. ESTRUCTURA.....29

5.2.3. DESCRIPCIÓN.....30

5.3. ESTADO DE APLICABILIDAD.....36

5.4. OTROS PROCEDIMIENTOS DE SEGURIDAD.....38

5.4.1. PROCEDIMIENTO DE SEGURIDAD.....38

5.4.2. ESTRUCTURA DE LA ORGANIZACIÓN.....39

6. PROCESO DE IMPLANTACIÓN.....41

6.1. INICIO. COMPROMISO DE LA DIRECCIÓN.....41

6.2. IMPLANTACIÓN DEL SGSI EN LA ORGANIZACIÓN.....42

6.3. EVALUACIÓN DE RIESGOS.....44

6.4. TRATAMIENTO DE RIESGOS.....49

6.5. PLAN DE SEGUIMIENTO DEL SGSI.....50

7. PROCESO DE OPERACIÓN.....51

7.1. IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGO.....51

7.2. GESTIÓN DE INCIDENTES.....54

8. PLAN DE MONITORIZACIÓN Y POSIBLES MEJORAS.....55

8.1. EVOLUCIÓN DEL ESTADO DE LOS RIESGOS.....56

8.2. OTROS MEDIOS.....58

9. CONCLUSIONES.....58

10. BIBLIOGRAFÍA.....61

3. INTRODUCCIÓN

La informática y su contribución al progreso de las redes de comunicaciones han permitido avanzar en la sociedad y mejorar las condiciones de vida. Como consecuencia, se han introducido conceptos como el de TIC (Tecnología de la Información y la Comunicación) asociado a las tecnologías de información y comunicación pero también a un sector económico que cada vez adquiere más importancia, sobre todo en las sociedades más desarrolladas.

Esta revolución ha influido en todo los campos, tanto sociales como privados y ha creado la Sociedad de la Información donde han ido cambiando paulatinamente los procesos de generación de bienes y servicios en todos los sectores de producción.

Centrándonos en el campo de producción de bienes y servicios, un impacto de esta magnitud ha provocado efectos que han afectado a todas las empresas, en unas más que en otras. Vamos a destacar dos de estos efectos, los cuales son las que más interesan en nuestro proyecto: la seguridad de la información y la continuidad del negocio.

3.1. LA SEGURIDAD DE LA INFORMACIÓN

En la Sociedad de la Información, lógicamente, la información es uno de los activos más valiosos tanto para las personas como para las empresas. Por ello, existe la necesidad de protegerla con lo cuál adquiere una gran importancia el definir lo que es la seguridad de la información en este tipo de sociedad. Es en este contexto que aparecen los conceptos de confidencialidad, integridad y disponibilidad de la información, como elementos que integran la seguridad de la información.

En este escenario se introduce el término SGSI que son las siglas que hacen referencia a un Sistema de Gestión de la Seguridad de la Información, una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones porque les proporciona la metodología para definir un modo de garantizar la confidencialidad, la integridad y la disponibilidad de su información.

Los requisitos de seguridad de una organización, da igual el tamaño, están derivados de tres fuentes principales y deben estar documentados en el SGSI:

-El conjunto de riesgos que, si suceden, conducirían a una pérdida importante.

-Los requisitos legales y normativos que han de ser satisfechos por la organización, sus socios y sus proveedores.

-El conjunto de objetivos, principios y requisitos para el proceso de información que una organización haya desarrollado para apoyar sus operaciones de negocio.

El SGSI no es un sistema estático sino que para que sea útil ha de ser revisado y mejorado continuamente por lo tanto la gestión de la seguridad de la información es un proceso de mejora continua.

Las organizaciones deben planear y gestionar los procesos necesarios para garantizar la mejora continua del SGSI. Deben facilitar esta mejora continua a través de la revisión del SGSI mediante la definición de objetivos, resultados de las auditorias, análisis de los datos, acciones correctoras y preventivas y la revisión por la dirección.

Ante el interés por implantar el SGSI se han desarrollado standares con el fin de unificar criterios y ofrecer una normativa que pueda ser seguida por toda la empresa que así lo desee.

Todo lo anterior es el concepto central sobre el que se define la norma ISO 27001, esta normativa es el standard que provee la organización ISO para facilitar la definición, implantación y desarrollo de un SGSI.

La organización deberá asegurar que proporciona los recursos adecuados para implementar los requisitos y procesos identificados en la norma ISO 27001:2003. También debe asegurar que los empleados obtengan la formación precisa.

3.2. LA CONTINUIDAD DEL NEGOCIO

Se preocupa por seguir ofreciendo los servicios o productos que genera la empresa después de una contingencia que pueda ser más o menos grave.

Este concepto que siempre ha estado presente en los empresarios más competentes se ha visto afectado por la importancia que ha adquirido la TIC y por la llegada de la Sociedad de la Información.

En este nuevo escenario, la información que se maneja se ha destacado como uno de los activos más importantes de las empresas. Por ello, se introduce

el concepto de BCP (Business Continuity Plan) que puede definirse como el proceso que las empresas definen para poder recuperarse de una situación de contingencia lo antes posible y empezar a funcionar con unas condiciones mínimas aceptables.

Y, como en el caso anterior de seguridad de la información, los standares se han preocupado por intentar ofrecer una normativa que pueda ser seguida por toda la empresa que así lo desee para desarrollar un plan que garantice la continuidad del negocio después de una contingencia.

En el presente proyecto vamos a aplicar estos dos conceptos fundamentales en la actual sociedad de la información a un caso real: vamos a desarrollar un Sistema de Gestión de la Seguridad de la Información (SGSI) aplicando el concepto de mejora continua y basada en el estándar de ISO 27001 para una empresa que ofrece un servicio fundamental para la continuidad del negocio como es ofrecer a otras empresas un "second location" para custodiar sus bases de datos y sistemas de aplicación.

4. ESCENARIO

4.1. RADIOGRAFÍA DE LA EMPRESA

4.1.1. Perfil

SeBackSA es una compañía que ofrece servicios de custodia y mantenimiento de backup de datos y sistemas de aplicación a otras empresas o particulares. La función principal de **SebackSA** es ofrecer un medio seguro y fiable donde los usuarios puedan confiar sus datos y sus sistemas de aplicación para en caso de necesidad recuperarlos y obtener todo lo necesario para poner en marcha su negocio de nuevo de modo rápido y sencillo.

SebackSA ofrece a sus usuarios la oportunidad de volcar sus datos en su propio centro de datos, vía internet. Sus servicios incluyen volcados de datos desde 250 megabytes hasta 2 terabytes. Presenta, además la posibilidad de guardar los archivos en un entorno aislado, en un lugar a salvo de cualquier tipo de desastre.

Tan importante como el hecho de ofrecer una alternativa para que una compañía pueda recuperarse de cualquier tipo de desastre y reiniciar su actividad sin

problemas insalvables, es ofrecer también un medio seguro, sin acceso desde la red, resguardado de cualquier intento de acceso no autorizado a la información incluida en los ficheros de los usuarios.

En definitiva **SebackSA**, es una compañía orientada a los usuarios con plan de continuidad de negocio definido o que requieran un segundo lugar de almacenamiento con unas condiciones de seguridad óptimas.

Para garantizar la calidad del servicio, **SeBackSA** orienta su oferta en tres sentidos: **confidencialidad, integridad y disponibilidad**.

Busca ser un servicio que ofrezca **una confidencialidad adecuada**, lo que significa ofrecer garantías de que el objeto confiado, en este caso la información y los sistemas de aplicación se mantendrán bajo custodia, lo que implica no solo prevenir el robo sino el aseguramiento de las condiciones de acceso solo a autorizados.

Tan importante como la confidencialidad, es la integridad por lo que **SeBackSA** provee un sistema que garantice la devolución en el momento que el usuario lo requiera, en las mismas condiciones en que se entregó lo que implica mantener el producto en un medio adecuado para evitar tanto su corrupción como su modificación por personal no autorizado.

El tercer punto en que **SeBackSA** basa su negocio es **en garantizar la disponibilidad de la información** por parte del usuario en el momento que éste lo requiera. Lo que implica disponer de una infraestructura tecnológica acorde con el servicio que se presta y que implica contar con servidores de correo electrónico, de bases de datos, de web etc, mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc.

4.1.2. Servicios

SeBackSA ofrece a sus potenciales usuarios dos tipos de servicio de custodia: en red o aislado.

Tipo de servicio on line. Es un servicio automático en que el usuario es el que maneja su propia información, se ofrece la posibilidad de que almacene sus backups en

nuestros servidores, accediendo de modo automático y facilitándole diferentes medios de encryptación con lo que el manejo de la información es del propio usuario.

SeBackSA no facilita más que los medios y el mantenimiento, una partición en sus discos para que el usuario sea quien lo maneje. Es un alquiler de espacio con restricciones de acceso, en las que el usuario mantiene el control sobre el acceso. Además, se le facilita la posibilidad de que almacene la información de modo encryptado si así lo estima conveniente y del manejo de los códigos de acceso.

Dadas las condiciones de este servicio se apunta como principal ventaja destacable la disponibilidad del acceso ilimitada y manejo de la información exclusivamente por parte del propio usuario o de quien él autoriza, mientras que el principal inconveniente es el grado de incertidumbre sobre la seguridad de la red, ya que los ataques y accesos de hacker permanecen latentes. Las aplicaciones de seguridad son más completas cada vez y las actualizaciones y respuestas ante nuevo malware son casi continuas, pero aunque la probabilidad de acceso no autorizado es cada vez menor, no es cero.

En definitiva, un servicio indicado para aquellos usuarios donde prima la accesibilidad sobre la seguridad, es el servicio complementario ideal para el Plan de Continuidad de Negocio de cualquier compañía o particular.

Tipo de servicio en entorno aislado. Es un servicio que consiste en custodiar los archivos del usuario en un lugar aislado de la red, con unas condiciones de seguridad que eviten el acceso a personal no autorizado y donde la información se mantiene igualmente a salvo de desastres naturales como fuegos o terremotos. En este caso el manejo de la información incluye el transporte de la misma hasta su lugar de almacenamiento para lo que la compañía ofrece diferentes medios siendo el cliente el que en última instancia decide. En este caso, el manejo de la información es compartido por el usuario y **SeBackSA**. La responsabilidad de la compañía comienza desde el momento que recibe los ficheros hasta, bajo requerimiento del usuario, devuelve los ficheros de información confiados. En consecuencia solamente **SeBackSA** accederá al lugar donde la información es almacenada y custodiada.

En este tipo de servicio prima la seguridad, desde el momento que la información se almacena en su lugar aislado, fuera de la red, y con las condiciones de seguridad adecuadas para evitar el acceso a personal no autorizado. En este caso, el

nivel de confidencialidad es prioritario sobre el de accesibilidad, aunque esto no quiere decir que no se adapten los procesos para ofrecer las condiciones de accesibilidad más óptimas para el usuario.

En este servicio se ofrecen diferentes niveles de confidencialidad desde entorno aislado hasta ignífugo es una alternativa para usuarios que necesitan disponer de un "second location" para datos muy confidenciales.

4.1.3. Escenario

Para poder ofrecer el servicio con las condiciones de calidad adecuadas, **SeBackSA** dispone de las siguientes instalaciones**.**

4.1.3.1 Entorno físico

Instalaciones localizadas en un edificio de oficinas con acceso restringido, una compañía de seguridad se encarga de mantener el control de acceso tanto al personal permanente como al temporal.

Ocupa la planta sótano del edificio con una única puerta de entrada, dispone de dos cuerpos de oficinas, uno el más cercano a la salida donde se ubican los departamentos encargados de las actividades de soporte al negocio: jurídicas, económicas y de gestión de recursos, marketing y gestión de clientes y proveedores.

Un segundo cuerpo con un nivel de seguridad más restrictivo, localizado en la parte menos accesible, donde se llevan a cabo las actividades principales del negocio: mantenimiento y custodia de las instalaciones donde se localizan la información y las aplicaciones de los clientes.

El acceso a este segundo cuerpo es restringido por clave, y solo puede acceder personal autorizado. El personal con autoridad para acceder es de la propia compañía, dispone de un código de acceso personal y ha firmado un compromiso específico que le obliga a no sacar, ni divulgar nada de la información custodiada.

La instalación principal de este segundo cuerpo de oficinas es la sala de operaciones donde se ubican las redes y el mobiliario donde se guarda la información confiada por los clientes.

La sala de operaciones está localizada en la parte más segura del edificio y a ella se accede por una puerta acorazada. El acceso es mediante clave personal y solo tiene acceso el personal de la compañía que maneja los sistemas de aplicación, las redes y los medios de seguridad donde se custodia la información de los clientes.

Otros medios de seguridad que protegen el acceso a la sala es una cámara de televisión de circuito cerrado controlada desde la garita de acceso al edificio, esta cámara esta conectada a un sistema de grabación supervisado desde la garita que guarda las imágenes. Además se dispone de un sistema de alarma que protege el acceso a las instalaciones.

Las instalaciones contenidas en la sala de operaciones son de dos tipos mobiliarias e informáticas.

- Mobiliarias: Armarios, Caja fuerte, Caja fuerte ignífuga.
- Informáticas: Servidores, y discos duros principalmente

Las instalaciones mobiliarias principales, son los armarios. Son dos armarios de seguridad marca SecureLine, modelo Secure SC-1, anclados al suelo, donde se almacenan, aparte de la información facilitada por los clientes en cualquier tipo de soporte, los volcados de datos de los discos duros de los servidores donde se almacena la información de los clientes que ha requerido el servicio de custodia online.

Existen igualmente cajas fuertes, para aquellos clientes que requieren un servicio de custodia en un entorno doblemente aislado, donde las condiciones de confidencialidad y de integridad son especialmente garantizadas. Incluye dos tipos de cajas fuertes:

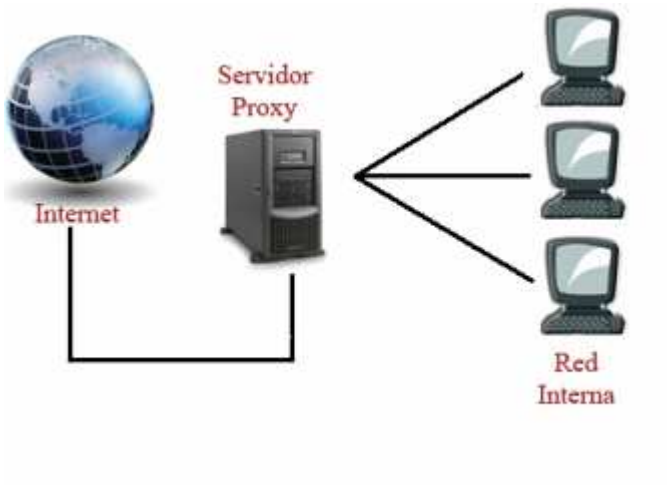
- Caja fuerte SENTRY QE 4531. Indicada para almacenar la información de usuario facilitada en soportes de CD y DVD.
- Caja fuerte CHUBB DuoGuard 60. Donde se almacenan la información del usuario facilitada en soporte de disco duro.

También conviene destacar un archivador ignífugo CHUBB 23-2, 60 P donde se almacenan la información especialmente sensible que es principalmente los contratos de los clientes y los compromisos de confidencialidad de los empleados y otras informaciones en soporte de papel de similar importancia.

4.1.3.2 Entorno de aplicaciones

La función principal del entorno de aplicaciones es dar servicio a los usuarios interesados en el servicio de online y mantener la página Web y el servicio de contacto con clientes y marketing para nuevos contactos y consultas, aparte de las funciones de mantenimiento.

Para el servicio online, la información del cliente va a residir en nuestro entorno con un acceso inmediato y para el resto se ha de proveer un servicio de consultas como de captación de nuevos clientes. Para cubrir estas necesidades se ha puesto en marcha la red que se indica a continuación.



Servidor

- NIS, Backup y discos.
- Dell Precision T3500
- RAM 24 GB
- Windows XP

3 puestos de trabajo clientes del servidor principal.

- Estaciones de Trabajo.
- Dell Precision T1500
- RAM 8 GB
- Windows XP

El entorno de la red contiene todas las herramientas y aplicaciones para ofrecer el servicio, en este sentido destacamos:

Symantec Backup Exec. Para gestionar los volcados de datos de los clientes sobre un disco duro externo y disponer de un segunda copia en caso de desastre. Esta aplicación está también indicada para el volcado online (electronic voulting) que, gestionado por el propio cliente, almacena los datos en un *second location* en un entorno seguro.

DPM 2010, (Data Protection Manager). Es el Nuevo standard de Windows para la protección de datos tanto en el volcado como en la recuperación de los mismos y es válido para todas las aplicaciones de Microsoft incluyendo Exchange, SQL Server y file servers.

Se dispone además de un juego de discos duros **IOSafe Solo USB** de 2TB, 1,5 TB y 500Gb. Compatibles con Windows XP e ignífugos en los que se vuelcan los datos de la red y de los clientes.

4.1.4. Estructura

4.1.4.1 Diagrama empresarial

Para llevar a cabo su cometido **SeBackSA** esta organizada en varias unidades que se indican a continuación:

- Unidad de gestión jurídica
- Unidad de gestión de clientes
- Unidad administrativa (externa)
- Unidad de gestión de seguridad (seguridad y SGSI)
- Unidad de seguridad (externa)
- Unidad informática (hosting, red y Web, mantenimiento de sistemas)
- Unidad de mantenimiento de edificios (externa)

Las unidades son de carácter funcional, por lo que existe la posibilidad que se compartan recursos porque, en principio, hasta que la compañía se consolide en el sector se persigue la optimización de recursos y el máximo aprovechamiento de la competencia de los miembros de **SeBackSA**, con lo que más de un miembro estará implicado en más de una unidad.

Las unidades más importantes y sus funciones más destacadas se indican a continuación:

Unidad de gestión de clientes

Principal interfaz desde que se establece el primer contacto, el interfaz principal cara a los clientes, y además los encargados de llevar a cabo las políticas de marketing y de captación de nuevas oportunidades de negocio.

Unidad de gestión jurídica

Unidad principal para dar soporte jurídico y legal. Necesaria en dos sentidos:

- Cara a los clientes. Para proteger la información confidencial de la empresa cuando es tratada por un tercero es necesario firmar un contrato de prestación de servicios en las que se establezcan las condiciones del tratamiento y especialmente las obligaciones de confidencialidad y secreto. Esta unidad es la que establece los compromisos de confidencialidad para que estén de acuerdo con la legalidad, tanto a nivel nacional como internacional.
- Cara a los propios trabajadores de la compañía. Ya que es necesario mantener compromisos de confidencialidad que obliguen a manejar la información tanto de los clientes como de la propia compañía con las debidas garantías.

Unidad de gestión de la seguridad

Es la unidad clave para sacar adelante el SGSI. Debe de:

- Dar soporte al equipo de dirección en implementación de estrategias que cubran los procesos en donde la información es el activo primordial.
- Fijar el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.
- Diseñar, planificar, operar y mejorar el SGSI en la línea con ISO 27001.
- Extender los procesos y procedimientos al resto de las unidades.
- Efectuar el seguimiento en la implantación del SGSI y corregir cualquier desviación de los objetivos previstos en el mismo.
- Preparar la certificación del SGSI.

Es fundamental aquí disponer de una competencia muy profunda en SGSI y en ISO 27001.

Unidad informática

Es una de las unidades clave del negocio, sus funciones principales son:

- Mantenimiento de la red y los soportes de almacenamiento.
- Configuración de las aplicaciones en función de las necesidades de los clientes.
- Configuración y mantenimiento de las páginas Web de SeBackSA.
- Mantenimiento de la red de contactos y bases de datos de clientes.
- Soporte técnico a la unidad de gestión de clientes.

Equipo de Dirección.

Equipo formado por los responsables de cada una de las unidades de la compañía y el director. Su principal función es la gestión de la compañía, incluyendo la fijación de la estrategia y de la fijación de los objetivos y el seguimiento de los mismos, así como la creación y actualización de los planes de negocio, incluyendo el de continuidad del mismo en caso de desastre.

Cara a la seguridad, es la unidad fundamental ya que para poder sacar adelante el SGSI se requiere la implicación del equipo de Dirección, bien a través de todo el equipo o de la persona, miembro del mismo, en la que se delega esta función.

4.2. METODOLOGÍA EMPLEADA

4.2.1. Definición de SGSI

SGSI son las siglas que hacen referencia a un Sistema de Gestión de la Seguridad de la Información, una herramienta de gran utilidad y de importante ayuda para la gestión de la seguridad de la información en las compañías independientemente de su tamaño, complejidad y sector de negocio.

Como ya se ha indicado, la información es uno de los activos más importantes de las compañías y, por lo tanto, es algo que esta sujeto a riesgo tanto dentro de la

organización como fuera. Por lo tanto, la preservación de la confidencialidad, integridad y disponibilidad de este activo es fundamental.

El modo mas adecuado para garantizar la conservación de este activo y mantenerlo a salvo de accesos no autorizados consiste en una gestión orientada a minimizar el impacto de los riesgos potenciales y para ello, lo primero es conocerlos y afrontarlos de forma ordenada. Seguidamente, teniendo en cuenta una evaluación de los mismos, habrá que definir unos procedimientos adecuados y planificar e implantar controles de seguridad.

Por lo tanto se trata de un sistema que permita establecer los criterios de seguridad, definir el modelo de acuerdo con esos criterios, desarrollar los procesos y controles, implementarlos en la organización, ponerlos en marcha, supervisar su operación, revisión del sistema de acuerdo con el resultado de la supervisión , establecer los programas de mejora e incluirlos en el sistema.

El Sistema de Gestión de la Seguridad de la Información (SGSI) en las empresas ayuda a establecer estos procedimientos, con el objetivo de mantener siempre el nivel de riesgo por debajo del nivel de seguridad de la propia organización. Para los responsables de las organizaciones, esta herramienta es muy útil, ya que les sirve para obtener una visión global sobre el estado de los sistemas de información, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de dicha aplicación. Todos estos datos permiten a la dirección una toma de decisiones sobre la estrategia a seguir.

Dada la importancia de la información y de la necesidad de preservar el establecimiento del SGSI debe de ser una decisión estratégica para una compañía con lo que esto representa en cuanto al grado de implicación de todos los escalones de la organización.

El SGSI puede ser como el usuario quiera desde el momento que la preservación del sistema de información es una necesidad que es independiente del tamaño de la empresa o del sector al que se dedica. El diseño y la implementación del SGSI dependerá de la empresa donde se vaya a introducir, ella deberá ajustarlo a sus necesidades y objetivos y en función de ellos deberá definir los procesos y el grado de exigencia en los controles de seguridad a aplicar.

Tan importante como el diseño de un SGSI que se ajuste a las necesidades de la empresa es el que sea un sistema abierto que permita las adaptaciones necesarias bien para mejorarlos o bien para actualizarlo de acuerdo con las nuevas necesidades de la empresa.

En definitiva, es un sistema para establecer, implementar, operar, supervisar, revisar, mantener y mejorar las condiciones de preservación de la información en cuanto a confidencialidad, integridad y disponibilidad. Un sistema que se ajuste a las necesidades de cada compañía y que permita su actualización continuamente.

4.2.2. La norma ISO 27001

Cuando una necesidad se generaliza, se tiende a definir un modelo que pueda ser utilizado como patrón para que cada cual lo pueda adaptar a su perfil particular. Este modelo general es el standard y existen organizaciones internacionales que son las que establecen dichos standares. ISO es el standard internacional y la ISO 27001/2005 es el modelo standard desarrollado por ISO para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI de una organización, independientemente de su perfil.

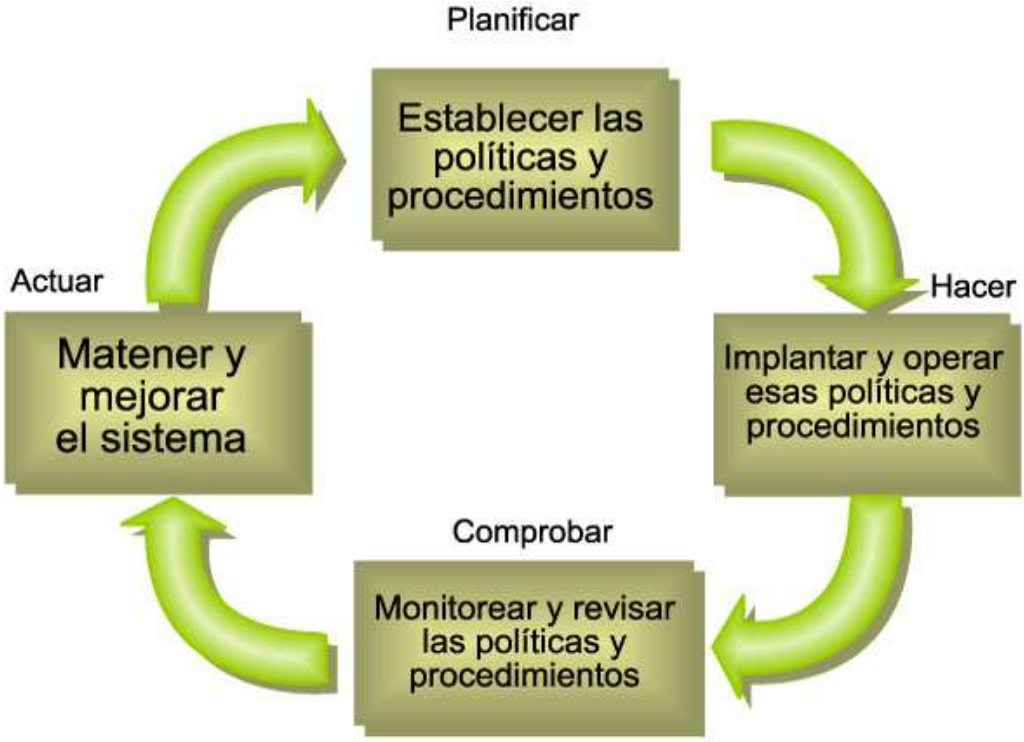
El modelo de SGSI propuesto por ISO está orientado a procesos, entendiendo como proceso el grupo de actividades que permite transformar unas determinadas entradas en productos mediante el uso de recursos, dotando al producto de salida de un determinado valor añadido. La gestión que sistematiza y organiza las actividades dentro de un proceso así como la interacción entre procesos determina el sistema de gestión de los procesos.

La ISO 27001 define las pautas para poder diseñar un sistema de gestión de seguridad de la información, atendiendo principalmente a

- Delimitar claramente los requisitos de seguridad, definiendo los objetivos y la política de seguridad.
- Evaluar los riesgos de modo sistemático mediante:
    1. Identificación y valoración de activos.
    2. Identificación y valoración de amenazas y vulnerabilidades asociándolas a los activos.
    3. Cálculo del riesgo.
    4. Identificación de la opción de tratamiento de riesgo.
    5. Selección de controles para reducir los riesgos a nivel aceptable.

- Definir, implementar y supervisar los controles que permiten hacer un seguimiento de la evolución de los riesgos.
- Supervisar y verificar la eficiencia del SGSI implementado.
- Adoptar de un sistema de mejora continua para mantener el SGSI actualizado y acorde con la evolución de las necesidades de la organización.

ISO 27001 está basado en el modelo de proceso Planear-Hacer-Chequear-Actuar (PDCA) que se resume en la figura adjunta.



Aplicando el modelo PDCA las etapas del SGSI definido por la ISO 27001 es como sigue:

Plan: Establecimiento del SGSI. Pautas más importantes

- Delimitación del escenario que cubre el SGSI.
- Definición de la política de seguridad incluyendo objetivos y estrategia de gestión de riesgos.
- Diseño del método de gestión de riesgos.
- Evaluación de riesgos inicial, delimitación de riesgo residual.
- Estado de aplicabilidad, definición de controles y excepciones.

Hacer: Implementación y operación del SGSI.

- Plan de acción para el tratamiento de los riesgos.

- Implementación de los controles.
- Formación y adiestramiento.

Chequear: Supervisión y verificación del SGSI

- Seguimiento de los objetivos marcados.
- Adaptación de buenas prácticas.
- Programas de revisiones y auditorias.

Actuar: Mejoramiento y actualización del SGSI

El hecho de que un SGSI este certificado por la norma ISO 27001 aporta a la organización las siguientes ventajas:

- Demuestra a los clientes que la seguridad de su información es lo primordial.
- Analiza los riesgos de la organización, evaluándolos y gestionándolos al tiempo que formaliza unos procedimientos para proteger la información.
- Demuestra que la dirección de la organización está comprometida a garantizar la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales.

En los capítulos siguientes vamos a aplicar este modelo basado en la norma ISO 27001 para definir e implementar el SGSI para la empresa **SeBackSA**

5. PROCESO DE DISEÑO

Al empezar desde cero, lo primero es diseñar la metodología y los procedimientos de seguridad que van a formar parte del SGSI. Tomando como base la norma ISO 27001 se incluye en este capítulo los procedimientos y procesos que se han diseñado para el SGSI de **SeBackSA**.

Los procedimientos principales se han incluido en subcapítulos aparte y se describen en detalle dado la importancia que tienen para la implantación y operación del SGSI y para su posterior certificación y son:

- Descripción General del SGSI.

- Proceso de Gestión de Riesgos.
- Estado de Aplicabilidad.
- Otros procedimientos.

5.1. DESCRIPCIÓN GENERAL DEL SGSI

La descripción general del SGSI es el documento principal del sistema. En él se incluye, resumido, todo el SGSI implementado en **SeBackSA**. A continuación, basado en la norma ISO 27001, se incluyen los capítulos, resumidos, de la descripción general.

5.1.1. Definición del escenario

El SGSI incluye todas las actividades y procesos encaminados a preservar la seguridad de los sistemas de información entregados por los clientes para su custodia, garantizando la confidencialidad, integridad y disponibilidad de los mismos desde que el cliente hace la entrega efectiva hasta que **SebBackSA** devuelve la información de acuerdo con los términos de la entrega acordados con cada cliente.

El servicio de conservación y custodia de los sistemas de información en un lugar alternativo es requerido por aquellos clientes (particulares o empresas) interesados en garantizar una continuidad de negocio en caso de desastre o en mantener sus sistemas de información en un lugar seguro a salvo de accesos no autorizados.

SeBackSA está en el edificio Aguamar, planta sótano en la Avda. de la Ilustración, 260, Zaragoza. 23222. España. La estructura de la organización se indica en el documento "Organización de seguridad de **SeBackSA**" que se ha resumido en el capítulo 4.1.4.2.

5.1.2. Política del SGSI

Debido a las características del negocio y a la naturaleza sensible de la información que se gestiona, es fundamental para **SeBackSA** ofrecer a los clientes potenciales argumentos sólidos y razones convincentes de que ofrecen un servicio de custodia seguro y eficiente. En este contexto, es fundamental disponer de un SGSI con la certificación ISO 27001 por parte de una entidad auditora facultada por ISO como BSI (compañía de estandarización) y el objetivo es conseguirlo en un plazo de seis meses. Las claves son:

- Diseño de los procesos de seguridad en línea con el escenario (punto 5.1.1).

- Elección en los puestos clave de personas con la competencia adecuada sobre todo el líder de seguridad y el experto SGSI (punto 5.4.2).
- Implicación de todos y concienciación en cuanto a la importancia de mantener la confidencialidad, integridad y disponibilidad de los sistemas de información.

5.1.3. Gestión de riesgos

La gestión de riesgos es una de las actividades fundamentales para fijar un plan de acción para conseguir los objetivos. En la descripción general de SGSI se hace referencia, en el punto 5.2, al método de gestión de riesgos de **SeBackSA**.

En este documento, como se verá mas adelante, se describe el método de gestión de riesgos definido, así como los criterios de evaluación para establecer qué riesgos necesitan un plan de acción definido y qué riesgos son considerados residuales y, como tales, que no requieren ninguna acción de mejora.

El análisis de riesgos se efectúa, de forma rutinaria, una vez cada seis meses en esta primera fase hasta que el sistema alcance un grado adecuado de madurez. Después, el análisis de riesgos se llevará a cabo una vez al año. De modo extraordinario se puede efectuar un análisis de riesgo si el impacto de un cambio sobre el alcance (entorno, de sistema o de recursos humanos) así lo aconseja.

La dinámica de la reunión en la que se lleva a cabo el análisis de riesgos es la indicada en ISO 27001 y se recoge en el documento "Gestión de Riesgos de **SeBackSA**".

5.1.4. Autorización de la dirección y establecimiento de objetivos.

La dirección de **SeBackSA** ha de autorizar la política y las líneas maestras del SGSI. Debe de aprobar, al menos, esta descripción general porque en él se incluyen tanto la política como los objetivos.

Se definen objetivos a largo plazo y anuales. Los objetivos a largo plazo, de carácter general, son:

- Establecimiento de un SGSI de alto nivel, certificado por BSI como prueba de que cumple con el standard ISO 27001.
- Mantenimiento del SGSI en el mismo o superior nivel, aplicando criterios de mejora continúa en todos los procesos y procedimientos.

- Establecimiento de procesos flexibles para ajustarse a los requisitos de los clientes de modo rápido y sin perder efectividad ni seguridad.
- Establecimiento y mejora continúa de las rutinas de continuidad de negocio establecidas y de acuerdo con el Standard ISO.

Sobre los objetivos de carácter anual, son más concretos y se refieren a mejoramiento en áreas específicas de trabajo, como por ejemplo, la gestión de incidentes. Los objetivos anuales son propuestos por las unidades de trabajo, prestando especial interés a los de las unidades de gestión jurídica, informática y de seguridad y han de estar en línea con los generales.

5.1.5. Estado de aplicabilidad.

El documento "Estado de Aplicabilidad del SGSI de SeBackSA" recoge todos los objetivos de control y los controles seleccionados para asegurar la correcta aplicación del SGSI de acuerdo con el Standard ISO.

Este documento se basa en el Anexo A de la norma ISO 27001, que contiene una lista exhaustiva de objetivos de control y controles que son relevantes para la mayoría de las compañías.

No todos los controles del Anexo son aplicables al SGSI de **SeBackSA,** por lo que, algunos de ellos se han excluido. En el "Estado de Aplicabilidad del SGSI de SeBackSA" se incluyen también los excluidos y la razón por la que no se han tenido en cuenta.

La dirección de SeBackSA debe de aprobar el "Estado de Aplicabilidad del SGSI de SeBackSA" para considerar este documento válido.

5.1.6. Implementación y operación del SGSI.

El SGSI de **SeBackSA** se basa en el Standard de ISO 27001 en el establecimiento del mismo. Ello implica llevar a cabo las siguientes actividades:

- **Análisis de Riesgos y Plan de Tratamiento de Riesgos (RTP).**

El análisis de riesgos facilita la situación real. Para los riesgos encontrados por encima del valor umbral se definen las acciones a tomar, los recursos a implicar y el plan de tiempos y de seguimiento. Todo ello se incluye en el Plan de Tratamiento de Riesgos (RTP). Las prioridades y las responsabilidades están también incluidas.

- **Elección de Métricas e indicadores adecuados**.

Es requisito obligado medir tanto la efectividad de las acciones tomadas como del cumplimiento de los objetivos. Esto implica definir indicadores que obtengan valores comparables y reproducibles. Los controles incluidos en el Estado de Aplicabilidad cumplen esta función.

La efectividad de los controles incluidos en el RTP se medirá al verificar la evolución del valor de cada riesgo. Se puede obtener tanto la evolución de cada riesgo de modo individual, y de modo general.

El seguimiento de los objetivos también se lleva a cabo con los controles. Procesos como la gestión de incidentes o la continuidad del negocio están muy relacionados con los objetivos y se evalúan mediante controles.

- **Formación y toma de conciencia**

La implicación y la motivación del personal es fundamental tanto para detectar agujeros de seguridad como para localizar oportunidades de mejora. La estructura de organización definida (punto 5.4.2) busca la implicación y la motivación de todos.

La competencia también es capital para adaptarse a necesidades cambiantes del negocio, tanto en el ámbito de seguridad informática, de nuevas aplicaciones y de nuevos requisitos de los clientes.

La formación se desarrolla de modo individualizado con el fin de que cada miembro obtenga la competencia adecuada. Uno de los objetivos anuales es conseguir la competencia adecuada en los miembros de las principales unidades de negocio: Jurídica, Informática y de Seguridad.

5.1.7. Monitorización y revisión del SGSI.

Los objetivos principales en la monitorización son:

- Detectar lo antes posible errores en los procesos u oportunidades de mejora.
- Detectar lo antes posible puntos débiles en el SGSI.
- Verificación de que las prácticas se hacen de modo adecuado y que se obtiene el mejor rendimiento.
- Determinación de la efectividad de los controles e indicadores implicados.
- Determinación de la efectividad de las acciones correctoras tomadas.

Los medios para hacer cumplir con estos requisitos en la compañía son:

- Reuniones periódicas de cada unidad: han de seguir la metodología indicada en el documento (Dinámica de Reuniones en Cia).
- Revisión del análisis de Riesgos: siguiendo la metodología recogida en "Gestión de Riesgos de **SeBackSA**.".
- Auditorias: se han planificado con una periodicidad anual, para verificar que el SGSI esta en línea con el standard ISO 27001. Se realizaran tres meses antes de la auditoria de certificación.
- Certificación: es uno de los objetivos principales de **SeBackSA**, para garantizar los niveles adecuados de seguridad. La primera está planificada para 6 meses después de la implantación del SGSI.
- Revisiones por parte de la dirección: especialmente orientadas a verificar el seguimiento de los objetivos y obtener feedback.
- Revisión de la efectividad del ISMS: realizada anualmente.
- Gestión de incidentes.

5.1.8. Requisitos de la documentación del SGSI

De acuerdo con las especificaciones de ISO 27001, en el SGSI se ha de documentar, al menos lo siguiente:

- Política y objetivos del SGSI (Capítulo "Política del SGSI").
- Alcance del SGSI (Capitulo "Definición del escenario").
- Procedimientos y controles.
- Descripción metodológica de la Gestión de Riesgos (Capítulo "Gestión de Riesgos").
- Informes de los Análisis de Riesgos.
- Plan de Tratamiento de los Riesgos (RTP) (Documento "Gestión de Riesgos de SeBAckSA").
- Registros de acuerdo con el standar ISO.
- Estado de Aplicabilidad (SOA) (Documento Estado de Aplicabilidad".

Como se puede apreciar la mayor parte de los requisitos que se han de documentar están incluidos en la descripción general del SGSI de **SeBackSA**.

El control de estos documentos y, en general, de toda la documentación del SGSI se ha de ajustar a unos requisitos que se resumen en:

- Los documentos han de ser revisados y aprobados por la persona autorizada, de acuerdo con la importancia del documento.

- En el caso de actualización o revisión de los documentos aprobados han de reaprobarse y mantener una gestión de versiones.
- La Unidad de Seguridad se encargará de mantener la gestión y actualización de versiones de todos los documentos del SGSI.
- Ésta unidad también se encargará de la confidencialidad, integridad y disponibilidad de cada documento del SGSI.
- La misma unidad garantizará que son almacenados, transferidos y destruidos salvaguardando el grado de confidencialidad adecuado.
- La Unidad de Seguridad también es la encargada de confirmar la identificación del origen de cualquier documento externo.

5.1.9. Compromiso de la dirección.

El compromiso de la dirección se lleva a cabo en:

- Aprobación de la política a seguir en la SGSI de **SeBackSA**.
- Aprobación de los objetivos del SGSI e implicación en su seguimiento.
- Colaboración con el experto SGSI para ayudar a alcanzar y mantener el nivel del SGSI requerido por el standard.
- Fomento de la implicación de todos tanto en el seguimiento como en la mejora continúa del SGSI.
- Colaboración en la gestión de los recursos, proporcionando los adecuados o facilitando los medios para que alcancen la competencia adecuada.

5.1.10. Planificación de auditorias.

La dirección de **SeBackSA** ha establecido un plan de auditorias con una empresa externa, la primera de las cuales esta planificada para después de tres meses de iniciar la implementación del SGSI. El objetivo principal de estas auditorias es verificar:

- Que el SGSI está en la línea con el modelo de ISO 27001 y definir las mejoras y seguimiento de aquellos puntos no conformes con la norma.
- Que el SGSI se está implementando y manteniendo de forma efectiva

Posteriormente, se procederá a auditar el SGSI una vez al año, tres meses antes de la auditoria de certificación de BSI.

5.1.11. Revisión del SGSI.

El SGSI se revisa una vez al año, de modo ordinario y, de modo extraordinario en el caso de que existan cambios significativos que puedan afectar a la efectividad o continuidad del propio SGSI. El líder de seguridad es quien tiene la autoridad para convocar esta revisión extraordinaria.

La dinámica a seguir en la revisión del SGSI esta indicada en la propia norma ISO 27001 y busca:

- Actualización del SGSI en función del feedback recibido desde la última revisión.
- Análisis de los eventos más significativos y su impacto en el funcionamiento y rendimiento del SGSI.

El resultado de la revisión será una serie de decisiones encaminadas a:

- Mejorar la efectividad del SGSI.
- Actualizar de los procedimientos y procesos incluidos en el SGSI.
- Verificar el dimensionamiento de recursos.

5.1.12. Mejoramiento del SGSI

El mejoramiento del SGSI implantado en **SeBackSA** se hace a partir de:

-Proceso de Mejora Continua.

Se hace a partir de la implicación de todos en el desarrollo de la política de seguridad, definición y seguimiento de los objetivos, participación en la preparación de las auditorias y en el análisis de los registros e incidentes detectados en el funcionamiento del SGSI. Es fundamental la colaboración de todos, sobre todo de los miembros de los equipos mas directamente implicados en la seguridad como son los de las unidades de informática, seguridad y gestión jurídica.

-Establecimiento y seguimiento de acciones correctoras.

Es uno de los principales registros para establecer posibles puntos de mejora en el establecimiento de acciones correctoras principalmente a partir de la gestión de incidentes.

-Establecimiento y seguimiento de acciones preventivas.

Se realiza principalmente por la detección de riesgos potenciales para lo cual se sigue el proceso de Gestión de Riesgos.

5.2. GESTIÓN DE RIESGOS

El método de gestión de riesgos que se va a aplicar está recogido en el documento "Gestión de Riesgos de SeBackSA"y sigue las directrices marcadas por la norma ISO IEC 13335-3 que se expone en el gráfico siguiente:

El diagrama delimita los conceptos principales que se manejan en la gestión del riesgo así como sus relaciones de dependencia. Son la base sobre la que se ha desarrollado la metodología que se va a aplicar en el SGSI.

El proceso de gestión del riesgo es una sección clave para una implementación adecuada de la norma ISO 27001, y es imprescindible para obtener la certificación. Como este es uno de los objetivos principales de **SeBackSA,** se ha prestado especial interés en incluir aquí las pautas principales del proceso. A continuación, exponemos un resumen del documento "Gestión de Riesgos de SeBackSA".

5.2.1. Propósito

El propósito del documento consiste en describir el método de Gestión de Riesgos que se va a aplicar en el SGSI de **SebackSA.** Por tanto, se ocupa de identificar los riesgos, evaluarlos en función de impacto y probabilidad, diseñar un tratamiento adecuado y efectuar el seguimiento con el fin de disminuir o evitar el impacto en el supuesto de que el riesgo se convirtiera en problema.

5.2.2. Estructura

El proceso recogido en el documento "Gestión de Riesgos de SeBackSA" esta estructurado en capítulos incluyendo las fases en las que se divide la gestión integral, que, basada en el concepto de mejora continua, empieza con la identificación y dimensionamiento de los riesgos y continua con su tratamiento y la verificación de que los riesgos se mantienen bajo control.

El proceso se divide en:

- Análisis del Riesgo (Risk Assessment).
- Tratamiento del Riesgo.
- Aceptación del Riesgo.
- Comunicación del Riesgo.
- Monitorización y Revisión del Riesgo

La estructura del proceso está en línea con el diagrama recogido en el inicio del capítulo. Por lo que, se incluye un glosario que incluye los conceptos que se manejan en el proceso, de los cuales los más importantes son:

- Activo: Todo aquello que aporta algún valor en el escenario de SGSI.
- Amenaza: Agente potencial que puede provocar daño sobre cualquier activo incluido en el escenario del SGSI.
- Vulnerabilidad: Punto débil que puede favorecer la materialización de alguna amenaza.
- Riesgo: Elemento potencial que puede provocar un daño o una pérdida sobre cualquier activo incluido en el escenario del SGSI.
- Problema: Materialización de un riesgo.
- Valor del riesgo: Está en función de la probabilidad de que se convierta en problema y del daño potencial sobre cualquier activo.
- Nivel Umbral del riesgo. El valor a partir del cual un riesgo no es admisible y requiere un plan de acción.
- Plan de Acción: Grupo de acciones que se toman para atenuar el valor de riesgo detectado. Requieren un plan de tiempo y controles seleccionados para verificar la efectividad del plan.
- Plan de Seguimiento. Grupo de controles que son verificados de forma periódica para comprobar que el valor del riesgo asociado no sobrepasa el nivel umbral, o si lo hace, definir las acciones de respuesta.

5.2.3. Descripción

Este capítulo incluye, en detalle, las fases en las que se divide el proceso de Gestión de Riesgos.

1. Establecimiento del Contexto

Fijación de los límites del escenario donde se va a llevar a cabo el análisis. De forma ordinaria, debe de coincidir con el escenario indicado en el punto primero de la descripción general del SGSI.

Cualquier cambio en el escenario implica un análisis de riesgo para ajustar el nivel de riesgo anterior al nuevo escenario.

2. Análisis del riesgo. (Risk Assesment)

Se identifican riesgos y se evalúan su magnitud. Se lleva a cabo en una reunión donde participan personas de todas las áreas estratégicas: informática, gestión jurídica y seguridad, y es dirigida por el líder de seguridad. Forman **el equipo de gestión de riesgos**. También se incluye en el equipo, alguien con competencia financiera para evaluar los costes de los activos y los impactos de cada amenaza y vulnerabilidad en términos de pérdidas financieras.

El equipo de gestión de riesgos tiene las siguientes funciones:

- Realizar el Análisis de Riesgo.
- Implicar a todos los miembros de las unidades en el conocimiento sobre el proceso y en su mejora continua.
- Realizar el Plan de tratamiento de riesgos (RTP).
- Asumir la responsabilidad de los puntos de acción que salgan como consecuencia del RTP.
- Participar en las reuniones de seguimiento del RTP.
- Participar en la asunción de controles y colaborar en la toma de medidas para verificar que el valor de los riesgos ha decrecido.

El experto SGSI da soporte al equipo de gestión de riesgos sobre la aplicación de SGSI y las normas ISO 27001-27005.

Como ya se ha indicado, las reuniones de Análisis de riesgo se van a realizar semestralmente hasta que el modelo SGSI esté efectivamente implantado. Posteriormente se llevarán a cabo anualmente.

El modo en que el Análisis de riesgo se lleva a cabo es como sigue:

- Revisión del escenario que cubre el SGSI.
- Identificación y revisión (en su caso) de los activos del escenario.

- Evaluación de los activos.
- Identificación y revisión (en su caso) de las amenazas sobre los activos.
- Evaluación de las amenazas.
- Identificación y revisión en su caso de las vulnerabilidades potenciales que pueden afectar a los activos del escenario.
- Evaluación de las vulnerabilidades.
- Análisis efectivo del riesgo.
- Aceptación del riesgo.

Revisión del escenario: centra el análisis en el objeto principal, que es el escenario, y verifica si algún cambio le ha afectado. La descripción del escenario se recoge en el punto 5.1.1 de la Descripción General del SGSI.

Identificación y revisión de los activos: consiste en crear (o actualizar) una lista o inventario con todos los activos que están incluidos en el escenario cubierto por el SGSI. Ha de incluir, las personas y su competencia, los recursos informáticos, tanto a nivel de hardware como de software, los servicios y sistemas de seguridad, bases de datos…

Es competencia del Responsable de seguridad mantener la lista de activos actualizada y, convocar un nuevo análisis extraordinario de riesgos en el caso de impactos serios sobre el inventario.

Evaluación de los activos. Los activos se evalúan de acuerdo con la importancia que para el negocio de la compañía representan. El activo se evalúa de acuerdo a un factor principal y dos factores secundarios.

El factor principal es el impacto en el negocio debido a la perdida de su confidencialidad, modificación, destrucción o no disponibilidad del activo. Y los secundarios son su coste intrínseco y su dependencia con relación a otros activos.

Y el modo de evaluarlo es aplicando a cada activo la tabla siguiente:

Impacto debido a:	Grado del impacto	IMPACTO
Acceso no autorizado	Residual (0), bajo (1), medio(2), alto(3) y muy alto(4)	
Modificación no autorizada	Residual (0), bajo (1), medio(2), alto(3) y muy alto(4)	
	Residual (0), bajo (1),	

Destrucción	medio(2), alto(3) y muy alto(4)	
No disponibilidad	Residual (0), bajo (1), medio(2), alto(3) y muy alto(4)	

Por ejemplo, el impacto de acceso no autorizado a cualquier información confiada por un cliente es de grado muy alto. El caso, de acceso no autorizado a los procesos SGSI de la compañía es de grado alto. El caso de acceder a cualquier otro proceso puede ser de grado medio. El impacto en el negocio por la pérdida de los contratos o compromisos de confidencialidad con los clientes es muy alto**,** desde el contrato de confidencialidad hasta los recursos informáticos.

Sobre el resto de los activos se mide su grado de impacto en función del esfuerzo que requiere su recuperación o su reconstrucción.

El valor del activo viene determinado por el grado de impacto más alto evaluado con relación a los cuatro: acceso no autorizado, modificación no autorizada, destrucción o no disponibilidad.

Factores secundarios que sirven para confirmar el valor del impacto son:

- **Coste** en la reposición y el mantenimiento del activo. Se revisarán para confirmar el valor del activo o para incrementar su grado de impacto.
- **Dependencia**. El valor del activo puede ser modificado al alza en el caso de que de él dependa cualquier activo de grado superior.

El resultado de esta actividad será la lista de activos con su valor que se asociará con el grado del impacto obtenido.

Identificación y revisión de las amenazas. Consiste en definir y revisar en su caso una lista de amenazas que pueden afectar a alguno de los activos incluidos en el inventario. La lista de las amenazas se hace en línea con las pautas propuestas en la norma ISO/IEC 13335-3.

El líder de Seguridad es el responsable de mantener actualizada la lista de amenazas acordada en la última reunión del Análisis de Riesgos.

Evaluación de las amenazas. Las amenazas se evalúan en función de su grado de probabilidad.

El grado de probabilidad esta en relación directa con:

- La frecuencia con la que se produce, utilizando la estadística, o una estimación sobre la probabilidad de ocurrencia.

- El grado de atracción que puede tener el activo para un posible intruso así como el grado de dificultad en la materialización de la amenaza.
- Factores intrínsecos como los geográficos, de localización....

El grado de cada amenaza se obtiene de acuerdo a la gráfica siguiente:

Grado de amenaza	Frecuencia	Atractivo	Otros factores
ALTO	Alta Media Alta	Alto Alto Medio	Alto Medio Alto
MEDIO	Media Media Baja	Medio Medio Medio	Alto Medio Bajo
BAJO	Baja Media Baja	Bajo Bajo Bajo	Bajo Bajo Medio

Identificación de vulnerabilidades. Ha de incluir todas las vulnerabilidades que puedan provocar la materialización de una amenaza sobre un activo.

El líder de seguridad ha de mantener actualizada la lista de vulnerabilidades. En el caso de impacto sobre la misma, convocará al grupo de riesgos para evaluar si hay que efectuar un análisis de riesgos extraordinario.

Evaluación de las vulnerabilidades. Las vulnerabilidades se han de evaluar en función del grado de probabilidad de la materialización de la amenaza.

- **Vulnerabilidad Alta**: Requiere plan de acción.
- **Vulnerabilidad Media**: Mejorable. Requiere Plan de acción en algunos casos o plan de seguimiento en otros. Depende del valor de la amenaza o del valor del activo asociado.
- **Vulnerabilidad Baja**: Adecuado. Requiere plan de seguimiento, en función del valor de la amenaza y del activo, o no requiere nada.

Análisis efectivo del riesgo: evaluación de hasta que grado las vulnerabilidades pueden facilitar alguna amenaza sobre un activo, el valor de cada riesgo se asociará con la matriz incluida mas abajo.

Aceptación del Riesgo. Se trata de fijar el nivel umbral del riesgo y es:

- Cálculo del nivel umbral = Todos aquellos riesgos cuyo valor se encuentre por encima del 9 requerirán un plan de acción.

- Se requerirá un plan de acción para todos aquellos riesgos donde se haya detectado un nivel de vulnerabilidad alta.
- Se requerirá un plan de seguimiento para todos aquellos riesgos que están asociados con un valor máximo bien de activo o de amenaza.

De acuerdo con el mapa, la fijación del plan a aplicar a cada riesgo en función del valor obtenido es como sigue:

- Color verde: Riesgo asumible, no se requiere ni acción ni seguimiento.
- Color amarillo: Riesgo que requiere un plan de seguimiento.
- Color rojo: Riesgo que requiere un plan de acción.

	Amenazas								
Activos	Baja	Media	Alta	Baja	Media	Alta	Baja	Media	Alta
Bajo	1	2	3	2	4	6	3	6	9
Medio	2	4	6	4	8	12	6	12	18
Alto	3	6	9	6	12	18	9	18	27
Muy Alto	4	8	12	8	16	24	12	24	36
	Baja			**Media**			**Alta**		
	Vulnerabilidades								

3. Tratamiento del riesgo.

Una vez identificados y fijados los riesgos, según el criterio indicado en la SGSI, se ha de definir el proceso de tratamiento de los riesgos detectados que sobrepasan el nivel adecuado. Esto se hace en esta fase.

Los tratamientos posibles son dos: seguimiento para supervisar su evolución y acción para ajustar su valor.

-Seguimiento. Se tiene que realizar a todos los riesgos de nivel amarillo. El objetivo principal es mantener bajo control el riesgo e iniciar un plan de acción en el momento en que se verifique que ha sobrepasado el nivel umbral, sin esperar a detectarlo en el siguiente análisis de riesgo rutinario.

La actividad principal en el seguimiento es la **identificación de los controles de seguridad** que se van a asociar al seguimiento del riesgo específico. Las fases para la identificación del control/controles de seguridad son:

- **Revisar controles ya incluidos en SGSI**. Se verifica si alguno de los controles de seguridad incluidos en el Estado de Aplicabilidad es adecuado para el seguimiento del riesgo.
- **Necesidad de definir un nuevo control de seguridad**. Si no existe ningún control, o no cubren totalmente las necesidades de seguimiento del riesgo se ha de definir uno nuevo.

  En este caso, el nuevo control ha de cumplir unos requisitos de entrada.

  - Fácil manejo.
  - En línea con los procesos y procedimientos de SGSI.
  - Posibilidad de medir su eficiencia.
  - Orientado a monitorización y detección de cualquier desviación.

  Una vez revisado se incluirá en el Estado de Aplicabilidad.
- **Plan de Seguimiento**. Cuando se han elegido los controles, se establece el plan de seguimiento que consiste en establecer la persona encargada, el plazo se seguimiento, el modo de monitorización y la rutina de actuación en caso de que el valor sobrepase el nivel umbral.

-Actuación. Se tiene que realizar a todos los riesgos de nivel rojo. El objetivo principal es atenuar el valor del riesgo hasta un nivel por debajo del valor umbral (9).

Las actividades que se van a llevar a cabo para rebajar el nivel del riesgo, así como el modo de medir su eficiencia y el medio de monitorizar la evolución del riesgo, se incluirán **en el Plan de Acción del Riesgo**.

El Plan de Acción del riesgo se compone de las siguientes actuaciones:

- Acciones para reducir el valor del riesgo, incidiendo sobre todo en las amenazas y las vulnerabilidades
- Identificación de los controles de seguridad mediante los que se va a medir la evolución del riesgo. (Ver apartado anterior).
- Plan de tiempos.
- Acciones a tomar en todos los casos.
- Persona responsable del plan.

Plan de tratamiento de Riesgos. Es el documento que incluye todos los planes tanto de seguimiento como de acción. Es una evidencia fundamental cara a medir la eficiencia del SGSI y a probar que el nivel de madurez del mismo es el adecuado para obtener la certificación de ISO 27001.

Los apartados principales del plan de tratamiento de riesgos son:

- Planes de Seguimiento de Riesgos de nivel amarillo.
- Planes de Acción de Riesgos de nivel rojo.
- Nivel de prioridad asignado a cada riesgo.
- Asignación de recursos y responsabilidades.
- Estrategia en el tratamiento de cada riesgo en función de recursos y prioridades (evitar, mitigar, transferir o aceptar…).
- Revisión y seguimiento del Plan. De modo mensual hasta alcanzar el nivel de madurez adecuado. Posteriormente de forma trimestral

El Plan de Tratamiento de Riesgos es aprobado por la dirección y supervisado por el líder de seguridad.

4. Aceptación del riesgo.

La dirección al aprobar el Plan de Tratamiento de Riesgos acepta tanto la estrategia del tratamiento de riesgos incluida en el Plan, (incluyendo qué riesgo se evitan, se transfieren, se mitigan o se aceptan) y el valor de cada riesgo que se prevé alcanzar una vez se ha aplicado las acciones.

5. Comunicación del riesgo.

Forma parte de la fase de implantación (DO) y tiene que ver con la implementación del Plan de Tratamiento de Riesgos y se desarrollarán en el capítulo 6.

6. Monitorización del riesgo.

La Monitorización del riesgo forma para de la fase de Chequeo (CHECK), como tiene con el modo en que se revisara la operación del proceso y la eficiencia de los planes se describirá en el capítulo 8.

5.3. ESTADO DE APLICABILIDAD

La Declaración de aplicabilidad (Statement of applicability SOA) recoge los objetivos de control y los controles que se aplican en el SGSI de **SeBackSA.** Basado en el anexo de la norma ISO/IEC 27001, se refleja en el SOA, la selección, tratamiento e implementación de los controles de seguridad que se aplican en el SGSI.

Los controles de seguridad sirven para verificar la evolución de los riesgos y si se mantienen bajo control gracias a las acciones implantadas. Otra función de los controles de seguridad es confirmar que el SGSI desarrollado cubre adecuadamente todos los procedimientos de seguridad y en la línea marcada por el standard de seguridad elegido, en nuestro caso ISO /IEC 27001.

La declaración de aplicabilidad de **SeBackSA** incluirá todos los controles definidos en el SGSI, todos están incluidos en el Anexo A de la norma, no ha sido necesario incluir ninguno adicional teniendo en cuenta los requisitos de seguridad identificados (legales, de negocio, análisis de riesgos, entre otros.).

Los controles quedan agrupados y numerados de la siguiente forma:

A.5 Política de seguridad.

A.6 Organización de la información de seguridad

A.7 Administración de recursos

A.8 Seguridad de los recursos humanos

A.9 Seguridad física y del entorno

A.10 Administración de las comunicaciones y operaciones

A.11 Control de accesos

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

A.13 Administración de los incidentes de seguridad

A.14 Administración de la continuidad de negocio

A.15 Cumplimiento (legales, de estándares, técnicas y auditorias)

La declaración de aplicabilidad se realizará la primera vez en el proceso de implantación; junto con el análisis de riesgos serán las herramientas principales para definir el punto de partida y el plan de actuación para conseguir alcanzar el objetivo de obtener la primera certificación en el tiempo previsto.

La elaboración de declaración de aplicabilidad, da como resultado una tabla con el siguiente formato:

Objetivo de control			
ISO	Control	Estado	Referencia
ISO	Control	Estado	Referencia

-Objetivo de Control: Definición del objetivo.
-ISO: Número de orden de acuerdo al Anexo A de la norma
-Control: Definición del control, según el Anexo A
-Estado: Se aplica o no en el SGSI de **SebackSA**
-Referencia: La evidencia de la aplicación del control, o si no se aplica el motivo

La declaración de aplicabilidad se elaborará la primera vez durante la fase de implantación. Se revisará y se actualizará junto con el análisis de riesgo y con su misma periodicidad, es decir, cada seis meses de modo ordinario, hasta que el SGSI alcance el nivel de madurez adecuado. Después, se hará anualmente. También se prevé la posibilidad de hacer una revisión de modo extraordinario si es necesario.

5.4. OTROS PROCEDIMIENTOS DE SEGURIDAD

Las rutinas de seguridad más características del SGSI se recogen en varios documentos. Estos procedimientos detallan los pasos a seguir y la forma de actuar en aquellas áreas específicas que cubre el SGSI y que no se han desarrollado en detalle en la descripción general de SGSI para no hacer un documento excesivamente farragoso. De este modo se consigue un manejo de la documentación más fácil y accesible.

En este capítulo se resumen los procedimientos del SGSI de **SeBackSA**.

5.4.1. Procedimientos de seguridad

Los procedimientos de seguridad son las rutinas de trabajo que deben de seguir todos los miembros de **SeBackSA** en todas las actividades. Son procedimientos encaminados a preservar la seguridad de los sistemas de información entregados por los clientes para su custodia, garantizando la confidencialidad, integridad y disponibilidad de los mismos desde que el cliente hace la entrega efectiva hasta que **SeBackSA** devuelve la información de acuerdo con los términos de la entrega acordados con cada cliente.

Las principales son:

- **Rutinas de acceso a las instalaciones**. Se describe el manejo de las alarmas, de las cajas fuertes y de los armarios y los protocolos de acceso a las instalaciones de SeBackSA y en especial el manejo de las tarjetas de acceso, la actualización y las condiciones que deben de cumplir las claves de acceso.
- **Rutinas de acceso y mantenimiento de la red**. Descripción desde la política de privilegios y claves de acceso a la red hasta la rutina para llevar a cabo los backups y el modo de acceder por parte de terceras personas para el caso de mantenimiento de la red que no pueda ser solventado por los propios miembros de la unidad de informática.
- **Gestión de incidentes**. Su objetivo es garantizar que los eventos y agujeros de seguridad asociados con los sistemas de información se

comunican y que se realizan las acciones correctivas oportunas. Para ello se ha diseñado un proceso que implica a todos y que describe los pasos a dar en el caso de detectar algún hecho que pueda impactar en el escenario cubierto por el SGSI. También describe el modo en que se efectúa el seguimiento, la resolución y la monitorización de todos con vistas a fijar objetivos y a mejorar las rutinas y procesos del SGSI.

5.4.2. Estructura de la organización

Este documento define el modo en que la organización se estructura y la principal información que contiene trata sobre:

- Puestos y funciones
- Personas que integran la organización y la función que desempeñan

Conviene subrayar que la organización que cubre el SGSI es una organización de carácter transversal, que se superpone a la estructura orgánica de **SeBackSA**. Como ya vimos en el capítulo anterior, **SeBackSA** es una compañía formada por distintas unidades con unas competencias muy definidas, coordinadas por un equipo de dirección, y con una serie de puestos y categorías en cada unidad orientadas a hacer el negocio rentable. La organización que se describe en este procedimiento está orientada a operar y mejorar el SGSI implementado en **SeBackSA**.

Para cumplir con su cometido, la organización tiene una serie de puestos que se describen en este documento incluyendo las funciones, autoridad y privilegios de acceso asignadas a cada puesto. Los puestos son:

-Líder de Seguridad. Es la persona que lidera la organización y que forma parte del equipo de dirección. Es el delegado de la dirección que asume todos los compromisos de **SeBackSA** sobre la implicación de la dirección en la implementación, operación y mejora del SGSI.

Sus funciones principales son:

- Coordinación de las actividades de acuerdo con la política a seguir en la SGSI establecida por el equipo de dirección.
- Seguimiento del plan para asegurar el cumplimiento de los objetivos establecidos para el SGSI por la dirección.
- Aprobación de cualquier cambio en los cargos y responsabilidades incluidos en este documento.
- Aprobación de las acciones a emprender por causa de un incidente se seguridad.

- Motivación a la organización para el seguimiento de la política del SGSI establecida por la dirección como para el cumplimiento de los objetivos.
- Aprobación de cualquier modificación que afecte a los procesos y procedimientos incluidos en el SGSI.
- Supervisión en la gestión de los recursos de la organización y adecuación de los recursos a las necesidades de la organización.
- Supervisión de la competencia de los miembros de la organización y establecimiento de los planes de mejora.
- Aseguramiento de que las auditorias se realizan de acuerdo al plan establecido y supervisión de las revisiones ordinarias (o extraordinarias en su caso) del SGSI.

-Experto SGSI. Es la persona que se encarga de todos los aspectos de seguridad en la línea con la SGSI establecida en **SeBackSA**. Es el principal colaborador del responsable de la Organización y con una gran competencia en SGSI y en ISO/IEC 27001.

Sus funciones principales son:

- Soporte a la organización en todos los aspectos relacionados con implementación, operación y mejora del SGSI.
- Soporte al equipo de dirección de **SeBaksa** en el establecimiento de la política y de los objetivos del SGSI.
- Diseño de los elementos principales del SGSI.
- Coordinación de la implementación del SGSI.
- Coordinación de todos los procesos de mejora del SGSI.
- Supervisión y revisión de los procesos y procedimientos de seguridad.
- Planificación y coordinación de los planes de gestión de riesgos.
- Supervisión y seguimiento de los controles incluidos en la declaración de aplicabilidad.
- Propuesta de análisis de riesgos extraordinarias.
- Coordinación de las actividades a llevar a cabo para la preparación y realización de las auditorias.
- Gestión de los incidentes de seguridad.

-Representante de unidad. Miembro de alguna de las unidades de **SeBackSA**, se encarga de desplegar en su unidad la parte de SGSI que les afecta, tanto a nivel de procesos como de rutinas y de cambios y, al mismo tiempo, de trasladar a la organización todos los aspectos de su unidad que sean relevantes para el SGSI.

Sus funciones principales son:

- Participar en los análisis de riesgos, trasladando la visión de su unidad encuanto a activos, amenazas y vulnerabilidades.
- Participar en las revisiones de los procesos y rutinas de seguridad de SGSI aportando la visión de su unidad.
- Obtener y trasladar a la organización cualquier propuesta de mejora o de feedback que venga de su unidad.
- Desplegar en su unidad todo lo relativo a política y objetivos del SGSI.

-Integrante Nivel 1. Miembro de la unidad de informática de SeBackSA, su principal función es encargarse de la operación y el mantenimiento de las aplicaciones y del entorno de la red que representa el negocio de **SeBackSA**. Al poder acceder a la información y sistemas de los clientes han de asumir un compromiso de confidencialidad que garantice que no se va a divulgar nada de lo referente ni a la información custodiada ni a los sistemas y procesos de seguridad implementados.

-Integrante Nivel 2. Miembro de alguna de las unidades de apoyo de **SeBackSA**, que no necesitan acceder a la sala de control, ni a la información de los clientes y que su compromiso de confidencialidad es menos estricto que el de los integrantes de nivel 1 pero les obliga igualmente a no divulgar nada de lo referente a los sistemas y procesos de seguridad implementados.

6. PROCESO DE IMPLANTACIÓN

6.1. INICIO. COMPROMISO DE LA DIRECCIÓN

El compromiso de la Dirección se obtiene desde el momento que todos convienen, dada la naturaleza del negocio de **SeBackSA,** que es fundamental disponer de un SGSI homologado que garantice la custodia de la información de los clientes. Para conseguirlo la implicación del equipo de dirección es fundamental.

La implicación de la dirección en la implementación del SGSI se traduce en las siguientes tareas, como se indicó en la descripción general de SGSI:

-Aprobación de la política de SGSI

- Diseño de los procesos de seguridad de acuerdo con el escenario. En línea con los procesos, el equipo de dirección revisó y aprobó la descripción general de SGSI. Para llevar a cabo un seguimiento más cercano, incorporó al equipo de dirección, al líder de seguridad,

máximo responsable de todo el equipo implicado en la implementación y desarrollo.

- Elección en los puestos clave de personas con la competencia adecuada, sobre todo el líder de seguridad y el experto SGSI. En este sentido se reclutó como experto SGSI a una persona, líder de auditorias de seguridad de BSI, con experiencia contrastada en desarrollo y mantenimiento de SGSI y con conocimientos profundos en la serie 27000 de ISO.

- Implicación de todos y concienciación en cuanto a la importancia de mantener la confidencialidad, integridad y disponibilidad de los sistemas de información. Diseño de un plan de concienciación de toda la plantilla y de un plan de competencia individualizado con un plan de tiempos y pautas de las que el Líder de seguridad dará cuenta en todas las reuniones del equipo de dirección.

-Aprobación de los objetivos de SGSI tanto de los de carácter general como de los anuales.

- Establecimiento de un SGSI de alto nivel, certificado por BSI como prueba de que cumple con el standard ISO 27001.
- Mantenimiento del SGSI en el mismo nivel o superior, aplicando criterios de mejora continúa en todos los procesos y procedimientos.
- Establecimiento de procesos flexibles para ajustarse a los requisitos de los clientes de modo rápido y sin perder efectividad ni seguridad.
- Establecimiento y mejora continúa de las rutinas de continuidad de negocio establecidas y de acuerdo con el Standard ISO.

El equipo de dirección toma la responsabilidad de implicarse en los objetivos, uno de los acuerdos es el incluir en el orden ordinario de las reuniones de dirección el seguimiento de objetivos. Se incorporará de modo temporal a las reuniones en este punto el experto de SGSI para asesorar sobre el seguimiento y acciones a tomar.

6.2. IMPLANTACIÓN DEL SGSI EN LA ORGANIZACIÓN

Una vez obtenido el compromiso del equipo de dirección, se buscó la implicación de todos los integrantes de **SeBackSA** ya que la colaboración de todos

facilitaría la implantación del SGSI. El primer paso que se dio durante la fase de implementación fue dar a conocer el SGSI a la organización.

Durante la fase de diseño (ver capítulo anterior) se desarrollaron las líneas maestras del SGSI de **SeBackSA** y los puntos principales fueron:

- Descripción general del SGSI
- Método de gestión de riesgos.
- Declaración de aplicabilidad
- Procesos de seguridad asociados.

La difusión del SGSI fue la segunda tarea que se llevó a cabo durante la fase de implantación y consistió en las siguientes actividades:

-Plan de presentaciones que consistieron en presentaciones específicas para cada unidad de **SeBackSA** orientadas a exponer la función de cada unidad en el SGSI y cuyos principales objetivos fueron:

- Difundir las líneas maestras del SGSI
- Explicar la importancia del SGSI en la evolución de SeBackSA
- Presentar los roles y organización
- Enseñar la metodología de la gestión de riesgos
- Presentación de los controles y del estado de aplicabilidad
- Presentación de los procesos de seguridad y pautas a seguir en cada caso
- Gestión de incidentes
- Buenas prácticas y propuestas

-Creación de los equipos y la asignación de roles: se valoró el grado de interés suscitado durante las presentaciones, el nivel de competencia de salida y el perfil de cada uno teniendo en cuenta el nivel de iniciativa y la capacidad de liderazgo.

-Formación en el trabajo (on the job training) que consistió principalmente en empezar a aplicar los procesos de trabajo de SGSI en las actividades del día a día. Para soportar cualquier pregunta o duda se crearon dos niveles de ayuda, el más cercano: el representante de la unidad y en caso de necesitar un soporte más complejo se acudía al experto SGSI.

-Definición de los planes de competencia para cada integrante teniendo en cuenta su nivel de conocimiento de partida y su nivel de competencia requerido. El medio utilizado para la valoración fue una lista de chequeo con las competencias y conocimientos necesarios para su puesto. A partir de la lista se fijaron para cada uno los puntos de mejora, el mejor medio de alcanzar la competencia y el tiempo para conseguirlo.

Finalmente, una vez asignados los puestos, creados los equipos y desarrollados los planes de mejora se tuvo una reunión de salida para hacer equipo y mentalizar en la importancia de la implicación de todos.

6.3. EVALUACIÓN DE RIESGOS

De acuerdo con el plan de tiempos, después de la reunión de partida se iniciaron las actividades para preparar la primera evaluación de riesgos a la que se implicó a toda la organización. Su duración fue de un mes y se desarrolló en dos fases:

-Feedback a nivel de equipo de trabajo. Liderado por el representante de cada equipo se hizo una primera evaluación de los riesgos, orientada principalmente a definir y valorar activos, amenazas y vulnerabilidades de acuerdo con el método de tratamiento de riesgos indicado en el capítulo anterior.

-Evaluación de riesgos. La realizo el equipo de gestión de riesgos, liderado por el responsable de seguridad y conducida por el experto SGSI y asistiendo todos los representantes de los equipos se hizo la evaluación de riesgos, una de cuyas principales entradas fue la evaluación obtenida en cada equipo una semana antes, en este caso se llevó a cabo el método completo de tratamiento de riesgos.

La evaluación de Riesgos definitiva se desarrolló siguiendo el método definido e incluido en el capítulo anterior. Asistió el equipo de gestión de riesgos en pleno y el resultado se incluyó en el documento Análisis de Riesgos. Número 1. Aprobado por el equipo de Dirección y cuyo resumen se expone a continuación.

-Revisión del Escenario. Primer Análisis de Riesgo que se ajusta al escenario definido y cubre “las actividades y procesos encaminados a preservar la seguridad de los sistemas de información entregados por los clientes para su custodia, garantizando la confidencialidad, integridad y disponibilidad de los mismos desde que el cliente hace la entrega efectiva hasta que **SebBackSA** devuelve la información de acuerdo con los términos de la entrega acordados con cada cliente”.

-Identificación y evaluación de los activos. Se evaluaron los activos de acuerdo con el método definido y el resultado se incluye en la tabla siguiente.

Activo	Impacto principal					Impacto Final
	Acceso no autorizado	Modific	Destrucc	No disponible	**Total**	
Documentación y contratos de clientes	M Alto 4	M Alto 4	M Alto 4	M Alto 4	4	**4**
Edificio	Medio 2	Bajo 1	Alto 3	Alto 3	3	**3**
SeBacksa	Alto 3	Medio 2	Alto 3	Alto 3	3	**3**
Sala de control	M.Alto 4	Alto 3	M Alto 4	Alto 3	4	**4**
Instalaciones Mobiliarias (Cajas fuertes y armarios	M.Alto 4	M.Alto 4	M.Alto 4	M.Alto 4	4	**4**
Red de datos	M.Alto 4	M.Alto 4	M.Alto 4	M.Alto 4	4	**4**
Datos y sistemas de aplicación de los clientes	M.Alto 4	M.Alto 4	M.Alto 4	M.Alto 4	4	**4**
Sistema de aplicación (standard)	Alto 3	Bajo 1	Medio 2	Medio 2	3	**4**
Personal de SeBacksa	-	Medio 2	Alto 3	Medio 2	3	**3**
Personal clave de SeBacksa	-	Alto 3	M.Alto 4	M.Alto 4	4	**4**
Personal de Seguridad	-	Bajo 1	Bajo 1	Medio 2	2	**2**
Personal de Mantenimiento	-	Bajo 1	Bajo 1	Bajo 1	1	**2**
Personal externo	**-**	Residual 0	Residual 0	Bajo 1	1	**1**

Nótese la diferencia en algunos casos entre el impacto principal sobre el activo y el final, de acuerdo con el método aplicado. El impacto principal se puede modificar en función del coste que representa o del grado de dependencia de otro activo.

-Identificación y evaluación de las amenazas. Igual que los activos, las amenazas se evaluaron según el método definido y el resultado se incluye en la tabla

siguiente, donde el grado de la amenaza se evalúa de acuerdo a la tabla recogida en el Método de Gestión de Riesgos en el capítulo anterior.

Amenaza	**Factores**			**Grado Final**
	Impacto	**Frecuencia**	**Otros**	
Acceso no autorizado	Alto	Baja	Bajo	Medio
Robo	Alto	Baja	Bajo	Medio
Error de operación	Alto	Alta	Bajo	Alto
Fallo de sistema	Alto	Media	Bajo	Alto
Desastre Natural	Alto	Bajo	Bajo	Medio
Fallo de energía	Medio	Baja	Bajo	Bajo
Perdida de competencia	Medio	Media	Bajo	Medio
Error interpretación	Alto	Baja	Bajo	Medio
Fallo de Mantenimiento	Medio	Baja	Bajo	Bajo
Fallo de Red	Medio	Media	Bajo	Medio

-Identificación y evaluación de las vulnerabilidades. Las vulnerabilidades se identifican como aquellos factores que pueden provocar la materialización de una amenaza sobre un activo. Se incluye en la tabla siguiente, junto con el valor que el equipo de gestión de riesgos ha fijado.

Vulnerabilidad	Valoración
Fallo del sistema de control de acceso del edificio	Baja. No requiere ninguna acción
Fallo del sistema de control de acceso en la compañía	Baja. No requiere ninguna acción
Fallo del sistema de control de acceso en la sala de control	Baja. No requiere ninguna acción
Fallo de mecanismos de seguridad informáticos	Baja. No requiere ninguna acción
Falta del sistema de protección de documentación	Media. Requiere plan de seguimiento
Fallo del sistema de protección de datos	Media. Requiere plan de seguimiento
Fallo del procedimiento de operación informático. Falta de backup de repuesto	Baja. No requiere ninguna acción
Falla de los procedimientos de seguridad del SGSI	Media. Requiere plan de seguimiento
Fallo de los procedimientos de operación de SGSI	Media. Requiere plan de seguimiento
Fallo de los procedimientos de formación y de la asignación de roles	Media. Requiere plan de seguimiento
Fallo de los procedimientos de energía alternativa de edificio	Baja. No requiere ninguna acción
Fallo del procedimiento de soporte externo	Media. Requiere plan de seguimiento

-Análisis efectivo del riesgo. Ahora se evalúa hasta que grado las vulnerabilidades analizadas pueden facilitar la materialización de alguna de las amenazas encontradas sobre alguno de los activos de **SebackSA.**, el valor de cada riesgo se asociará con la matriz incluida en el capítulo anterior, como se describe a continuación:

Nº	Activo	Amenaza	Vulnerabilidad	Valoración
1	Edificio	Acceso No autorizado	Falta del sistema de control de acceso del edificio	**6**
2	SeBackSA	Acceso No autorizado	Falta del sistema de control de acceso en la compañía	**6**
3	Sala de Control	Acceso No autorizado	Falta del sistema de de control de acceso en la sala de control	**8**
4	Red de Datos	Acceso No autorizado	Falta de mecanismos de seguridad informáticos	**8**

5	Documentación y contratos de clientes	Robo	Falta del sistema de protección de documentación	**16**
6	Datos y sistemas de aplicación de los clientes	Robo	Falta del sistema de protección de datos	**16**
7	Sistemas de aplicación de la Cia	Error de operación	Falta del procedimiento de seguridad informático. Falta de backup de repuesto	**12**
8	Red de Datos	Error de operación	Falta del procedimiento de seguridad informático. Falta de backup de repuesto	**12**
9	Sala de Control	Error de operación	Falla de los procedimientos de seguiridad del SGSI	**24**
10	Red de Datos	Error de operación	Falla de los procedimientos de seguiridad del SGSI	**24**
11	Datos y sistema de aplicación de los clientes	Error de operación	Fallo de los procedimientos de seguridad del SGSI	**24**
12	Red de Datos	Fallo del sistema	Falta del procedimiento de seguridad informático. Falta de backup de repuesto	**12**
13	Edificio, Sebacksa	Desastre natural	Falla de los procedimientos de seguridad del SGSI.	**12**
14	Sala de control, instalaciones mobiliarias	Desastre natural	Falla de los procedimientos de seguridad del SGSI.	**16**
15	Personal clave de Sebacksa	Perdida de competencia	Fallo de los procedimientos de formación y de la asignación de roles	**16**
16	Personal clave de SebackSA	Robo	Fallo de los procedimientos de seguridad del SGSI	**16**
17	Personal de Sebacksa	Robo	Fallo de los procedimientos de seguridad del SGSI	**12**
18	Personal de seguridad y mantenimiento	Robo	Fallo de los procedimientos de seguridad del SGSI	**8**
19	Personal externo	Robo	Fallo de los procedimientos de seguridad del SGSI	**6**
20	Edificio, Sebacksa,	Fallo de energia	Fallo de los procedimientos de energia alternativa de edificio	3
21	Sala de control	Fallo de energia	Fallo de los procedimientos de energia alternativa de edificio	4
22	Personal de mantenimiento, personal externo	Fallo de mantenimiento	Fallo del procedimiento de soporte externo	2

De acuerdo con el método definido en el SGSI:

- Color verde: Riesgo asumible, no se requiere ni acción ni seguimiento.
- Color amarillo: Riesgo que requiere un plan de seguimiento.
- Color rojo: Riesgo que requiere un plan de acción.

Los planes tanto de seguimiento como de acción se incluirán en el subcapítulo siguiente.

6.4. TRATAMIENTO DE RIESGOS

Corresponde hacerlo para todos los riesgos de nivel rojo. El objetivo principal es atenuar el valor del riesgo hasta un nivel por debajo del valor umbral (9).

Las actividades que se van a llevar a cabo para rebajar el nivel del riesgo, así como el modo de medir su eficiencia y el medio de monitorizar la evolución del riesgo se incluirán **en el Plan de Acción del Riesgo** e incidirán principalmente en atenuar el valor de la amenaza.

El hecho de que **SebackSA** sea una compañía de nueva creación ha incidido en la valoración de los factores de riesgo sobre todo el de las amenazas. Se ha considerado el caso más desfavorable con lo que la valoración de los riesgos ha salido muy alta. La valoración debe de salir más ajustada cuando se tengan datos del rendimiento real.

Teniendo en cuenta la evaluación de riesgos efectuada el Plan de Tratamiento de Riesgos resultante se presenta a continuación:

Nº	Prioridad	Riesgo	Plan	Estrategia	Responsable
9 y 10	**24**	**Error de operación en la sala de control o la red de datos por fallo de los procedimientos de seguridad de SGSI**	**Plan de acción 1**	**Mitigar**	
11	**24**	**Error de operación en el manejo de datos de clientes por fallo de los procedimientos de seguridad de SGSI**	**Plan de acción 1**	**Mitigar**	
5	**16**	**Robo de documentación de clientes por fallo de los procedimientos de protección de codumentacion**	**Plan de acción 2**	**Mitigar**	
6	**16**	**Robo de sistemas de datos de clientes por fallo de los procedimientos de protección de datos de SGSI**	**Plan de acción 3**	**Mitigar**	

14	**16**	**Interrupción del negocio debido a desastre naturla en la sala de control de SGSI por fallo de los procedimientos de protección de SGSI**	**Plan de acción 4**	**Mitigar**	
15	**16**	**Pérdida de competencia de personal clave debido a fallo en los procedimientos de formación y de competencia**	**Plan de acción 5**	**Mitigar**	
16	**16**	**Robo por parte del personal clave de SeBackSA debido a fallos de los procedimientos de seguridad de SGSI**	**Plan de acción 1**	**Mitigar**	
7 y 8	**12**	**Error de operación en los sistemas de aplicación debido a fallos en los procedimientos de seguridad informática**	**Plan de acción 5**	**Mitigar**	
12	**12**	**Fallo de sistema en la red de datos debido al procedimiento de seguridad informática**	**Plan de acción 5**	**Mitigar**	
20	**12**	**Interrupción del negocio debido a desastre natural en SeBackSA por fallo de los procedimientos de protección de SGSI**	**Plan de acción 4**	**Mitigar**	
17	**16**	**Robo por parte del personal clave de SeBackSA debido a fallos de los procedimientos de seguridad de SGSI**	**Plan de acción 1**	**Mitigar**	

En el resto de los riesgos debido a que el nivel está por debajo del umbral considerado aceptable (9) la estrategia a seguir es de aceptarlos. En aquellos de nivel amarillo se llevará a cabo un seguimiento por parte del experto SGSI que informará del estado en las reuniones periódicas del equipo de gestión de riesgos.

6.5. PLAN DE SEGUIMIENTO DEL SGSI

Una vez obtenida la evaluación de riesgos y el plan de tratamiento de riesgos con los planes de acción a seguir se estableció el modo de seguimiento del mismo, teniendo en cuenta que el principal objetivo era tener el SGSI listo para la certificación en un periodo de seis meses, con una auditoria externa intermedia en un plazo de tres meses.

En este escenario se decidieron dos acciones en la misma reunión:

- Presentar a toda la organización los resultados de la evaluación de riesgos y el plan de tratamiento de los mismos.
- Establecer reuniones semanales del equipo de gestión de riesgos cuyo objetivo principal sería evaluar la efectividad de los planes de acción así como del de seguimiento y verificar la implantación de los diferentes procesos y procedimientos del SGSI con especial atención al de gestión de incidencias.

7. PROCESO DE OPERACIÓN

En el proceso de operación se inicia la ejecución del SGSI. En la fase de diseño se definió la metodología y los procedimientos de seguridad a seguir en **SeBackSA.** En la fase de implantación se introdujo el modelo, primero implicando a la dirección y luego implicando al resto de la organización asignando los roles; luego todos efectuaron la primera evaluación de riesgos y el plan de tratamiento de riesgos. En la fase de operación se aplica el modelo en el trabajo de SeBackSA, las actividades se realizan de acuerdo con los procesos del SGSI y aplicando los planes para atenuar los riesgos.

En este capítulo se describen los elementos más destacados del SGSI en la fase de Operación, que han sido la aplicación de los planes de mejora del RTP y la evolución de los incidentes de seguridad.

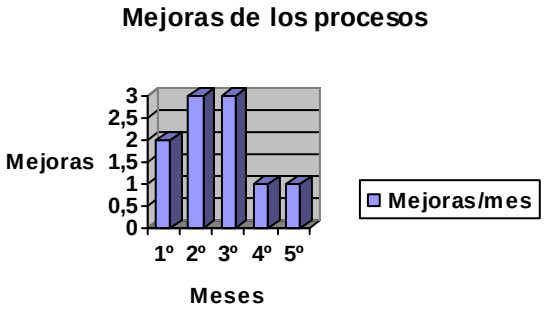
7.1. Implementación del plan de tratamiento de riesgos

Plan de Acción 1:

Tiene el objetivo de limitar la amenaza del error de operación, su probabilidad de aparición a un valor bajo. Además también busca limitar la vulnerabilidad de fallos en los procedimientos de seguridad de SeBackSA.

El medio de verificarlo es mediante el seguimiento del número de mejoras que se introducen en los procedimientos y el número de incidentes que se producen por un error de operación.

El responsable del Plan es el experto SGSI y la evolución se refleja abajo.



La evolución indicó que al principio el número de incidentes se incrementó manteniéndose estable durante los primeros tres meses para ir paulatinamente bajando, mientras que la evolución de las mejoras en los procesos fue similar.

La evolución podría explicarse en que en una primera fase los incidentes y las propuestas son menores debido sobre todo a la falta de experiencia y familiaridad en la aplicación del SGSI, a medida que se va conociendo las incidentes y las posibilidades de encontrar puntos de mejora aumentan alcanzando el punto máximo en el tercer mes, a partir del cual el perfil disminuye porque ya se conocen los procesos y los errores son menos y las mejoras también al estar los procesos mas depurados.

Plan de Acción 2:

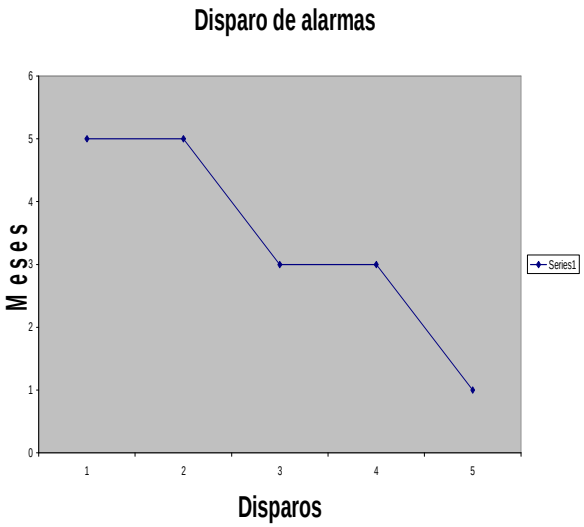
Su objetivo es limitar la amenaza de robo, fijándolo en una probabilidad baja. Igualmente, se busca disminuir la vulnerabilidad de fallos en los procedimientos de protección de datos y de seguridad del SGSI.

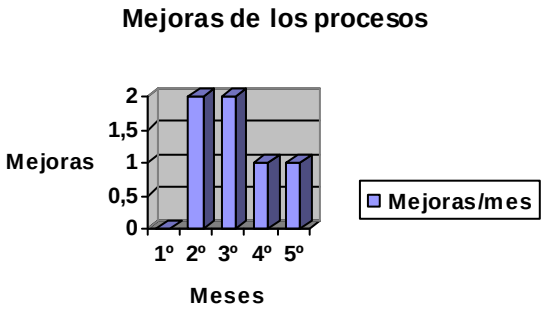
El medio de verificarlo es mediante el seguimiento del número de actualizaciones que se introducen en los procedimientos de protección de datos y en las rutinas de seguridad de las cajas fuertes y armarios y el número de incidentes que se producen por activación de alarmas.

El responsable del Plan es el experto SGSI y la evolución a lo largo de cinco meses marca una tendencia similar en cuanto a las mejoras en los procesos pero diferente en cuanto a los incidentes por alarmas.

Los disparos de las alarmas mantienen una tendencia descendente, que se explicaría porque las alarmas disminuyen a medida que la gente se va familiarizando con su manejo, las mejoras de los procesos mantienen la tendencia ascendente hasta que alcanza un máximo y luego desciende que se explicaría por el mismo motivo que en el caso del plan anterior.

La evolución de ambos se representa en los gráficos siguientes:





Plan de Acción 3:

El objetivo principal del plan fue limitar al mínimo la vulnerabilidad de fallo en los procesos ya que la posibilidad de limitar el valor de la amenaza era muy baja.

Se desarrollo un procedimiento nuevo: un procedimiento de continuidad de negocio. La ubicación de una segunda localización donde poder reiniciar las actividades en caso de necesidad. El procedimiento definió las condiciones iniciales necesarias e identificó los recursos y las personas necesarias y desarrolló una rutina de trabajo para calcular el tiempo necesario para reiniciar la actividad.

El modo de verificarlo fue el simulacro de desastre y demostrar que era posible la reconstrucción del entorno de trabajo con todos los datos de partida, aunque en un periodo mayor del previsto. Quedando como punto de acción el mejorar ese tiempo que llegando a un objetivo de tener el entorno listo en 36 horas.

El responsable fue el representante de la unidad de informática y aunque no se consiguió el objetivo en tiempo si se verificó que se podía reiniciar las actividades desde el punto donde se interrumpieron a causa del supuesto desastre.

Plan de Acción 4:

El plan incide en disminuir la vulnerabilidad de fallo en los procesos sobre todo, y en menor medida en disminuir el valor de la amenaza porque el hecho de motivar a las personas claves depende de la dirección de la compañía y del mercado.

El elemento principal del plan fue el desarrollo de un modelo de competencia compartida. Se estableció un plan de tiempos y de actividades para que cada puesto clave tuviera más de una persona con el nivel adecuado para cubrirlo y se hizo una lista con las personas que cubrían el rol y las que mejor podrían sustituirlas.

El medio de verificarlo consistiría a través de una lista de chequeo. En esta lista se incluyen las competencias necesarias para cada perfil y se evalúa si la persona sustituta tiene la competencia adecuada o no.

Se realizó la evaluación a los cinco meses de arrancado el plan y se verificó que la mayoría de los puestos clave estaban cubiertos adecuadamente, el caso del experto SGSI requería mayor tiempo para adquirir la competencia fijando en un año el tiempo necesario.

Plan de Acción 5:

Su objetivo es limitar la amenaza de error de operación en la red de datos, fijándolo en una probabilidad baja. Igualmente, se busca disminuir la vulnerabilidad de fallos en los procedimientos de protección de datos y de seguridad del SGSI.

El medio de verificarlo es mediante el seguimiento del número de actualizaciones que se introducen en los procedimientos de protección de datos y en el número de incidentes que se producen por errores de operación en la red de datos.

El responsable del Plan es el experto SGSI y la evolución a lo largo de cinco meses marca una tendencia similar en cuanto a las mejoras en los procesos pero diferente en cuanto a los incidentes por alarmas.

La tendencia de los incidentes por errores de operación en la red de datos mantuvieron una ligera línea descendente, dada la competencia y la experiencia de los operadores de red no fue difícil la adaptación de los mismo al entorno de trabajo.

7.2. Gestión de incidentes

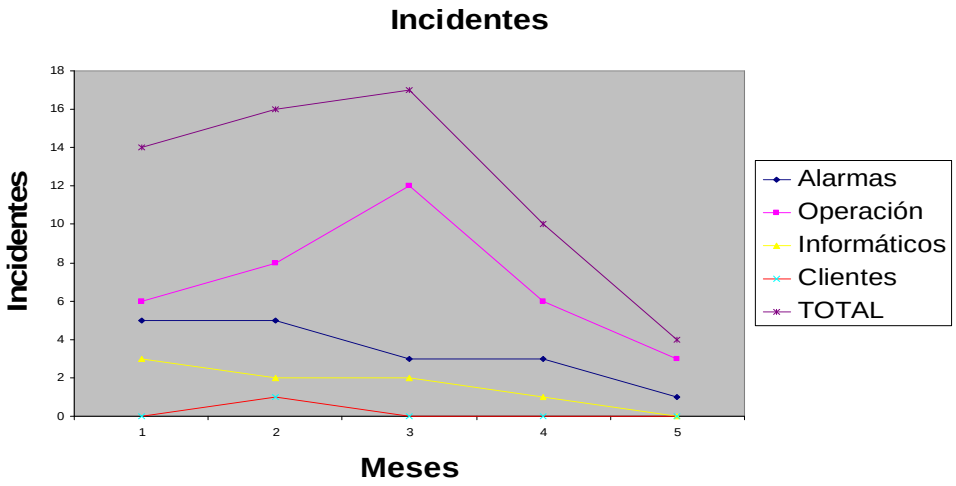
El proceso de gestión de incidentes es fundamental en un SGSI ya que persigue hacer frente a cualquier contingencia de forma rápida para evitar o atenuar el impacto sobre la integridad, disponibilidad y confidencialidad de los activos de una compañía.

SeBackSA dispone de un proceso de gestión de incidentes que se ajusta a su dimensión, estructura organizativa y tipo de activos y como elementos mas destacados están los tipos de incidentes y el tiempo de respuesta.

Los tipos de incidentes son:

- Alarmas. Error en la activación desactivación de cualquier alarma
- Operación. Hecho realizado en contra o sin tener en cuenta los procedimientos de seguridad del SGSI.
- Informático. Operación que provoca un mal funcionamiento en los sistemas de aplicación de Sebacksa.
- Cliente. Operación que pueda significar una amenaza para la integridad, confidencialidad o disponibilidad de los activos de los clientes.

La evolución de los incidentes producidos en la fase de operación fue como indica el gráfico siguiente:



La tendencia general de los incidentes presenta un perfil primero ascendente y posteriormente descendente. La línea ascendente se debe al número de los errores de operación que ya se explicó en el Plan1. Las Alarmas y los informáticos presentan una evolución descendente, lógica ya que los incidentes van en relación inversa al aumento de la familiaridad con el entorno de trabajo y con el SGSI. Acerca de los incidentes de los clientes, es de destacar la baja incidencia, lógico porque son los activos más sensibles y en consecuencia los que se salvaguardan más.

8. PLAN DE MONITORIZACIÓN Y POSIBLES MEJORAS

En esta primera fase de 6 meses que cubre el presente trabajo, el objetivo principal era preparar a la organización para obtener la certificación ISO 27001 como muestra de que se había alcanzado el nivel de madurez adecuado.

En este sentido las funciones principales de la monitorización son:

- Detectar lo antes posible errores en los procesos de seguridad y protección de datos.
- Detectar lo antes posible puntos débiles en el SGSI.
- Verificación de que las actividades de negocio se hacen de modo adecuado y de acuerdo al modelo de SGSI.
- Determinación de la efectividad de los planes de acción definidos para mitigar el valor de los riesgos encontrados.

En este capítulo vamos a resumir lo más destacado de los medios utilizados para monitorizar el modelo.

8.1. Evolución del estado de los riesgos

El medio más importante utilizado para monitorizar la evolución del modelo en este caso fue la evolución del estado de los riesgos. Ver el impacto de los planes de acción sobre el valor de los riesgos y verificar que éstos se mitigaban.

Se tomó la decisión de hacer una evaluación extraordinaria a los tres meses para hacer un seguimiento más cercano y poder realizar cualquier rectificación en el caso de que algún plan de acción no estuviera dando el resultado previsto.

La evolución de los riesgos se puede observar en el gráfico de abajo, se recoge la evolución a partir del valor de cada riesgo asignado en las tres evaluaciones que se hicieron, de izquierda a derecha, la ordinaria del primer mes (Ver 6.3), la extraordinaria del tercer mes y la ordinaria del sexto.

Nº	Activo	Amenaza	Vulnerabilidad	Valoración		
5	Documentación y contratos de clientes	Robo	Falta del sistema de protección de documentación	16	16	4
6	Datos y sistemas de aplicación de los clientes	Robo	Falta del sistema de protección de datos	16	16	4
7	Sistemas de aplicaciones de SeBackSA	Error de operación	Fallo del procedimiento de seguridad informáticos	12	8	8
8	Red de Datos	Error de operación	Falta del procedimiento de seguridad informático. Falta de backup de repuesto	12	8	8

9	Sala de Control	Error de operación	Falla de los procedimientos de seguiridad del SGSI	24	24	8
10	Red de Datos	Error de operación	Falla de los procedimientos de seguiridad del SGSI	24	24	8
11	Datos y sistema de aplicación de los clientes	Error de operación	Fallo de los procedimientos de seguridad del SGSI	24	24	8
12	Red de Datos	Fallo del sistema	Falta del procedimiento de seguridad informático.	12	12	8
13	Edificio, Sebacksa	Desastre natural	Falla de los procedimientos de seguridad del SGSI.	12	6	6
14	Sala de control, instalaciones mobiliarias	Desastre natural	Falla de los procedimientos de seguridad del SGSI.	16	8	8
15	Personal clave de Sebacksa	Perdida de competencia	Fallo de los procedimientos de formación y de la asignación de roles	16	16	16
16	Personal clave de SebackSA	Robo	Fallo de los procedimientos de seguridad del SGSI	16	16	4
17	Personal de Sebacksa	Robo	Fallo de los procedimientos de seguridad del SGSI	12	12	3

Se verifica que en los seis meses transcurridos los planes de acción han provocado que todos los riesgos se hayan mitigado pasando de un valor que requería plan de acción a otro que requiere un plan de seguimiento.

El único error que necesitará plan de acción es el número 15 y el riesgo está asociado con el hecho de que solo una persona de la organización tiene la competencia adecuada para ser experto SGSI, el plan seguirá vigente hasta que otra persona más adquiera la competencia.

De acuerdo con la evolución alcanzada, el estado actual de los riesgos indica que el SGSI de SeBackSA ha alcanzado un nivel de madurez adecuado y estaría listo para ser certificado.

8.2. Otros medios

Otros medios de monitorización confirmaron el nivel de madurez alcanzado por el SGSI, fueron principalmente:

- Auditoria externa. Realizada a los tres meses de iniciado el proceso, para verificar la implantación y operación del SGSI.
- Supervisión de la dirección. Orientada a verificar el nivel de compromiso y de implicación de la plantilla.

Todos los medios de monitorización confirmaron que el SGSI de SeBackSA estaba listo para presentarse a la auditoria de certificación de la ISO 27001.

9. CONCLUSIONES

La primera conclusión es que el establecimiento de un SGSI en una compañía es de gran utilidad al proporcionar la metodología adecuada para garantizar la confidencialidad, la integridad y la disponibilidad de los activos de su negocio que tengan que ver con la información, como queda demostrado con la aplicación a un caso tan dependiente del manejo seguro de la información como es SeBackSA.

Para llevar a cabo un SGSI es fundamental realizar un diseño del mismo adaptado a las necesidades y el perfil de la compañía por ello se ha dedicado gran parte de este trabajo a describir de forma pormenorizada tanto las características de la compañía como el SGSI diseñado para ella. Un diseño de SGSI claro y concreto, ajustado a la realidad de la compañía es clave para evitar problemas y errores de interpretación a la hora de insertar el modelo en la rutina normal de trabajo.

El SGSI diseñado ha de ser dinámico y fácilmente adaptable a los cambios y las mejoras a introducir en la compañía, la aplicación del modelo PDCA (Plan Do Check Act) es fundamental, basado en el concepto de mejora continua, la competencia en su manejo puede ser de gran utilidad en el manejador de procesos de cualquier compañía en cualquier sector, no solo en el contexto de un SGSI.

Es fundamental la definición clara de los objetivos y del escenario, un escenario bien delimitado permite ajustar las condiciones del SGSI, así el modelo se

diseñara para garantizar la confidencialidad, integridad y disponibilidad de los activos de información en el escenario delimitado, ni más ni menos.

Los objetivos son capitales para definir claramente los niveles de seguridad que se incluirán en el SGSI, en el caso de SeBakSA el hecho de marcar como objetivo el obtener la certificación y ser una empresa para la que la información es clave ha llevado a diseñar un SGSI con un maximo nivel de seguridad, aunque no siempre haya de ser así.

Es muy importante incluir en la descripción general las principales pautas del SGSI para lo cual el modelo reflejado en la ISO 27001 es capital.

Tan importante como los procesos y procedimientos es el diseño de una organización que pueda desarrollar todas las actividades del negocio en la línea con lo indicado en el SGSI para lo cual es importante que la organización sea transversal con el fin de que implique a todos los estamentos y unidades de la organización.

Hay que destacar que hay unos puestos clave, fundamentales para que el SGSI alcance el nivel de madurez adecuado, de ellos el experto SGSI es capital. Tan importante como el perfil y la competencia es el mantener esa competencia compartida para evitar riesgos como el que se mantiene en el caso de SeBackSA.

Es fundamental para establecer, desarrollar y alcanzar el nivel de madurez adecuado tanto la motivación y la implicación de los miembros del equipo como el dedicar un tiempo fundamental al diseño del plan sobre todo: la descripción general y la primera evaluación de riesgos.

En el caso de que la importancia de la información para el negocio sea fundamental, como es el caso de SeBacksa, se necesitará la implicación máxima del equipo de dirección, como se ha demostrado en el trabajo y que ha ido desde la definición de los objetivos, el fomento de la motivación y la implicación de las unidades a la implicación activa en la mitigación de los riesgos provisionando los recursos necesarios o incluyendo en el equipo de dirección al experto SGSI para darles soporte.

Es contraproducente desarrollar procedimientos de seguridad excesivamente complejos, porque limitan la operatividad y dificultan la toma de decisiones rápidas en el tratamiento de incidentes sobre todo en empresas de dimensión pequeña como es el caso de SeBakSA.

Otra conclusión es la importancia que para garantizar la seguridad de los activos de la información tiene desarrollar una gestión orientada a mitigar el impacto

de los riesgos para lo cual se ha de diseñar un método de evaluación de riesgos completo que ha de permitir conocerlos y afrontarlos de forma coordinada, como lo hace el método de evaluación incluido en el trabajo. Y, seguidamente, definir unos planes bien de acción o bien de seguimiento con unos controles de seguridad que permitan verificar el rendimiento de cada plan.

Es fundamental la concreción de los controles de seguridad para supervisar el seguimiento de los planes de acción, unos controles como los incluidos en el trabajo, (número de alarmas, de errores de operación, de mejoras de los procesos…) concretos y medibles en el tiempo permiten evaluar la efectividad de los planes de acción.

La efectividad de los planes de acción definidos para mitigar los riesgos es fundamental, en nuestro caso se demuestra ya que gracias a los planes de acción se han podido mitigar la mayor parte de los riesgos ajustándolos a valores más asumibles que solo requieren un seguimiento más que una actuación.

La importancia de la gestión de riesgos en cualquier empresa es indiscutible por lo que es fundamental diseñar un método de evaluación de riesgos que se ajuste al escenario y que obtenga la aportación de todos los equipos implicados, así se consigue una imagen muy completa de todos los riesgos al contar con la aportación de las vistas de todos los equipos implicados.

Un ejemplo de ello se ha obtenido en el análisis de riesgo de SeBackSA. El plan de continuidad del negocio se ha desarrollado a partir de uno de los riesgos detectados. Es cierto que uno de los atractivos de SeBackSA es el ofrecer un “second location” a otras empresas para facilitarles la continuidad de su negocio en caso de desastre, sin embargo no se había tenido en cuenta para la misma SeBackSA, gracias a un análisis de riesgos metódico ese riesgo se detectó y se diseño el plan de acción necesario.

En resumen se ha diseñado un SGSI ajustado a las necesidades de SeBackSA, empresa pequeña cuyo principal activo es la información y listo para ser certificado como modelo SGSI de acuerdo con la norma ISO 27001.

El número de horas dedicadas para la realización de este proyecto ha sido de 630 horas.

10. BIBLIOGRAFÍA

-Estandard Internacional ISO/IEC 27001-2005

-Parámetros fundamentales para la implantación de un Sistema de Seguridad de la Información según ISO 27001:2005. José Manuel Fernández Domínguez. Nexus Consultores y Auditores.

-Página web: https://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos

-Página web: http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/ISOIEC-27001/