Módulo 9:
Gestión y tratamiento de los riesgos. Selección de los controles

Este apartado describirá en qué consiste la gestión de riesgos, cómo se deben escoger los controles, se darán recomendaciones para la selección y se explicará la manera de documentar esta selección.

Los puntos a tratar son:

- Gestión del Riesgo.
- Mitigación del Riesgo.
- Documentar la Gestión del Riesgo.

I. Gestión del riesgo:

La gestión de esos riesgos implica seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.

Un resultado del análisis de riesgos habrá sido el criterio para determinar cuáles van a ser los niveles de riesgo aceptables y en consecuencia, cuáles van a ser los niveles inaceptables y que por lo tanto son susceptibles de ser gestionados. La gestión de los riesgos tiene como objetivo reducir los riesgos que estén por encima de los niveles aceptables, a niveles que puedan ser asumidos por la organización.

Una vez que conocemos los riesgos de la organización y decidido el tratamiento que se le va a dar para cada uno de los activos, se deben tomar acciones en consecuencia. Los cuatro tipos de tratamiento requieren de acciones de distinta naturaleza:

- **Mitigar el riesgo:** Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

- **Asumir el riesgo:** La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.

- **Transferir el riesgo a un tercero:** Como por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

- **Eliminar el riesgo:** Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

No caben más acciones a la hora de gestionar los riesgos para la correcta implantación de un sistema de gestión de la seguridad de la información, ya que una organización que conoce sus riesgos jamás podrá ignorarlos, puesto que, de este modo, no estaría vigilando que no se convirtiesen en riesgos que la organización no es capaz de asumir o que, por no haberlos tenido en cuenta, se materialicen y den lugar a un incidente de seguridad.

Una vez decididas las acciones a tomar, se debe realizar un nuevo análisis de riesgos, teniendo en cuenta la nueva situación considerando que los controles y medidas que se ha decidido implantar van a reducir en mayor o menor medida el riesgo que existía, ya que ese es su objetivo. El nivel de riesgo resultante de este segundo análisis es el riesgo residual. Este se define como el riesgo remanente que existe después de que se hayan tomado las medidas de seguridad apropiadas

En una organización nunca se podrá eliminar totalmente el riesgo, siempre quedará un cierto nivel de riesgo, por lo que es importante que todos los riesgos residuales sean aceptados por la Dirección.

II. Mitigación del riesgo:

En el caso de se decida mitigar el riesgo, los pasos a seguir son:

1. Seleccionar los controles apropiados para los riesgos a los que se quiere hacer frente, en principio del Catálogo de Buenas Prácticas de la ISO/IEC 27002 (133 controles posibles), pero pueden añadirse otros que la organización considere necesario.

2. Implantar los controles para lo que deben desarrollarse procedimientos. Aunque sean controles tecnológicos deben desarrollarse para su instalación, uso y mantenimiento.

3. Verificar que los controles están correctamente implantados.

4. Establecer indicadores para saber en qué medida la implantación de los controles seleccionados reduce el riesgo a un nivel aceptable.

Los controles se seleccionarán e implementarán para minimizar en lo posible la posibilidad de que los riesgos detectados en el análisis de riesgos dañen los activos.

Existen dos grandes grupos de controles. Por un lado los técnicos, tales como sistemas de cifrado, copias de seguridad, sistemas de detección de intrusos, actualizaciones de software, antivirus o cortafuegos, y por otro los organizativos que son medidas organizativas tales como la Política de Seguridad, procedimientos de uso de los sistemas de información para los usuarios, los planes de formación o los planes de continuidad del negocio.

Es muy importante conseguir un conjunto de controles que contenga controles de los dos tipos, ya que muchas medidas técnicas no pueden impedir que los usuarios de los sistemas cometan errores o dañen intencionadamente los activos y, al contrario, emitir muchas normas internas puede ser inútil si no hay una mínima seguridad técnica implantada.

Por ejemplo, el estudio del uso de ordenadores portátiles para trabajos fuera de las instalaciones de la organización puede haber determinado que existe un riesgo alto de robo para los portátiles. Se pueden escoger varios controles para mitigar este riesgo. Uno de ellos será diseñar unas normas de utilización de este tipo de activos, que obligue a los usuarios a no dejar sus portátiles desatendidos y a no dejarlos a la vista en el coche. Con este control es probable que se reduzca la probabilidad de robo, sin embargo la posibilidad todavía existe. Así que es necesario tomar otras medidas como el cifrado del disco duro y un proceso de autenticación de usuario, que servirán para reducir el daño a la confidencialidad que se produciría si el equipo es robado.

La combinación de las medidas técnicas y organizativas consigue un nivel de seguridad razonable con unos recursos limitados para el escenario de riesgo que se trataba de mitigar.

Otra clasificación que se puede hacer de los controles para facilitar su selección es la de controles preventivos y correctivos. Los controles de tipo preventivo son aquellos que sirven para evitar incidentes de seguridad no deseados mientras que los correctivos son aquellos que se pondrán en marcha ante la ocurrencia de fallos o incidentes de seguridad.

Por ejemplo, para prevenir accesos no autorizados a una red se crean cuentas de usuario y se otorgan privilegios a estos usuarios, diferenciando aquellos que sí pueden acceder de los que no. En el caso de que ocurriera un acceso no autorizado, por ejemplo, un empleado que ha cambiado de departamento y conserva sus antiguos privilegios de los que hace uso, lógicamente primero hay que ser capaces de detectarlo y una vez detectado, esos privilegios deberían ser automáticamente eliminados.

Muchos controles están interrelacionados, por lo que hay que tener en cuenta estas dependencias para que no queden lagunas de seguridad que puedan suponer nuevas vulnerabilidades.

Hay que tener en cuenta que la implantación de un control requiere de ciertos recursos y su mantenimiento también. Por lo tanto hay que valorar al escoger un control, si se cuenta con dinero y mano de obra suficientes tanto para ponerlos en marcha como para gestionarlos.

Esto significa que hay que considerar varios factores y restricciones a la hora de seleccionar un control, ya que puede darse el caso de que a pesar de cubrir un riesgo detectado, no se puede o no debe ser aplicado, como por ejemplo:

- El mencionado coste de la implementación y el mantenimiento del control. Por ejemplo, se escoge el control 11.6.1 Restricción del acceso a la información y para implantarlo se decide instalar un firewall. Esta decisión tiene el coste de su compra, más el de su instalación, configuración y gestión.

- La disponibilidad del control. Puede ser necesario instalar un firewall pero si el modelo específico necesario para la organización tiene un plazo de entrega muy largo, puede ser necesario optar por alguna otra medida al menos temporalmente.

- Ayuda que hay que otorgar a los usuarios para desempeñar su función. Siguiendo con el ejemplo del firewall, hay que considerar que el responsable de su gestión dentro de la organización debe saber hacerlo. Si no es así, habrá que valorar darle formación o bien subcontratar el servicio. Además los usuarios de la red verán probablemente restringidos sus privilegios de acceso, por lo que habrá que informar de la nueva situación y buscar soluciones alternativas si surge algún problema.

- Controles que ya existen y sólo hace falta modificarlos. Si se diera el caso de que ya existe un firewall en la organización realizando las funciones requeridas por el control, quizás se pueda solucionar el problema con un cambio en la configuración o con una actualización del software. También podría suceder que ya hay aplicados otros controles que mitigan el mismo riesgo, y añadir otro resulte excesivo o demasiado costoso.

- Su aplicabilidad de acuerdo con los riesgos detectados. En cualquier caso, si no hay un riesgo claro en la organización respecto a los accesos a la información la aplicación del control 11.6.1 no estaría justificada.

No todos los controles deben ser seleccionados, pero los hay que siempre deben ser implantados si no lo están ya y son aquellos que constituyen un requisito de la Norma UNE/ISO-IEC 27001 tales como la Política de Seguridad o las auditorías internas.

Seleccionados los controles pertinentes, debe definirse los procedimientos para su implantación. Los controles de tipo organizativo se prestan más a ser implantados mediante procedimientos, como por ejemplo la gestión de los recursos humanos. Pero incluso los de corte tecnológico pueden ser susceptibles de necesitar documentación, como por ejemplo la realización de copias de seguridad.

Debe analizarse la lista de controles seleccionados y establecer qué procedimientos necesitan ser desarrollados. Hay que contar también que si la organización no tiene procesos muy complejos puede ser posible que varios controles puedan agruparse en un único procedimiento. No es necesario ni recomendable, desarrollar un procedimiento para cada control. La cantidad de documentación generada puede hacer francamente difícil que se logren gestionar correctamente los controles. Por otro lado, los procedimientos deben ser lo más breves y claros posible. No deben incluir demasiadas instrucciones ni particularidades de la tarea a realizar. El objetivo del procedimiento es contar con una herramienta que permita a cualquiera ejecutarla con un mínimo de rigor aun sin contar con formación o experiencia previa.

Una vez puestos en marcha, debe comprobarse periódicamente que los controles funcionan como se esperaba. Si no es así, deberán tomarse las acciones necesarias para corregir esa situación.

Una herramienta fundamental del SGSI es la verificación de la eficacia de los controles implantados. Para ello deben establecerse objetivos de rendimiento para los controles, marcar puntos de control y medición y registrar los resultados de manera que se sepa si el control realmente protege los activos hasta el punto que la organización necesita.

Por ejemplo, se detecta el riesgo de que los puestos de usuarios se infecten de virus, por lo que se determina aplicar el control 10.4.1, Controles contra el código malicioso. Para implantar este control se decide instalar en todos los puestos un antivirus actualizable automáticamente a diario. Se prepara la compra de la aplicación, se valoran distintas opciones, se compra la que se considera más apropiada y el responsable de sistemas se encarga de instalarla en todos los puestos. Se ha hecho un gasto para la compra del material y otro de mano de obra del responsable de sistemas, para los que he necesario presentar una justificación. Esta justificación vendrá dada por la reducción de las infecciones de virus en los puestos y la consiguiente reducción de horas de trabajo perdidas solucionando estas incidencias. Si hasta la instalación del antivirus teníamos 4 infecciones mensuales, en las que se empleaban 6 horas de trabajo, los objetivos pueden declararse como sigue:

- Reducir el Nº de infecciones /mes a 2
- Reducir el Nº de horas empleadas en repararlas/mes a 3

Se establece que semanalmente el responsable de sistemas comprobará el número de infecciones y registrará el tiempo empleado en su resolución, reportando los resultados mensualmente. Los registros de los tres meses siguientes son:

1. Mes 1. Nº de infecciones 0. Horas empleadas en reparación: 0
2. Mes 2. Nº de infecciones 3. Horas empleadas en la reparación: 3
3. Mes 3. Nº de infecciones 1. Horas empleadas en la reparación: 2

De estos datos podemos inferir que más o menos se está consiguiendo el objetivo, y en cualquier caso ha habido una reducción significativa de las pérdidas en términos de costes de horas de trabajo que originaban las infecciones, que justifican sobradamente la inversión en la compra e instalación del antivirus.

III. Documentar la gestión de riesgos:

La documentación de la gestión de riesgos se realiza mediante la Declaración de Aplicabilidad también conocida por sus siglas en inglés SOA (“Statement Of Applicability”). Este documento, requerido por la Norma UNE/ISO-IEC 27001, es un resumen de las decisiones que se han tomado para tratar los riesgos analizados.

Este documento registra todo lo que se ha realizado y se va a realizar en el futuro inmediato para que la seguridad de la información de la organización llegue al nivel que se haya estimado apropiado para sus necesidades y recursos. La declaración de aplicabilidad debe incluir los 133 controles del Anexo A de la Norma, mas los controles adicionales a los de la Norma que la organización hubiera estimado conveniente aplicar. Para cada uno de los controles debe reflejarse en este documento:

- Si está implantado actualmente en la organización, con una breve descripción de cómo se aplica.
- Si se va a implantar, es decir, si es uno de los controles escogidos para mitigar el riesgo, junto con las razones para haberlo seleccionado.
- Si no se va a implantar, y entonces hay que exponer los motivos que han llevado a esta decisión. Las exclusiones deben justificarse adecuadamente.

El principal objetivo de este documento es que, al tener que repasar todos y cada uno de los controles, se hace una comprobación de que no se ha pasado por alto ningún control por error o descuido, que podría ser útil o necesario para la gestión de la seguridad de la información.

Este documento constituye de alguna manera un registro de los resultados finales del SGSI, ya que concreta de manera clara y directa en qué va a consistir el sistema de seguridad, detallando cada uno de los controles que se tiene la intención de aplicar de manera explícita.

Sólo insistir en que no es necesario seleccionar todos los objetivos ni todos los controles asociados a cada uno de los objetivos. Deben escogerse los objetivos y controles apropiados a las circunstancias, es decir, aquellos que se considera que cubren los requisitos de seguridad de la organización y son viables.

Una vez que está claro que se va a hacer, debe prepararse un plan para la realización de todo lo que se ha decidido hacer. Este plan, que la Norma denomina Plan de Tratamiento de Riesgos, contempla todo las acciones necesarias tanto para implantar el SGSI y gestionarlo como para la puesta en marcha de los controles escogidos.

El plan tiene que contar con los recursos materiales, técnicos y humanos necesarios para que pueda ser llevado a cabo con ciertas garantías de éxito. Debe ser revisado a intervalos regulares para comprobar que no se producen desviaciones. Estas pueden ser de plazo porque no hay recursos para ejecutarlas o han resultado ser más difíciles de ejecutar de lo que se preveía en un principio o también de que no se llevan a cabo las acciones planificadas sino otras, normalmente porque se han tomado decisiones sobre la marcha para solventar problemas no previstos.

Dentro de este plan pueden quedar recogidos los objetivos definidos para medir la eficacia de los controles, estableciendo asimismo el mecanismo de recogida y análisis.

El avance en la consecución de los objetivos suele ser unos de los puntos que se tratan en el Comité de Seguridad, ya que es en este Comité donde se deciden los objetivos y se modifican según sea necesario.

Evaluación Módulo 9

1. **Para gestionar adecuadamente el riesgo:**

   - [ ] Deben implantarse todos los controles del Anexo A de la Norma UNE/ISO-IEC 27001
   - [ ] Deben implantarse todos los controles necesarios para las necesidades de la organización.
   - [ ] Deben implantarse pocos controles para que el proyecto no sea muy costoso
   - [ ] Dejar en blanco

2. **Gestionar el riesgo implica:**

   - [ ] Mitigarlo o asumirlo
   - [ ] Transferirlo o eliminarlo
   - [ ] Todas las de arriba
   - [ ] Dejar en blanco

3. **Se sabe si un control es efectivo cuando:**

   - [ ] Cumple los objetivos que se le han marcado
   - [ ] Funciona bien
   - [ ] Es fácil y barato de mantener
   - [ ] Dejar en blanco

4. **La declaración de aplicabilidad es un documento que recoge todos los controles que la organización piensa utilizar en el futuro:**

   - [ ] Verdadero
   - [ ] Falso
   - [ ] Sólo si va a hacerlo dentro del año
   - [ ] Dejar en blanco