Seguridad de la información y continuidad de negocio en Tecnatom

C. Fernández de Miguel

La seguridad de la información es una característica indispensable en las organizaciones que manejan y procesan datos relativos al negocio nuclear. La apertura de los sistemas de información las facilidades de intercambio de recursos a través de sencillas y extensas redes de comunicación constituyen los ejes de la cooperación entre las diferentes organizaciones generando un ahorro importante de costes y ampliando su capacidad de minimización. En este contexto la seguridad de la información es uno de los mayores retos para las Direcciones de Sistemas.
En este artículo Tecnatom presenta su experiencia en el proyecto de "Implantación de la gestión de la Seguridad de la Información". A lo largo de varios años, desde el 2004, la gestión de la seguridad de la información se ha ido construyendo y consolidando como un proceso continuo y horizontal.

Information security is a key issue for companies that manage and process nuclear business related data. Availability of information systems as well as new data exchange facilities through simple and broad communication networks are the pillars of cooperation between different organizations, generating significant savings in costs and expanding the capacity to minimize them.
In this regard, information security is one of the major challenges for IT departments. This article presents Tecnatom's experience in the "Information Security Management Implementation" project. Over several years, since 2004, the information security management has been developed and consolidated as an ongoing and horizontal process.

CONSUELO FERNÁNDEZ DE MIGUEL es licenciada en Ciencias Químicas, máster en Informática por la U.P.S y máster en Seguridad Informática por la UOC. Incorporada a Tecnatom S.A. en el 1989 en la Dirección de Sistemas de la Información, ha sido la jefe de Proyecto de Implantación de Seguridad de la Información y actualmente ejerce las funciones de consultor de Seguridad de la Información.

INTRODUCCIÓN

Las Tecnologías de la Información y las Comunicaciones (TIC) desempeñan un papel dinamizador de la competitividad de la economía a nivel global e impulsan la innovación, la creatividad y la eficiencia en nuestras organizaciones.

La evolución de las TIC en los últimos años ha sido extraordinaria, aumentando la capacidad de gestión y almacenamiento de manera exponencial. Pero esta evolución tecnológica también ha generado nuevas amenazas y vulnerabilidades para las organizaciones.

Todo ello, unido a la naturaleza de la información que el sector nuclear gestiona, hace necesaria la adopción de planes y políticas de seguridad que permitan asegurar la disponibilidad, integridad y confidencialidad de la información, controlando dicha información durante todo su ciclo de vida: creación, almacenamiento, tratamiento, comunicaciones y destrucción.

Ello conlleva un desafío permanente con la seguridad de la información, incorporando la política de seguridad en todos nuestros procesos y actuaciones.

De esta manera, en Tecnatom, según se indica en la Figura 1, la seguridad de la información no es tratada como un producto, sino como un proceso continuo y horizontal a toda la organización y servicios que presta la Dirección de Sistemas de la Información al resto de la compañía y clientes.

El proyecto de implantación de la seguridad de la información: reseña histórica

En 2004, la situación de Tecnatom era la de una empresa con seguridad informática. Es decir, se disponía de las medidas técnicas necesarias para garantizar la seguridad perimetral: cortafuegos, el centro de proceso de datos –que comparte medidas de seguridad física con el Centro de Simulación– tenía de las medidas básicas de seguridad (falso suelo, climatización, UPS, control de accesos, medidas anti-incendios etc.), la información estaba respalda por un sistema de *back up*, se disponía de un sistema *antimalware* y se habían establecido las medidas necesarias para el cumplimiento de la LOPD.

Pero en una auditoría de seguridad perimetral se detectaron varias áreas de mejora y se decidió abordar un proyecto de gestión de la seguridad de la información basándonos en los estándares internacionales ISO 17799 cuya experiencia en la implantación vamos a desglosar en este artículo.

Paso 1. ¿Qué se debe proteger?

La primera fase del proyecto fue responder a la pregunta ¿qué información debemos proteger? Para ello se identificaron y clasificaron los activos informáticos: activos de información (ficheros y bases de datos, documentación de clientes y suministradores, material de formación, procedimientos operativos y de soporte etc.), activos de *software* (aplicaciones, sistemas operativos, programas de desarrollo etc.) y activos físicos (servidores, ordenadores personales, tabletas, *smartphones*, sistemas de almacenamiento, equipos de comunicaciones etc.).

Figura 1. Gestión de las TIC.

Figura 2. ¿Qué tenemos que proteger?

Dado que las necesidades de protección y recuperación no son las mismas para todos los activos informáticos, una seguridad eficaz y eficiente requiere clasificar el valor de cada activo en función de las tres dimensiones de la seguridad (Figura 2):

Confidencialidad. Asegurar que únicamente las entidades (personas ó sistemas) autorizadas tengan acceso a la información.

Integridad. Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.

Disponibilidad. Garantizar que el acceso a los activos de información o al resto de activos informáticos se produce correctamente y en tiempo. Es decir, la disponibilidad garantiza que los sistemas funcionan cuando se les necesita.

Y para ello se estableció el siguiente sistema de clasificación:

Una vez realizado el inventario de activos informáticos la gestión del mismo se realiza mediante una CMDB o Base de Datos de la Gestión de Configuración donde se encuentran inventariados los activos de información, aplicaciones, *hardware* y *software* asociado, así como las relaciones entre los mismos y su clasificación. En la actualidad tenemos 187 activos de información y 276 aplicaciones que la gestionan.

Paso 2. ¿Cuáles son las amenazas? ¿Qué riesgo tenemos en los activos?

Una vez conocidos los activos críticos a proteger realizamos un análisis de riesgos con la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) por ser una de las metodologías más extendida en España.

El objetivo del análisis de riesgo es el conocimiento y reducción del nivel de riesgo al que los activos informáticos de una organización se encuentran expuestos, entendiendo como riesgo de seguridad la posibilidad de que una amenaza dada aproveche una vulnerabilidad para dañar un activo o un grupo de activos de información.

Los pasos seguidos para el análisis de riesgos fueron:

1. Valorar los activos informáticos en el sentido del perjuicio (coste) supondría su degradación y/o ausencia.
2. Determinar las amenazas a que están expuestos los activos informáticos.
3. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
4. Estimar el riesgo, definido como el impacto ponderado con la probabilidad de ocurrencia de la amenaza.

Una vez detectados los riesgos, se puede actuar:

- Reduciendo el riesgo implantando una serie de controles de seguridad que permitan reducir la amenaza, la probabilidad o el impacto.
- Asumiendo el riesgo en el caso de que los costes de protección sean elevados y la probabilidad de que suceda sea pequeña. En el caso de que el incidente llegara a suceder, la organización tendrá que ejecutar su plan de continuidad de negocio, del que se habla más adelante.
- Transfiriendo el riesgo a terceros (seguros, proveedores, etc.).

Paralelamente al análisis de riesgos se realizó una autoevaluación del estado de la seguridad de la información frente al estándar ISO 17799. El resultado de ambas acciones fue un

Figura 3. Clasificación de los activos.

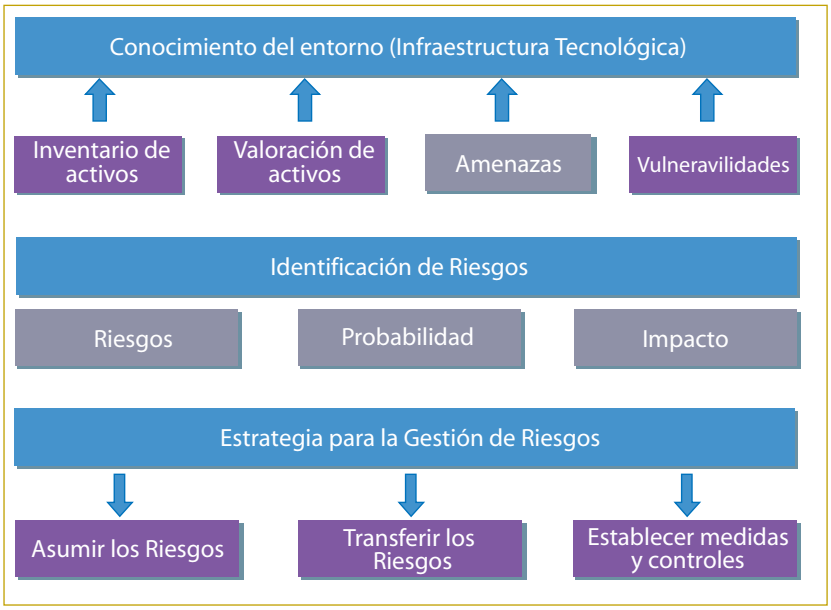

Figura 4. Analisis de Riesgos.

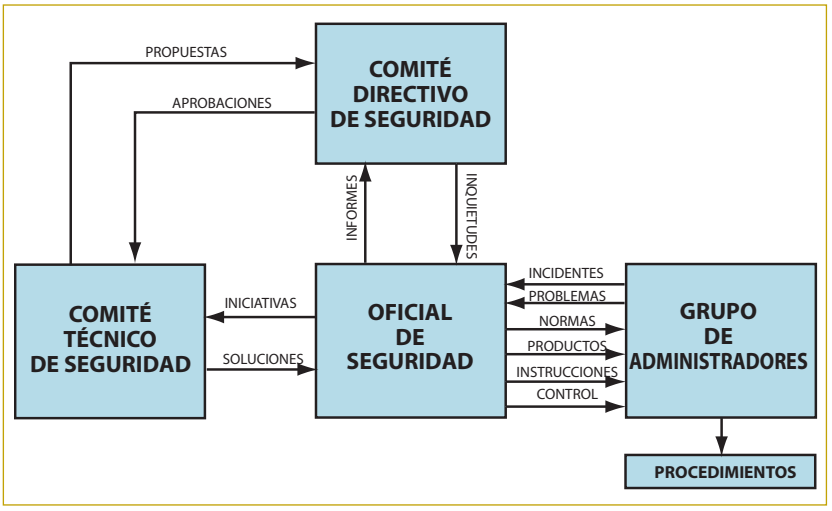

Figura 5. Organización de Seguridad de la Información.

Plan Director de la Seguridad de la Información.

Paso 3: ¿Cómo proteger? La selección e implantación de controles de seguridad, desde el aspecto más técnico al más organizativo

La mejora la seguridad de la información en una organización consiste, no solamente en centrarse en la implantación de controles técnicos, sino tener una visión global de la seguridad de la información y que tecnología, procesos y personas funcionen de manera conjunta y coordinada.

Para todo ello es vital el compromiso de la dirección de la organización con la seguridad de la información y la existencia de unas principios y criterios básicos que rigen la seguridad de la información en Tecnatom y que se plasman en una "Política de Seguridad de la Información" y una "Norma de Seguridad de la Información". La definición de estos dos documentos y su difusión fue el primer hito del Plan Director de Seguridad.

Dichos documentos responden a preguntas como: ¿por qué la información es importante y estratégica para la Organización? ¿cuáles son los requisitos legales y de negocio para la seguridad de la información? ¿qué pasos debe tomar la organización para garantizar la seguridad de la información? ¿cuáles son las responsabilidades en materia de seguridad de la información?

Definida la Política de Seguridad de la Información por la Dirección, se establecieron las diferentes funciones de las personas con responsabilidad directa sobre la seguridad de la información. La Organización de Seguridad de Tecnatom está constituida por un oficial de Seguridad (director de Sistemas de Información) que se apoya en un Comité Técnico de Seguridad (mensual) y un Comité Directivo de Seguridad (bianual).

Continuando con el desarrollo del Plan de Director de Seguridad se fueron incorporando los siguientes controles de seguridad:

- Política de control de accesos basada en el principio "Acceso a lo que se requiere para el trabajo" y proceso de Gestión de Identidades para asegurar que los permisos sobre los sistemas de información y aplicaciones están autorizados, documentados y se revisan periódicamente.
- Formación y concienciación del personal interno. En toda organización se cumple que el eslabón más débil es el personal y por mucha inversión que se realice, la seguridad siempre estará en manos de cada una de las personas que conforman la organización. En este sentido el personal de Tecnatom firma una cláusula de confidencialidad en su contrato laboral y se dispone de un Manual de Seguridad de la Información del Personal Interno y existe un Plan de Concienciación que recoge tanto la formación en esta materia como la publicación en el *Portal del Empleado* de artículos relativos a seguridad de la información y seminarios específicos, como los realizados sobre LOPD.
- Acceso de Terceras Partes (clientes, suministradores, socios). Se han procedimentado los pasos a seguir en cuanto a Seguridad de la Información para dar acceso a nuestros sistemas/activos de información a personal de un cliente, de un socio o de un suministrador de una manera segura y gestionada, elaborando un Manual de Seguridad de la Información para Terceras Partes.
- Manual General de Operaciones. Recoge todos los procedimientos de operación de los diferentes sistemas de información con el objetivo de asegurar la operación correcta y segura de los recursos de tratamiento de la información y su disponibilidad.
- Conformidad con los requisitos legales. Implantación de la LOPD y más específicamente del Real Decreto 1720/2007, de 21 de diciembre. Desde su implantación ya se han realizado dos auditorías bianuales.
- Incorporación de sistemas de monitorización y control para adelantarse a los incidentes y asegurar la disponibilidad de los servicios TI.
- Implantación del proceso de gestión de incidentes. Cualquier incidencia en los sistemas de información es analizada desde el punto de vista

de la integridad, confidencialidad y disponibilidad y si, se ha puesto en riesgo cualquiera de ellas, se abre una incidencia de seguridad realizándose un análisis de causa raíz y estableciéndose las medidas necesarias para que no se vuelva a repetir.

¿Y en caso de desastre? Paso 4: Continuidad del negocio

Una pérdida de suministro, una inundación, un incendio, un robo o un ataque informático masivo, son amenazas reales que, en caso de materializarse, pueden impedir la continuidad de una empresa.

Invertir en una estrategia y un plan de continuidad de negocio en caso de desastre es un seguro y cuando más se optimice el alcance de lo que queremos proteger menor será su coste. ¿Y cómo podemos saber que debemos y que no debemos proteger en caso de desastre? Para ello tenemos una herramienta, el Análisis de Impacto. Cuanto mayor sean los requisitos, mayor será el coste anual del "seguro".

En Tecnatom, realizamos el Análisis de Impacto en el año 2005 y lo revisamos en 2011, con dicho análisis delimitamos por cada servicio/proceso que se presta en la compañía los recursos informáticos, humanos y materiales que se requieren en situación de normalidad y los mínimos necesarios para funcionar en caso de desastre. De esta manera, para servicio/proyecto tenemos:

- Los recursos mínimos (humanos, materiales, servicios TI, etc.) que debemos disponer para prestar el servicio/proyecto en condiciones degradadas, sin que ello conlleve pérdida económica o de imagen para la compañía.
- El tiempo máximo que podemos estar sin prestar el servicio/proyecto.
- La valoración del servicio/proceso en términos cuantitivos (pérdidas económicas en caso de no prestarse) o cualitativos (nivel de criticidad).
- La información del servicio/proyecto que se puede perder en caso de desastre (horas, días, semanas ...).

Si el Plan de Continuidad de Negocio contiene todos los procedimientos a seguir para garantizar la continuidad de las operaciones críticas de una compañía, el Plan de Contingencia es un caso particular del plan de continuidad del negocio aplicado al departamento de informática o tecnologías y está, por lo tanto dirigido a asegurar la continuidad de los servicios de TI críticos.

EL resultado del Análisis de Impacto fue una lista de servicios TI con tres parámetros: nivel de criticidad, RTO (*Recovery Time Objective*: tiempo en que un servicio TI debe ser restaurado después de un desastre) y RPO (*Recovery Point Objective*: es el máximo periodo de tiempo tolerable de pérdida de datos en un Servicio TI) así como la estrategia a seguir para la recuperación de los servicios TI.

En Tecnatom, hemos apostado por disponer de un centro de replicación de datos donde tanto el almacenamiento como el *backup* en disco y los servidores mínimos necesarios, se replican una vez al día asegurando la disponibilidad de los servicios TI más críticos en caso de desastre.

LA MEJORA CONTINUA

La definición de Programas de Evaluación y Mejora, Mantenimiento y Auditoría han permitido procedimentar los procesos de mejora continua de la seguridad mediante:

- Conjunto de indicadores que miden el estado de salud de la seguridad y la eficacia y eficiencia de los controles establecidos.
- Establecimiento de procedimientos de revisión y auditoría.

Así, a modo de ejemplo desde 2005:

- Se han hecho varias actualizaciones de la política, las normas y los manuales de seguridad del personal interno y terceras partes, recalificando al personal en estos aspectos.
- Se ha revisado el sistema antivirus, incorporando servicios en la nube (*cloud*).
- Se han realizado varios proyectos de mejora del proceso de copia de seguridad (*backup*) hasta finalizar en la arquitectura actual de sistema de copia de seguridad en disco y replicado, a su vez, en el centro de replicación, lo que disminuya los costes operativos y optimiza los tiempos necesarios para su realización.
- Se han incorporado nuevas tecnologías de cortafuegos, mejorando la seguridad y simplificando la infraestructura.
- El Manual General de Operaciones está en constante revisión actualización.

RESULTADOS

La mejora de la seguridad de la información con los controles implantados se refleja los siguientes aspectos:

- Evolución del porcentaje de cumplimiento de los controles del estándar ISO 27002 que ha evolucionado de un 64,3 % en el año 2004 al 81,9 % en 2012.
- El bajo número de incidentes de seguridad. Frente a un total de 458 activos informáticos, en el año 2012 solamente se registraron 33 incidencias menores, de las que 14 han sido debidas a caídas de sistemas que han causado indisponibilidad, lo que representa una media mensual del 0,6 % sobre el total de activos informáticos.
- El nivel de disponibilidad de los servicios TI que en el año 2012 estuvo en el 98 %.

CONCLUSIONES

Mediante el proceso de gestión de la seguridad de la información en Tecnatom se asegura que la información clasificada como confidencial y crítica como puede ser la documentación de diseño del plantas e instalaciones, los resultados de inspecciones e informes que afectan a la seguridad de las plantas e instalaciones, la base de datos de experiencias operativas o la documentación de instituciones altamente sensibles(INPO, EPRI...), tiene establecidas medidas de control de acceso estrictas para asegurar su correcta protección y recuperación en caso de desastre.

Para cada activo, en función de su clasificación y los riesgos existentes, se establecen las medidas técnicas y organizativas necesarias que pueden ir desde el control de acceso de datos confidencial mediante el directorio activo, sistemas cortafuegos y almacenamiento en cabinas con una disponibilidad del 99,9 % pasando por la encriptación de los datos secretos, hasta la certificación FSA (*Facility security clearance*) disponiendo de un *bunker* aislado con estricto control físico de acceso y caja fuerte de seguridad, para aquella documentación definida como *Top Secret*.

REFERENCIAS

[1] Código de buenas prácticas ITIL Versión 3.0 / ISO 20000 para la Gestión de Servicios TI

[2] ISO/IEC 27001:2005 Information technology: Security techniques. Information security management systems. Requirements.

[3] ISO/IEC 27002:2009 Information Technology. Code of practice for information security management

[4] Modelo para el gobierno de las TIC basado en las normas ISO. AENOR Ediciones.

[5] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[6] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal

[7] Directiva de la Unión Europea 95/46/CE, de 24 de octubre, sobre protección de las per-sonas físicas en lo que respecta al tratamiento de datos personales y a la libre circula-ción de éstos (DOCE 24-VII-1995).

[8] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.