Operativa de servicios de SI/TI

Dídac López
Ferran Martí

PID_00207672

Universitat Oberta de Catalunya

Índice

Introducción

En este módulo de la operativa del servicio SI/TI describiremos un conjunto de procesos (gestión de incidencias, gestión de configuración y gestión de seguridad) y las actividades relacionadas con la arquitectura tecnológica (hardware, software, redes, datos,...), que forman parte del día a día de la operativa del servicio, orientados a proporcionar la entrega y el uso del servicio.

Los servicios TI de los entornos de producción disponen de actividades operacionales para asegurar que la tecnología está alineada con el servicio en su globalidad, así como con los objetivos de los procesos. En algunas ocasiones las actividades que se mencionarán a continuación son descritas como procesos, pero en realidad se trata de actividades técnicas especializadas.

Las actividades operacionales tienen como objetivo principal asegurar que la tecnología requerida para la entrega y soporte de servicios esté operando de manera eficaz y eficiente.

Es importante tener en cuenta que el conjunto de actividades de operación de servicio no tienen como objetivo gestionar la tecnología para disponer de un buen rendimiento, sino conseguir el rendimiento que integrará los componentes de tecnología con las personas y procesos necesarios para conseguir los objetivos de negocio y de servicio.

Entre las actividades de operaciones más comunes podemos encontrar las siguientes:

- monitorización y control,
- gestión de consolas y puentes de operación remoto,
- planificación de trabajos (*job scheduling*),
- copias de seguridad y restauración,
- gestión de impresión,
- gestión y soporte de servidores y *mainframes*,
- gestión de redes,
- gestión del almacenaje (*storage*) y archivo,
- administración de bases de datos,
- gestión de los servicios de directorio,
- soporte de dispositivos móviles y de escritorio,
- gestión de *middleware*,
- gestión de internet y webs,
- gestión de instalaciones.

Es importante no confundir las actividades agrupadas anteriores con departamentos. Es posible que en determinadas organizaciones las actividades las lleven a cabo departamentos especializados, pero puede suceder que un departamento sea el responsable de una o más de las actividades mencionadas. En todo caso, corresponde a la estructura organizativa de cada empresa decidir de qué modo se departamentalizan las actividades mencionadas.

Objetivos

El objetivo principal de este módulo es observar de qué modo deben ser garantizados determinados procesos para que los servicios puedan ser soportados de manera adecuada. Es imposible que los servicios sean perfectos, los errores forman parte de la existencia de los servicios, y por lo tanto, tienen que existir mecanismos que aseguren cómo pueden ser reparados dichos errores

Tras la lectura de este módulo se deberán haber conseguido los siguientes objetivos de aprendizaje:

1. Saber cómo el entorno tecnológico, incluyendo su evolución, debe ser considerado como un elemento para actualizar la gestión de la operativa.

2. Conocer detalladamente el proceso de gestión de las incidencias.

3. Conocer de qué modo del proceso de gestión de la configuración puede contribuir a que la gestión operacional sea mucho más eficiente.

4. Conocer detalladamente el proceso de gestión de la seguridad.

1. Entorno tecnológico

Además de las actividades operativas mencionadas en el apartado anterior, es preciso que forme parte de la operativa diaria de los servicios la supervisión de las tendencias tecnológicas que aparecen en el mercado.

Es de sobras sabido que los períodos de actualización de versiones de aplicaciones son muy cortos. Sucede lo mismo, aunque con unos períodos más largos con la infraestructura (hardware y redes). No incorporar las nuevas versiones puede convertir la arquitectura tecnológica en un elemento obsoleto que pueda comprometer los resultados que necesita el negocio. Pero al mismo tiempo, hay que considerar otro factor importante consistente en no introducir en los entornos de producción tecnologías que no estén lo suficientemente probadas y consolidadas como para poder asegurar la estabilidad de la infraestructura.

Una buena gestión del contexto tecnológico pasará por estar atento a las evoluciones y oportunidades que ofrecen los avances tecnológicos, para ir incorporándolos a las arquitecturas cuando se considere que el equilibrio de coste-riesgo y beneficio se pueda considerar favorable para los intereses de los clientes.

Una reflexión adicional a tener en cuenta para la gestión del entorno tecnológico es la selección de soluciones abiertas[1], es decir, no exclusivas de un único proveedor que no sean compatibles con otros entornos o fabricantes. La adquisición de soluciones cerradas, aunque puedan ofrecer características muy particulares no encontradas en otras alternativas, tiene la enorme desventaja de no poder evolucionar fuera del marco del proveedor. Puede interpretarse como un modo de encadenarse y se incrementa el riesgo de falta de continuidad en el caso de que el proveedor desaparezca. Nuevamente, se impone el criterio fruto de una evaluación del equilibrio entre obtener resultados muy concretos frente a estar sujeto, con el riesgo que conlleva, a un único fabricante.

(1)Soluciones abiertas u *open source*.

2. Gestión de incidencias

La gestión de incidencias es un proceso importante dentro de la operativa del servicio. De hecho, incluso de manera informal, suele ser el proceso que habitualmente se encuentra más desarrollado dentro de los departamentos de SI/TI.

Los objetivos principales del proceso de gestión de incidencias son restaurar la operativa normal de servicio y minimizar el impacto adverso que puedan tener las incidencias. Por su propia naturaleza, se trata de un proceso puramente reactivo, esto es, reacciona cuando las incidencias ya se han producido y por tanto no ha podido evitarlas.

Es importante en este punto recordar que suele recaer sobre otro proceso, el de **gestión de problemas**, la investigación de las causas que originan las incidencias y su posible extirpación mediante el desarrollo de una solución definitiva.

El valor que aporta este proceso radica en su capacidad para recuperar una situación de normalidad lo antes posible cuando algún aspecto del servicio no está funcionando correctamente. Desde el punto de vista del usuario final, es un proceso importante puesto que permite asegurar que la infraestructura tecnológica tiene un soporte así como una supervisión. Probablemente entra dentro de lo lógico que los recursos o sus configuraciones no sean perfectos, pero no se encontraría tan lógico que no existieran los grupos de soporte apropiados para tratar de corregir las situaciones de error que permitan que los procesos de negocio se ejecuten con normalidad.

Sin embargo, cabe destacar que este proceso está muy ligado al factor temporal, es decir, normalmente al tiempo de resolución de las incidencias. Un error común consiste en obstinarse en corregir totalmente la incidencia sin tener en cuenta que lo más importante es la pronta restauración del servicio. Por lo tanto, aunque pueda suceder que se encuentren soluciones definitivas a las incidencias dentro de los tiempos acordados, lo habitual será poder resolver las incidencias con soluciones provisionales. En ocasiones este último punto es mal interpretado en el sentido de que se corrigen las situaciones con chapuzas. Este no es el sentido correcto. Las soluciones provisionales (o *workarounds*) permiten restaurar el servicio, y en función de la naturaleza de la incidencia, de su repetición y de su impacto, se tratará el tema con mayor profundidad, mediante la apertura de un problema, para conocer la causa y poder eliminarla de raíz. Quede claro que toda incidencia tiene una o más causas ocultas que las

generan, pero que no siempre va a ser necesario buscarlas. Solamente cuando resulte útil para el negocio en términos de tiempo y recursos empleados frente al beneficio que se puede obtener.

Service desk: canal de comunicación de las incidencias

En la resolución de las incidencias aparecen claramente varias funciones. El *service desk* juega un papel muy importante como único punto de contacto o *single point of contact* (SPOC), es decir, como canal único a través del cual los usuarios deberían hacer constar sus quejas, incidencias o reclamaciones. Se recomienda que la comunicación de incidencias al proveedor del servicio se realice siempre a través de este canal y no a través de los especialistas. Entre otras ventajas, a continuación se enumeran algunas:

- Es más improbable que las incidencias queden desatendidas. En el caso de que una incidencia llegue a un especialista, puede no quedar registrada y olvidada encima de su mesa.

- Queda un registro único y unificado que facilita la gestión durante y después de las incidencias.

- Es más fácil asignar la incidencia al especialista que corresponde para la resolución de la incidencia. El criterio de selección de especialista de los usuarios suele no ser válido por desconocimiento del área de especialización.

- Es más fácil poder gestionar adecuadamente los recursos y tener siempre una respuesta. La asignación de las incidencias se realiza de acuerdo a criterios de disponibilidad de los especialistas.

- Se evita matar moscas a cañonazos. Si el criterio de asignación de una incidencia corre a cargo del usuario puede suceder que se ponga en contacto con algún recurso que debe estar priorizando otros aspectos.

Desde el punto de vista del usuario, la perspectiva no suele ser la misma. El usuario considera que es atendido con mayor eficacia y rapidez cuando habla directamente con un especialista. Es posible que en cierto modo no les falte razón, pero las consecuencias que se pueden derivar de la lista anterior (que no es exhaustiva) aconsejan optar como mejor práctica por un modelo centralizado en el *service desk*. Para que el usuario no perciba una merma en la calidad del soporte recibido es necesario que el *service desk* esté configurado y formado de acuerdo a las necesidades específicas. Un *service desk* que se limite a dirigir llamadas sin aportar ningún valor añadido difícilmente podrá ser observado como una mejora en la calidad, por mucho que lo recomienden los marcos de referencia de mejores prácticas.

Responsabilidades del *service desk* en la gestión de incidencias

Las funciones del *service desk* se pueden agrupar en: registrar la incidencia, si es posible, resolverla en primera línea, si no, escalarla a la línea de soporte.

a) Registrar incidencia

Dentro de las responsabilidades del *service desk*, además de recibir incidencias a través de múltiples canales (teléfono, email, formulario web…) es el de registrar, categorizar y priorizar las incidencias. La categoría consiste en facilitar la clasificación de acuerdo al tipo de elemento de infraestructura que está fallando, de ahí que sea muy recomendable disponer de una herramienta que esté integrada con una base de datos de la gestión de la configuración (CMDB), donde pueden aparecer todos los elementos que constituyen la infraestructura tecnológica. Por su lado, la priorización consiste en la asignación de un valor que determinará en qué orden y dentro de qué tiempos comprometidos, debe ser resuelta una incidencia. Normalmente, se sugiere que el valor de la prioridad venga determinado por un valor de impacto y otro de urgencia. El impacto determina cuántos usuarios pueden verse afectados y también la severidad o criticidad que el servicio tiene sobre el negocio. Por su lado, la urgencia determina la demora aceptable sin que se resuelva la incidencia.

b) Resolver en primera línea

También forma parte de las responsabilidades del *service desk* tratar de realizar un diagnóstico inicial y si es posible, encontrar una solución provisional o definitiva. Para ello puede basarse en su propia experiencia, o en la consulta a una base de datos de conocimiento, donde aparecen recogidas múltiples soluciones provisionales y definitivas de incidencias que han ocurrido en el pasado. Además de intentar encontrar una solución, se puede delimitar el alcance de la incidencia y dicha información debe quedar registrada con el objeto de que, si es necesario un escalado funcional, los equipos que recibirán la asignación puedan disponer del máximo de información.

Es deseable que la tasa de resolución en primera línea, esto es en el *service desk*, sea lo más elevada posible. Cuanto más cercana al 100% de incidencias resueltas sin necesidad de escalado, más credibilidad, eficiencia y rapidez de resolución generará entre los usuarios. Existen distintos elementos que pueden facilitar el incremento de esta tasa, y entre ellos se cuenta el fácil acceso a una base de datos de conocimiento actualizada y ajustada al propósito, la formación técnica de los operadores, la creación-documentación-formación-concienciación de los procedimientos de uso.

c) Escalar la incidencia

Cuando no sea posible la resolución en primera línea, el proceso de incidencias continúa en alguna de las líneas de soporte que recibirán la asignación. Las líneas de soporte existen principalmente en razón de su especialización. Por lo tanto, una vez reciben el aviso de incidencia asignada, deben proceder a encontrar una solución provisional dentro de los tiempos asignados en función de la prioridad establecida. Se insiste en no confundir el escalado funcional que acabamos de describir con el objetivo de encontrar la causa. No corresponde a una línea de soporte de incidencias encontrar la causa, sino encontrar con prontitud una solución que recupere el servicio lo antes posible.

Tanto si la solución provisional o definitiva es encontrada por el *service desk* como por alguna de las líneas de soporte adicionales, el paso siguiente consiste en la resolución y recuperación del servicio, es decir, en construir la solución si es necesario y aplicarla al entorno de producción. El paso final en el proceso consiste en el cierre de las incidencias. El cierre es, en principio, una responsabilidad del operador del *service desk* y consiste en validar (mediante el método que se considere oportuno) que el usuario está satisfecho con la solución aplicada y acabar de documentar adecuadamente.

Una adecuada gestión de las incidencias es clave para que la operativa del servicio sea correcta. En el caso de que no se resuelvan las incidencias dentro de los intervalos acordados con el negocio, dada la visibilidad tan directa que tiene una interrupción de servicio, tiene un impacto muy negativo sobre la credibilidad y la capacidad del proveedor del servicio.

Se ha hablado en algunos de los párrafos precedentes de la necesidad de acordar los tiempos con el negocio. Este aspecto es fundamental si no queremos que la gestión de incidencias acabe convirtiéndose en un caos, donde el criterio estará más basado en la gestión de decibelios (es decir, quien grita más) que en la lógica marcada por la necesidad del negocio. Por lo tanto, un factor crítico de éxito consiste en asegurar que los acuerdos de nivel de servicio existan, y que además recojan cómo serán tratadas las incidencias, en función de la prioridad asignada. Estos acuerdos de nivel de servicio deberían ser negociados en la fase de diseño del servicio y recogidos en un documento formal, el acuerdo de nivel de servicio (ANS) o *service level agreement* (SLA), que deben firmar ambas partes, cliente y proveedor.

Es habitual que el mismo proceso de gestión de incidencias, a través del *service desk*, sea el que se encarga de gestionar también peticiones de servicio, quejas, consultas y reclamaciones. Sin embargo, algunas de las referencias de mejores prácticas, tal como es el caso de ITIL® a partir de la versión 3 o superior, recomiendan realizar una gestión distinta a pesar de compartir la función del *service desk*. Por lo tanto, la gestión de incidencias se debería ocupar exclusivamente de tratar las interrupciones no planificadas de un servicio o las reducciones en la calidad del mismo. Las peticiones de servicio, quejas, consultas

Ved también

Las peticiones de servicio han sido tratadas en el módulo "Provisión de servicios SI/TI", apartado 2. Peticiones de servicio.

y reclamaciones se aconseja que sean tratadas a través del proceso de gestión de peticiones de servicio. Y, por último, las peticiones de cambio deberían ser tratadas a través del proceso de gestión de cambios. Quien debe realizar la adecuada identificación de cada caso y proceder a arrancar el proceso oportuno es el *service desk*, que actúa como punto común para cada uno de los casos comentados.

3. Gestión de la configuración

El proceso de gestión de la configuración, mediante las herramientas de gestión apropiadas, pretende poner a disposición de todos los procesos y funciones un repositorio de conocimiento que facilite la toma de decisiones, así como la gestión global de los servicios.

Conocer qué elementos constituyen la infraestructura tecnológica que da soporte a los servicios necesarios para ejecutar los procesos de negocio, y lo que es más importante, saber de qué modo dichos componentes están relacionados y cómo dependen unos de los otros es sin duda un conocimiento esencial que ayuda en la toma de decisiones rápidas y correctas. El propósito del proceso de gestión de la configuración es fundamentalmente el que ha quedado descrito en este párrafo.

El marco de referencia ITIL® utiliza tres capas distintas para definir los contenidos del sistema de configuración: base de datos de la gestión de la configuración (CMDB), sistema de gestión de la configuración (CMS) y sistema de gestión del conocimiento del servicio (SKMS).

En primer lugar aparece la **base de datos de la gestión de la configuración (*CMDB*)** o *configuration management database*, que contiene los elementos de configuración (*CI*) o *configuration item*.

Por **elementos de configuración (CI)** hay que entender cualquier recurso que sea necesario para la entrega y soporte del servicio y cuya modificación puede tener un impacto, del tipo que sea, sobre la calidad del servicio. Dentro de esta definición, por lo tanto, podemos considerar servidores, *routers*, *switchers*, aplicaciones, módulos, discos…

En principio, el nivel de detalle, por lo tanto el desglose de los elementos de configuración (CI) constituidos por otros CI, es una de las decisiones importantes a la hora de realizar el diseño de la CMDB. Y esto es así, puesto que habrá que alcanzar un equilibrio entre la cantidad de información introducida, frente al esfuerzo que se requiere para mantenerla actualizada. Hay que tener en cuenta que un elemento fundamental de una buena gestión de la configuración es que la información esté al día. De no ser así, las decisiones que se puedan tomar basadas en la CMDB pueden ser erróneas y por lo tanto, deja de generar valor añadido disponer de este tipo de sistemas.

También hay que tener en cuenta que los CI que integran una CMDB no son solo de tipo tecnológico, que es lo que se podría deducir de la lista que se ha presentado en el párrafo anterior. También puede ser un CI la definición de un servicio, o de un contrato, o de un proveedor, o de un usuario, departamento, edificio… Por lo tanto, una CMDB contiene información de los elementos tecnológicos y de gestión que los acompañan. Además, tal como ha sido comentado previamente, lo más relevante es la definición de las relaciones entre los distintos CI. La tipología de relaciones puede ser muy variada con el objetivo de representar las dependencias existentes.

Una base de datos de gestión de la configuración (CMDB) contiene información de los elementos tecnológicos y de gestión que los acompañan, y de la relación que existe entre los diferentes elementos de configuración (CI).

La segunda capa, recibe el nombre del **sistema de gestión de la configuración (CMS)** o *configuration management system*. Esta capa incluye la anterior, pero la complementa fundamentalmente con información de gestión asociada. Por ejemplo, el registro de incidencias puede estar vinculado caso por caso con los CI de la CMDB. A su vez, el registro de incidencias puede estar relacionado también con el registro de problemas, y a su vez, con el de cambios. De modo que es posible pensar en un sistema más extenso que no solamente describe la topología de la arquitectura tecnológica sino que, además, es posible disponer, y en consecuencia gestionar, todos los elementos relativos al comportamiento, modificación, adición de elementos. Una dificultad que puede tener el pasar a la práctica estos conceptos es el de realizar un crecimiento controlado de la información de modo que siga siendo útil. Cuando los vínculos entre distintos sistemas de gestión se realizan sin un criterio bien establecido, puede ocurrir que no obtengamos el valor esperado. Por lo tanto, los proyectos de puesta en marcha de sistemas CMS tienen que tener presente cómo se produce el crecimiento.

La tercera capa recibe el nombre de **sistema de gestión del conocimiento del servicio (SKMS)** o *service knowledge management system*. Esta capa incluye, además de las anteriores, todo el conjunto de repositorios que contengan conocimiento sobre la experiencia, perfiles, habilidades que pueden ser útiles para la toma de decisiones.

Es útil relacionar el sistema de capas anterior con el denominado modelo DIKW (*data-information-knowledge-wisdom*) propuesto en el proceso de gestión del conocimiento de ITIL®. En realidad se trata de un proceso de transformación que parte de la capa más elemental, la de datos, hasta la más sofisticada, la de sabiduría o wisdom. La transformación se realiza en base al incremento o bien de la comprensión o bien de la contextualización.

Ejemplo

Un sistema de CMDB que solamente nos proporciona una fichas descriptiva de un *router* aislado podríamos considerarlo como un elemento de la capa de datos. Sin embargo, ese mismo ítem acompañado del histórico de incidencias asociado no solo a él, sino también a otros *routers*, junto con información recogida de otros procesos podría complementar adecuadamente una toma de decisión que corresponde a la capa de sabiduría.

Existen en el mercado, actualmente, herramientas muy potentes que permiten la creación de CMDB de cierta entidad. Además, algunas de estas herramientas son gratuitas aunque requieren un grado de configuración que quizás no esté al alcance de cualquiera. Es habitual que acompañen a las herramientas de configuración las llamadas herramientas de descubrimiento (o *discovery tools*). Estas son herramientas que proporcionan en tiempo real información sobre el hardware y software que existe en una determinada infraestructura. Además, permiten realizar alertas cuando se detecta una discrepancia entre la infraestructura real y la documentada en la CMDB, de manera que sea necesario arrancar un proceso de reconciliación.

Las principales actividades del proceso de gestión de la configuración son: la planificación, la identificación, el control, la gestión de información y la auditoría.

- Las actividades de **planificación y la identificación** están relacionadas con la planificación y la definición de todos los elementos que integrarán la CMDB, así como qué tipos y qué nomenclatura tendrán.

- La actividad de **control** está más relacionada con describir los procedimientos que aseguren que cada modificación de un CI tenga garantizada su actualización sobre la base de datos. Esto requerirá un nivel de coordinación importante con el proceso de gestión del cambio.

- La actividad de **gestión de la información** es la relacionada con proporcionar el conocimiento requerido a la persona apropiada en el momento en el que lo requiere.

- La actividad de **auditoría** tiene como finalidad asegurar que existen mecanismos que comprueben que la información contenida dentro de la CMDB es vigente.

Es difícil comprender la existencia de un proceso de gestión de la configuración sin la existencia en paralelo de un proceso de gestión del cambio. Básicamente, porque es necesario tener un control apropiado que asegure que cualquier modificación, adición o supresión de un CI tiene que estar reflejada sobre la base de datos. De otro modo, está claro que los contenidos pueden convertirse en obsoletos en poco tiempo invalidando por completo el objetivo principal del proceso.

La planificación de un proceso de gestión de configuración tiene que tener en cuenta, entre otros factores, la diversidad de la plataforma tecnológica, su magnitud, la existencia o no de agentes que informen sobre el descubrimiento, las personas que se podrán dedicar a la recogida y validación de información al menos en una etapa inicial de volcado (*population*) de la base de datos, las herramientas de que se disponga, el nivel de detalle que se quiere alcanzar. En general, suele recomendarse que el inicio de estos proyectos se realice de modo paulatino. Es decir, se inicia con un ámbito reducido (por ejemplo, determinando qué servicios son los más apropiados por el retorno que puede ocasionar controlarlos mediante una CMDB) y con un nivel de detalle que sea asumible dada la cantidad de recursos de que se disponga. A partir de este inicio y conforme se vaya demostrando la viabilidad y retorno del proyecto, se puede ir incrementando el número de servicios incluidos, o cualquier otro criterio que se haya considerado oportuno.

La actual denominación del proceso de gestión de la configuración tal como aparece en la última actualización de ITIL® es la **gestión de la configuración y de los activos de servicio** o *service asset and configuration management* (SACM). Por activo de servicio se puede entender, de manera general, los recursos y capacidades, pero suele quedar reducido al primer bloque. Por lo tanto, al referirse a la gestión de activos, normalmente se interpreta como el control de inventario de los recursos. La gestión de la configuración tiene, por lo tanto, un propósito más extenso, puesto que al conjunto de detalles financieros relativos a los recursos se consideran las relaciones y por ende, las dependencias entre los mismos, dando una capa mayor de información que favorece la toma de decisiones.

4. Gestión de la seguridad

A menudo se ha definido la seguridad como una actitud, como un estado de ánimo, que hace que se implique toda la organización y en todos los aspectos, y que al igual que la calidad, esta empieza por la propia actitud de la organización, no únicamente sobre los servicios de SI/TI.

Esta se debe aplicar de extremo a extremo, desde los recursos e infraestructuras conectados hasta el propio diseño de los servicios y las aplicaciones que los soportan. Disponer de una gestión de datos e información segura implica adoptar de manera global esta actitud, y más en el momento en que la seguridad de la información es clave para el negocio.

La seguridad de la información, consustancial al negocio, se fundamenta en:

- **Confidencialidad**: la información debe ser solo accesible a sus destinatarios predeterminados.
- **Integridad**: la información debe ser correcta y completa.
- **Disponibilidad**: debemos tener acceso a la información cuando la necesitamos.

La gestión de la seguridad debe velar por que la información sea correcta y completa, esté siempre a disposición del negocio y sea utilizada solo por aquellos que tienen autorización para hacerlo.

La gestión de la seguridad es uno de los aspectos esenciales para obtener altos niveles de fiabilidad y disponibilidad, y es tan importante determinar cuándo el servicio estará disponible como el "quién y cómo" va a utilizarlo. La disponibilidad y seguridad son interdependientes y cualquier fallo en una de ellas afectará gravemente a la otra.

Las medidas preventivas requieren un detallado análisis previo de riesgos y vulnerabilidades. Algunos de ellos serán de carácter general (incendios, desastres naturales, etc.), mientras que otros tendrán un carácter estrictamente tecnológico (fallo de sistemas de almacenamiento, ataques de *hackers*, virus informáticos, etc.).

La adecuada prevención de los riesgos de carácter general depende de la coherencia con la gestión de la continuidad del negocio y requieren medidas que implican a la infraestructura de la organización.

Los principales objetivos de la gestión de la seguridad se resumen en:

- Diseñar una política de seguridad, en colaboración con clientes y proveedores, correctamente alineada con las necesidades del negocio.
- Asegurar el cumplimiento de los estándares de seguridad acordados en los acuerdos de niveles de servicio (SLA).
- Minimizar los riesgos de seguridad que amenacen la continuidad del servicio.

La correcta gestión de la seguridad no es responsabilidad, al menos exclusiva, de responsables de la seguridad, que desconocen los otros procesos de negocio. Si caemos en la tentación de establecer la seguridad como una prioridad en sí misma, limitaremos las oportunidades de negocio que nos ofrece el flujo de información entre los diferentes agentes implicados y la apertura de nuevas redes y canales de comunicación, etc.

La gestión de la seguridad debe conocer en profundidad el negocio y los servicios que presta el departamento de SI/TI, para establecer protocolos de seguridad que aseguren que la información esté accesible cuando es necesaria para aquellos que tengan autorización para utilizarla.

Una vez comprendidos cuáles son los requisitos de seguridad del negocio, la gestión de la seguridad debe supervisar que estos se hallen convenientemente plasmados en los SLA correspondientes para, a renglón seguido, garantizar su cumplimiento.

La gestión de la seguridad debe, asimismo, tener en cuenta los riesgos generales a los que está expuesta la infraestructura TI, y que no necesariamente tienen por qué figurar en un SLA, para asegurar, en la medida de lo posible, que no representan un peligro para la continuidad del servicio.

Es importante que la gestión de la seguridad sea proactiva y evalúe *a priori* los riesgos de seguridad que pueden suponer los cambios realizados en la infraestructura, nuevas líneas de negocio, etc.

Para que esa colaboración sea eficaz, es necesario que la gestión de la seguridad:

- Establezca una clara y definida política de seguridad que sirva de guía a todos los otros procesos.

- Elabore un plan de seguridad que incluya los niveles de seguridad adecuados tanto en los servicios prestados a los clientes como en los acuerdos de servicio firmados con proveedores internos y externos.

- Implemente el plan de seguridad.

- Monitorice y evalúe el cumplimiento de dicho plan.

- Supervise proactivamente los niveles de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades.

- Realice periódicamente auditorías de seguridad.

Es imprescindible disponer de un marco general en el que encuadrar todos los subprocesos asociados a la gestión de la seguridad. Su complejidad y las numerosas interrelaciones necesitan de una política global clara en donde se fijen aspectos tales como los objetivos, responsabilidades y recursos.

En particular la política de seguridad debe determinar:

- La relación con la política general del negocio.
- La coordinación con los otros procesos TI.
- Los protocolos de acceso a la información.
- Los procedimientos de análisis de riesgos.
- Los programas de formación.
- El nivel de monitorización de la seguridad.
- Los informes que deben ser emitidos periódicamente.
- El alcance del plan de seguridad.
- La estructura y responsables del proceso de gestión de la seguridad.
- Los procesos y procedimientos empleados.
- Los responsables de cada subproceso.
- Los auditores externos e internos de seguridad.
- Los recursos necesarios: software, hardware y personal.

El objetivo del plan de seguridad es fijar los niveles de seguridad que han de ser incluidos como parte de los acuerdos de nivel de servicio (SLA), acuerdos de nivel de servicio internos (OLA) y acuerdos de nivel de servicio externos (UC).

Este plan ha de ser desarrollado en colaboración con el responsable de la gestión del nivel de servicio, que es la responsable en última instancia tanto de la calidad del servicio prestado a los clientes como la del servicio recibido por la propia organización TI y los proveedores externos.

El plan de seguridad debe ser diseñado con el fin de ofrecer un mejor y más seguro servicio al cliente y nunca como un obstáculo para el desarrollo de sus actividades de negocio.

Una buena gestión de la seguridad debe traducirse en:

- Disminución del número de incidentes relacionados con la seguridad.
- Acceso eficiente a la información por el personal autorizado.
- Gestión proactiva, que permita identificar vulnerabilidades potenciales antes de que estas se manifiesten y provoquen una seria degradación de la calidad del servicio.

Resumen

En este módulo se han descrito los procesos más relevantes que proporcionan el soporte y conjunto de actividades operativas más habituales, que garantizan que los usuarios puedan ser adecuadamente atendidos mientras se entrega el servicio.

Bibliografía

Clayton, I. M. (2008). *The Guide to the Universal Service Management Body of Knowledge: A Definitive Guide to Service Management*. Service Management 101.

Du Moulin, T. (2005). *What Does IT Cost? Viewpoint, Focus On: CMDB* (vol. 1, pág. 1-7). BMC Software.

Du Moulin,T.; Flores, R.; Fine, B. (2008). *Defining IT Success Through The Service Catalog: A Practical Guide* (2.ª ed). Pink Elephant.

Fernández Sánchez, C. M.; Piattini Velthuis, M. (2012). *Modelo para el Gobierno de las TIC basado en normas ISO*. AENOR ediciones.

Leopoldi, R.; Howells, V. (2004). *The Service Catalog*. HDI.

Menken, I. (2010, 2ª. ed). *ITIL V3 Implementation Quick Guide: the art of the stress-free IT Service Management*. Emereo Pty Limited.

Office of Government Commerce (2011). *The official introduction to the ITIL Service Lifecycle*. Londres: TSO.

Quesnel, J. (2010). *Entender ITIL v3: Normas y mejores prácticas para avanzar hacia ISO 20000*. ENI editions.

Tjassing, R. (2008). *Fundamentos de la Gestión de Sevicios de TI Basada en ITIL V3 (ITSM Library)*. Van Haren Publishing.

UNE-ISO-IEC 20000-1 (2011). *Tecnologías de la Información. Gestión del Servicio. Requisitos del Sistema de Gestión de Servicios (SGS)*. AENOR ediciones.