Seguridad en CPD

Manuel Márquez Garrido ,José Manuel Pavón Álvarez,

Antonio José Sáenz Albanés, José Luis Sánchez del Coso

{mmarquez,jmpavon,ajsaenz,jlsanchez}@isotrol.com

ISOTROL S.A., Av. Isaac Newton, nº 3, 4ª planta, 41092 Sevilla, España

Tel. +34 955 036 800, Fax +34 955 036 849

RESUMEN: El despliegue de un centro de proceso de datos que responda adecuadamente a las demandas empresariales tanto internas como de mercado ha requerido considerar un gran conjunto de factores.

En concreto, abordar los factores relativos a la seguridad de la información involucra un elevado número de aspectos a tener en cuenta, entre ellos acceso físico a instalaciones, seguridad en el perímetro de red, configuración segura de sistemas operativos y aplicaciones, aseguramiento de la continuidad de negocio, seguridad de los recursos humanos, requisitos legales y gestión de la operación.

Plantear todos estos problemas sin una sistemática consolidada y probada es garantía de fracaso.

A continuación presentamos una sistemática probada internacionalmente para proporcionar una posible solución a todas las cuestiones mencionadas.

1. Introducción

El Centro de Proceso de Datos de una Organización proporciona el núcleo de la infraestructura tecnológica de la misma. La disponibilidad de los servicios albergados en el mismo es fundamental para el desarrollo de la actividad de la Organización. Por ello, la seguridad de la información en un CPD es un aspecto crucial cuyas implicaciones deben ser consideradas con suma prudencia.

La seguridad implica garantizar unos niveles de la tríada CIA (siglas en inglés de Confidencialidad, Integridad y Disponibilidad). En el caso de un CPD, es primordial que la búsqueda de la integridad y disponibilidad no recorten la disponibilidad de los servicios hasta un límite en el que éstos no sean de utilidad para la Organización.

A la hora de abordar la gestión de la seguridad de la información, existen diversos aspectos técnicos y organizativos que es necesario tener en cuenta. La implantación de un nuevo CPD no debe diferenciarse del resto de tareas TIC de la Organización en este sentido: todos los aspectos de la seguridad en la Organización que puedan verse afectados por la situación de su CPD deben ser gestionados mediante el análisis de los riesgos implícitos al CPD y el establecimiento de las medidas de seguridad asociadas.

Esta ponencia describe los aspectos de seguridad principales que es necesario considerar en el despliegue de un nuevo CPD.

2. Seguridad Física

Las necesidades de seguridad del nuevo CPD comienzan por considerar las amenazas que físicamente pueden afectar al mismo. Las amenazas físicas pueden clasificarse en tres grupos:

- Acceso físico no autorizado: incluye amenazas como robo, destrucción de equipos, acceso a la consola de administración, etc.
- Desastres naturales: ya sean terremotos, tormentas eléctricas, inundaciones, etc.
- Desastres industriales: incendios, errores en la red eléctrica (picos, caídas), temperatura o humedad no adecuada, etc.

La primera medida de seguridad a adoptar es evidente pero es común que no se realice: es necesario estudiar la localización del edificio, las características geológicas del terreno, la cercanía de ríos, lagos, etc. Dentro del edificio, deberá localizarse el CPD en un lugar adecuado: se recomienda evitar las plantas altas –las más afectadas por un temblor de tierra– el sótano y la planta baja –las afectadas en caso de inundación. Asimismo, la situación de los equipos dentro del CPD debe evitar que se coloquen en el suelo y en superficies elevadas, siendo lo más recomendable el uso de armarios rack.

La limpieza y el orden del CPD es fundamental a la hora de evitar desastres como el fuego o el fallo del hardware por contaminación. Es un fallo común la presencia de embalajes, rollos de cable, latiguillos de red sueltos, etc. Toda la basura debe ser retirada y el cableado debe ser realizado de forma pulcra, con etiquetado de todos los cables y rosetas y, si es

posible la instalación de falso suelo y falso techo.

El uso de sistemas de alimentación ininterrumpida, aire acondicionado y control de humedad y temperatura (HVAC) y sistemas de protección contra incendios homologados protegerá los equipos del resto de desastres. En caso de albergar soportes de almacenamiento en el propio CPD, se recomienda la adquisición de un armario con llave, si es posible, ignífugo.

Finalmente, el acceso al CPD debe estar restringido al personal de operación y administración del mismo, a ser posible mediante un sistema de acceso controlado electrónicamente con identificadores personales y registro de entradas y salidas –por ejemplo, usando tarjetas personales RFID. Asimismo, las entrada y salida de material de y hacia el CPD deben quedar registradas.

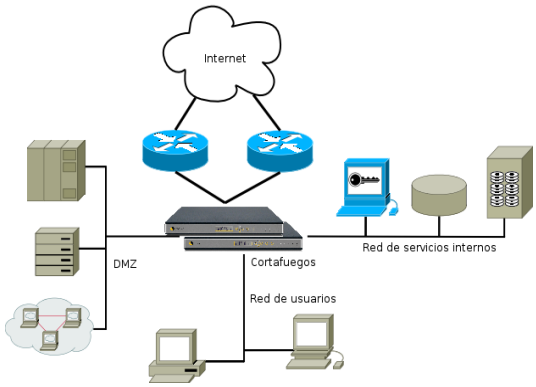
3. Seguridad perimetral

La infraestructura del CPD debe incluir medidas de seguridad que protejan frente a ataques a través de las redes a las que ésta esté conectado. Puesto que el núcleo de la electrónica de red suele –y debe– estar situado en el CPD, es necesario contemplar estas necesidades a la hora de implantar un nuevo CPD.

Es común que el acceso a internet sea un recurso crítico para la Organización, por lo que se recomienda contratar dos proveedores de acceso distintos y establecer una configuración en alta disponibilidad de todos los elementos de red que se encuentren en la ruta hacia Internet (cortafuegos, routers, switches, etc.). Esto es especialmente crítico si la organización proporciona servicios *on-line*, tales como comercio electrónico o *hosting* web.

Si es necesario implementar medidas adicionales de seguridad perimetral como IDS/IPS, filtrado de contenidos o antivirus de correo electrónico y/o navegación web, así como mecanismos de acceso remoto (VPN), el cortafuegos corporativo –o incluso el *proxy*, si se dispone de él– es el lugar idóneo para ello. De este modo se centraliza la administración de estas medidas y se reducen los posibles puntos de fallo. Actualmente, existe gran cantidad de dispositivos que implementan todas estas funcionalidades en un único equipo.

Además de los evidentes mecanismos de control que es necesario establecer desde y hacia Internet, es muy conveniente realizar una segregación de redes. Es decir, conviene realizar una división de la red interna de la Organización en distintas subredes, interconectadas entre sí por cortafuegos que establezcan los flujos de información permitidos entre cada una. Cada servidor, en función de las necesidades de control de acceso de las aplicaciones que ejecute, se conectará finalmente a una de estas subredes. El siguiente esquema muestra una arquitectura de red de ejemplo que sigue estas directrices.



4. Seguridad del sistema operativo

El sistema operativo de los equipos que se encuentren albergados en el CPD es el siguiente elemento a proteger, puesto que constituye la base del software que proporcionará los servicios a la Organización y a sus clientes.

Obviamente, las medidas de seguridad a aplicar dependerán en gran medida del sistema operativo que se trate, pero pueden agruparse según su función:

- Autenticación: el establecimiento de contraseñas seguras, especialmente para las cuentas de administración del sistema operativo y los servicios del mismo, para lo que puede usarse software de generación de contraseñas seguras y de detección de contraseñas inseguras (*password crackers*). Asimismo, puede considerarse el uso de mecanismos de autenticación fuerte para los sistemas más importantes.

- Control de acceso: el establecimiento de listas de control de acceso (ACL) que limiten los recursos del sistema a los que los usuarios y aplicaciones pueden acceder es un pilar fundamental para proteger la integridad y confidencialidad de los mismos.

- Limitación de privilegios de usuario: siguiendo el principio de mínimo privilegio[1], el uso de cuentas de usuario del sistema con privilegios especiales, tales como root o Administrador, debe limitarse o incluso prohibirse. En su lugar deben usarse métodos de ejecución segura de comandos

1 El principio de mínimo privilegio (*least privilege*) establece que una entidad debe poseer únicamente el mínimo privilegio posible que le permita realizar su labor.

privilegiados, como RunAs o sudo.

- Monitorización: una revisión periódica de los registros de actividad (*logs*) de los registros de actividad, unido a un correcto sistema de autenticación e identificación de usuarios, facilita la detección y la identificación de las causas de errores o ataques sufridos, que es el primer paso para mitigarlos.
- Gestión de recursos: la limitación del espacio en disco o la capacidad máxima de proceso a utilizar (cuotas de disco y procesador) evitarán que el sistema agote estos recursos por causa de un usuario o aplicación, lo que provocaría una *denegación de servicio*.
- Desactivación de servicios innecesarios: el principio de mínimo privilegio establece que todo aquéllo que no sea estrictamente necesario debe ser desactivado, para reducir posibles puntos de fallo.
- Opciones de seguridad: la aplicación de opciones de configuración de seguridad al sistema operativo y a las aplicaciones debe realizarse siempre que éstas no interfieran el funcionamiento correcto de los mismos.
- Uso de software de seguridad para el sistema: puede instalarse software específico de seguridad, como sistemas de detección de intrusiones a nivel de equipo (HIDS, *Host Intrusion Detection System*) o antivirus, en los servidores corporativos.

Para realizar la configuración segura de los sistemas operativos, se recomienda el uso de guías de configuración segura de los fabricantes del software. Asimismo, existen diversas entidades, como el NIST[2], que proporcionan guías de configuración segura para los sistemas operativos más comunes.

5. Seguridad de las aplicaciones

Las aplicaciones son el elemento final que procesa la información que es necesario proteger, por lo que cualquier amenaza que las afecte podrá verse reflejada en los datos que manejan.

Las aplicaciones principales que se ejecutan en los equipos situados en el nuevo CPD serán principalmente de tipo cliente/servidor, modelo según el cual uno o varios clientes se conectan al servidor para introducir datos, ordenar operaciones con los mismos y recibir la salida de estas operaciones. Ejemplos de este tipo de aplicaciones son sistemas de gestión de bases de datos (DBMS, *DataBase Management System*), aplicaciones web, ERP (*Enterprise Resource Planning*), servicio de correo electrónico, etc.

Aunque en este tipo de arquitectura es necesario asegurar el cliente mediante el que se accede a los datos, nos centraremos en la medidas de seguridad que sean directamente aplicables a los servidores.

Al igual que ocurre con el sistema operativo, es necesario realizar una configuración segura de las aplicaciones disponibles. Los aspectos principales a considerar son:

- Identificación y autenticación de usuarios: la correcta identificación de los usuarios y la autenticación de los mismos es fundamental para asegurar la trazabilidad[3].
- Control de acceso: las aplicaciones deben incluir mecanismos de control de acceso que limiten la funcionalidad y los datos a los que cada usuario tiene acceso, en función de las necesidades del mismo, siguiendo siempre el principio de mínimo privilegio. La mayor parte de aplicaciones *off the shelf* proporciona esta funcionalidad, y es fundamental asegurar que todo desarrollo a medida también la implemente.
- Monitorización: toda acción que implique acceso o modificación de datos debe ser registrada, incluyendo en dicho registro fecha, hora y autor de la misma.
- Desactivación de funcionalidad innecesaria: de nuevo según el principio de mínimo privilegio, cualquier funcionalidad incluida en el software que no sea estrictamente necesaria debe ser desactivada o desinstalada.
- Opciones de seguridad: la aplicación de opciones de seguridad debe realizarse siguiendo las guías del fabricante del software o guías de otras organizaciones expertas.
- Realización de comprobaciones de seguridad, auditorías y tests de intrusión: aplicable a las aplicaciones y al sistema operativo, la realización periódica de auditorías, tests de intrusión y comprobaciones de seguridad, especialmente si son realizados por terceros, proporciona una medida objetiva del nivel de seguridad existente en la Organización.

6. Recuperación y continuidad de negocio

Las medidas de recuperación y continuidad tienen como objetivo garantizar la disponibilidad máxima del servicio, especialmente en caso de desastre. Como parte de los planes de

2 National Institute of Standards and Technology

3 La trazabilidad permite determinar el responsable de cada acción realizada sobre el sistema.

continuidad de negocio/planes de contingencia de la Organización, el establecimiento de medidas de recuperación y alta disponibilidad para los elementos del CPD juega un papel fundamental a la hora de cumplir dicho objetivo.

Las medidas de recuperación y continuidad pueden diferenciarse en dos grupos:

- Medidas de redundancia: su objetivo es garantizar que el sistema no quedará inoperante en caso de que un único elemento del mismo falle. Para ello, se duplican los recursos que podrían fallar, como pueden ser fuentes de alimentación, discos duros o equipos completos.
- Medidas de salvaguarda y recuperación: tienen como objetivo la recuperación de la información en caso de borrado de la misma o fallo total de los soportes de almacenamiento que la conservan.

Las medidas de redundancia más comunes son el uso de unidades RAID[4] para el almacenamiento de datos y la instalación de servidores en alta disponibilidad. En este último caso, suele ser posible utilizar la capacidad de ambos servidores en lo que se denomina configuración de alta disponibilidad y equilibrado de carga (HA/LB, *High Availability & Load Balancing*).

Respecto a las copias de seguridad, es necesario tener en cuenta varios aspectos, como el tipo de copia de seguridad a realizar (totales, incrementales, diferenciales) y el período de rotación de los soportes (es decir, el tiempo que se conservarán las copias). Es fundamental que, para permitir la recuperación de los datos en caso de destrucción total del CPD, se realicen al menos dos copias de la información y una de éstas se almacene fuera de las instalaciones de la Organización.

Es muy importante recalcar que un tipo de medidas no sustituye al otro, aunque pudiese parecerlo: por ejemplo, un sistema RAID no proporciona protección frente a un borrado accidental de datos.

7. Seguridad del personal

Los usuarios y administradores de los sistemas albergados en el CPD son los que utilizarán finalmente el software y los datos. La seguridad de los sistemas de información se ve afectada por todos los componentes que los forman, y las personas suelen ser el elemento más inseguro. Por ello, la seguridad debe considerarse una labor de toda la Organización, no únicamente de los administradores de sistemas y los responsables de seguridad.

Los planes de formación del personal deben incluir temas específicos sobre de seguridad de la información, a distintos niveles (usuario, administrador, directivo, etc.). Asuntos tan simples y a su vez tan importantes como la elección de contraseñas seguras o el uso correcto de los servicios de la Organización suelen ser obviados frecuentemente.

Asimismo, es fundamental que exista una definición clara de las responsabilidades del personal en cuanto a la seguridad del sistema, así como un procedimiento disciplinario a adoptar en caso de que su incumplimiento. Un método sencillo para que todos los empleados conozcan estas responsabilidades es publicarlas en la intranet e incluirlas como clausulas en los contratos laborales.

Análogamente, las relaciones con terceros, ya sean clientes, proveedores o subcontratas, deben incluir clausulas específicas sobre seguridad, especialmente en cuanto al tratamiento de datos de carácter personal, como luego veremos.

8. Requisitos legales

Aparte de los requisitos legales arquitectónicos y frente a riesgos laborales de las instalaciones de la Organización, los requerimientos legales principales vienen determinados por la LOPD[5] y el RMS[6].

Los aspectos regulados por la LOPD se refieren al uso y tratamiento de los datos de carácter personal que se alberguen en los equipos de la Organización. Los requisitos principales que establece la ley, cuyo cumplimiento será necesario asegurar para los ficheros con datos de carácter personal en la Organización, son:

- Información al afectado y necesidad de disponer de su aceptación a la hora de recabar y ceder los datos.
- Registro de los ficheros que contengan datos de carácter personal en el Registro General de Protección de Datos (RGPD).
- Uso de los datos únicamente para el cometido para el que fueron recogidos, deber de secreto y mantenimiento de la calidad (exactitud) de los mismos.
- Garantía de los derechos de acceso, rectificación, cancelación y oposición para el

4 *Redundant Array of Inexpensive Disks*

5 Ley Orgánica de Protección de Datos de carácter personal, Ley Orgánica 15/1999

6 Reglamento de Medidas de Seguridad, Real Decreto 994/1999

afectado.

- Cumplimiento de las medidas de seguridad pertinentes, que actualmente se recogen en el RMS.
- Regulación de las transferencias internacionales de datos de carácter personal.

El RMS define tres niveles de seguridad aplicables a los ficheros que contengan datos de carácter personal y establece una serie de medidas técnicas que es necesario cumplir en función de cada nivel de seguridad. Las principales medidas de seguridad que pueden afectar al despliegue de un CPD son:

- Existencia de un documento de seguridad que recoja la normativa de seguridad y defina las obligaciones del personal en relación a datos de carácter personal. (Nivel básico)
- Mantenimiento de un registro de incidencias específicas sobre datos de carácter personal. (Nivel básico)
- Implementación de mecanismos de identificación, autenticación y control de acceso de usuarios a los datos de carácter personal. (Nivel básico)
- Gestión de soportes que contengan datos de carácter personal, incluyendo la identificación inequívoca de los mismos y el requerimiento de autorización para su salida de las instalaciones de la Organización. (Nivel básico)
- Realización de copias de respaldo, al menos semanales, que garanticen la reconstrucción de los datos en caso de desastre. (Nivel básico)
- Identificación de uno o varios responsables de seguridad en el Documento de seguridad. (Nivel medio)
- Realización de auditorías sobre el cumplimiento de las medidas de seguridad, internas o externas, al menos cada dos años. (Nivel medio)
- Limitación de la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. (Nivel medio)
- Limitación del acceso físico a las instalaciones que alberguen datos de carácter personal únicamente a los responsables recogidos en el Documento de seguridad. (Nivel medio)
- Gestión de soportes: elaboración de un registro de entrada/salida de soporte, existencia de mecanismos de destrucción de soportes tras su vida útil e implantación de medidas que impidan el acceso a la información albergada en soportes en tránsito. (Nivel medio)
- Las pruebas de sistemas de información se realizarán con datos ficticios, salvo que se asegure el mismo nivel de seguridad sobre los datos de carácter personal utilizados que tendrían sobre los sistemas en producción. (Nivel medio)
- Existencia de un registro de acceso que almacene usuario, fecha y hora, éxito o fracaso del intento de acceso y, en caso de éxito, el registro accedido. Este registro se conservará al menos dos años, será gestionado y revisado mensualmente por el responsable de seguridad competente. (Nivel alto)
- Se almacenarán copias de respaldo en un lugar diferente de aquél que almacene los datos, que debe cumplir estas mismas medidas de seguridad. (Nivel alto)
- La transmisión de los datos a través de redes de telecomunicaciones se realizará cifrándolos previamente, o utilizando cualquier otro mecanismo que impida el acceso a los mismos. (Nivel alto)

El cumplimiento de los requisitos legales establecidos por la LOPD y el RMS implicarán el establecimiento o endurecimiento de las medidas de seguridad planificadas para el CPD, especialmente en cuanto a los mecanismos de control de acceso y monitorización, copias de respaldo, cifrado, gestión de soportes y realización de pruebas.

Asimismo, será necesario considerar una estructura organizativa necesaria para el cumplimiento de estos requisitos, que a ser posible conviene integrar con la infraestructura organizativa para la seguridad y la explotación de sistemas que se describe en los siguientes apartados.

Finalmente, cabe destacar que, en caso de que la Organización se dedique a la prestación de servicios de la Sociedad de la Información, tales como comercio electrónico o servicios de acceso a Internet, será de aplicación la LSSI[7], que establece otra serie de requisitos, la mayor parte de los cuales son organizativos y de inscripción en registros de la Administración Pública y otros de índole técnica.

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

9. Gestión del CPD: ITIL

La gestión de un CPD medianamente complejo puede convertirse en una tarea caótica si no se establece una infraestructura organizativa adecuada para ello.

En un entorno empresarial donde las necesidades y exigencias de los clientes y usuarios son cada vez mayores, ITIL (Librería de Infraestructura de TI) aparece como la solución de referencia para alinear los sistemas de información con la estrategia de negocio dotando de robustez, fiabilidad y control a los sistemas de producción dentro del ámbito de las TIC.

Los continuos cambios en los sistemas productivos y la exigencias de tiempo que estos conllevan, han derivado en el aumento progresivo de la variable reactiva en el desempeño de los departamentos de TI de las organizaciones frente a la capacidad proactiva, deseable en cualquier entorno, con el consiguiente aumento de los costes de TI asociados a labores de soporte y mantenimiento. ITIL, como conjunto de buenas prácticas, se configura a partir de las experiencias extraídas de organismos de referencia mundial, tanto en el entorno privado como en el público, y junto a la clara orientación a los modelos de excelencia empresarial actuales, orientados a procesos y a sistemas de gestión de la calidad total (TQM, *Total Quality Management*), dota a la solución de una garantías innatas de éxito de cara a su implantación.

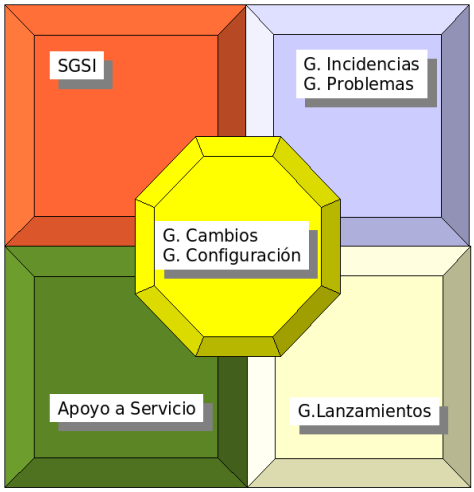
Las mejores prácticas en la gestión de servicios informáticos, dentro del marco de referencia ITIL, se incluye en dos libros principales: *Service Support* (apoyo de servicios) y *Service Delivery* (provisión de servicios). Si bien, la librería de servicios ITIL incluye otras guías para cubrir la gestión completa de servicios de TI, otras metodologías o normas internacionales existentes en el ámbito de la seguridad o la gestión y desarrollo de aplicaciones interrelacionadas de forma adecuada con ITIL, ofrecen un solución más potente a la gestión integral de la TI.

En un sistema de gestión integral orientado a procesos debemos tener en cuenta los siguientes marcos de trabajo para obtener los máximos beneficios de nuestra inversión y un ROI más rápido y controlado de estas:

- Gestión de Aplicaciones y Ciclo de vida del Desarrollo Software.
- Gestión de la Seguridad.
- Gestión de la Infraestructura.
- Gestión del Negocio.
- Gestión de la Innovación Tecnológica.

Donde ITIL, y mas concretamente los procesos asociados a los componentes de apoyo a servicios y provisión de servicios, actúa como punto de unión y control de todos ellos asegurando la máxima calidad del servicio ofrecido al cliente y usuario final.

Desde el punto de vista de la seguridad y en el ámbito de los grandes Centros de Proceso de Datos, ITIL habilita por medio del proceso de Gestión de Cambios, un lugar donde validar y controlar las cambios en producción, incluyendo en estas, el cumplimiento de las políticas de seguridad y la revisión posterior de los sistemas. Las interrelaciones entre los procesos de un SGSI y un sistema de gestión de servicios basado en el marco de trabajo ITIL, se extiende a otros procesos como el proceso de gestión de incidencias, el proceso de gestión de problemas, el proceso de gestión de la configuración o el proceso de gestión de la continuidad, ya que, cada una de las actuaciones realizadas o analizadas por estos pueden tener implicaciones de seguridad en el entorno.



ITIL ofrece un elemento que resulta diferencial para una correcta Gestión de Riesgos: el conocimiento actualizado y detallado de todos los activos de la Organización y dependencias entre ellos. Dicho conocimiento, gestionado desde el proceso de Gestión de la Configuración de Apoyo al Servicio, se alamcena en la CMDB (Configuration Management Database) que da soporte al resto de procesos del modelo.

Disponer del repositorio actualizado de elementos del sistema habilita de forma casi natural el Análisis de Riesgos en la fase de Planificación del SGSI y cuya permanente actualización resultará de vital importancia una

vez implantado el SGSI.

Adicionalmente, desde el punto de vista de la certificación de nuestro sistema de gestión integral de servicios y nuestro SGSI, cabe destacar que la integración de ISO 20000 (alineada con ITIL) con ISO 27001 e ISO 9001 puede componer un sistema de gestión completo y potente en empresas que tengan los suficientes recursos como para cometer un proyecto de estas características.

A la hora de analizar tanto un sistema gestión de TI, gestión del desarrollo y/o de gestión de la seguridad (SGSI) es aconsejable establecer, *a priori* y de forma clara y acotada, los puntos de unión y el mapa de procesos completo del sistema a implantar, identificando los canales y actividades donde se van a establecer las validaciones y controles necesarios para asegurar la estabilidad y seguridad de nuestro *live enviroment*. De esta forma maximizaremos desde un principio las posibilidades de éxito de nuestra implantación y minimizaremos el rechazo al cambio producido por constantes cambios de alcance y flujos de trabajo necesarios al evolucionar los procesos por falta de definición e integración.

10. Sistema de Gestión de la Seguridad de la Información

Abordar los aspectos de seguridad descritos anteriormente de forma sistemática exige la utilización de un código de buenas prácticas y estándares con experiencia demostrada.

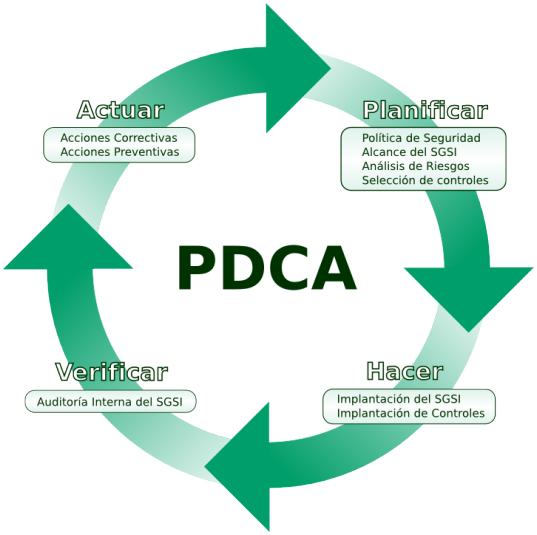
Como respuesta a esta necesidad, la reciente norma ISO/IEC27001 define los requisitos para el establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI).

El SGSI permite a la Organización alinear las actuaciones en materia de seguridad de la información con los objetivos estratégicos de negocio de la misma. Asimismo, facilita la identificación de las iniciativas de seguridad prioritarias a abordar y proporciona mecanismos de medición del ROI en materia de seguridad.

Para conseguir su objetivo, el SGSI se basa en un ciclo PDCA[8] continuo, cuyas tareas principales se describen brevemente a continuación:

- Planificación: consiste en la realización de un análisis de riesgos que permita establecer qué medidas de seguridad es necesario implantar en las siguientes fases del ciclo.
- Acción: durante esta fase, se realizará la implantación de las medidas de seguridad seleccionadas.
- Medición: mediante la definición de unas métricas, se comprobará la efectividad de las medidas de seguridad adoptadas.
- Actuación: se estudiarán acciones correctivas y preventivas que permitan mejorar la seguridad del sistema, volviendo de nuevo a la fase de planificación.

El siguiente esquema resume el ciclo PDCA.



11. Conclusiones

El empleo de los estándares de seguridad ISO/IEC 27001 y de operaciones ITIL e ISO 20000, así como de calidad ISO 9001:2000, complementados con la experiencia y conjunto de buenas prácticas descritos en los diferentes apartados de este documento, permiten abordar con ciertas garantías unos niveles de seguridad aceptables en la instalación, despliegue y operación de un CPD.

Como conclusión podemos asegurar que la seguridad de un CPD no se limita a un conjunto de procedimientos y políticas publicados en la intranet de la Organización: son un conjunto de procesos que interactúan con los distintos marcos de gestión de cada uno de los elementos de un sistema de información para controlar y garantizar la seguridad integral de un entorno empresarial, que se ven respaldados por una serie de medidas técnicas y herramientas.

12. Referencias

LOPD: `http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf`

8 *Plan Do Check Act* o Planificar, Hacer, Medir y Actuar

RMS: http://www.boe.es/boe/dias/1999/06/25/pdfs/A24241-24245.pdf

LSSI: http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

ITIL: http://www.itil.co.uk/