Mejores prácticas en la Implantación de ISO27001:2013 y PCI/DSS 3.1

Carlos Ortiz de Zevallos
Gestión de Proyectos

Xavier Martínez

14-6-2016

FICHA DEL TRABAJO FINAL

Título del trabajo:	Mejores prácticas en la Implantación de ISO27001:2013 y PCI/DSS 3.1
Nombre del autor:	Carlos Ortiz de Zevallos Torrents
Nombre del consultor:	Xavier Martínez Munné
Fecha de entrega (mm/aaaa):	06/2016
Área del Trabajo Final:	Gestión de Proyectos
Titulación:	*Ingeniería Técnica en Informática de Gestión*

Resumen del Trabajo (máximo 250 palabras):

En un entorno cada vez más tecnificado y dependiente de los medios técnicos que nos rodean se hace necesario normalizar los mecanismos que aseguran que dicha información cumple con los requisitos de seguridad. Se constata la necesidad de proteger los activos valiosos de las compañías que cada vez más tienden a ser activos de información. La Organización Internacional de Estándares (ISO) ha confeccionado normas que regulan dicha protección siendo un estándar de facto a nivel mundial la norma ISO27001 en tanto que protege no sólo los activos lógicos sino los físicos. Por otra parte el entorno bancario se halla en el dilema de cómo garantizar que la información que procesa se halla garantizada frente a ataques a su confidencialidad integridad y disponibilidad. Las principales empresas de pago por tarjeta emiten su propia norma PCI/DSS la cual regula y protege dicha información desde el punto de venta hasta que la transacción se almacena.

Las empresas que desean adoptar dichas normas se hallan ante el dilema de cómo realizar la implantación y qué supone esto a sus estructuras dado que no sólo es un cambio tecnológico sino que abarca la cultura de la compañía, cómo entiende sus procesos y relaciones tanto dentro como fuera de la misma.

Este trabajo pretende guiar a aquéllas compañías que requieran de ambas normas en un enfoque claro y útil a la vez que las previene de los principales peligros que un proyecto de esta magnitud conlleva.

Abstract (in English, 250 words or less):

In an environment increasingly technically sophisticated and dependent on the technical means around us is necessary to normalize the mechanisms to ensure that such information meets the safety requirements. The need to protect the valuable assets of companies which increasingly tend to be information assets is found. The International Standards Organization (ISO) has drawn up rules governing such protection being a de facto standard worldwide is the ISO27001 while protecting not only logical but physical assets. Moreover, the banking environment is in the dilemma of how to ensure that the information processed is guaranteed against attacks on their confidentiality integrity and availability. The main credit card companies issue their own PCI / DSS standard which regulates and protects the information from the point of sale until the transaction is stored.

Companies wishing to adopt such standards are faced with the dilemma of how to implement and what this means to their structures since it is not only a technological change but embraces the culture of the company, how to understand their processes and relationships both within and outside it.

This work aims to guide those companies requiring both standards in a clear and useful approach preventing from major risks that a project of this magnitude entails.

Palabras clave (entre 4 y 8):

ISO, ISO27001, PCI/DSS, SGS, CDE, ISO/IEC

Índice

Lista de figuras

1. Contexto y justificación

En una sociedad cada vez más interconectada y dependiente de los sistemas de información existen dos necesidades clave en cuanto a seguridad de los sistemas:

- Contar con mecanismos que aseguren la fiabilidad de los sistemas así como garanticen las dimensiones claves en seguridad de la información que son: Confidencialidad, Disponibilidad e Integridad de los activos.
- Contar con metodologías que de forma universal garanticen dichas características para establecer un sistema común y superar el esquema actual (por país).

Es por ello lógico y necesario que se planteen las formas de llevar a cabo dichos objetivos, la sensación de inseguridad en los medios de pago telemáticos, cada vez más usados plantea el reto de mantener la funcionalidad de los sistemas a la par que garantizar la ausencia de fraude en las transacciones reto que supone, por el advenimiento del Internet de las cosas una tarea mayúscula y un aspecto a desarrollar dentro de los próximos años.
Las normas específicas de seguridad son:

- ISO/IEC27001:2013: familia de normas que regulan la seguridad de los sistemas de información.
- PCI DSS 3.1: conjunto de normas que regulan los prestatarios de pago por tarjeta constituido por un consorcio de las principales empresas de tarjetas a nivel mundial.

2. Alcance

El objetivo del presente trabajo será mostrar una forma de implantar ISO27001 y PCI para dotar a la empresa que decida adoptarlas de los mecanismos eficaces descritos en ambas normas para la protección de sus sistemas no sólo a nivel lógico sino físico desarrollando ambas recomendaciones de forma conjunta.

2.1. Enfoque y metodología seguida

Las empresas que optan por realizar un proceso de certificación tienen diversas alternativas en función de su tipología:

Norma	Acción
PCI	Certificación mediante empresas certificadoras y documento (ROC)
ISO27001	Certificación mediante empresa certificadoras o documento de autoconformidad y documento (SOA)
GMP	Certificación para empresas manufactureras
FDA…	Certificaciones sectoriales

Tabla 2-1 Alternativas de certificación en seguridad

- El documento de autoconformidad es un documento interno a la empresa cubre la norma dentro de su alcance sin hacer sido certificada de forma oficial.[1]

Pese a que PCI también desarrolla aspectos cubiertos en la ISO27001, exige cumplimientos en muchos puntos más allá de lo que exige 27001 lo importante para esta norma es la protección de los datos de la tarjeta pudiendo descuidar otros aspectos que sí cubre la ISO27001.
El planteamiento en que se basa éste trabajo es el obtener la estrategia más conveniente basada en las mejores prácticas para la implantación de ambas normas. Los criterios de planificación de acciones se basan en la experiencia mediante el uso de la auditoría de sistemas como disciplina (ISO19011, ISO29148, ISO20000, ISO16085).

[1] En cuyo caso la empresa no obtendría el consiguiente certificado de conformidad no estando permitido el uso de los logotipos de la norma ni del esquema de certificación.

3. Recomendaciones de implantación iso27001

3.1. Introducción Iso27001:2013

La implantación de una norma ISO requiere:

- Compromiso de cambio y soporte por parte de la organización
- Compromiso en tiempo y recursos de la organización
- Esfuerzo por parte del implantador

El proceso de implantación realiza cambios/crea procedimientos y políticas así como establecimiento de nuevas formas de trabajar que afectan a las siguientes funciones de negocio:

- Dirección
- Recursos Humanos (Contratación y Formación)
- Compras
- Relaciones con Proveedores
- Seguridad Física
- Seguridad Lógica
- Infraestructuras
- Gestión de activos
- Gestión de las relaciones con los clientes
- Comunicación

Es un proceso largo y de resistencia en el que la negociación y las capacidades de comunicación del implantador así como la predisposición al cambio y la buena disposición del mismo por parte todas las partes interesadas es fundamental para el éxito del proyecto.
Es fundamental que el implantador realice una tarea de formación continua en las partes interesadas de forma que se conviertan en valedores del proyecto.

ISO27001:2013

ISO27001:2013 se halla dividida en 10 Capítulos:

#	Título	Objetivo
1	Objetivo y campo de aplicación	Presentación y compatibilidad con otras normas
2-3	2. Referencias normativas y 3.Términos y definiciones	Referencia a la ISO27000 como base de nomenclatura
4	Contexto de la organización	Comprensión de la organización y alcance de la norma

5	Liderazgo	Compromiso de la dirección, roles y política de seguridad
6	Planificación	Riesgos y objetivos de seguridad y planes para lograrlos
7	Soporte	Competencia, Formación, establecimiento de mecanismos de comunicación así como requisitos y control en la documentación
8	Operación	Planificación de las operaciones, Gestión del riesgo
9	Evaluación del Desempeño	Seguimiento de los objetivos, Auditoría interna y revisión por la dirección
10	Mejora	Tratamiento de las no conformidades y acciones correctivas, Mejora continua

Tabla 3-1Capítulos de la ISO27001:2013

ANEXO A (a la norma): Objetivos de control y controles de referencia (ISO27002)

3.2. Recomendación Inicial: Prepararse

La asunción de una norma dentro de una empresa es un proceso de cambio que impacta en la producción por el cambio organizativo, procedural y de reporte así como la necesidad de dotar de herramientas y mecanismos para el mantenimiento de la misma. La recomendación (R de ahora en adelante) inicial es:

- Obtener asesoramiento que permita establecer el esfuerzo aproximado necesario para su implantación, indicando:
  - Alcance aproximado
  - Recursos necesarios (tanto personal como funciones de negocio)
  - Esfuerzo necesario
  - Plazo de realización
- Establecer un plan de proyecto (el presente documento sirve de guía para este fin)
- Dotar de recursos a su cumplimiento: indicar a los recursos identificados de la necesidad de un porcentaje de su tiempo en la implantación

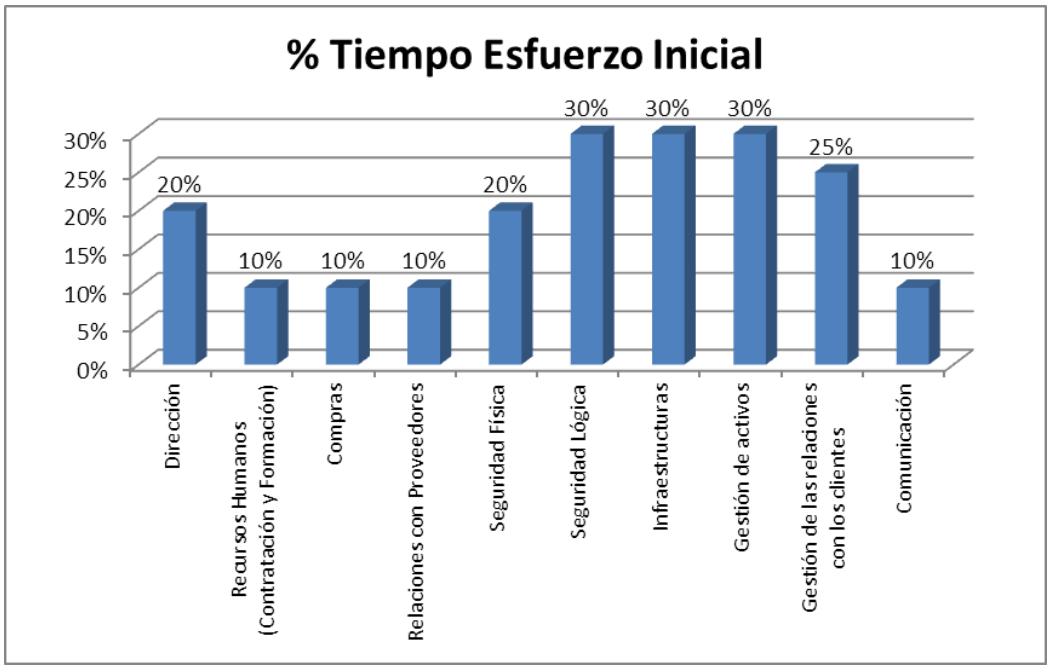

Ilustración 3-1 % Tiempo y esfuerzo implantación inicial

- Dotar de recursos para las implicaciones en Tecnología (inversiones y mantenimientos)

Aunque en un primer momento no es necesario realizar un desembolso de capital para ello es importante que la dirección asuma que el proceso puede ser costoso y sea aceptado.
Acto seguido iniciar una Pre auditoría para obtener el diferencial entre lo que la norma implica y la situación real de la compañía, acotar el esfuerzo y obtener una vez más la aprobación de la dirección.
Finalmente como aspecto de Preparación es escoger un implantador experto que guíe a la organización y facilite el cambio organizacional.

3.3. R1: Seguir la estructura de la norma

La primera recomendación de implantación es seguir la propia estructura de la norma, como se demostrará es sumamente práctica dicha distribución.
La primera acción a realizar por parte del implantador será la de crear la estructura en un volumen seguro pero alcanzable por los componentes del SGSI (ver roles).
Respecto al Anexo A se hablará más delante de la importancia que tiene.

3.4. R2: Identificar al sponsor

En una implantación es fundamental disponer el máximo nivel posible de soporte por parte de la organización. Cuanto más alto en la cadena jerárquica mejor. Éste punto es fundamental en la implantación, siendo responsabilidad del implantador identificar y conseguir el mejor nivel de soporte durante la misma.

3.5. R3: Determinar el alcance

El alcance (punto 4.3 de la norma) es el punto de partida de la implantación, formará parte del certificado a emitir por parte de la empresa auditora y estará a disposición de las partes interesadas que quieran saber qué se halla certificado.
El alcance como tal es un párrafo que debe contar con las siguientes características:

- Identificar la unidad o servicios certificada
- Identificar la ubicación geográfica desde donde se presta el servicio
- Identificar el objetivo de la certificación

3.5.1. Ejemplos de mal uso del alcance

Una empresa de hosting certifica el proceso de reserva de salas, implementando la norma, estableciéndolo así en su alcance y certificándolo. Nosotros como clientes deseamos contratar como proveedor de hosting a dicha empresa y conocer si desarrolla sus actividades en un entorno seguro. Inicialmente la empresa alega que cumple ISO27001. Lo que debemos hacer es solicitar su certificado en donde se especifica el alcance de su certificación. En este caso la empresa puede realizar su reserva de salas de forma segura pero eso no garantiza que sus procesos de hosting sean igualmente seguros.
Otro ejemplo: deseamos contratar a un proveedor e indica que dispone de una certificación vigente de ISO27001 para el servicio que deseamos contratar. Pero dicho proveedor dispone de varios centros de trabajo (pe: Madrid y Barcelona), nosotros estamos en Barcelona y el centro certificado es el de Madrid según consta en su alcance.
Estos ejemplos –reales por otra parte, pero de empresas confidenciales- indican que los proveedores sí cumplen ISO27001, pero en ninguno de los casos sería garantía de seguridad de su SGSI para contratarlos como proveedores debido a su alcance de certificación.
La definición del alcance: La empresa, y el auditor externo deben velar porque dicho alcance se halle correctamente definido.

3.6. R4: Establecer el contexto de aplicabilidad

Una vez se ha definido claramente el alcance a certificar sobre dicho alcance es necesario realizar una investigación profunda acerca de cómo se halla organizado siendo necesario:

3.6.1. Estudiar la organización

El implantador debe disponer de información correcta acerca de lo establecido en el alcance siendo necesario:

- Topología de Red
- Topografía de Red
- Inventario de los activos informáticos o CIs (en caso de tener ISO20000)
- Diagramas de sistemas (relaciones entre los activos)
- Listado de procedimientos
- Personal y organización del mismo que lo opera
- Clientes afectados por la operación
- Relación empresa-cliente
- Relación empresa-trabajadores

3.6.2. Determinar al grado de aplicabilidad

Para ello es necesario contar con el Anexo A que es de facto la ISO27002 y cuyo documento de cumplimiento se denomina Estado de Aplicabilidad (SOA en inglés), que es un conjunto de 114 controles sobre los cuales el implantador deberá:

- Identificar cuáles son aplicables y cuáles no (por ejemplo una empresa no emplea controles criptográficos, se indicará que dicho control no es aplicable en el ámbito de certificación)
- Identificar el grado de cumplimiento mediante la identificación con un estándar (se emplea comúnmente un Modelo de Madurez de la Capacidad (CMM) para la seguridad de la información estableciendo niveles de cumplimiento por control siendo éstos:
    - N/A. No aplicable: No se considera el control
    - 0. Inexistente: El control no se está realizando
    - 1. Informal: El control no está definido formalmente
    - 2. Repetible: El control está definido pero no se dispone de métricas
    - 3. Gestionado: El control se mide y comprueba su cumplimiento
    - 4. Optimizado: El control se halla en un ciclo de mejora continua
- Confeccionar la argumentación basada en evidencias de cómo se establece la categorización de madurez de cada control
- Formalizar la SOA en un documento de trabajo (generalmente una hoja de cálculo) y almacenarlo en 6.Planificación- 6.1 SOA
- Establecer la línea base de seguridad a lo representado en la SOA
- Dictaminar el grado de madurez de los controles y establecer un roadmap de consecución de la certificación involucrando recursos y tiempo.

De la SOA se desprende:

a. Necesidad de realizarla Semestralmente
b. Necesidad de estar disponible (de ahí que se ubique dentro de la estructura en el punto 6. Planificación) [El auditor siempre pedirá: Alcance y SOA]

c. Un listado de controles necesarios a implementar que sirven para la implementación de la norma, el sponsor delimitará y calendarizará junto con el implantador la idoneidad de su implantación así como el plazo y esfuerzo necesario.

3.7. R5: Política de Seguridad

Una vez establecido el alcance y el estado de la seguridad la organización debe confeccionar una política de seguridad que proteja los activos objeto del alcance.
La política de seguridad debe contar con las siguientes características:

- No debe ocupar más de una página
- Centrarse en las dimensiones de la seguridad de la información que son:
    - Confidencialidad: medidas para asegurar que el acceso confidencial está garantizado a quien debe.
    - Disponibilidad: medidas para asegurar que la información estará disponible en base a las necesidades de negocio.
    - Integridad: medidas para asegurar que la información es correcta y modificada por quien debe hacerlo.
- Ser un documento de alto nivel firmado por el sponsor o por la cúpula directiva como declaración de intenciones. Intención de preservar la seguridad.
- Indicar que existe un mecanismo de control y defensa frente a agresiones (ya sea lógico como procedimiento sancionador al trabajador que lo incumpla).
- Ser notificado a la plantilla objeto del alcance (centro de trabajo, sede, grupo…).
- Formar al personal sujeto al cumplimiento de la política en la misma.

3.8. R6: Establecer los roles

Definir los roles de:

- Seguridad: los cuales formarán parte del comité SGSI
    - Sponsor
    - Responsable de Seguridad Lógica
    - Responsable de Seguridad Física
    - Operaciones
    - Aplicaciones

Los roles deben contener necesariamente las responsabilidades en seguridad de la información, por ejemplo:
Rol de Responsable de Seguridad (extracto ejemplo)

- Cumplir la normativa de seguridad así como las leyes vigentes
- No desvelar la información confidencial de la empresa

- Propietario de los procedimientos de seguridad
- Custodiar las copias de seguridad…

Es necesario:

- Acordar con RRHH el establecimiento del perfil por trabajador
    - Constatar en cada perfil sus obligaciones en cuanto a seguridad de la información
    - Constatar en cada perfil la necesidad del cumplimiento de la política de seguridad
    - Instar a que las nuevas incorporaciones dispongan de dicha información

3.9. R7: Constituir el SGSI

Realizando las siguientes acciones:

- Formalizar el Acta a seguir por parte del SGSI
- Objetivos, KPI y Cuadro de mando
- Revisión por la dirección, cuándo se realizará una reunión de SGSI extraordinaria para revisar los objetivos de seguridad.
- Acciones correctivas: qué procedimiento se empleará en caso de haber acciones correctivas en el ámbito del SGSI
- Gestión del ciclo de vida de los Activos y de los trabajadores: establecer un procedimiento de alta y baja de activos instando a los trabajadores a firmar la entrega de los mismos en su entrada (registrando qué se le da a cada uno) y formalizando la entrega a su salida mediante la correspondiente firma y cotejo entre lo que se entregó y lo que se devuelve.

La constitución del SGSI debe ser formada por los roles de seguridad, el sponsor pero no ceñirse únicamente a ellos, debe ser un foro de discusión de seguridad en donde se invitará a cualquier perfil involucrado para su participación, no es extraño pues que los comités acaben siendo una representación del comité directivo pudiendo tener representación –en función del tamaño de la empresa- de forma continuada los siguientes:

- Recursos Humanos: con la afectación que tiene la definición de roles y la aplicación de las medidas de custodia y formación de los formatos de alta/modificación de usuarios.
- Marketing: por la necesidad de realizar acciones formativas bien presencialmente bien mediante técnicas de márquetin (píldoras, espacio intranet, material recordatorio como posters, esterillas de ratón entre otras).
- Formación: a menudo unida a RRHH por lo antes expuesto.
- Gerencia/COO: por la necesidad de envío de información a toda la empresa, para acordar el tiempo y la forma junto con márquetin.

- Relaciones Laborales/PRL: por la necesidad de abordar los simulacros de contingencia.

3.10. R8: Iniciar un plan de formación

Iniciar un plan en el que todo el personal que se halle sujeto a la política de seguridad reciba la formación adecuada para su uso y cumplimiento, guardando evidencia de:

- Su realización (convocatoria, firma de asistencia…)
- Prueba de validación en el que se pregunten aspectos de la política al finalizar cada curso para cada asistente
- Valoración de la formación por cada asistente
- Compromiso firmado de cada asistente al cumplimiento de la política de usuario (acuerdo de confidencialidad)
- Instar a RRHH a que cada nueva incorporación firme la política de usuario debiendo custodiar dicho documento con la ficha del empleado / contrato de trabajo / préstamo de equipo, móvil etc. Hasta la finalización de la relación del empleado con la empresa.

Toda la información generada deberá ser almacenada en 5.2 Política – 5.2.1 Formación

3.11. R9: Realizar análisis de Riesgos

Realizar un análisis de riesgos que contemple:

- SOA y cumplimiento de controles
- Amenazas basadas en mejores prácticas como Magerit se puede emplear para el cálculo aproximado del riesgo mediante la identificación de las amenazas por activos y las amenazas estructurales o de entorno que puedan ocurrir.

Ilustración 3-2 Dimensiones de Riesgo

- Activos y aportación de los mismos a los objetivos de negocio mediante diagramación de los mismos enlazando los activos con el servicio que prestan a la empresa (servicio de negocio). Ésta mejor práctica constituye un cambio importante de cara a la implantación debido a que se debe instar a la empresa a la instalación de una Base de datos de la configuración para el control de los activos. El esfuerzo empleado en esta iniciativa es compensado con creces debido al control que aporta en los activos de la empresa.
- Como mejor práctica se recomienda establecer un análisis basado en metodología de gestión de riesgos contrastada, así CRAMM, OCTAVE o PILAR pueden constituir una fuente fiable de información.
    - En éste trabajo se recomienda establecer un análisis de riesgos basado en tres puntos clave:
        - SOA: cumplimiento normativo
        - Activos: diagramados para identificar los puntos de conexión entre la SOA y el inventario
        - Amenazas conocidas: Octave por ejemplo como fuente de amenazas a enlazar con los activos y con la SOA
    - El resultado del análisis de riesgos es la identificación de los riesgos mediante la lectura de éstas tres dimensiones para extraer:
        - No se evidencia el control X o bien con un nivel de madurez inadecuado, el cual afecta a los activos Y, por tanto son vulnerables a las amenazas Z.
        - Dictaminar el nivel de riesgo que se desprende como el impacto multiplicado por la probabilidad de ocurrencia

en una escala 5x5 teniendo que efectuar acciones y elevando el mismo al SGSI quien debe gestionar el riesgo resultante.

3.11.1. La Gestión del riesgo

Frente a un riesgo identificado caben las siguientes alternativas en función de quién lo asume:

- Diferirlo: traspasar el riesgo a un tercero que asumirá las consecuencias del mismo, por ejemplo una póliza de seguros.
- Aceptarlo: en cuyo caso es el sponsor quien asume el riesgo y acepta las responsabilidades que puedan derivarse.
- Eliminarlo: realizar las acciones oportunas para eliminar o dejar el riesgo en términos de aceptabilidad, acto seguido aceptarlo.
- Establecer acciones mitigadoras: establecer acciones para mitigar el riesgo –reducirlo- un ejemplo de esto es la instalación de SAIS en la infraestructura o duplicar las líneas de telecomunicaciones.

3.11.2. Consideraciones respecto a la gestión de riesgos

Como la gestión de riesgos es una disciplina cambiante en el tiempo bien por las acciones mitigadoras del mismo, bien porque los activos cambian o porque aparecen/desaparecen amenazas, ésta debe tomarse de forma periódica recomendando la realización de la misma en base semestral.
Cada análisis de riesgos debe ser documentado, explicada su metodología y elevado al SGSI quien hará constar en acta las acciones, recursos y plazo en su gestión.

3.12. R10: Establecer Políticas de Activos

- Uso de Activos: como se ha visto anteriormente establecer y formar de la política al personal de soporte, tanto si es interno como externo.
- Gestión del ciclo de vida de los activos: formalizar los procesos de compra, uso y documentación, permisos, modificación, apagado/discontinuado, eliminación de información confidencial en los mismos, eliminación del inventario.
- Política de control de accesos: establecer política de control de accesos tanto físicos como lógicos, formalizando la revisión de los accesos lógicos y auditoría de los mismos con el fin de controlarlos. Esto incluye la necesidad de establecer un procedimiento de revisión formal de los mismos de forma planificada.

3.13. R11: Política de gestión de incidencias

- De Servicio: establecer, ligado a la base de datos de configuración la necesidad de trabajar por incidencias estableciendo los acuerdos internos de nivel de servicio correspondientes para dotar de transparencia la acción de los equipos de soporte.
- De Seguridad: formalizar el incidente de seguridad y establecer su tratamiento, los incidentes de seguridad se resolverán por los equipos de soporte pero asimismo serán evaluados por el SGSI para identificar riesgos potenciales.

3.14. R12: Procedimientos de Continuidad

- Simulacro: formalizar la periodicidad y formato de los simulacros controlando aspectos como las visitas, cómo queda la oficina cuando hay un simulacro o el tiempo de evacuación de la misma.
- DRS: formalizar documentación, escenarios disruptivos y planificar simulacro de contingencia en que la afectación sea un conjunto de activos críticos, establecer comportamiento, movilización del equipo y estrategia de gestión en caso de contingencia.

3.15. R13: Procedimientos Operativos

- Altas/Bajas de Personal: formalizar junto con RRHH de los procedimientos de Alta y baja de personal, como se ha visto anteriormente es necesario contar con una custodia formal del acuerdo de confidencialidad del empleado. Asimismo es necesario establecer dentro del puesto de trabajo la descripción de las responsabilidades en cuanto a seguridad para cada rol, esto debe ser aceptado asimismo por el empleado.
  En la práctica esto supone que en la publicación del puesto de trabajo se establezca, junto con los requerimientos del candidato también las obligaciones de seguridad.
- Altas/Bajas Activos: revisión del procedimiento de altas y bajas de forma periódica y mejoras al mismo.
- Plan de Capacidad: establecer el plan de capacidad del personal para la prestación del servicio, por ejemplo si la empresa presta servicio 24x7, se deberán establecer los consiguientes turnos para cubrir la capacidad y establecer asimismo equipos de respaldo por si algo falla.
- Formato Documentación: establecer el formato de documentación a emplear, numeración y formato necesario, como por ejemplo la necesidad de etiquetar los documentos en función de su categorización (Restringido, Confidencial, Interno, Público).

3.16. R14: Política de control de proveedores

- Modelo de Relación y escalado: formalizar con los proveedores sus responsabilidades en seguridad así como establecer una matriz de comunicación y de escalado a disposición de los equipos de soporte.
- Contractuales (SLA): formalizar los acuerdos de nivel de servicio con los proveedores como parte de la prestación del servicio a los clientes.
- Contacto en caso de emergencia: dentro de la matriz de escalado indicar los contactos en caso de contingencia.

3.17. R15: Relaciones con el exterior

- Listado de legislación aplicable: establecer las leyes y normativas a las que la empresa se halle sujeta. Por ejemplo una farmacéutica puede tener requerimientos extraordinarios por parte de la FDA, aspectos que se deben observar en la implantación.
- Relaciones con grupos de interés: indicar una lista de contactos en caso de necesidad como bomberos, pero también de suministros como agua, gas o electricidad.

3.18. R16: Auditoría Interna

- Revisión de documentación: formalizar y planificar la función del auditor (de seguridad) interno quien debe velar porque el sistema de seguridad se mantenga al día realizando de forma periódica controles sobre los procesos implicados y estableciendo Acciones Correctivas sobre los mismos.
- Custodia: indicar en cada documento qué custodia va a tener, por defecto son tres años pero la empresa puede escoger un modelo de custodia acorde a sus necesidades.

  Periodicidad: periodicidad de la auditoría interna, esta suele ser anual o semestral. En caso de acercarse la fecha de auditoría de certificación puede variar el período para adaptarse a las necesidades de la empresa y su nivel de cumplimiento.

4. Recomendaciones de implantación PCI DSS 3.1

4.1. Qué es PCI DSS

PCI DSS es una norma del consorcio *Payment Cards Industrie* formado por las principales emisoras de tarjetas del mundo (AMEX, Dicover, JCB, VISA y MasterCard) el cual regula y protege la Confidencialidad y Disponibilidad de los datos necesarios para la autenticación y operación de la tarjeta, estos son:

- PAM: Número de tarjeta
- Fecha caducidad de la misma
- CVV: código de validación de la tarjeta

Ilustración 4-1 Empresas intervinientes en PCI

4.2. A quién Aplica

A todos los intervinientes en una transacción mediante uso de tarjeta bancaria.

4.3. Alcance

Cualquier empresa que acepte tarjetas bancarias, las procese y/o almacene.

4.4. Implantación

PCI establece la siguiente priorización:

Milestone	Goals
1	Remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it
2	Protect systems and networks, and be prepared to respond to a system breach. This milestone targets controls for points of access to most compromises, and the processes for

	responding.
3	Secure payment card applications. This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.
4	Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.
5	Protect stored cardholder data. For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.
6	Finalize remaining compliance efforts, and ensure all controls are in place. The intent of Milestone Six is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

Ilustración 4-2 Alcance Priorizado según PCI DSS Fuente PCI Prioritized Approach

La priorización de PCI pese a ser perfecta se halla con la vicisitud de considerar como única la norma PCI, en el alcance del presente trabajo no emplearemos dicha priorización salvo en caso de tener que implantar PCI sola.
PCI DSS se halla organizada en 12 Requisitos organizados en 6 secciones llamados Objetivos de Control:

Objetivo de Control	Requisito
Desarrollar y Mantener una Red Segura	1: Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas. 2: No usar contraseñas del sistema y otros parámetros de seguridad predeterminados provistos por los proveedores.
Proteger los Datos de los propietarios de tarjetas.	3: Proteger los datos almacenados de los propietarios de tarjetas. 4: Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.
Mantener un Programa de Gestión de Vulnerabilidades	5: Usar y actualizar regularmente un software antivirus. 6: Desarrollar y mantener sistemas y aplicaciones seguras.
Implementar	7: Restringir el acceso a los datos tomando como base

Medidas sólidas de control de acceso	la necesidad del funcionario de conocer la información. 8: Asignar una identificación única a cada persona que tenga acceso a un computador. 9: Restringir el acceso físico a los datos de los propietarios de tarjetas.
Monitorizar y probar regularmente las redes	10: Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los propietarios de tarjetas. 11: Probar regularmente los sistemas y procesos de seguridad.
Mantener una Política de Seguridad de la Información	12: Mantener una política que contemple la seguridad de la información

Tabla 4-3 Organización interna PCI DSS

4.5. Recomendación

Implantar los controles en el siguiente orden:

Objetivo de Control	Requisito
Mantener una Política de Seguridad de la Información	Definir el alcance 12: Mantener una política que contemple la seguridad de la información
Desarrollar y Mantener una Red Segura	1: Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas. 2: No usar contraseñas del sistema y otros parámetros de seguridad predeterminados provistos por los proveedores.
Mantener un Programa de Gestión de Vulnerabilidades	5: Usar y actualizar regularmente un software antivirus. 6: Desarrollar y mantener sistemas y aplicaciones seguras.
Proteger los Datos de los propietarios de tarjetas.	3: Proteger los datos almacenados de los propietarios de tarjetas. 4: Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.
Monitorizar y probar regularmente las redes	10: Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los propietarios de tarjetas. 11: Probar regularmente los sistemas y procesos de seguridad.
Implementar Medidas sólidas de control de acceso	7: Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información.

	8: Asignar una identificación única a cada persona que tenga acceso a un computador. 9: Restringir el acceso físico a los datos de los propietarios de tarjetas.

Tabla 4-4 Recomendación de implantación de PCI DSS 3.1

5. Recomendaciones de implantación conjunta ISO27001 y PCI

5.1. Quién debiera plantearse ambas normas?

Cualquier empresa que esté sujeta al cumplimiento de PCI puede plantearse cumplir ISO27001 dado que la estructura más restrictiva de PCI hará que la implantación de la 27 sea más sencilla.

5.2. Alcance

El alcance de 27001 es a priori más amplio que el de PCI por lo que se recomienda tomar el alcance de dicha norma y ver qué implicaciones tiene para PCI.

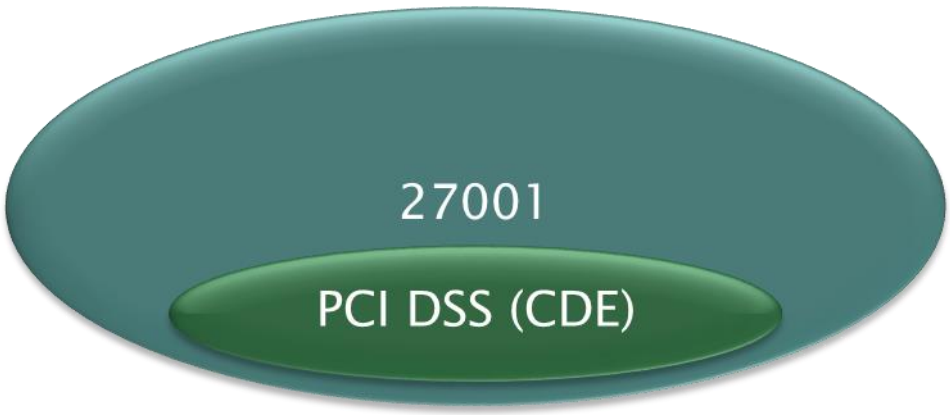

Ilustración 5-1 Alcance ISO27001-PCI DSS

5.3. Recomendaciones

Seguir la recomendación de implantación antes expuesta observando los siguientes puntos:

- Identificar el CDE, esto es el entorno en que se mueven los datos de las tarjetas de crédito, nótese como una infraestructura objeto del alcance de ISO27001 puede asimismo hallarse dividida entre lo que se considera CDE y lo que no. En éste aspecto es importante delimitar claramente dichos entornos.

- Para cada entorno debe asegurarse la independencia del mismo, PCI establece la necesidad de separación físico/lógica entre los equipos que gestionan el CDE y los que no teniendo que elevar dicha separación al plano físico (Firewalls por ejemplo).
- Iniciar la implantación con la aplicabilidad de PCI para identificar el CDE, acto seguido fusionar la aplicabilidad de PCI con la SOA de ISO27001 hallando la parte física como crítica y a implementar teniendo en cuenta el CDE y la SOA (seguridad por diseño)
- Establecer las relaciones entre CDE-SOA-Empresa en la siguiente ilustración se muestra la misma.

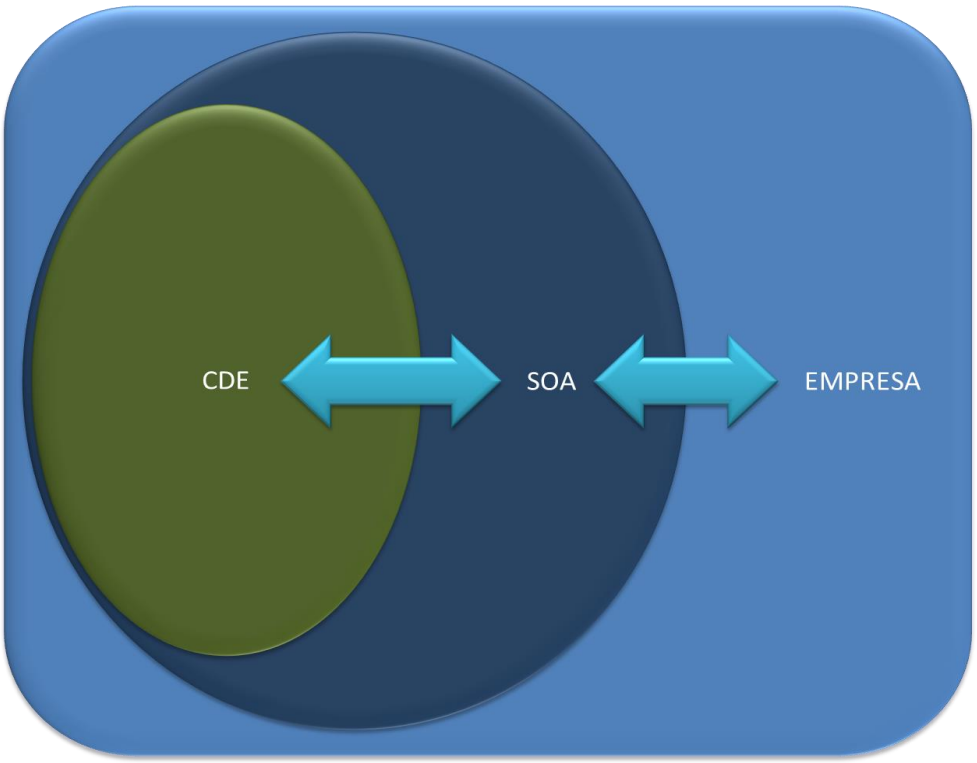

Ilustración 5-2 Relación CDE-SOA-Empresa

- Teniendo como premisa que la SOA engloba el CDE y que mediante la misma se vehicula la relación con la empresa, en el SGSI se incorpora el responsable de seguridad de CDE aportando su asesoramiento a los cambios o incidentes de seguridad que pueda sufrir su entorno disponiendo además del vehículo para hacer llegar sus necesidades al sponsor.

5.4. Problemas posibles

5.4.1. La definición del alcance

La definición del alcance puede dar pie a confusión, un alcance de certificación a modo de ejemplo sería:
Servicio de AAAAA a UUUU prestado desde las oficinas XXXX sitas en YYYYY en base a la SOA establecida el DD/MM/YYYY así como la correcta gestión del CDE en base a cumplimiento (CCCCCCC) sito en RRRRR de acuerdo a PCI DSS 3.1 con fecha DD/MM/YYYY.

5.4.2. Imposibilidad de acción

Hay un punto a tener en cuenta y es la imposibilidad por parte de la empresa de emprender las acciones necesarias, en éste caso se deberá establecer el análisis de riesgo e implantar cuantas acciones mitigadoras del mismo lo hagan aceptable o gestionable, en caso de no ser posible debiera aparecer en las aplicabilidad debiendo ser abordado por el SGSI tan pronto como sea detectado.

5.4.3. Falta de presupuesto

Otro punto clave es la falta de presupuesto para emprender las acciones de cumplimiento o las medidas mitigadoras del riesgo. Para mitigar éste riesgo se inicia el proyecto identificando al sponsor y estableciendo claramente el alcance de certificación, es fundamental que el consultor conozca las implicaciones de cada acción para poder asesorar correctamente a la dirección tanto en tiempo como en esfuerzo.
En caso de finalmente constatar la falta de recursos se deberá plantear la idoneidad de proseguir con el proyecto o bien de diferirlo en el tiempo mediante el uso de Sprints que permitan el fraccionamiento de las tareas a realizar de acuerdo con los recursos disponibles. Es responsabilidad del consultor establecer un calendario realista que gestione adecuadamente las expectativas de los involucrados en el proceso de certificación.

6. Correspondencia entre normas

Análisis de Riesgos: el análisis de riesgos es transversal a ambas normas con la salvedad de la necesidad de independencia entre sistemas. Las conclusiones son de uso de ambas dado que los análisis de riesgos de forma separada deben coincidir con el conjunto. Pese a ello se recomienda abarcar análisis de riesgos realizados de forma independiente dado el impacto financiero y de reputación que pueden tener las amenazas en el CDE respecto al área de cumplimiento e impacto financiero de las mismas.
Seguridad perimetral: las acciones de seguridad perimetral tales como zonas protegidas, control de acceso o identificación del personal servirán para ambas normas siendo sus procedimientos estandarizables.
Inventario => Bastionado (2.4), en el apartado inventario se deberá hacer énfasis en el bastionado PCI el cual establece una línea base de configuración (recomendación de ISO20000) y su seguimiento, en caso que la empresa no se halle familiarizada con ISO20000 se recomienda la realización de una acción que plantee a los mantenedores de los sistemas de la necesidad de contar con un proceso de gestión de bastionado de imágenes, esto es, un proceso que inventaríe y controle las imágenes de servidores en base a las mejores prácticas de gestión de la seguridad, esto es:

- Seguridad basada en mínimos: por defecto el acceso es denegado, sólo se tiene acceso a aquello para lo que se ha otorgado permiso, conocido como DENY=ALL.
- Control de versiones: controlar los equipos que usan la versión y establecer una política de control de las mismas habilitando el despliegue conjunto en caso de ser necesario.
- Seguridad por grupos, antes que por persona, como mejor práctica los usuarios pertenecerán a grupos de seguridad a quienes se les asignará el acceso.
- Control de licencias: el bastionado se basa en software licenciado propiedad de la empresa, el control de las licencias en uso debe constituirse como un proceso a implementar.

Protección Antivirus => 5. Antivirus: los equipos que vayan a procesar información deben disponer de un antivirus y el mismo debe ser actualizado de forma transparente para el usuario de forma regular. A tal efecto es necesario contar con una plataforma de gestión de versiones de antivirus que controle las definiciones implantadas y permita:

- Escaneo remoto de un equipo
- Actualización masiva de definiciones

Contacto grupos especial interés => 6.1 Al día de las vulnerabilidades, con el fin de disponer del máximo nivel de actualizaciones y vulnerabilidades

detectadas se recomienda suscribirse a los foros de vulnerabilidades (NIST, por ejemplo) en donde aparecen de forma periódica vulnerabilidades. Es responsabilidad del mantenedor de la seguridad del sistema mantener un proceso que recupere las vulnerabilidades, identifique los objetivos y en caso de ser dichos objetivos parte del bastionado establezca las acciones a emprender junto con el responsable de Seguridad.
O => 6.3 Guías de programación segura: debe asegurarse la seguridad por diseño, esto es diseñar los programas con un enfoque de seguridad, siguiendo mejores prácticas en su desarrollo y publicación. Esto incluye:

- Entornos de desarrollo/Integración/test y producción separados
- El no uso de información real en entornos que no sean producción
- Evitar el *hardcoding* (establecer credenciales en código) mediante el uso de criptografía, hash o cualquier medio criptográfico al alcance que sea aceptado por la auditoría interna

O => 6.4 Entornos Separados, separación, como se ha mencionado antes de los entornos de desarrollo de los de producción, de forma física por la mayor vulnerabilidad que suponen los entornos de desarrollo (bugs y problemas de seguridad) y la posibilidad de mediante accesos a entornos de pruebas pueda hacerse a producción.

6.1. Puntos a tener en cuenta

Es necesario diferenciar claramente el alcance
Los roles de seguridad pueden cambiar apareciendo un rol de Responsable de seguridad CDE el cual es optativo pero altamente recomendable como asesor en los cambios que puedan afectar a su entorno y la necesidad de establecer la mejor política de despliegue que no afecte a producción o minimizar el impacto (calendarizando las mismas en momentos valle o involucrando a la gerencia en caso necesario).

7. Conclusiones

7.1. Logros Obtenidos

La planificación de las acciones derivadas de dos procesos normativos relacionados pero con ópticas diferentes entraña una complejidad conceptual que no fue correctamente evaluada en la fase de planificación inicial habiendo desarrollado en profundidad ISO27001 y en menor medida PCI. Pese a ello el resultado permite la implementación de la ISO27001:2013 así como la identificación de los puntos fundamentales de PCI con la óptica de certificación. Los puntos clave de PCI se han identificado y establecido los nexos entre ambas normas.

7.2. Análisis crítico de la planificación y metodología

Como regla general la planificación se ha seguido teniendo las siguientes excepciones:

- Análisis de controles comunes y casamiento entre ambas normas: ha sido una tarea que requiere de un esfuerzo ingente, ha sido posible llevarla a cabo gracias a duplicar el tiempo requerido para su consecución.
- La propia tarea de planificación y organización del trabajo ha llevado a la necesidad de trabajar en paralelo en:
    - Iso 27001: con la consecución de los puntos clave
    - PCI con las recomendaciones de implantación
    - Fusión entre ambas y la imposibilidad de publicar el resultado por estar la norma sujeta a Copyright incorporando los puntos clave al presente.
    - Identificación de puntos comunes
- Todo esto ha desembocado en una estructura de documento compleja, habiendo tenido que dedicar un esfuerzo no planificado a mejorar la legibilidad moviendo bloques de información para dotar de lógica y coherencia al documento.

7.3. Líneas de trabajo futuro

Las líneas de trabajo futuro que no se han podido explorar en este trabajo y han quedado pendientes son:

- Establecimiento del listado de formatos comunes e identificación del órden de implantación para PCI DSS.
- Do’s & Don’ts: recomendaciones cruzadas de mejores prácticas y puntos a evitar los cuales darán mayor consistencia al producto.

- Documentar todos los formatos mediante evidencias documentales estandarizadas, no se ha podido abarcar por falta de tiempo, constituiría un proyecto en sí.

7.4. Lecciones aprendidas

Como lecciones aprendidas de la confección del trabajo, y debido a que el mismo es fruto de la experiencia profesional de quien lo escribe he aprendido la importancia del análisis de riesgos basado en mejores prácticas por ser una no conformidad menor detectada en varias de mis auditorías. El uso de un esquema en tres dimensiones dota al conjunto de robustez y fiabilidad. Aunque como punto débil a destacar es la dificultad del mantenimiento posterior.

Debido a la orientación eminentemente práctica del enfoque normativo perseguida en éste trabajo el análisis de riesgos ha sido el único punto teórico añadido en el mismo, el modelo propuesto –incluido el análisis de riesgos- es fruto de la experiencia exitosa en varias implantaciones normativas de una o varias normas en empresas de todo tamaño.

Docemur docendo (el que enseña aprende) este ejercicio ha servido para fijar conceptos y adquirir mayor seguridad en la implantación normativa. Si bien se exige a un auditor jefe certificado el conocimiento de la norma, es claramente recomendable el ejercicio de enfrentarse a dos normas complejas, la 27001, quizás la más completa y la PCI que es quizás la más estricta, un objetivo ambicioso.

14 de junio de 2016

8. Las familias de normas

La norma ISO27001:2013 es una norma auditable de la ISO cuyo desarrollo es controlado por la IEC. Aparece como ISO/IEC27001:2013, siendo el 2013 el año en que se realizó la última revisión conjunta por parte de ISO e IEC. Para el presente documento se empleará ISO indistintamente para referirse al organismo ISO/IEC así como para nombrar las normas.
La norma se implanta dentro de una familia de normas englobadas con el prefijo ISO2700x siendo las más relevantes y sobre las que se desarrollará el presente trabajo las siguientes:

Nombre	Contenido
ISO27000	Terminología
ISO27001	Sistema de Gestión de la Seguridad de la información (SGSI)
ISO27002	Controles de seguridad
ISO27004	Indicadores de Gestión de la Seguridad
ISO27005	Gestión del riesgo
ISO27006	Requerimientos para la auditoría
ISO27007	Guía para la auditoría
ISO27008	Guía para la verificación de controles de Seguridad
ISO27010	Gestión de la seguridad en empresas inter-sector
ISO27011	Gestión de la seguridad en empresa de Telecomunicaciones
ISO27013	Guía para la implementación de la 27001 y la 20000-1
ISO27014	Guía del Gobierno de la seguridad de la información
ISO27015	Guía gestión de la seguridad en servicios financieros
ISO27016	Guía para identificar el impacto económico en las decisiones de seguridad

Tabla 8-1 La familia ISO27000

Cuando en una norma aparece un concepto explicado en otra, la primera simplemente referencia a la segunda. Por ejemplo: concepto de Riesgo en ISO27001, referencia a ISO31000.

Norma	Referencia a	Objetivo
ISO27000 : Terminología	ISO 15939	Establecer un vocabulario común
ISO27005 : Gestión del riesgo	ISO 31000	Identificar pautas para una correcta gestión del riesgo
ISO27006 : Requerimientos para la auditoría	ISO 17021	Necesidades del equipo auditor para ser considerado como tal y requisitos de auditoría
ISO27007 : Guía para la auditoría	ISO 19011	Metodología de auditoría
ISO27001/Continuidad	ISO 22301	Gestión de la continuidad
Otras normas		

referenciadas		
ISO19011	ISO17021 e ISO9001 NIST 800-53A	Auditoría de sistemas de Gestión
ISO29148	IEEE Std 1233	Requisitos de Sistemas y Software
ISO16085	ISO15288	Gestión de Riesgo en Ingeniería de Software
ISO20000	ISO27001 e ISO9001	Prestación del servicio
NIST 800-30	ISO27001	Gestión del Riesgo

Tabla 8-2Referencias Normativas

La ISO27001:2013, como Sistema de Gestión es auditable, lo que supone su orientación a un cumplimiento normativo regulado por organismos propios que se constituyen durante la implantación, cuya finalidad es la gestión y la evidencia del cumplimiento de los controles que se detallan en la misma.

9. La Certificación

Las fases que una empresa debe seguir para completar la certificación son:

1. La empresa realiza las acciones necesarias para cumplir con la norma siguiendo el alcance que haya definido.
2. La empresa escoge el esquema normativo a emplear dado que la ISO admite particularizaciones por país, así en España existe AENOR o el Esquema Nacional de Seguridad, por ejemplo en Inglaterra UKAS y BSI (*British Standards Institution*).
3. Una empresa auditora externa realiza una auditoría de cumplimiento normativo en base a la norma y al esquema nacional escogido. Pueden ocurrir tres escenarios:
   3.1. La empresa cumple con el esquema y la norma con lo que se expediría el certificado de cumplimiento.
   3.2. La empresa no cumple la norma (en la auditoría se hallan No Conformidades Mayores[2]) y no puede ser expedido el certificado por haber hallado evidencias de incumplimiento. Con lo que la empresa debiera corregir las No Conformidades y presentarse de nuevo a una auditoría de certificación.[3]
   3.3. La empresa cumple parcialmente la norma, en la auditoría se hallan No Conformidades menores y observaciones, con lo que la empresa tendría un período de corrección para corregir las no conformidades detectadas y repetir la auditoría. Puede pasar que en la auditoría se halle una No Conformidad Mayor por falta de evidencia de algo que la empresa sí realice por lo que entonces la empresa podría acogerse al período de corrección para evidenciar el cumplimiento.
4. En caso que la empresa sí cumpla con el esquema y norma dentro del alcance la empresa auditora expediría el certificado de cumplimiento normativo y permitiría a la empresa el uso del sello como empresa certificada.
5. Cada año la empresa auditora externa revisa el cumplimiento y mantenimiento del sistema emitiendo certificados de continuidad. La empresa cliente debe mantener la aplicabilidad de la norma y evidenciarlo en la revisión.
6. Cada tres años se renueva la certificación por completo.

[2] Los requisitos de auditoría se hallan descritos en la ISO17021

[3] A menudo las empresas desean saber su grado de cumplimiento sin llegar a una auditoría de certificación por lo que realizan una Pre-Auditoría, esto es, una auditoría no vinculante por la cual obtienen un diagnóstico de qué aspectos de la implantación de la norma cumplen y cuales no con el fin de planificar la auditoría de certificación. Hay que considerar que el coste de una auditoría de certificación es considerablemente más alto que el de una Pre-Auditoría razón por la cual muchas empresas optan por ésta vía a la hora de plantearse la certificación como primer paso.

9.1. Factores Clave de Éxito

Hay dos factores clave en la implantación de la norma que son:

- La gestión del riesgo
- La previsión de trazabilidad de las acciones mediante la obtención de evidencias, este punto merece especial atención por ser un punto fundamental para ligarlo con otras normas y conseguir el Cumplimiento normativo (*Compliance*).

9.2. Privacidad y otras consideraciones

Las normas ISO no son públicas, se hallan a la venta de estando perseguida su publicación sin permiso del organismo. Cada norma se halla personalizada con un pie de página indicando su propietario.

9.3. Coexistencia de normas

La ISO ha dotado a las normas de una estructura similar (Anexo SL) para que su implantación sea más sencilla.
Finalmente existen otras normas que pueden implantarse conjuntamente con la ISO27001 o en serie que cubren aspectos específicos, como por ejemplo:

- ISO20000: prestación de servicios bajo el concepto de catálogo de servicios, o se dispone de un marco de relación basado en Acuerdos de Nivel de Servicio (ANS o SLA en inglés). (Prestatarios de servicios de Tecnologías de la Información)
- ISO22301: Continuidad de Negocio (Prestatarios con requerimientos de Continuidad), conceptos de riesgo, BIA, BCP y planes de continuidad.
- ISO14001: Seguridad laboral PRL y OSHAS (Centros de trabajo)
- ISO9001: Sistema de Gestión de la Calidad (Producción)
- SOX: Sistema de control de *reporting* bancario (Financieras)
- PCI/DSS: Sistema de Pago con tarjeta de crédito (Venta con tarjeta de crédito)
- GMP: Mejores prácticas Manufactureras (Empresas Industriales)

10. ANEXO I– Puntos de control del SGSI

#	Título control	Descripción del control
5.1.1	Políticas de información seguridad	Se debe aprobar por la gerencia, comunicar y publicar un documento de política de seguridad a todos los empleados y personal externo interesado.
5.1.2	Revisión de las políticas de información seguridad	Las políticas de seguridad de la información serán revisadas de forma periódica y planificada y si se producen cambios significativos asegurar continuamente su idoneidad, adecuación y eficacia.
6.1.1	Seguridad de la información roles y responsabilidades	Se debe definir y asignar todas las responsabilidades de seguridad de la información.
6.1.2	Segregación de funciones	Las funciones que entran en conflicto y áreas de responsabilidad estarán separadas para reducir las posibilidades de realizar una modificación no autorizada o accidental o un mal uso de los activos de la organización.
6.1.3	Póngase en contacto con las autoridades	Se mantendrán los contactos apropiados ante las autoridades competentes.
6.1.4	Póngase en contacto con especial grupos de interés	Se mantendrán los contactos apropiados con grupos de interés especial u otro especialista seguridad foros y asociaciones profesionales.
6.1.5	Seguridad de la información en gestión de proyectos	Seguridad de la información se aplicará en gestión de proyectos, independientemente del tipo de proyectos
6.2.1	Política de dispositivos móviles	Se definirá una política de seguridad que aplicará sobre la gestión de dispositivos móviles.
6.2.2	Teletrabajo	Se aplicarán una política y medidas de seguridad para proteger la información accesible, los datos tratados o almacenados en los sitios de teletrabajo.
7.1.1	Proyección	Verificación de antecedentes de todos los candidatos de empleo se debe realizar de acuerdo con las leyes, reglamentos y ética y serán proporcionales a los requerimientos del negocio, la clasificación de la información, cómo debe accederse y los riesgos percibidos.
7.1.2	Términos y condiciones de empleo	Los acuerdos contractuales con los empleados y contratistas deberán indicar las responsabilidades de la organización para la seguridad de la información.
7.2.1	Responsabilidades de gestión	Dirección exigirán a todos los empleados y contratistas aplicar las políticas de seguridad de la información establecidas en los procedimientos de la organización.

7.2.2	Etiquetado y manejo de la información Formación, educación y sensibilización de seguridad de información	Todos los empleados de la organización y, cuando proceda, contratistas, recibirán formación adecuada, concienciación y actualizaciones regulares y capacitación de las políticas y procedimientos de seguridad relevantes para su función de trabajo.
7.2.3	Proceso disciplinario	Habrá un proceso disciplinario formal para tomar medidas contra los empleados que han cometido una infracción de seguridad de información y dicho procedimiento será comunicado de forma oficial a todos los empleados.
7.3.1	Terminación o cambio de las responsabilidades del empleo	Las responsabilidades y deberes de seguridad de la información que siguen siendo válidas después de finalización o cambio de un empleado deben ser definidas, comunicadas a empleados y contratistas.
8.1.1	Inventario de activos	Se deberá tener identificados los activos e instalaciones asociadas a la seguridad en el procesamiento de la información, dichos activos deberán ser inventariados y mantenidos.
8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario serán propiedad de la compañía.
8.1.3	Uso aceptable de los activos	Se identificarán, documentarán y aplicarán normas para el uso aceptable de la información y de activos asociados a las instalaciones de procesamiento de la información y la información.
8.1.4	Restitución de bienes	Todos los empleados y asociados externos devolverá todos los activos de la organización que tengan en posesión a la finalización de su empleo o contrato o acuerdo
8.2.1	Clasificación de la información	Información se clasificarán en función de los requisitos legales, el valor, la criticidad y sensibilidad a la divulgación o modificación no autorizada.
8.2.2	Etiquetado de información	Se desarrollará e implementará un conjunto de procedimientos para el etiquetado de información conforme al esquema de clasificación de la información adoptado por la organización.
8.2.3	Gestión de activos	Se desarrollarán e implantarán procedimientos para la gestión de activos conforme al esquema de clasificación de la información adoptado por la organización.
8.3.1	Gestión de medios extraíbles	Se aplicarán los procedimientos para la gestión de los medios extraíbles de acuerdo al esquema de clasificación adoptado por la organización.
8.3.2	Disposición de los medios	Medios se eliminarán de forma segura, cuando ya no sea necesario, utilizando procedimientos formales.
8.3.3	Transferencia de medios físicos	Los medios de comunicación que contenga información estarán protegidos contra el acceso no

		autorizado, mal uso o corrupción durante el transporte.
9.1.1	Política de control de acceso	Se establecerá, documentará y revisará una política de control de acceso en base a los requisitos de seguridad de información y del negocio.
9.1.2	Acceso a redes y servicios de red	Los usuarios sólo deberán disponer de acceso a los servicios de red y a la red que han sido autorizados específicamente para su uso.
9.2.1	Registro de usuario y para cancelar el registro	Se implementará un proceso formal de registro y cancelación de usuario que permitir la asignación de derechos de acceso.
9.2.2	Aprovisionamiento de acceso de usuarios	Se implementará un proceso formal de aprovisionamiento de acceso de usuario que permita asignar o revocar los derechos de acceso para todos los tipos de usuario para todos los sistemas y todos los servicios.
9.2.3	Gestión de privilegios derechos de acceso	La asignación y utilización de los derechos de acceso privilegiados serán restringidas y controladas.
9.2.4	Gestión de secreto información de autenticación de los usuarios	Se debe controlar a través de un proceso de gestión la asignación de información de autenticación.
9.2.5	Informe sobre acceso de los usuarios derechos	Los propietarios de activos deberán revisar los derechos de acceso de los usuarios periódicamente.
9.2.6	Su revocación o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y usuarios asociados externo a la información y al procesado de la información serán eliminados en caso de finalización de su empleo, contrato o acuerdo, o modificados si se realiza un cambio.
9.3.1	Uso de autentificación secreta información	Los usuarios deberán seguir las prácticas de la organización en el uso de la información de autenticación secreta.
9.4.1	Restricción al Acceso a la información	Se limitará el acceso a la información y la aplicación de las funciones del sistema según la política de control de acceso.
9.4.2	Procedimientos del inicio de sesión seguros	Donde sea requerido por la política de control de acceso, el acceso a los sistemas y las aplicaciones deberán ser controlados por un procedimiento de inicio de sesión seguro.
9.4.3	Sistema de Gestión de contraseñas	Los Sistemas de gestión de contraseñas deben ser interactivos y garantizarán las contraseñas de calidad.
9.4.4	Uso de la utilidades privilegiadas	El uso de programas de utilidades que podrían ser capaces de anular sistemas y controles de aplicaciones estará restringido y estrechamente controlado.
9.4.5	Control de acceso a los códigos fuente de	Se restringirá el acceso al código fuente de los programas.

	los programas	
10.1.1	Política sobre el uso de controles criptográficos	Se deberá desarrollar e implementar una política sobre el uso de controles criptográficos que permita la protección de la información.
10.1.2	Gestión de claves	Se deberá desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas.
11.1.1	Seguridad física perimetral	Se definirán zonas perimetrales de seguridad para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información.
11.1.2	Controles de entrada física	Las áreas seguras deberán estar protegidas por los controles de entrada apropiados para garantizar que sólo se permite acceso al personal autorizado.
11.1.3	Oficinas de seguridad, salas e instalaciones	Se deberá diseñar y aplicar seguridad física para oficinas, salas e instalaciones.
11.1.4	Protección contra amenazas externas y ambientales	Se deberá diseñar y aplicar Protección física contra desastres naturales, ataque malicioso o accidentes.
11.1.5	Trabajando en zonas seguras	Se diseñarán y aplicarán procedimientos para trabajar en zonas seguras.
11.1.6	Entrega y zonas de carga	Puntos de acceso, puntos de entrega y carga y otros puntos donde las personas no autorizadas podrían entrar al recinto deberán ser controlados y, si es posible, aislados de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.
11.2.1	Ubicación y protección de los equipos	Equipo deben situarse en lugares que permitan reducir los riesgos de las amenazas ambientales y minimizar el el acceso no autorizado a la información.
11.2.2	Utilidades de apoyo	Los equipos estarán protegidos de apagones y otras interrupciones causadas por fallas en el apoyo a servicios públicos.
11.2.3	Cableado de seguridad	Energía y el cableado de telecomunicaciones que transportar datos o servicios de información deben estar protegido de intercepción, interferencia o daño.
11.2.4	Mantenimiento de equipos	Los equipos deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.
11.2.5	Eliminación de activos	No se realizará la baja de equipos información o software sin previa autorización.
11.2.6	Seguridad de equipos y activos fuera de los locales	Se aplicarán políticas de seguridad e inspecciones a activos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de los locales de la organización.

11.2.7	Eliminación o reutilización de equipos de forma segura	Se verificará todos los elementos del equipo que contiene los medios de almacenamiento para asegurar que cualquier información confidencial y software con licencia ha sido eliminado o sobrescrito firmemente antes de la eliminación o reutilización.
11.2.8	Equipo de usuario desatendidos	Los usuarios se asegurarán de que el equipo desatendido tiene una protección adecuada.
11.2.9	Política mesa y pantalla limpia	Se adoptará una política de escritorio limpio de papeles y soportes de almacenamiento extraíbles y una política pantalla limpia para las instalaciones de procesamiento de información.
12.1.1	Documentar los procedimientos de operación	Procedimientos operativos serán documentados y puesto a disposición de todos los usuarios que lo necesiten.
12.1.2	Gestión del cambio	Los cambios en la organización, los procesos de negocio, instalaciones y sistemas que afectan la seguridad de la información de procesamiento de información deberán ser controlados.
12.1.3	Administración de la capacidad	El uso de los recursos deberá ser monitorizado, afinado y permitirá proyecciones de los requerimientos de capacidad futura para asegurar el funcionamiento de los sistemas.
12.1.4	Separación del desarrollo, pruebas y entornos operativos	Desarrollo, pruebas y entornos operativos estarán separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.
12.2.1	Controles contra el malware	Se aplicarán controles de detección, prevención y recuperación para proteger contra malware, combinado con la sensibilización apropiado de los usuarios.
12.3.1	Copias de seguridad	Copias de seguridad de la información, software y sistema de imágenes se probados regularmente de acuerdo con una política de copia de seguridad acordada.
12.4.1	Registro de eventos	Se debe generar, guardar y analizar periódicamente registros de eventos, grabación de las actividades de usuario, excepciones, fallos y eventos de seguridad de la información
12.4.2	Protección de la información de registro	Las funcionalidades de los Registro y la información de los registros deben ser protegidos contra la manipulación y acceso no autorizado.
12.4.3	Administrador y operador de registros	Las actividades del administrador de sistemas y del operador de sistemas deben estar registradas, protegidas y periódicamente revisadas.
12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de información dentro de la organización o del dominio de deberán estar sincronizados a una fuente de tiempo única de referencia.
12.5.1	Instalación del	Se aplicarán procedimientos para controlar la

	software en sistemas operativos	instalación de software en los sistemas operativos.
12.6.1	Gestión de vulnerabilidades técnicas	Se deberá obtener de forma oportuna información acerca de las vulnerabilidades técnicas de los sistemas de información. La exposición de la organización a dichas vulnerabilidades deberán evaluarse y determinar las medidas oportunas para minimizar el riesgo
12.6.2	Restricciones sobre la instalación de software	Se deberá establecer e implementar normas que rigen la instalación de software para los usuarios
12.7.1	Controles de auditoría de sistemas de información	Los requerimientos de Auditoría y las actividades que implican verificación de sistemas operativos deben planificarse y acordarse con el fin de minimizar las interrupciones a los procesos del negocio.
13.1.1	Controles de red	Redes serán gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.
13.1.2	Seguridad de servicios de red	Los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de toda la red servicios serán identificados e incluidos en los acuerdos de servicios de red, si estos servicios se prestan en la empresa o son subcontratados.
13.1.3	Segregación en redes	Grupos de servicios de información, usuarios y sistemas de información estarán segregados en diferentes redes.
13.2.1	Los procedimientos y las políticas de transferencia de información	Se debe definir políticas de transferencia, procedimientos y controles para proteger a la transferencia de información a través de cualquier tipo de medios de comunicación.
13.2.2	Acuerdos sobre transferencia de información	Se debe definir acuerdos de transferencia segura de información entre la organización y los colaboradores externos.
13.2.3	Mensajería electrónica	Información involucrada en mensajería electrónica deberá estar adecuadamente protegido.
13.2.4	Confidencialidad o no divulgación acuerdos	Se identificarán, revisarán y documentarán requerimientos de confidencialidad o acuerdos de no-divulgación que reflejen las necesidades de la organización para la protección de la información.
14.1.1	Seguridad de la información Análisis de requerimientos y especificaciones	Los requisitos relacionados con la seguridad de la información se incluirán en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.
14.1.2	Asegurar servicios de aplicación en las redes públicas	Información generada en servicios de aplicación que pasa a través de las redes públicas debe ser protegida de actividades fraudulentas, disputa contractual y la divulgación no autorizada y modificación.

14.1.3	Protección de aplicaciones transacciones de servicios	Información generada en las transacciones de servicio de aplicación deberá estar protegida para evitar la transmisión incompleta, *mis-routing*, alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación no autorizada del mensaje o la repetición.
14.2.1	Política de desarrollo seguro	Serán establecidas reglas para el desarrollo de software y sistemas y dichas reglas serán aplicadas a los desarrollos dentro de la organización.
14.2.2	Procedimientos de control de cambio de sistema	Los cambios en los sistemas en el desarrollo del ciclo de vida serán controlados mediante el uso de los procedimientos de control de cambio formal.
14.2.3	Revisión técnica de las aplicaciones después de los cambios de la plataforma de funcionamiento	Cuando se cambian los plataformas que operan, las aplicaciones críticas del negocio serán revisadas y probadas para asegurar que no hay ningún impacto adverso en las operaciones de la organización o la seguridad.
14.2.4	Restricciones sobre los cambios en los paquetes de software	Modificaciones a paquetes de software deben ser limitados a los cambios necesarios y todos los cambios deberá ser estrictamente controlada.
14.2.5	principios Ingeniería de sistemas seguros	Se establecerán, documentarán, mantendrán y aplicarán principios de ingeniería de sistemas seguro a cualquier implantación de sistema de información.
14.2.6	Entorno de Desarrollo seguro	Las organizaciones deberán establecer y proteger adecuadamente entornos de desarrollo seguras para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida de desarrollo del sistema.
14.2.7	Desarrollo subcontratado	La organización deberá supervisar y monitorizar la actividad de desarrollo del sistema externalizado.
14.2.8	Pruebas de seguridad del sistema	Prueba de funcionalidad de seguridad se efectuará durante el desarrollo.
14.2.9	Aceptación del sistema de pruebas	Se establecerán programas y criterios relacionados con las prueba de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones.
14.3.1	Protección de datos de prueba	Datos de prueba serán seleccionados cuidadosamente y estarán protegidos y controlados.
15.1.1	Política de seguridad de la información para relaciones con los proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedor a los activos de la organización deberán ser acordados con el proveedor y documentados.
15.1.2	Abordar la seguridad dentro de los acuerdos de proveedor	Todos los requisitos de seguridad de la información pertinente serán establecidos y acordado con cada proveedor que puede tener acceso, procesar, almacenar, comunicar o proveer componentes de la infraestructura, información de la organización.

15.1.3	Información y la comunicación tecnología cadena de suministro	Acuerdos con los proveedores deberán incluir requisitos para abordar los riesgos de seguridad de la información asociados con información y cadena de suministro de productos y servicios de tecnología de comunicaciones.
15.2.1	Seguimiento y revisión de servicios a proveedores	Organizaciones deberán supervisar regularmente, revisar y auditar la prestación de servicios de proveedor.
15.2.2	Gestión de cambios a los servicios de proveedor	Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, serán gestionados, teniendo en cuenta la criticidad de la información empresarial, los sistemas y los procesos involucrados y re-evaluación de los riesgos.
16.1.1	Responsabilidades y procedimientos	Se establecerán los procedimientos y las responsabilidades de gestión para asegurar una respuesta rápida, eficaz y ordenada a incidentes de seguridad de la información.
16.1.2	Notificación de eventos de seguridad de la información	Eventos de seguridad de la información se notificarán a través de canales de gestión apropiada lo más rápidamente posible.
16.1.3	Reportando las debilidades de seguridad de información	Los empleados y contratistas utilizando sistemas de información y servicios de la organización estará obligados a observar y reportar cualquier debilidad de seguridad información observada o sospechada en los sistemas o servicios.
16.1.4	De evaluación y decisión sobre eventos de seguridad de la información	Los eventos de seguridad de la información deben ser evaluados y se decidirá si han de ser clasificados como incidentes de seguridad de la información.
16.1.5	Respuesta a la información incidentes de seguridad	Incidentes de seguridad de información deberán recibir una respuesta de conformidad con los procedimientos documentados.
16.1.6	Aprender de incidentes de seguridad de la información	Los conocimientos adquiridos desde el análisis y la resolución de los incidentes de seguridad de la información se utilizarán para reducir la probabilidad o el impacto de futuros incidentes.
16.1.7	Obtención de pruebas	La organización deberá definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia.
17.1.1	Planificación de continuidad de seguridad de información	La organización deberá determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.

17.1.2	Implementación de continuidad de seguridad de información	La organización establecerá, documento, implementar y mantener los procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.
17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de información	La organización verificará los controles de información establecida e implementando seguridad y continuidad a intervalos regulares para asegurar que son válidos y eficaces en situaciones adversas.
17.2.1	Disponibilidad de la información procesamiento instalaciones	Instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para satisfacer los requisitos de disponibilidad.
18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	Todo statuto legal, normativos, los requisitos contractuales y enfoque de la organización para cumplir con estos requisitos serán explícitamente identificados, documentados y actualizados para cada sistema de información.
18.1.2	Derechos de Propiedad intelectual	Se aplicarán los procedimientos adecuados para garantizar el cumplimiento con los requisitos legales, reglamentarios y contractuales relacionados con derechos de propiedad intelectual y el uso de productos de software privativo.
18.1.3	Protección de registros	Los registros estarán protegidos de la pérdida, destrucción, falsificación, acceso y liberación no autorizada, conforme a los requisitos legales, reglamentarios, contractuales y comerciales.
18.1.4	Privacidad y protección de datos personales	Privacidad y protección de datos personales se garantizará según lo dispuesto en la legislación y la regulación.
18.1.5	Reglamento de controles criptográficos	Se utilizarán controles criptográficos en el cumplimiento de todos los acuerdos pertinentes, la legislación y los reglamentos.
18.2.1	Revisión independiente de seguridad de la información	El enfoque de la organización para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos de seguridad de la información) se revisará de forma independiente a intervalos planificados o cuando se producen cambios significativos.
18.2.2	Cumplimiento de las normas y políticas de seguridad	Los administradores deberán revisar periódicamente el cumplimiento de los procedimientos de procesamiento y la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad.
18.2.3	Revisión de Cumplimiento de técnico	Los sistemas de información se revisarán periódicamente del cumplimiento de las políticas y normas de seguridad de la información de la

		organización.

Tabla 10-Puntos de Control de SGSI

Reconocimiento: la norma se halla sujeta a compra, por tanto no puede reproducirse aquí, el listado de controles está basado en la difusión gratuita de controles de www.ISO27000.es y la explicación de cada uno es obra del autor del documento como se indica en el apartado Referencias más adelante en el presente documento.

11. ANEXO II CONTROLES PCI DSS 3.1

PCI DSS 3.1		
Punto	Área	Texto
1.1	Firewall	Establish and implement firewall and router configuration standards that include the following:
1.1.1	Firewall	A formal process for approving and testing all network connections and changes to the firewall and router configurations
1.1.2	Firewall	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks
1.1.3	Firewall	Current diagram that shows all cardholder data flows across systems and networks
1.1.4	Firewall	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
1.1.5	Firewall	Description of groups, roles, and responsibilities for management of network components
1.1.6	Firewall	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.
1.1.7	Firewall	Requirement to review firewall and router rule sets at least every six months
1.2	Firewall	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.
1.2.1	Firewall	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
1.2.2	Firewall	Secure and synchronize router configuration files.
1.2.3	Firewall	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
1.3	Internet	Prohibit direct public access between the Internet and any system component in the cardholder data environment.
1.3.1	Internet	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
1.3.2	Internet	Limit inbound Internet traffic to IP addresses within the DMZ.
1.3.4	Internet	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.

1.3.5	Internet	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
1.3.6	Internet	Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)
1.3.7	Internet	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.
1.3.8	Internet	Do not disclose private IP addresses and routing information to unauthorized parties.
1.4	Internet	Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network
1.5	Internet	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.
2.1	Internet	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.
2.1.1	Internet	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
2.2	Internet	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.
2.2.1	Internet	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)
2.2.2	Internet	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.
2.2.3	Internet	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP,
2.2.4	Internet	Configure system security parameters to prevent misuse.
2.2.5	Internet	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
2.3	Internet	Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.

2.4	Internet	Maintain an inventory of system components that are in scope for PCI DSS.
2.5	Internet	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.
2.6	Internet	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.
3.1	CDE	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:
3.2	CDE	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.
3.2.1	CDE	Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.
3.2.2	CDE	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.
3.2.3	CDE	Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.
3.3	CDE	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.
3.4	CDE	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:
3.4.1	CDE	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.
3.5	CDE	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:
3.5.1	CDE	Restrict access to cryptographic keys to the fewest number of custodians necessary.
3.5.2	CDE	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:

3.5.3	CDE	Store cryptographic keys in the fewest possible locations.
3.6	CDE	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:
3.6.1	CDE	Generation of strong cryptographic keys
3.6.2	CDE	Secure cryptographic key distribution
3.6.3	CDE	Secure cryptographic key storage
3.6.4	CDE	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines
3.6.5	CDE	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.
3.6.6	CDE	If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.
3.6.7	CDE	Prevention of unauthorized substitution of cryptographic keys.
3.6.8	CDE	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.
3.7	CDE	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.
4.1	CDE	Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following:
4.1.1	CDE	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.
4.2	CDE	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
4.3	CDE	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.
5.1	Antivirus & Malware	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
5.1.1	Antivirus & Malware	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious

		software.
5.1.2	Antivirus & Malware	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.
5.2	Antivirus & Malware	Ensure that all anti-virus mechanisms are maintained as follows:
5.3	Antivirus & Malware	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.
5.4	Antivirus & Malware	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.
6.2	SW	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
6.3	SW	Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:
6.3.1	SW	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.
6.3.2	SW	Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:
6.4	CHANGE MNG	Follow change control processes and procedures for all changes to system components. The processes must include the following:
6.4.1	CHANGE MNG	Separate development/test environments from production environments, and enforce the separation with access controls.
6.4.2	CHANGE MNG	Separation of duties between development/test and production environments
6.4.3	CHANGE MNG	Production data (live PANs) are not used for testing or development
6.4.4	CHANGE MNG	Removal of test data and accounts before production systems become active
6.4.5.1	CHANGE MNG	Documentation of impact.
6.4.5.2	CHANGE MNG	Documented change approval by authorized parties.
6.4.5.3	CHANGE MNG	Functionality testing to verify that the change does not adversely impact the security of the system.
6.4.5.4	CHANGE MNG	Back-out procedures.

6.5	Attacks	Address common coding vulnerabilities in software-development processes as follows:
6.5.1	Attacks	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.
6.5.10	Attacks	Broken authentication and session management
6.5.2	Attacks	Buffer overflows
6.5.3	Attacks	Insecure cryptographic storage
6.5.4	Attacks	Insecure communications
6.5.5	Attacks	Improper error handling
6.5.6	Attacks	All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).
6.5.7	Attacks	Cross-site scripting (XSS)
6.5.8	Attacks	Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).
6.5.9	Attacks	Cross-site request forgery (CSRF)
6.6	Attacks	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:
6.7	Attacks	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.
7.1	Attacks	Limit access to system components and cardholder data to only those individuals whose job requires such access.
7.1.1	Privilegios	Define access needs for each role, including:
7.1.2	Privilegios	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
7.1.3	Privilegios	Assign access based on individual personnel’s job classification and function.
7.1.4	Privilegios	Require documented approval by authorized parties specifying required privileges.
7.2	Privilegios	Establish an access control system for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.
7.2.1	Privilegios	Coverage of all system components
7.2.2	Privilegios	Assignment of privileges to individuals based on job classification and function.
7.2.3	Privilegios	Default “deny-all” setting.
7.3	Privilegios	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

8.1	Privilegios	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:
8.1.1	Privilegios	Assign all users a unique ID before allowing them to access system components or cardholder data.
8.1.2	Privilegios	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
8.1.3	Privilegios	Immediately revoke access for any terminated users.
8.1.4	Privilegios	Remove/disable inactive user accounts within 90 days.
8.1.5	Privilegios	Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:
8.1.6	Privilegios	Limit repeated access attempts by locking out the user ID after not more than six attempts.
8.1.7	Privilegios	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
8.1.8	Privilegios	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
8.2	Privilegios	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:
8.2.1	Privilegios	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
8.2.2	Privilegios	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.
8.2.3	PWD	Passwords/phrases must meet the following:
8.2.4	PWD	Change user passwords/passphrases at least once every 90 days.
8.2.5	PWD	Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.
8.2.6	PWD	Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
8.3	PWD	Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).
8.4	PWD	Document and communicate authentication policies and procedures to all users including:
8.5	PWD	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

8.5.1	PWD	Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.
8.6	PWD	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:
8.7	PWD	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:
8.8	PWD	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
9.1	FÍSICAS	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
9.1.1	FÍSICAS	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.
9.1.2	FÍSICAS	Implement physical and/or logical controls to restrict access to publicly accessible network jacks.
9.1.3	FÍSICAS	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.
9.10	FÍSICAS	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.
9.2	FÍSICAS	Develop procedures to easily distinguish between onsite personnel and visitors, to include:
9.3	FÍSICAS	Control physical access for onsite personnel to sensitive areas as follows:
9.4	FÍSICAS	Implement procedures to identify and authorize visitors.
9.4.1	FÍSICAS	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.
9.4.2	FÍSICAS	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.
9.4.3	FÍSICAS	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.
9.4.4	FÍSICAS	Todos los empleados y asociados externos devolverá todos los activos de la organización que tengan en posesión a la finalización de su empleo o contrato o acuerdo
9.5	MEDIA	Physically secure all media.

9.5.1	MEDIA	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.
9.6	MEDIA	Maintain strict control over the internal or external distribution of any kind of media, including the following:
9.6.1	MEDIA	Classify media so the sensitivity of the data can be determined.
9.6.2	MEDIA	Send the media by secured courier or other delivery method that can be accurately tracked.
9.6.3	MEDIA	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).
9.7	MEDIA	Maintain strict control over the storage and accessibility of media.
9.7.1	MEDIA	Properly maintain inventory logs of all media and conduct media inventories at least annually.
9.8	MEDIA	Destroy media when it is no longer needed for business or legal reasons as follows:
9.8.1	MEDIA	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.
9.8.2	MEDIA	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
9.9	MEDIA	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.
9.9.1	MEDIA	Maintain an up-to-date list of devices. The list should include the following:
9.9.2	MEDIA	Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).
9.9.3	MEDIA	Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. - Do not install, replace, or return devices without verification. - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).
10.1	AUDIT	Implement audit trails to link all access to system components to each individual user.
10.2	AUDIT	Implement automated audit trails for all system components to

		reconstruct the following events:
10.2.1	AUDIT	All individual user accesses to cardholder data
10.2.2	AUDIT	All actions taken by any individual with root or administrative privileges
10.2.3	AUDIT	Access to all audit trails
10.2.4	AUDIT	Invalid logical access attempts
10.2.5	AUDIT	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
10.2.6	AUDIT	Initialization, stopping, or pausing of the audit logs
10.2.7	AUDIT	Creation and deletion of system-level objects
10.3	AUDIT	Record at least the following audit trail entries for all system components for each event:
10.3.1	AUDIT	User identification
10.3.2	AUDIT	Type of event
10.3.3	AUDIT	Date and time
10.3.4	AUDIT	Success or failure indication
10.3.5	AUDIT	Origination of event
10.3.6	AUDIT	Identity or name of affected data, system component, or resource.
10.4	AUDIT	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.
10.4.1	AUDIT	Critical systems have the correct and consistent time.
10.4.2	AUDIT	Time data is protected.
10.4.3	AUDIT	Time settings are received from industry-accepted time sources.
10.5	AUDIT	Secure audit trails so they cannot be altered.
10.5.1	AUDIT	Limit viewing of audit trails to those with a job-related need.
10.5.2	AUDIT	Protect audit trail files from unauthorized modifications.
10.5.3	AUDIT	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
10.5.4	AUDIT	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.
10.5.5	AUDIT	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
10.6	AUDIT	Review logs and security events for all system components to identify anomalies or suspicious activity.
10.6.1	AUDIT	Review the following at least daily:

10.6.2	AUDIT	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.
10.6.3	AUDIT	Follow up exceptions and anomalies identified during the review process.
10.7	AUDIT	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).
10.8	AUDIT	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.
11.1	AUDIT	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.
11.1.1	AUDIT	Maintain an inventory of authorized wireless access points including a documented business justification.
11.1.2	AUDIT	Implement incident response procedures in the event unauthorized wireless access points are detected.
11.2	AUDIT	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
11.2.1	AUDIT	Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.
11.2.2	AUDIT	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.
11.2.3	AUDIT	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.
11.3	AUDIT	Implement a methodology for penetration testing that includes the following:
11.3.1	PENTEST	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).
11.3.2	PENTEST	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

11.3.3	PENTEST	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.
11.3.4	PENTEST	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.
11.3.4a	PENTEST	a Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.
11.3.4b	PENTEST	b Examine the results from the most recent penetration test to verify that:
11.4	DETECTION	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.
11.5	DETECTION	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.
11.5.1	DETECTION	Implement a process to respond to any alerts generated by the change-detection solution.
11.6	Security Police	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.
12.1	Security Police	Establish, publish, maintain, and disseminate a security policy.
12.1.1	Security Police	Review the security policy at least annually and update the policy when the environment changes.
12.10	Security Police	Implement an incident response plan. Be prepared to respond immediately to a system breach.
12.10.1	Security Police	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:
12.10.2	Test	Test the plan at least annually.
12.10.3	Test	Designate specific personnel to be available on a 24/7 basis to respond to alerts.
12.10.4	Test	Provide appropriate training to staff with security breach response responsibilities.
12.10.5	Test	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.

12.10.6	Test	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
12.2	Test	Implement a risk-assessment process that:
12.3	Test	Develop usage policies for critical technologies and define proper use of these technologies.
12.3.1	Test	Explicit approval by authorized parties
12.3.10	Test	For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.
12.3.2	Test	Authentication for use of the technology
12.3.3	Test	A list of all such devices and personnel with access
12.3.4	Test	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)
12.3.5	Test	Acceptable uses of the technology
12.3.6	Test	Acceptable network locations for the technologies
12.3.7	Test	List of company-approved products
12.3.8	Test	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
12.3.9	Test	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use
12.4	Responsabilidades	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
12.5	Responsabilidades	Assign to an individual or team the following information security management responsibilities:
12.5.1	Responsabilidades	Establish, document, and distribute security policies and procedures.
12.5.2	Responsabilidades	Monitor and analyze security alerts and information, and distribute to appropriate personnel.
12.5.3	Responsabilidades	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
12.5.4	Responsabilidades	Administer user accounts, including additions, deletions, and modifications.
12.5.5	Responsabilidades	Monitor and control all access to data.
12.6	Responsabilidades	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
12.6.1	Responsabilidades	Educate personnel upon hire and at least annually.
12.6.2	Responsabilidades	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.

12.7	Test	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)
12.8	Test	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:
12.8.1	Service Providers	Maintain a list of service providers.
12.8.2	Service Providers	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.
12.8.3	Service Providers	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
12.8.4	Service Providers	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
12.8.5	Service Providers	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
12.9	Service Providers	Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

Tabla 11-1 Controles PCI

12. Glosario

ISO: International Standards Organization (Organización Internacional de Estándares)
IEC: International Electrotechnical Comission (Comisión Electrotécnica Internacional)
SGSI: Sistema Gestor de la Seguridad de la Información, es el sistema que se construye al implantar la norma ISO27001.
PCI: Payment Card Industrie, consorcio de las principales emisoras de tarjetas a nivel mundial.
PCI DSS: DSS es Data Security Standard la norma es el estándar de seguridad a cumplir con la industria de pago con tarjeta.
NIST: National Institute of Standards and Technology
IEEE: Institute of Electrical and Electronics Engineers

13. Referencias

ANEXO Controles ISO27002:2013 Listado de Controles ISO27002
ISO/IEC 27001:2013 – Sistemas de Gestión de la Seguridad de la Información
ISO/IEC 27002:2011 – Controles de seguridad para Gestión de la Seguridad de la Información
ISO/IEC 17799 – Code of Practice of Information Security Management
ISO/IEC 19011:2011 – Directrices para la auditoría de Sistemas de Gestión
PCI DSS 3.1 - Requirements and Security Assessment Procedures: PCI Library
ISO27001 Toolkit: http://advisera.com/27001academy/iso-27001-documentation-toolkit/
Web Divulgativa ISO27001 en Español: http://www.iso27000.es/
List of Mandatory Documentation ISO27001 Implementation: http://advisera.com/27001academy/free-downloads/
Web de la organización internacional de Estándares (ISO): http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
Punto de venta de normas ISO: http://www.iso.org/iso/store.htm
Precio ISO27001:2013: 118 CHF (Francos Suizos), equivalentes a 108,1 € (14/6/2016).
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534
Modelo de Madurez de la Capacidad: http://www.sei.cmu.edu/cmmi/
NIST 800-30: Norma NIST 800-30