



information
security



Políticas, Normativas, Lineamientos, Directrices, y Procedimientos

SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI)

Implementa los procesos que permiten que una Organización realice un producto o servicio de manera confiable y **en conformidad con unas especificaciones internacionales**.

Que es un SGSI?

Ha estudiado los riesgos a los que está sometida toda su información.

Ha documentado las políticas y procedimientos relacionados

Ha implantado controles tecnológicos, organizativos y legales para aquellos riesgos que superan dicho nivel.

Ha entrado en un proceso continuo de revisión y mejora de todo el sistema.

El SGSI da así la garantía a la empresa de que los riesgos que afectan a su información son conocidos y gestionados.

Un SGI implica que la organización

Un enfoque de gestión integral debe desarrollarse para lograr estos objetivos satisfactoriamente.

Esto es porque todo el mundo dentro de una organización puede tener un conjunto diferente de valores y experiencias personales que aportan al medio ambiente en materia de seguridad.

Es importante asegurarse de que todo el mundo este en materia de seguridad a un nivel que satisfaga las necesidades de la organización según lo determinado por las leyes, reglamentos, requisitos y objetivos de negocio que han sido determinados por las evaluaciones de riesgos del entorno de la organización.

Debe empezar en el nivel superior y ser útil y funcional en todos los niveles dentro de la organización única.



Top Down

La alta dirección debe definir el ámbito de la seguridad e identificar y decidir lo que debe ser protegido y en qué medida.

Debe asegurarse de que la empresa en su conjunto cumpla con sus obligaciones.

Debe comprender los reglamentos, y temas de responsabilidad y legalidad, que es responsable de cumplir con respecto a la seguridad.

Debe determinar lo que se espera de los empleados y cuáles serán las consecuencias de su incumplimiento.

Para el plan de seguridad de una empresa tenga éxito



Estas decisiones deben ser llevadas a cabo por los individuos que serán responsables, en última instancia si algo sale mal.



Es una práctica común contar con la experiencia de los agentes de seguridad para colaborar y garantizar que se están implementando políticas y controles suficientes para alcanzar las metas que se fijaron y se determinaron por la alta dirección.

Un programa de seguridad contiene todas las piezas necesarias para proporcionar una protección general para la corporación y establece una estrategia de seguridad a largo plazo.

El lenguaje, nivel de detalle, la formalidad de los documentos, y los mecanismos de apoyo **debe ser examinada por los desarrolladores de políticas.**

Policy

A **policy** typically described as a statement of intent to achieve particular outcome(s). The task of achieving the outcome(s) is actually done by other documents. Whereas a policy may contain the protocols contain the details.

La documentación de un programa de seguridad debe estar compuesto por

Las políticas de seguridad.
Procedimientos.
Normas.
Directrices.
Lineamientos base.

| | |
|---|--|
| Policy | Documento de alto nivel que describe las directivas de seguridad de la alta dirección. |
| Policy types(Tipos de políticas) | Organizacional, sobre temas específicos, específica del sistema. |
| Policy functionality types | Reguladora, asesoramiento, informativo. |
| Standards(Normativas) | Reglas obligatorias(normas, actos, regulaciones) que apoyan las políticas de seguridad. Ej. ISO 27001 |
| Guidelines(Directrices) | Sugerencias y mejores prácticas. Se refiere a las guías recomendadas de operaciones o acciones de usuarios, personal de TI, personal de operaciones, entre otros. Ej. Security Password Guidelines. |
| Procedures(Procedimientos) | Instrucciones paso a paso de la implementación, que permiten lograr un objetivo específico. |
| Baselines(Lineamientos Base) | Es el estado o punto de referencia que se establece para una comparación a futuros cambios. Ej. El FW debe denegar todo y permitir lo específico. |

Conceptos

- ❑ Las políticas de seguridad.
- ❑ Normas.
- ❑ Directrices.
- ❑ Procedimientos.
- ❑ Líneas de base.

Deben desarrollarse con una visión realista para ser más eficaces.

Mientras más detalladas sean las reglas, más fácil es saber cuándo una ha sido violada.

La política proporciona la base. Los procedimientos, normas, directrices y líneas de base proporcionan el marco de seguridad(Security Framework).

Los recursos humanos y departamentos legales

Deben participar en el desarrollo y aplicación de las normas y requisitos establecidos en estos documentos.



Hay un montón de cuestiones de responsabilidad legal que rodean la documentación de seguridad.

Security Policy

Una política de seguridad es una declaración general/global **producida por la alta dirección o comité** que dicta el rol que juega la seguridad dentro de la organización.

Puede ser una política de la organización, una política de tema específico, o una política específica del sistema.

Tiene por objeto establecer las medidas técnicas y de organización, necesarias para garantizar la seguridad de las tecnologías de la información



Políticas de Seguridad

La seguridad comienza a nivel de políticas, que son las directivas de gestión de alto nivel que ofrecen los objetivos fundacionales de un sistema general y los componentes que la integran desde una perspectiva de seguridad.

Es el punto de inicio de las especificaciones de un sistema y proporciona la base para la evaluación de dicho sistema después de que se construya.

Es un término abstracto que representa a los objetivos y metas, que un sistema debe cumplir para lograr que se considere seguro y aceptable.

Es una herramienta estratégica que dicta como los recursos e información sensible serán administrados y protegidos.

Expresa exactamente cuáles deberían ser los niveles de seguridad estableciendo los objetivos de los mecanismos que se llevarán a cabo.

Políticas de Seguridad

En una política de seguridad organizacional, la gerencia establece cómo un programa de seguridad se implementara.



Top Down

Establece las metas del programa.

Muestra el valor estratégico y táctico de la seguridad.

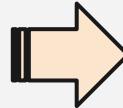
Asigna responsabilidades.

Describe cómo la ejecución debe llevarse a cabo.

Esta política debe abordar temas relativos a leyes, reglamentos y cuestiones de responsabilidad, y cómo han de ser satisfechos.

La política de seguridad de la organización proporciona el alcance y la dirección de todas las actividades de seguridad futuras dentro de la organización

También **describe la cantidad de riesgo que la alta gerencia está dispuesto a aceptar.**



COSO define el apetito de riesgo como el riesgo que se está dispuesto a aceptar en la búsqueda de la misión/visión de la entidad.

Políticas de Seguridad Organizacional

Los objetivos de negocio deben impulsar la creación, implementación y ejecución de la política.

Debe ser un documento de fácil comprensión y evitar que sea mayor a dos páginas, para que sirva como punto de referencia para todos los empleados y directivos.

Debe ser desarrollado y utilizado para integrar la seguridad en todas las funciones y procesos de negocio.

Debe de estar **soportada por todas las regulaciones** y legislaciones aplicables a la empresa.

Debe de ser **revisada y modificada** a medida que la empresa cambia o evoluciona.

Cada iteración de la política debe estar **calendarizada y bajo control de versiones**.

Las unidades y los individuos que se rigen por la política **deben tener fácil acceso a ella**.

Las políticas se publican habitualmente
en los portales en una intranet.

Características de las políticas de seguridad.

Debe ser revisado de manera regular y **adaptado para corregir incidentes** que se han producido desde el último examen y revisión de las políticas.

Deben ser creadas con la intención de que una vez implementadas duren varios años en vigor.

El nivel de profesionalismo en la presentación de las políticas refuerza su importancia, así como la necesidad de adherirse a ellos.

Se deben utilizar declaraciones claras que sean fáciles de entender y adoptar.

La política proporciona dirección y estructura para el personal mediante la indicación de lo que pueden y no pueden hacer.

Las políticas no deben ser técnicas. Deben describir los objetivos y misiones, pero no vincular a la organización a formas específicas de cumplimiento de ellos.

Características de las políticas de seguridad.

Política sobre temas específicos

También llamado **política funcional**, aborda temas de seguridad específica que la gerencia siente que necesita explicación más detallada y atención, para asegurarse que todos los involucrados comprendan cómo se van a cumplir esos problemas específicos de seguridad.

Ej. “Todos los datos confidenciales deben estar debidamente protegidos.”

issue-specific policy

Política específica del sistema.

Una política específica del sistema presenta las decisiones de la administración que son específicas de los actuales ordenadores, redes y aplicaciones.

Una organización puede tener una política específica del sistema que **expondrá cómo debe ser protegida una base de datos** que contiene información sensible, que puede tener acceso, y cómo la auditoría debería tener lugar.

política específica del sistema que expondrá cómo las computadoras portátiles deben ser bloqueados y gestionados.

Este tipo de política está dirigida a uno o un grupo de sistemas similares y describe la forma en que deben ser protegidos.

System Specific Policy

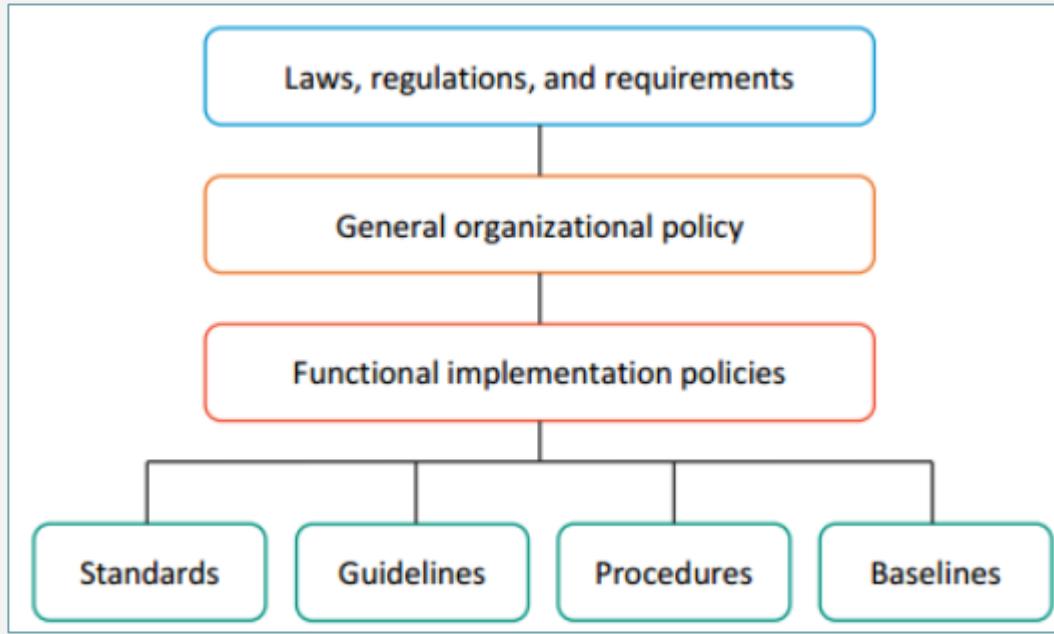
- Política Organizacional.
- Política de uso aceptable.
- Política de manejo de riesgo.
- Política de manejo de vulnerabilidades.
- Política de protección de datos.
- Política de control de acceso.
- Política de continuidad del negocio.
- Política de log y auditorías.
- Política de seguridad personal.
- Política de seguridad física.
- Política de seguridad de desarrollo de aplicaciones.
- Política de control de cambios.
- Políticas de correo electrónico.
- Política de respuesta a incidentes.

Dotar de información necesaria a los usuarios, empleados y gerentes de las normas y mecanismos que deben cumplir y utilizar para proteger los activos de la organización.

Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad de los sistemas de información.



Objetivo de la Política de Seguridad



Un objetivo estratégico puede ser visto como el punto final definitivo, mientras que los objetivos tácticos son los pasos necesarios para lograrlo.

Types of Policies

Diferentes políticas de seguridad trabajan en conjunto para cumplir con los objetivos de un programa de seguridad integral



Política Regulatoria (regulatory policy) asegura que la organización está siguiendo los reglamentos o normas específicas de la industria. Ej. (HIPAA, GLBA, SOX, PCI-DSS)



Política Consultiva (advisory policy) este tipo de política **recomienda encarecidamente** a los empleados en cuanto a qué tipos de comportamientos y actividades deben y no deben tener lugar dentro de la organización. Ej. para describir cómo manejar la información médica o financiera.



Política Informativa (informative policy) Este tipo de política **informa** a los empleados de ciertos temas. No es una política exigible, sino más bien uno que enseña a los individuos acerca de temas específicos de interés para la empresa.



Los documentos de política a menudo vienen con el endoso o la firma de los poderes ejecutivos dentro de una organización.

Elementos de una Política

- Propósito
- Alcance
- Responsabilidades
- Conformidad

Responsabilidad de gestión de la política.

- La protección de los activos de los recursos dentro de su control.
- Implementación de seguridad de acuerdo con la política de la empresa.
- Iniciar acciones correctivas para violaciones de seguridad.

Todo empleado es responsable del cumplimientos de **normativas, directrices y procedimientos de control**, así como también de notificar a su nivel jerárquico superior cuando no pueda cumplir con las políticas de seguridad, indicando el motivo por el cual no le es posible apegarse a la normativa de seguridad.

Policies Samples

Política de instalación de Software.

Uso aceptable de los activos.

Uso contra software malicioso.

Control de accesos.

Uso de correo electrónico/Navegación.

Puestos de trabajos despejados.

Uso de contraseña de usuario.

Uso de equipos portátiles.

POLÍTICA DE USO DE CONTRASEÑAS

Todas las contraseñas del sistema (administradores, cuentas de administración de aplicaciones, etc.) deben ser cambiadas al menos una vez cada 3 meses.

Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica.

Las contraseñas no deben ser comunicadas las contraseñas en conversaciones telefónicas sin antes proceder a la identificación del interlocutor.

Se evitarán nombres comunes o cualquier otra combinación que pueda identificar al usuario. Se evitarán nombres comunes, o cualquier otra combinación que pueda identificar al usuario (fecha nacimiento, matrículas de vehículos, etc.).

No se accederá al sistema utilizando el identificador y la contraseña de otro usuario

Ejemplos de Políticas

POLÍTICA CREACION DE CORREO ELECTRÓNICO

TI se encargara de asignar las cuentas a los usuarios para el uso de correo electronico en los servidores que administra.

Para fines de solicitud de cuenta de correo, el área de RRHH deberá llenar una solicitud en formato establecido para tal fin y entregarlo a la gerencia de TI.

La cuenta será activada en el momento que el usuario ingrese por primera vez a su correo, y será obligatorio el cambio de contraseña asignado.

La longitud mínima de la contraseña será igual o superior a 8 caracteres.

La cuenta de correo será utilizada para uso exclusivo de la corporacion.

POLÍTICA DE USO DE CORREO ELECTRÓNICO

Todo uso del correo electrónico debe ser coherente con las políticas y procedimientos de conducta ética, la seguridad, el cumplimiento de las leyes aplicables y las prácticas empresariales adecuadas.

La cuenta de correo electrónico debe ser utilizada principalmente para fines relacionados con el negocio. Se permite la comunicación personal en forma limitada, pero los usos no relacionados la labor que realiza están prohibidos.

Todos los datos contenidos en un mensaje de correo electrónico o un archivo adjunto debe ser asegurado de acuerdo a la Norma de Protección de Datos.

El sistema de correo electrónico no será utilizado para la creación o la distribución de mensajes perturbadores u ofensivos, incluyendo comentarios ofensivos sobre raza, género, color de pelo, discapacidad, edad, orientación sexual, la pornografía, las creencias religiosas y las prácticas, creencias políticas u origen nacional. Los empleados que reciban correos con este tipo de contenido de cualquier otro empleado debe reportarlo a su supervisor inmediato.

Ejemplos de Políticas

POLÍTICA DE INSTALACIÓN DE SOFTWARE

Los empleados no pueden instalar software en los dispositivos informáticos de <Nombre de la empresa> operados dentro de la red de <Nombre de la empresa>.

Las peticiones de Software primero deben ser aprobados por el gerente del solicitante y solicitarlas al departamento de Tecnología de la Información o Help Desk o via correo electrónico.

El software debe ser seleccionado de una lista de software aprobado, mantenido por el departamento de tecnología de la información, a menos que ninguna selección en la lista cumple con las necesidades del solicitante.

El Departamento de Tecnología de la Información obtendrá y realizar un seguimiento de las licencias, probará los softwares nuevos, de conflicto y compatibilidad, y llevará a cabo la instalación.

Ejemplos de Políticas

Elaborar políticas de seguridad para

- Servidores.
- Redes.
- Grupos de trabajo(Workstations).
- Acceso al Data Center.

Rik Ferguson - Advanced Persistent Threats

<https://www.youtube.com/watch?v=fpeMR1214t0>

Standards

- Las normativas se refieren a actividades obligatorias, acciones o reglas.**
- Es un documento interno que establece reglas que hay que seguir.**

Normativas(Standards)

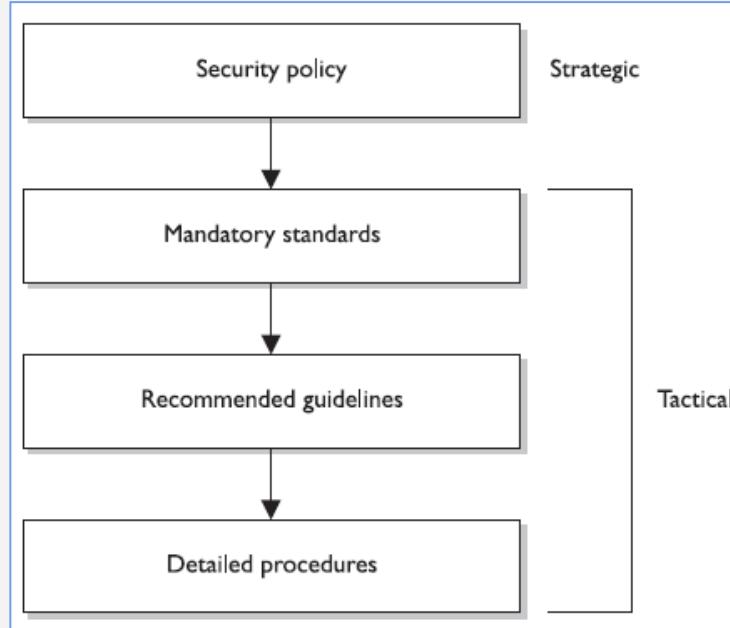
Las normas pueden dar a una política su apoyo y refuerzo en la dirección.

Estándares de seguridad de la organización(Organizational security standards). Pueden especificar cómo los productos de hardware y software se van a utilizar.

Proporcionan un medio para asegurar que determinadas tecnologías, aplicaciones, parámetros y procedimientos se apliquen de manera (estandarizada) uniforme en toda la organización.

Puede requerir que todos los empleados usen sus tarjetas de identificación de empresa en todo momento.

Normas, directrices y procedimientos son las herramientas tácticas utilizadas para lograr y apoyar a las directivas de la política de seguridad, que se considera el objetivo estratégico.



La política establece los planes estratégicos, y los elementos inferiores proporcionar el apoyo táctico.

Se refiere a un punto en el tiempo que se utiliza como una comparación para el futuro cambios.

Una vez que los riesgos han sido mitigados y la seguridad puesta en marcha, una línea de base se revisa y se aprueba formalmente, después todos los procedimientos creados se miden a partir de esta. **Una línea de base se traduce en un punto de referencia constante.**

También se utilizan para definir el nivel mínimo de protección requerido.

Pueden definirse según el tipo de sistema, que indica los ajustes necesarios y el nivel de protección que se ofrece.

El personal de seguridad debe evaluar los sistemas, a medida que se dan los cambios y asegurarse de que siempre se está cumpliendo el nivel básico de seguridad.

Lineamientos Base(Baselines)

Directrices pueden lidiar con las metodologías de la tecnología, el personal o la seguridad física.

Mientras las normativas son reglas obligatorias específicas, **las directrices son enfoques generales que proporcionan la flexibilidad necesarias para circunstancias imprevistas.**

Guidelines(Directrices)

Son tareas detalladas paso a paso que se deben realizar para alcanzar un determinado objetivo.

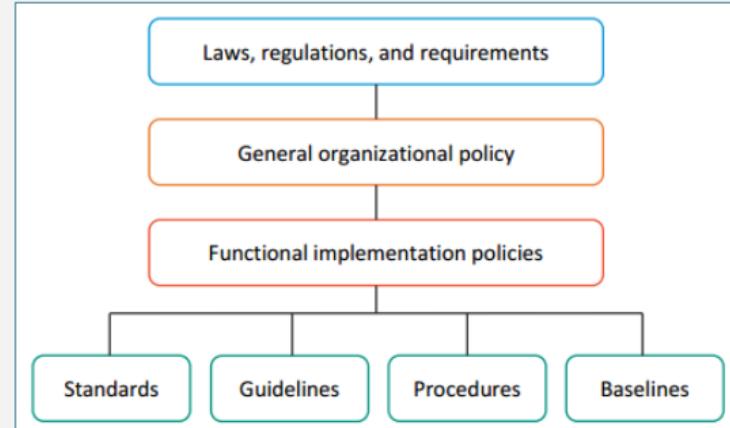
Procedures(Procedimientos)

Pueden aplicarse a todos aquellos que quieran realizar tareas específicas.

- Usuarios.
- Personal de TI.
- Personal de operaciones.
- Personal de Seguridad.

Los procedimientos pueden ser:

- Instalar sistemas operativos.
- Configurar mecanismos de seguridad.
- Listas de control de acceso.
- Configurar nuevas cuentas de usuarios.
- Asignar privilegios.
- Actividades de auditorias.
- Reporte de incidentes.



Los procedimientos se consideran el nivel más bajo en la cadena de documentación, ya que son más cercanos a los equipos y usuarios (en comparación con las políticas) y proporcionan pasos detallados para los problemas de configuración e instalación.

Los procedimientos explican cómo la política, las normas y directrices deben ser implementadas en un entorno operativo.

Los procedimientos **deben ser lo suficientemente detallados** para ser a la vez comprensible y útil a un grupo diverso de personas.

ERROR:

Las políticas de seguridad, normas, procedimientos, parámetros de referencia y directrices **a menudo se escriben porque un auditor instruyó una empresa** para documentar estos artículos, pero luego se colocan en un servidor de archivos y no se comparten, se explica o se utilizan.

Para ser útiles, deben ser puestos en acción.

Nadie va a seguir las reglas, si no saben las reglas existen.

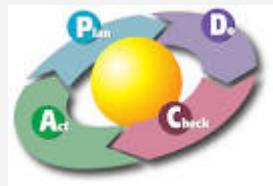
Las políticas y sus documentos de apoyo necesitan visibilidad.

No sólo deben desarrollarse, sino que también debe ser adoptado y aplicado.



- Entrenamientos.
- Manuales.
- Presentaciones.
- Boletines.
- Banners legales.

Pueden lograr esta visibilidad



Debe quedar claro que las directivas vienen de la alta dirección y que el personal de gestión completo apoya estas políticas.

Los empleados deben entender lo que se espera de ellos en sus acciones, comportamientos, la responsabilidad y el rendimiento.



Resumen

La implementación de políticas de seguridad y los elementos que la apoyan les **muestra el debido cuidado(due care)** por parte de la empresa y su personal de gestión.



Informar a los empleados de lo que se espera de ellos y las consecuencias de la falta de cumplimiento puede reducirse a una cuestión de la responsabilidad.

Empresas que no proporcionan entrenamientos concientizando a sus empleados no están practicando el debido cuidado(due care) y puede ser considerado negligente y responsable ante la ley.

Resumen

Si una empresa despidió a un empleado porque estaba descargando material pornográfico a la computadora de la empresa, el empleado puede llevar a la compañía a los tribunales y ganar si el empleado puede demostrar que no fue debidamente informado de lo que se consideraba el uso aceptable e inaceptable de la propiedad de la compañía y cuáles fueron las consecuencias.



ISO/IEC 27000

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission), que **proporcionan un marco de gestión de la seguridad de la información** utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, **la organización británica es responsable de la publicación de importantes normas** como:



1979 Publicación BS 5750 - ahora **ISO 9001**



1992 Publicación BS 7750 - ahora **ISO 14001**



1996 Publicación BS 8800 - ahora **OHSAS 18001**

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa británica o no, un **conjunto de buenas prácticas para la gestión de la seguridad de su información(SGSI)**.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación.

La segunda parte (BS 7799-2), publicada por primera vez en 1998, establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999

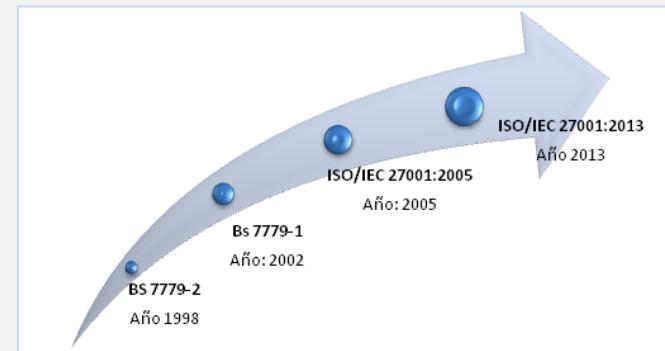
La primera parte se adoptó por ISO, sin cambios sustanciales, como **ISO 17799** en el año 2000.

En 2002, se revisó **BS 7799-2** para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2.

BS7799-2 se publicó por ISO como estándar **ISO 27001**, al tiempo que se revisó y actualizó ISO17799.

ISO17799 se renombra como **ISO 27002:2005** el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.



| | |
|---|---|
| <p>ISO/IEC 27000</p> <p>Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación.</p> | <p>Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI.</p> |
| <p>ISO/IEC 27001</p> <p>Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.</p> | <p>Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Tiene su origen en la BS 7799-2: 2002</p> |

| | |
|---|---|
| ISO/IEC 27002 Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. | Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. |
| | Actualmente, la <u>última edición de 2013 este estándar</u> ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles. |

Aplica una arquitectura de gestión de la seguridad que **identifica y evalúa los riesgos que afectan al negocio**, con el objetivo de implantar contramedidas, procesos y procedimientos para su apropiado control y mejora continua

Ayuda a la entidad a **gestionar, de una forma eficaz, la seguridad de la información**, evitando las inversiones innecesarias, ineficientes o mal dirigidas.

Que se producen por

contrarrestar amenazas sin una evaluación previa.

por desestimar riesgos.

por la falta de contramedidas

por implantar controles desproporcionados y de un coste más elevado del necesario.

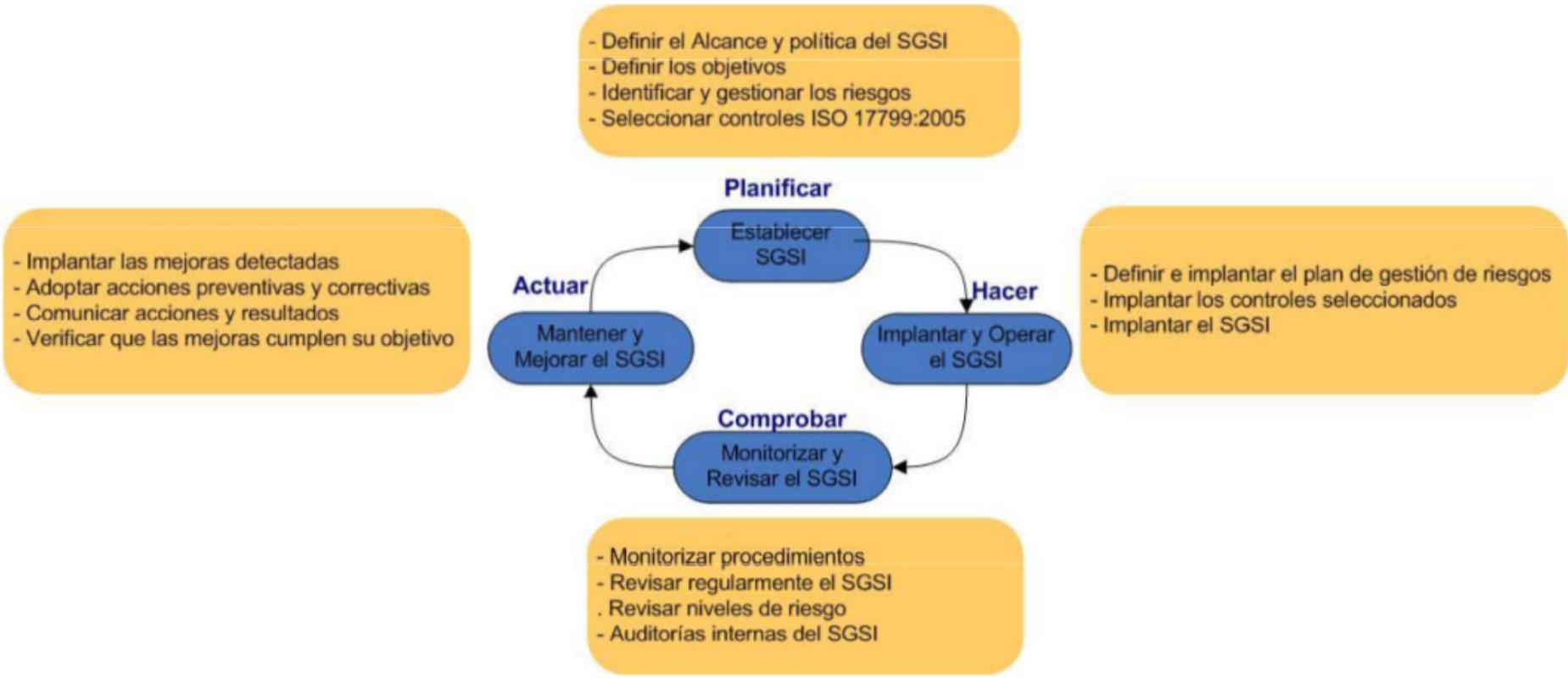
Por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno.

por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información

por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio

Que aporta ISO 27001 a la seguridad de la información?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, 27001 se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.



La norma ISO/IEC 27001:2005

“Especificaciones para los Sistemas de Gestión de la Seguridad de la Información”, requeridas para obtener la certificación del SGSI implantado.

El estándar ISO/IEC 27002

Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”.

Cubren todos los aspectos fundamentales de la seguridad en el tratamiento de la información.

Para la implantación de un SGSI se consideran

Con un SGSI, la organización conoce los riesgos a los que está sometida su información

- Los asume.**
- Minimiza.**
- Transfiere.**
- Controla.**

Mediante una sistemática definida, documentada, que se revisa y actualiza constantemente.



Fuente: www.ISO27000.es

Un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001

Está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles.



Documentos de Nivel 1



Alcance del SGSI

Política y objetivos de seguridad

Metodología de evaluación de riesgos

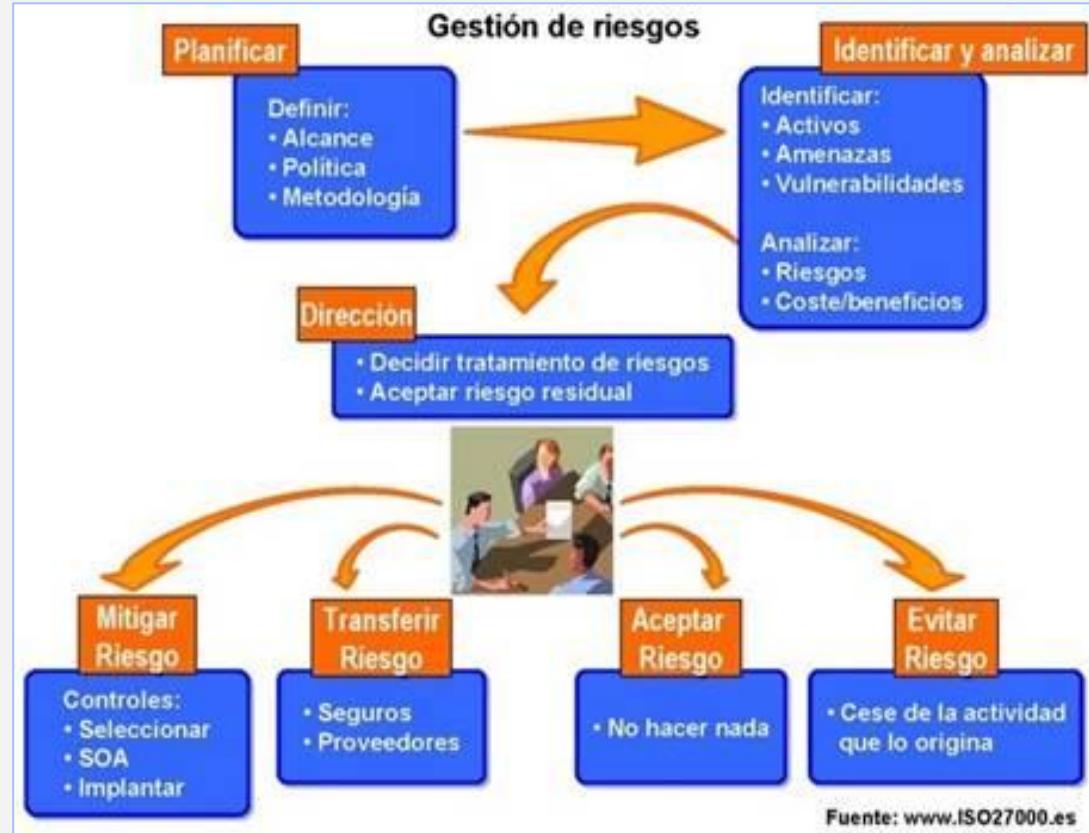
Informe de evaluación de riesgos

Plan de tratamiento del riesgo

Declaración de aplicabilidad

Procedimientos relativos al nivel 1

Proceso de identificar los riesgos de la seguridad, determinando su magnitud e identificando las áreas que requieren medidas de salvaguarda.



ANÁLISIS DE RIESGOS

Definir Objetivos y Metas

Integrar la Gestión de la Seguridad de la Información con el resto de sistemas de gestión existentes.

Análisis de riesgos, identificando amenazas, vulnerabilidades e impactos, en su SGSI.

Cumplimiento de la legislación vigente sobre protección de datos de carácter personal, comercio electrónico, etc.

Mejora continua de la gestión de la seguridad.

Incremento de confianza de clientes y partners.

Mejorar la imagen ante sus clientes, proveedores y empleados, convirtiéndose en un factor diferenciador frente a la competencia.

Garantía de continuidad del negocio.

Beneficios de Implementación de un SGSI

| | |
|-------------------------------|---|
| Aspecto Humano. | Mejora la sensibilización y responsabilidades del personal ante la seguridad en la organización. |
| Aspecto Financiero | Reducción de los costos vinculados a los incidentes de seguridad y seguridad. |
| Aspecto Organizacional | El registro permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización en todos sus niveles. |
| Aspecto Funcional | Gestión de los riesgos. |
| Aspecto Legal | Conformidad con leyes y normativas aplicables. |
| Aspecto Comercial | Credibilidad y confianza de los socios, los accionistas y los clientes y clientes. |

Beneficios de Implementación de un SGSI



Establecimiento de una metodología de gestión de la seguridad clara y estructurada.

Reducción del riesgo de pérdida, robo o corrupción de información.

Los clientes tienen acceso a la información a través medidas de seguridad

http://www.iso27000.es/download/doc_iso27000_all.pdf

Beneficios



Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS - Data Security Standard - consiste en una serie de estándares de seguridad que incluyen:

- Requerimientos para administrar la seguridad.
- Las políticas, procedimientos.
- La arquitectura de redes.
- El diseño de software.
- Otras medidas críticas de protección de la información.



Debido al incremento en el riesgo de posibles ataques fraudulentos y el uso ilícito de identidad, las marcas de aceptación han desarrollado un sistema común de normas conocido como.

PCI DSS (Payment Card Industry Data Security Standards) para asegurar el manejo apropiado de información de transacciones de tarjetas de pago.

La industria de las tarjetas de crédito tomó medidas proactivas para frenar el problema y estabilizar la confianza del cliente en las tarjetas de crédito como forma segura de realizar transacciones.



Cada proveedor de la tarjeta de crédito desarrolló su propio programa que sus clientes tenían que cumplir.

Visa's program Cardholder Information Security (**CISP**)

MasterCard's program Site Data Protection (**SDP**)

Discover Information Security and Compliance program (**DISC**)

Se rigen por un organismo internacional independiente denominado **Consejo de Estándares de Seguridad de la PCI** (PCI SSC).



- Visa International
- Mastercard Worldwide
- American Express
- JBC
- Discover Financial Services

Diciembre 15, 2014

Quien respalda la norma de seguridad PCI?



PCI SSC es una organización dedicada a estandarizar y proteger la seguridad de las tarjetas de pago y reducir los fraudes.



Who Are The Players?



CARD BRANDS

Created the SSC and responsible for approving the DSS controls framework



PCI SSC

Developed the DSS, PA-DSS, PIN standards, and conduct training and certification for QSAAs and ASVs



ACQUIRERS

Banks and payment processors that own the responsibility for enforcing the DSS



MERCHANTS

Responsible for implementing DSS controls, as well as demonstrating and maintaining compliance

¿El cumplimiento de la norma de Seguridad PCI DSS es obligatoria para su negocio?



Existen niveles variables de cumplimiento y sanciones y dependen del tamaño del cliente y el volumen de transacciones.

Su adopción es obligatoria desde junio de 2007 y las marcas pueden imponer sanciones a las entidades que no realicen las auditorías prescritas.

Parte del arreglo es que los que no estén en cumplimiento no pueden participar en el ambiente de tarjetas de pago eventualmente.

¿La norma de Seguridad PCI – DSS es para su negocio?

Las PCI DSS se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago, entre las que se incluyen **comerciantes, procesadores, instituciones financieras y proveedores de servicios**, así como también todas las demás entidades que almacenan, procesan o transmiten datos del titular de la tarjeta o datos de autenticación confidenciales.

A quien se aplica?

PCI DSS es una iniciativa de la industria del sector privado. No es una ley.



El incumplimiento o violaciones de PCI DSS pueden dar lugar a sanciones financieras o la posible revocación de la condición de comerciante dentro de la industria de tarjetas de crédito, **pero no ir a la cárcel**.



Sin embargo, Minnesota se convirtió en el primer estado en exigir el cumplimiento de PCI como una ley, y otros estados, así como el gobierno federal de los Estados Unidos, están aplicando medidas similares.

La adopción de la norma PCI le permite a los comercios contar con los siguientes beneficios:

Promover la integridad del comercio y aumentar la confianza de los consumidores en el negocio.

Incrementar las ventas como consecuencia del aumento en la confianza de los consumidores.

Proteger al comercio de posibles pérdidas de ingresos, investigaciones no deseadas y costos legales.

Reducir el riesgo de atención no deseada de la prensa como resultado de un compromiso o fuga de información de clientes.

Proyectar mayor conciencia de los controles y medidas preventivas de seguridad disponibles para el comercio.

Reducir las disputas de Tarjetahabientes y costos asociados a transacciones fraudulentas resultantes de un compromiso de información.

Prevenir el robo masivo de información de clientes.

Facilitar la adopción de estándares de seguridad válidos a nivel global.

Generar una herramienta que establece las posibles vulnerabilidades que tiene el sistema de información.

El cumplimiento de PCI DSS puede traer grandes beneficios a las empresas de todos los tamaños. Aquí hay algunas razones por qué:

- Ser PCI DSS- compatible sugiere que sus sistemas sean seguros, y los clientes pueden confiar al negocio la información sensible de sus tarjetas de pago.
- Puede mejorar su reputación con adquirentes y las marcas de pago.
- El seguimiento continuo es un proceso continuo que ayuda a prevenir las violaciones de seguridad y el robo de datos de tarjetas de pago.

Las Normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial.

Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas.

Las PCI DSS se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago entre las que se incluyen **comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios**, como también todas las demás **entidades que almacenan, procesan o transmiten datos del titular de la tarjeta** o datos de autenticación confidenciales.

Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger los datos de titulares de tarjetas y se pueden mejorar por medio de controles y prácticas adicionales a fin de mitigar otros riesgos y de leyes y regulaciones locales, regionales y sectoriales.

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



El PCI DSS se compone de 12 requisitos principales divididos en seis categorías principales.

12 requisitos de las DSS de la PCI.

Las seis categorías de PCI DSS son construir y mantener una

- Red Segura.
- Proteger los datos del tarjetahabiente.
- Mantener un programa de gestión de vulnerabilidades.
- Implementar fuertes medidas de control de accesos.
- Regularmente monitorear y probar redes.
- Mantener una Política de Seguridad de la Información.

Desarrolle y mantenga redes y sistemas seguros.

- Instalar y mantener una configuración de firewall, para proteger los datos del titular de la tarjeta.
- No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.

Proteger los datos del titular de la tarjeta.

- Proteja los datos del titular de la tarjeta que fueron almacenados.
- Cifrar la transmisión de los datos del titular de la tarjeta, en las redes públicas abiertas.

Mantener un programa de administracion de vulnerabilidad.

- Utilizar y actualizar con regularidad los softwares antivirus.
- Desarrolle y mantenga sistemas de aplicaciones seguras.

Implementar medidas sólidas de control de acceso.

- Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber (need to know) que tenga la empresa.
- identifique y autentique el acceso a los componentes del sistema.
- Restringir el acceso físico a los datos del titular de la tarjeta.

Supervisar y evaluar las redes con regularidad.

- Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.
- Pruebe con regularidad los sistemas y procesos de seguridad.

Mantener una política de seguridad de la información.

- Mantenga una política que aborde la seguridad de la información para todo el personal.

Se desarrolló para utilizarse durante las evaluaciones de cumplimiento con las PCI DSS como parte del proceso de validación de una entidad.

Los datos del titular de la tarjeta y los datos de autenticación confidenciales se definen de la siguiente manera

| Datos de cuentas | |
|---|---|
| Los datos de titulares de tarjetas incluyen: | Los datos confidenciales de autenticación incluyen: |
| <ul style="list-style-type: none">▪ Número de cuenta principal (PAN)▪ Nombre del titular de la tarjeta▪ Fecha de vencimiento▪ Código de servicio | <ul style="list-style-type: none">▪ Contenido completo de la pista (datos de la banda magnética o datos equivalentes que están en un chip)▪ CAV2/CVC2/CVV2/CID▪ PIN/Bloqueos de PIN |



Las PCI DSS no sustituyen las leyes locales ni regionales, las regulaciones gubernamentales ni otros requisitos legales.

Biblioteca de documentos, que incluye lo siguiente

El sitio web de **PCI Security Standards Council (PCI SSC)** (www.pcisecuritystandards.org) contiene algunos recursos adicionales para ayudar a las organizaciones con las evaluaciones y validaciones de las PCI DSS, entre otros:

PCI DSS: Resumen de cambios de la versión 2.0 a 3.0 de las PCI DSS

Guía de referencia rápida de las PCI DSS

Glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS

Suplementos informativos y directrices

Enfoque priorizado para las PCI DSS

Recursos de las PCI DSS

ROC (Informe sobre cumplimiento), plantilla para crear informes e instrucciones para crear informes

SAQ (Cuestionarios de autoevaluación) e instrucciones y directrices del SAQ

AOC (Atestación de cumplimiento)

PCI para los sitios web de pequeños comerciantes

Cursos de capacitación y webinars informativos sobre PCI

Recursos de las PCI DSS

Welcome to the PCI Security Standards Council



MERCHANTS

Find out why and how to become compliant with PCI Security Standards

[Learn More](#)



FINANCIAL INSTITUTIONS

Resources to assist with compliance efforts for your organization

[Learn More](#)



HARDWARE / SOFTWARE

Resources designed for developers and device manufacturers

[Learn More](#)



SERVICES AND PROFESSIONALS

Quick access to resources developed for industry professionals

[Learn More](#)

<https://www.pcisecuritystandards.org/>

PA-DSS

Para el propósito de cumplir con PA-DSS, una aplicación de pago es elegible para revisión y listado por la PCI-DSS si es definida como una aplicación que.

No todas las aplicaciones de software que juegan un papel en las transacciones son elegibles para la revisión y el listado por el PCI SSC en el marco del programa PA-DSS.

- Almacene
- Procese
- Transmite datos del tarjetahabiente.
- Si se vende, distribuye, o con licencia a terceros

Cuales aplicaciones son elegibles para PA-DSS Validation?

Si la respuesta es sí a cualquiera de las siguientes preguntas, la solicitud no reúne los requisitos para la validación bajo PA-DSS.

¿Es esta una versión beta de la aplicación?

¿La aplicación maneja datos de los tarjetahabientes, pero la aplicación en sí no facilita la autorización?

La aplicación facilita la autorización, pero no tiene acceso a los datos del tarjetahabiente o datos de autenticación sensitiva?

La aplicación requiere personalización del código fuente o configuración significativa por el cliente, siendo así que esos cambios impacten uno o más requerimientos PA-DSS?

Es la aplicación un sistema operativo, base de datos o plataforma, que almacena, procesa o transmite datos de la tarjeta de crédito?

Es la aplicación de desarrollo propio(in-house) y sólo es utilizada por la empresa que desarrolló el aplicación?

Se desarrolló la aplicación y se vende a un solo cliente para el uso exclusivo de ese cliente?

La aplicación funciona como una librería compartida(DLL) que debe ser implementada con otro componente de software para funcionar?

¿Depende la aplicación de otro software con el fin de cumplir con uno o más requisitos de PA-DSS, pero no se incluye (con licencia y / o distribuido como un solo paquete) con el software de soporte?

Es la aplicación de un único módulo que no se presentó como parte de una suite, y que no facilita la autorización por sí sola?

La aplicación es ofrecida como software como servicio (SAAS) que no se vende, distribuye o licencia a terceros?

La aplicación opera en cualquier dispositivo electrónico de mano(handheld) que no es dedicado exclusivamente para el pago de alguna transacción?

Tenga en cuenta que la lista anterior está destinado sólo para fines ilustrativos, no es exhaustiva, y puede ser modificada en cualquier momento por el PCI SSC.

Key Definitions

- **PCI DSS:** Payment Card Industry Data Security Standard
- **PCI SSC:** Payment Card Industry Security Standards Council
- **CDE:** Cardholder Data Environment
- **QSA:** Qualified Security Assessor
- **SAQ:** Self-Assessment Questionnaire
- **ASV:** Approved Scan Vendor



Information Classification

La razón de ser de la asignación de valores a los diferentes tipos de datos, es que permita a una empresa **medir la cantidad de recursos que deberían dirigirse hacia la protección de cada tipo de datos**, ya que no todos los datos tiene el mismo valor a una empresa.

Después de identificar toda la información importante, debe ser clasificada correctamente.

La razón para clasificar los datos, es organizar de acuerdo a su sensibilidad a la pérdida, divulgación o indisponibilidad.

Una vez que los datos se segmentan de acuerdo a su nivel de sensibilidad, la empresa puede decidir que controles de seguridad son necesarias para proteger los diferentes tipos de datos.



Information Classification

The primary purpose of data classification

is to indicate the level of **confidentiality, integrity, and availability** protection that is required for each type of data set.

Data classification helps ensure data is protected in the most cost-effective manner.

Protecting and maintaining data costs money, but it is important to spend this money for the information that actually requires protection.



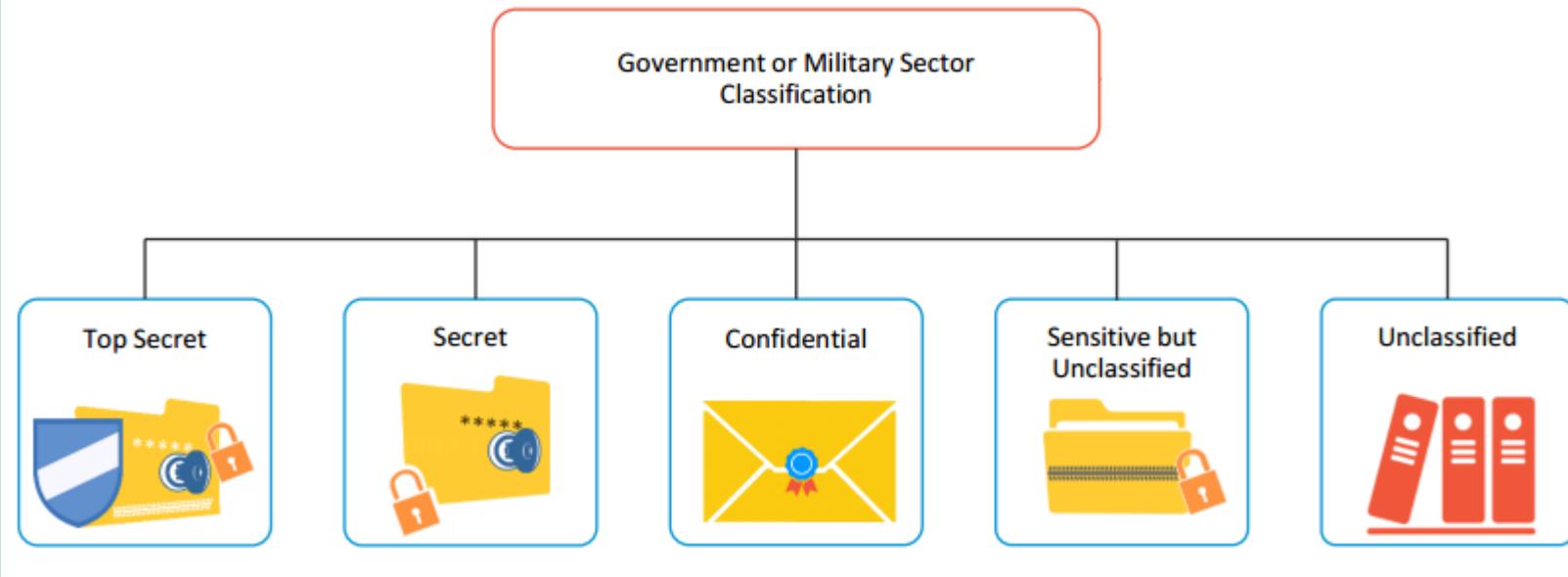
Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed.

CLASSIFIED

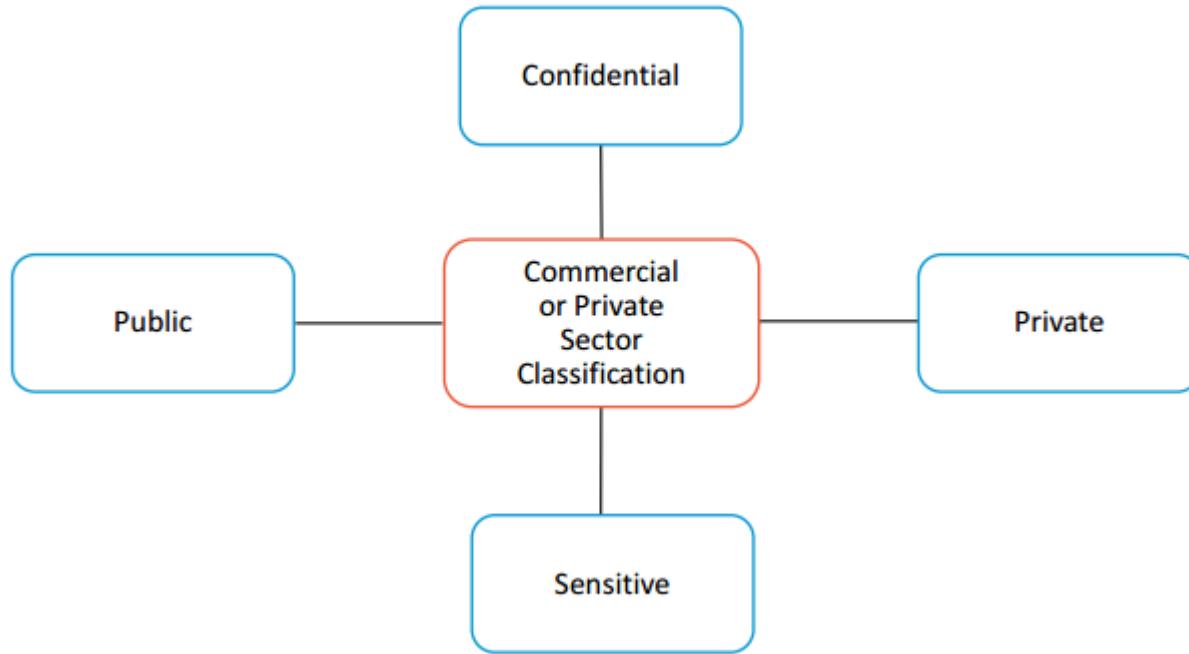
To properly erase this data from the media, degaussing or zeroization procedures may be required.



The information classification scheme followed by the Government or Military sector has five levels.



The information classification scheme followed by the Commercial or Private sector has four levels.



No hay reglas duras y rápidas en los niveles de clasificación que una organización debe utilizar.

| Classification | Definition | Examples | Organizations That Would Use This |
|----------------|--|--|-----------------------------------|
| Public | La divulgación no es bienvenida, pero no causaría un impacto adverso para la empresa o el personal. | Cuántas personas están trabajando en un proyecto específico. | Commercial business |
| Sensitive | Requiere precauciones especiales para garantizar la integridad y confidencialidad de los datos, por los que lo protege de modificación o eliminación no autorizada. | información financiera. | Commercial business |

Commercial Business and Military Data Classification

Classifications Levels

| Classification | Definition | Examples | Organizations That Would Use This |
|----------------|---|--|-----------------------------------|
| Private | <p>información personal para su uso dentro de una compañía.</p> <p>La divulgación no autorizada pudiera afectar negativamente el personal o la empresa</p> | <ul style="list-style-type: none"> - Historia de trabajo. - Información de RRHH. - Informacion Medica. | Commercial business |
| Confidential | <p>Solo para el uso dentro de la empresa.</p> <p>La divulgación no autorizada pudiera afectar seriamente a una compañía.</p> | <ul style="list-style-type: none"> - secretos comerciales. - Información Salud. - Código de programación. - La información que mantiene la empresa competitiva | Commercial business Military |

Classifications Levels

| Classification | Definition | Examples | Organizations That Would Use This |
|---|---|---|-----------------------------------|
| Unclassified | La información no es sensible o clasificada. | <ul style="list-style-type: none"> - Manual del computador y garantía - Información de reclutamiento. | Military |
| Sensitive but unclassified (SBU) | <p>Secreto Menor.</p> <p>Si se da a conocer, puede que no cause daños graves.</p> | <ul style="list-style-type: none"> - Datos medicos. - Respuestas a las calificaciones de las pruebas | Military |

Classifications Levels

| Classification | Definition | Examples | Organizations That Would Use This |
|-------------------|--|--|-----------------------------------|
| Secret | Si se da a conocer, podría causar graves daños a la seguridad nacional. | <ul style="list-style-type: none"> - Planes de implementación para las tropas. - Colocación de una bomba nuclear. | Military |
| Top secret | Si se da a conocer, podría causar un grave daño a la seguridad nacional. | <ul style="list-style-type: none"> - Planos de nuevas armas de guerra - Información del satélite espía - Datos de espionaje | Military |

Classifications Levels

Las clasificaciones no deben ser demasiado restrictiva y orientada al detalle, ya sea, porque pueden necesitar ser clasificado muchos tipos de datos.

El proceso de clasificación también debe delinear cómo la información es controlada y manejada a través de sus ciclos de vida

Cada clasificación debe ser único y separado de los demás y no tiene efectos superpuestos.



La siguiente lista muestra algunos criterios y parámetros que una organización puede utilizar para determinar la sensibilidad de los datos.

La utilidad de los datos.

El valor de los datos.

La edad de los datos.

El nivel de daños que pudieran ser causados si se dieron a conocer los datos.

El nivel de daños que pudieran ser causados si se modificaron los datos.

La responsabilidad legal, reglamentario o contractual para proteger los datos.

Efectos que los datos tienen sobre la seguridad.

¿Quién debe ser capaz de acceder a los datos?

¿Quién debe mantener los datos?

¿Quién debería ser capaz de reproducir los datos?

Los datos no son las únicas cosas que pueden necesitar para ser clasificados.



Aplicaciones y algunas veces sistemas enteros pueden necesitar ser clasificados.



Las aplicaciones que contienen y procesan información clasificada deben ser evaluados para el nivel de protección que proporcionan.

Las clasificaciones de aplicación deben basarse en la seguridad (nivel de confianza) que la empresa tiene en el software y el tipo de información que puede almacenar y procesar.

Una organización debe asegurarse de que todo el que realiza backup de seguridad de datos clasificados y el que tiene acceso a la copia de seguridad de datos tiene los niveles de autorización, necesarios.

Las reglas de clasificación deben aplicarse a los datos sin importar el formato es en: digital, papel, video, fax, audio, y así sucesivamente.

El hombre que descubrió secretos de la NASA y el Pentágono.

<https://www.youtube.com/watch?v=hjcHzm4f8ME>





ACERCA DE MI

- ✓ Ingeniero en Sistemas Informáticos Universidad Central del Este (UCE)
- ✓ Profesor Universidad Dominicana O&M
- ✓ Maestría en Gerencia y Productividad - Universidad APEC
- ✓ Postgrado de Auditoria de Sistemas - Universidad O&M
- ✓ Comptia Security+ Certified

twitter



@ksanchez_cld

skype

ksanchez_cld

