

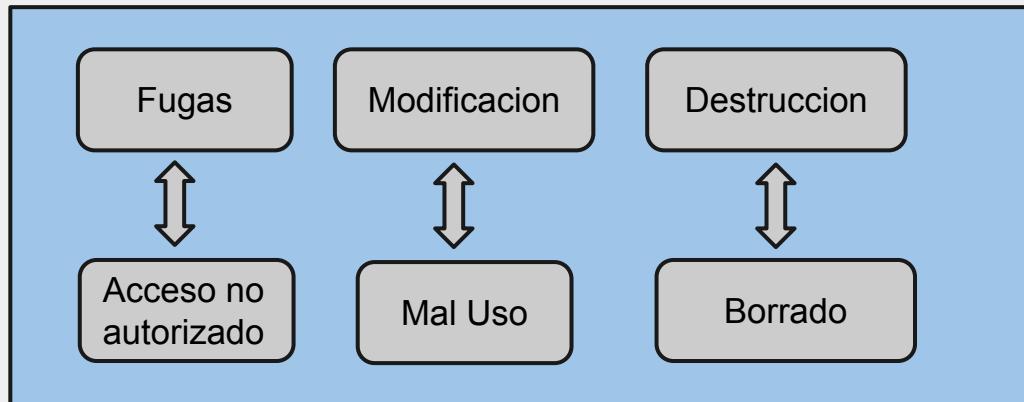




information
security

La Seguridad de la información es el proceso de proteger la información y los sistemas de información de:

D
I
G
I
T
A
L
E
S



N
O
D
I
G
I
T
A
L
E
S

Políticas, Normativas, Lineamientos, Directrices, y Procedimientos

SGSI

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

Es una herramienta de gestión que nos va a permitir conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en nuestra empresa.

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?

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.

Nos va a permitir preservar la **confidencialidad, integridad y disponibilidad** de la misma, en el interior de la empresa, ante nuestros clientes y ante las distintas partes interesadas en nuestro negocio.

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

Un SGSI implica que la organización

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
Aspecto Organizacional	seguridad.
Aspecto Funcional	El registro permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización en todos sus niveles.
Aspecto Legal	Gestión de los riesgos de manera adecuada.
Aspecto Comercial	Conformidad con leyes y normativas aplicables.
	Credibilidad y confianza de los socios, los accionistas y los clientes.

Beneficios de Implementación de un SGSI

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, 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

La implantación de un SGSI es una decisión estratégica que debe involucrar a toda la organización y que debe ser apoyada y dirigida desde la dirección.



La mesa de directores(Governance) asegura que las estrategias de seguridad estan alineadas a los objetivos del negocio y consistentes con las regulaciones.

"Gobernanza de la seguridad de la información es el conjunto de responsabilidades y prácticas ejercidas por el directorio y la gerencia ejecutiva con el objetivo de proporcionar dirección estratégica, asegurar que se alcanzan los objetivos, determinar que los riesgos se gestionan adecuadamente, y verificar que los recursos de la empresa se utilizan con responsabilidad."

— IT Governance Institute

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



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 que SGSI de una empresa tenga éxito

Para hacer más sencillo el proceso de implantación, es bueno contar con la ayuda de una **empresa especializada que nos asesore durante todo el proceso**, especialmente durante el primer año.



El tiempo de implantación del sistema de gestión de seguridad de la información varía en función del tamaño de la empresa, el estado inicial de la seguridad de la información y los recursos destinados a ello.



6 - 1

Un SGSI 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
- Mecanismos de apoyo

deben ser examinada por los desarrolladores de políticas.

Policy

A **policy** typically described as a set of rules or principles that are adopted by an organization to achieve particular outcomes(s). The term "policy" is often used to describe what actually remains to be done. Whereas a policy may contain the "what", protocols contain the "how".

La gestión de la seguridad de la información, debe asegurarse de hacer cumplir lo siguiente:

- Las políticas de seguridad - (Security Policy).
- Procedimientos - (Procedures).
- Normas - (Standards).
- Directrices - (Guidelines).
- Lineamientos base - (Baselines).
- Clasificación de la Información - (Information Classification).
- Manejo de Riesgo - (Risk Management).
- Educación de Seguridad - (Security Awareness)

Policy	Documento de alto nivel que describe las directivas de seguridad de la alta dirección.
Policy types(Tipos de políticas)	<ul style="list-style-type: none"> - Organizacional. - Sobre temas específicos. - Específica del sistema.
Policy functionality types	<ul style="list-style-type: none"> - 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.

- ❑ 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.

El Responsable del Área de Recursos Humanos incluirá las funciones relativas a La seguridad de la información

- En las descripciones de puestos de los empleados.
- Informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información.
- Gestionará los Compromisos de Confidencialidad con el personal.
- Coordinará las tareas de capacitación de usuarios respecto de la presente Política.



El Responsable del Área Legal

- Participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo.
- En el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política.
- En el tratamiento de incidentes de seguridad que requieran de su intervención.





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.

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 fundamentales 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

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.

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



Top Down

Establece las metas del programa.

Muestra el valor estratégico y táctico de la seguridad.

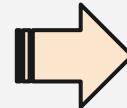
Asigna responsabilidades.

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.

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.

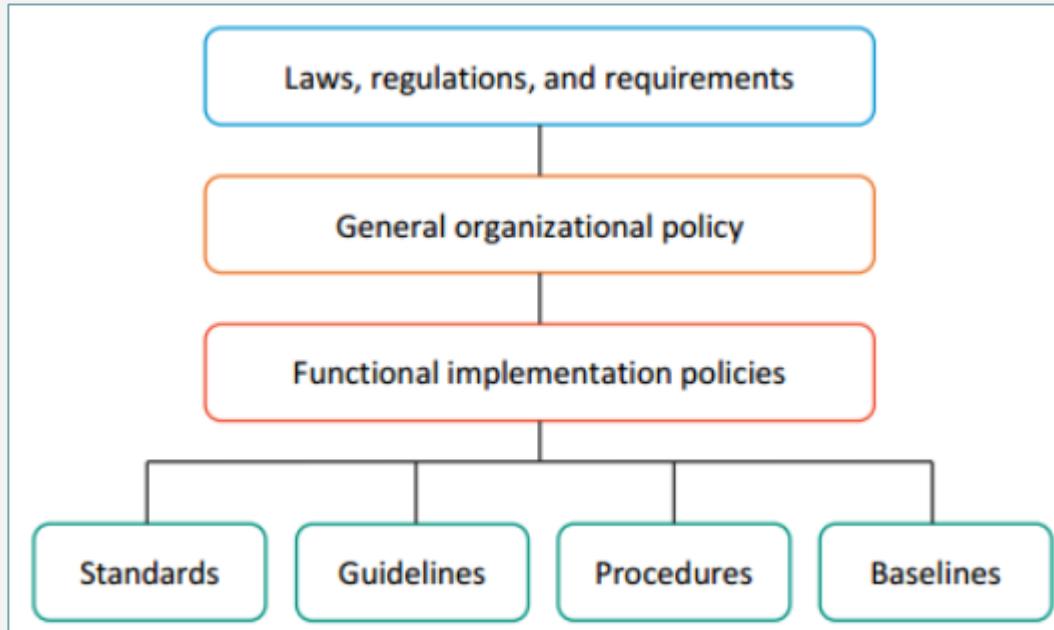
System Specific Policy

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.

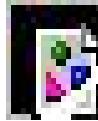
Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad de los sistemas de información.



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.



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 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.

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 en conversaciones telefónicas sin antes proceder a la identificación del interlocutor.

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.



Account banned due to policy violation(s).

This account has been put on suspension due to a violation of our acceptable use policy. The ban will be in effect until Thu, 28 May 2020 19:25:03 GMT.

If you have any questions, please email ban@koding.com and allow 2-3 business days for a reply. Even though your account is banned, all your data is safe.

Please note, repeated violations of our acceptable use policy will result in the permanent deletion of your account.

Team Koding

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)

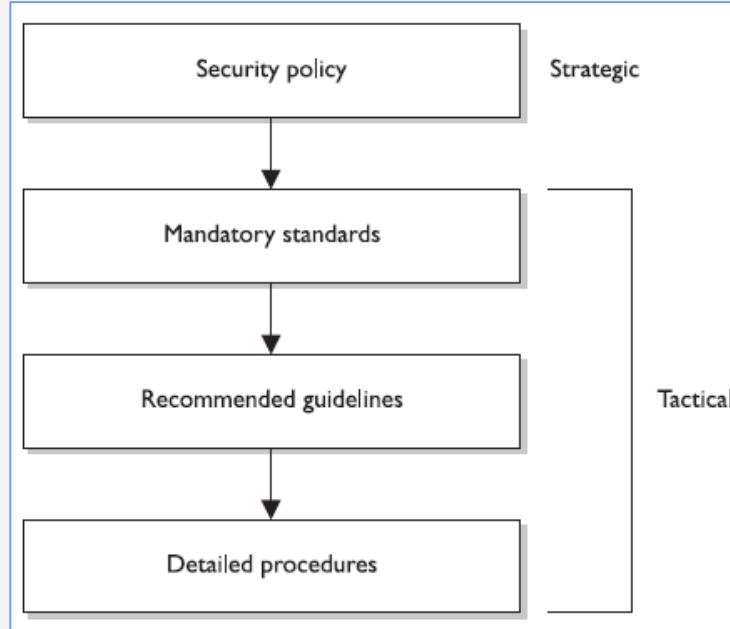
Las normas pueden dar a una política su apoyo y refuerzo en la dirección.

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.

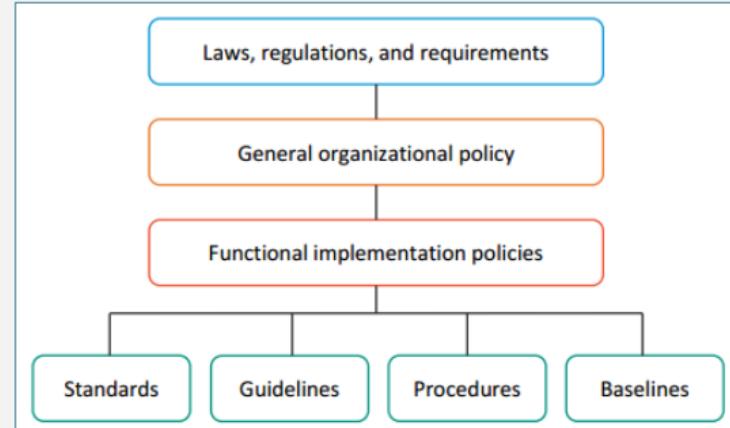
Procedures(Procedimientos)

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.

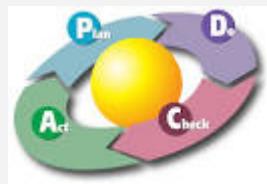
Los procedimientos explican cómo la política, las normas y directrices deben ser implementadas en un entorno operativo.

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, 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 que las reglas existen.

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

Las políticas y sus documentos de apoyo necesitan visibilidad.



- 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 e irresponsable 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.



La primera norma, la ISO/IEC 27000, recoge los términos y definiciones empleados en el resto de normas de la serie. Con ello se evitan distintas interpretaciones sobre los conceptos que aparecen a lo largo de las mismas.

ISO/IEC 27000

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

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(SGSI)** utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Estas normas nos van a permitir disminuir de forma significativa el impacto de los riesgos, sin necesidad de realizar grandes inversiones en software y sin contar con una gran estructura de personal.

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

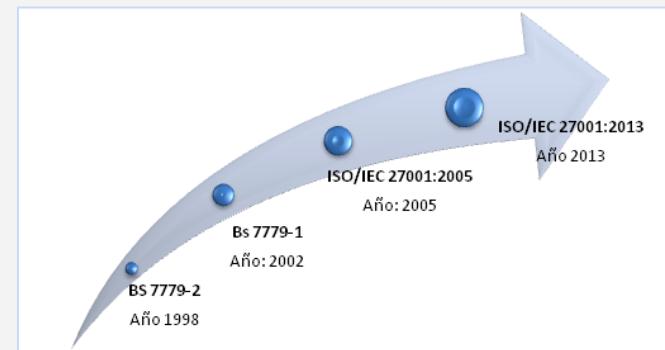
La primera parte se adoptó por ISO, sin cambios sustanciales, como **ISO 17799 en el año 2000**.

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 de una organización.

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 [última edición de 2013](#) este estándar 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



Esta norma ha sido preparada para servir de modelo para **establecer, implementar, operar, monitorear, revisar, mantener y mejorar** un Sistema de Gestión de Seguridad de la Información (SGSI).

El diseño e implementación de SGSI de una organización están influenciados por sus necesidades y objetivos, requisitos de seguridad, los procesos empleados y el tamaño y la estructura de la organización.

Estos y sus sistemas de apoyo se espera que cambien con el tiempo.



Se espera que una implementación ISMS será escalado de acuerdo con las necesidades de la organización.

a simple situation requires a simple ISMS solution.

El enfoque basado en procesos para la gestión de seguridad de la información presentada en esta Norma Internacional anima a sus usuarios a hacer hincapié en la importancia de:

- Comprender los requisitos de seguridad de información de una organización y la necesidad de establecer políticas y objetivos de seguridad de la información.
- Implementación y operación de los controles para la gestión de riesgos de seguridad de la información de una organización en el contexto de los riesgos globales de negocio de la organización.
- El seguimiento y la revisión del rendimiento y la eficacia del SGSI.
- Mejora continua basada en mediciones objetivas.

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.

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.

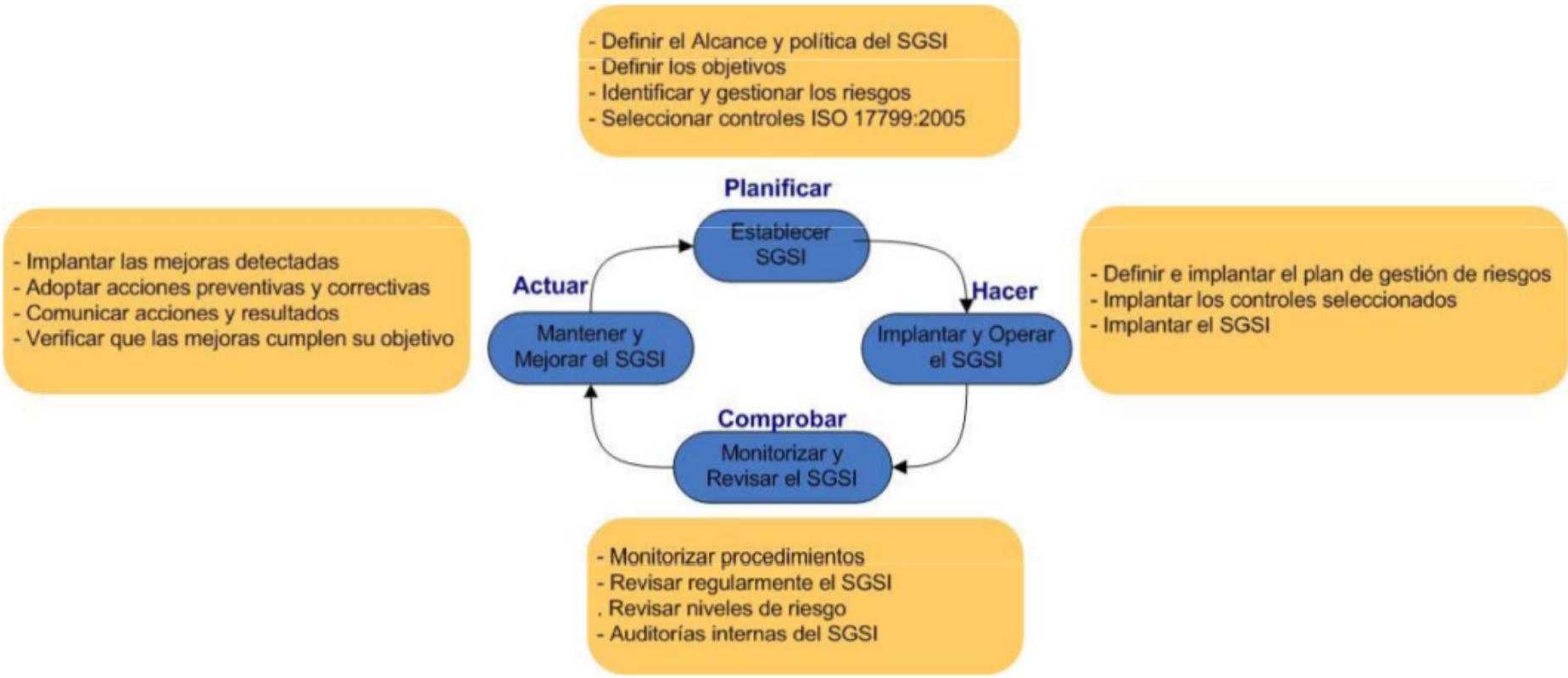
Por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información

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 un SGSI?



Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, este standard adopta el ciclo de mejora continua - PDCA, tradicional en los sistemas de gestión de la calidad, para la aplicación en los procesos de un SGSI.



PDCA model applied to ISMS processes

SGSI + PDCA



Establecer

La organización debe hacer lo siguiente.

Establecer un plan de tratamiento de riesgos que identifique la gestión apropiada de acción, recursos, responsabilidades y prioridades para la gestión de riesgos de seguridad de la información.

Implementar el plan de tratamiento de riesgos con el fin de alcanzar los objetivos de control identificados, lo que incluye la consideración de la financiación y la asignación de funciones y responsabilidades.

Definir la forma de medir la eficacia de los controles o grupos de controles seleccionados y especificar cómo estas medidas se van a utilizar para evaluar la efectividad del control para producir resultados comparables y reproducibles.

Implementar programas de sensibilización y formación.

Administrar la operación del SGSI.

Administrar los recursos para el SGSI.

Implementar procedimientos y otros controles capaces de permitir la detección oportuna de los eventos de seguridad y respuesta a incidentes de seguridad.

La organización debe hacer lo siguiente.

Ejecutar el seguimiento y la revisión de los procedimientos.

Llevar a cabo revisiones periódicas de la eficacia del SGSI, tomando en cuenta los resultados de las auditorías de seguridad, los incidentes, los resultados de las mediciones de efectividad, sugerencias y comentarios de todos los interesados.

Medir la efectividad de los controles para verificar que se cumplen los requisitos de seguridad.

Revisar las evaluaciones de riesgo a intervalos planificados y revisar los riesgos residuales y los niveles aceptables de riesgos identificados.

Realizar auditorías internas a intervalos planificados.

Llevar a cabo un examen de la gestión del SGSI en forma regular para asegurar que el ámbito siga siendo adecuado y las mejoras en el proceso SGSI puedan ser identificadas.

La organización debe hacer lo siguiente.

Implementar las mejoras identificadas en el SGSI.

Tomar acciones correctivas y preventivas adecuadas.

Comunicar las acciones y mejoras a todas las partes interesadas con un nivel de detalle adecuado a las circunstancias y, en su caso, acordar la forma de proceder.

Asegúrarse de que las mejoras alcancen sus objetivos previstos.

Management Controls	Vulnerability Assessment Mapping
1. Risk Management	Risk Assessment Itself
2. Review of Security Controls	InfoSec Documentation
3. Lifecycle	Configuration Management
4. Certification and Accreditation	InfoSec Documentation
5. System Security Plan	InfoSec Documentation InfoSec Roles and Responsibilities
Operational Controls	
6. Personnel Security	Personnel Security
7. Physical Security	Physical Environment
8. Production, Input/Output Controls	Media Sanitization/Disposal
9. Contingency Planning	Contingency Planning/Backups
10. HW/SW Maintenance	Maintenance
11. Data Integrity	Virus Protection
12. Documentation	InfoSec Documentation
13. Security Awareness and Training	Security Awareness and Training
14. Incident Response	Incident Handling/Security Advisory Handling
Technical Controls	
15. Identification and Authentication	Identification and Authentication
16. Logical Access Controls	Account Management/Access Controls Session Controls
17. Audit Trails	Audit
	Security Products External Connectivity

Preventative	Detective	Corrective	Compensatory
Security Awareness Training	System Monitoring	OS Upgrade	Backup Generator
Firewall	IDS	Backup Data Restoral	Hot Site
Anti-virus	Anti-Virus	Anti-Virus	Server Isolation
Security Guard	Motion Detector	Vulnerability Mitigation	
IPS	IPS		

Tipos de Controles

La documentación debe incluir un registro de las decisiones de gestión, garantizar que las acciones tienen su origen en las decisiones y políticas de gestión, y asegurar que los resultados registrados son reproducibles.

Declaraciones documentadas de la política SGSI.

El alcance del SGSI.

Procedimientos y controles en apoyo del SGSI.

Una descripción de la metodología de evaluación de riesgos.

El informe de evaluación de riesgos.

El plan de tratamiento de riesgos.

Registros requeridos por esta Norma Internacional.

procedimientos documentados requeridos por la organización para asegurarse de la planificación eficaz, operación y control de sus procesos de seguridad de la información y describen la forma de medir la eficacia de los controles.

Los requisitos de documentación

Documents required by the ISMS shall be protected and controlled.

aprobar los documentos a su adecuación antes de su emisión.

revisar y actualizar los documentos cuando sea necesario y volver a aprobar los documentos.

asegurar que los cambios y el estado de revisión actual de los documentos se identifican.

garantizar que las versiones pertinentes de los documentos aplicables están disponibles en los puntos de uso.

aseguran que los documentos permanecen legibles y fácilmente identificables.

aseguran que los documentos están disponibles para aquellos que los necesitan.

Asegurar que los documentos de origen externo se identifican.

garantizar que se controla la distribución de los documentos.

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

establishing an ISMS policy;

ensuring that ISMS objectives and plans are established;

establishing roles and responsibilities for information security;

communicating to the organization the importance of meeting information security objectives and conforming to the information security policy,

providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS

deciding the criteria for accepting risks and the acceptable levels of risk;

ensuring that internal ISMS audits are conducted

conducting management reviews of the ISMS

The organization shall determine and provide the resources needed to:

establish, implement, operate, monitor, review, maintain and improve an ISMS;

ensure that information security procedures support the business requirements;

identify and address legal and regulatory requirements and contractual security obligations;

maintain adequate security by correct application of all implemented controls;

carry out reviews when necessary, and to react appropriately to the results of these reviews;

where required, improve the effectiveness of the ISMS.

The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

determining the necessary competencies for personnel performing work effecting the ISMS

providing training or taking other actions to satisfy these needs;

evaluating the effectiveness of the actions taken

maintaining records of education, training, skills, experience and qualifications

The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

Training, awareness and competence

Esta Norma Internacional está alineada con la norma **ISO 9001: 2000** e **ISO 14001: 2004** con el fin de apoyar la aplicación coherente e integrada y el funcionamiento de las normas de gestión relacionados.



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

Compatibilidad con otros sistemas de gestión



La norma ISO/IEC 27002 es una guía de buenas prácticas que recoge las recomendaciones sobre las medidas a tomar para asegurar los sistemas de información de una organización.

ISO / IEC 27002

“Guía de Buenas Prácticas”

0) Introducción

5) Política de Seguridad

4) Análisis y
Gestión de Riesgos

6) Estructura Organizativa para la Seguridad

8) Seguridad
en el personal

9) Seguridad
Física y del
Entorno

10) Gestión de
Comunicaciones
y Operaciones
(Seg. Lógica)

12) Desarrollo
y Mantenimiento de
Sistemas

11) Control de Accesos

13) Gestión de Incidencias

14) Gestión de Continuidad del Negocio

15) Cumplimiento

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

CLASIFICACIÓN Y CONTROL DE ACTIVOS/INFORMACION

La organización debe tener un acabado conocimiento sobre los activos que posee como parte importante de la administración de riesgos.

Algunos ejemplos de activos son:

- Recursos de información.
- Recursos de software.
- Activos físicos.
- Servicios.

RECURSOS DE INFORMACION

- Bases de datos y archivos.
 - Documentación de sistemas.
 - Manuales de usuario.
 - Material de capacitación.
 - Procedimientos operativos o de soporte.
 - Planes de continuidad.
 - Información archivada.
-

RECURSOS DE SOFTWARE

- Software de aplicaciones.
 - Sistemas operativos.
 - Herramientas de desarrollo.
 - Utilitarios, etc.
-

ACTIVOS FÍSICOS

- **Equipamiento informático.**
(procesadores, monitores, computadoras portátiles, módems).
 - **Equipos de comunicaciones.**
(routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos).
 - **Otros equipos técnicos.**
(relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
-

SERVICIOS

- **Servicios informáticos y de comunicaciones.**
 - **Utilitarios generales.**
(calefacción, iluminación, energía eléctrica, etc.).
-

LOS ACTIVOS DE INFORMACIÓN DEBEN SER
CLASIFICADOS DE ACUERDO A LA
SENSIBILIDAD Y CRITICIDAD DE LA
INFORMACIÓN QUE CONTIENEN O DE ACUERDO
A LA FUNCIONALIDAD QUE CUMPLEN.

LA INFORMACIÓN DEJA DE SER SENSIBLE O CRÍTICA DESPUÉS DE UN CIERTO PERÍODO DE TIEMPO.



➤ CUANDO LA INFORMACIÓN SE HA HECHO PÚBLICA.

LA CLASIFICACIÓN DE UN ÍTEM DE INFORMACIÓN DETERMINADO PUEDE CAMBIAR DE ACUERDO CON UNA POLÍTICA PREDETERMINADA. SE DEBE CONSIDERAR LA CANTIDAD DE CATEGORÍAS A DEFINIR PARA LA CLASIFICACIÓN DADO QUE LOS ESQUEMAS DEMASIADO COMPLEJOS PUEDEN RESULTAR POCO PRÁCTICOS.

LA INFORMACIÓN ADOPTA MUCHAS FORMAS

- **Puede ser almacenada** (medios portátiles).
- **Transmitida** (a través de redes o entre sistemas).
- **Impresa o escrita en papel.**

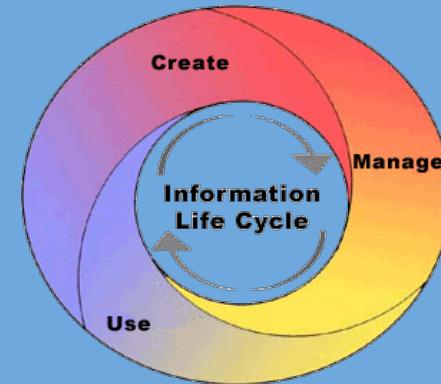
Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la

- **Confidencialidad.**
 - **Integridad.**
 - **Disponibilidad** de la información.
-

LOS PROPIETARIOS DE LA INFORMACIÓN SON
LOS ENCARGADOS DE CLASIFICARLA DE
ACUERDO CON SU GRADO DE SENSIBILIDAD Y
CRITICIDAD, DE DOCUMENTAR Y MANTENER
ACTUALIZADA LA CLASIFICACIÓN EFECTUADA,
Y DE DEFINIR LAS FUNCIONES QUE DEBERÁN
TENER PERMISOS DE ACCESO A LA
INFORMACIÓN.



CADA CLASIFICACIÓN DEBE TENER REQUISITOS
DE MANEJO SEPARADAS Y PROCEDIMIENTOS
RELATIVOS A CÓMO SE ACCDE A LOS DATOS,
USA Y DESTRUYE.



LA INFORMACIÓN PUEDE PASAR A SER OBSOLETA Y POR LO TANTO, SER NECESARIO ELIMINARLA. LA DESTRUCCIÓN DE LA INFORMACIÓN ES UN PROCESO QUE DEBE ASEGURAR LA CONFIDENCIALIDAD DE LA MISMA HASTA EL MOMENTO DE SU ELIMINACIÓN.



TO PROPERLY ERASE THIS DATA FROM THE MEDIA, DEGAUSSING OR ZEROIZATION PROCEDURES MAY BE REQUIRED.

CLASIFICACIÓN DE LA INFORMACIÓN

CLASSIFIED

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 PARA 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 QUE NO ESTÉ DISPONIBLE CUANDO SE NECESITA..

UNA VEZ QUE LOS DATOS SE SEGMENTAN DE ACUERDO A SU NIVEL DE SENSIBILIDAD, LA EMPRESA PUEDE DECIDIR QUE CONTROLES DE SEGURIDAD SON NECESARIOS PARA PROTEGER LOS DIFERENTES TIPOS DE DATOS.



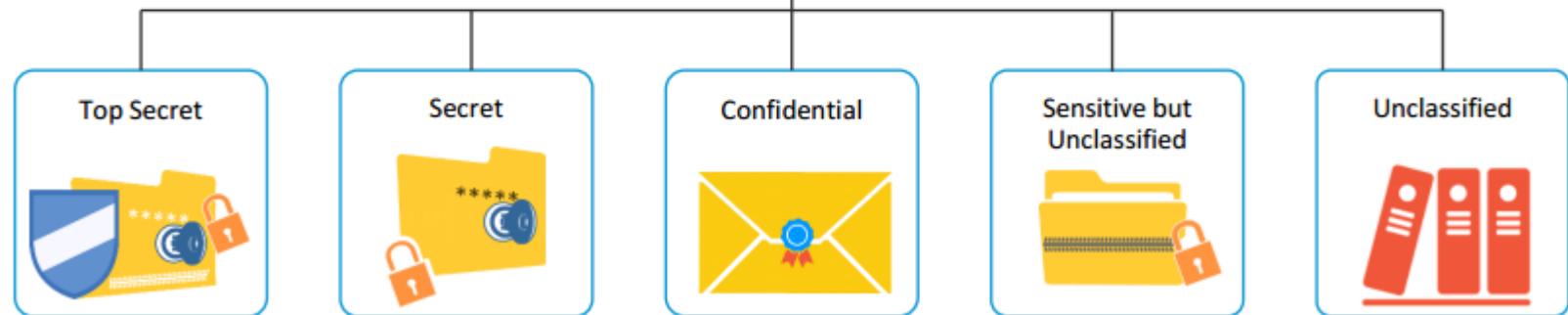
LA CLASIFICACIÓN DE LA INFORMACIÓN
AYUDA A ASEGURAR QUE LOS DATOS ESTÁN
PROTEGIDOS DE UNA MANERA
COSTO/EFECTIVA.



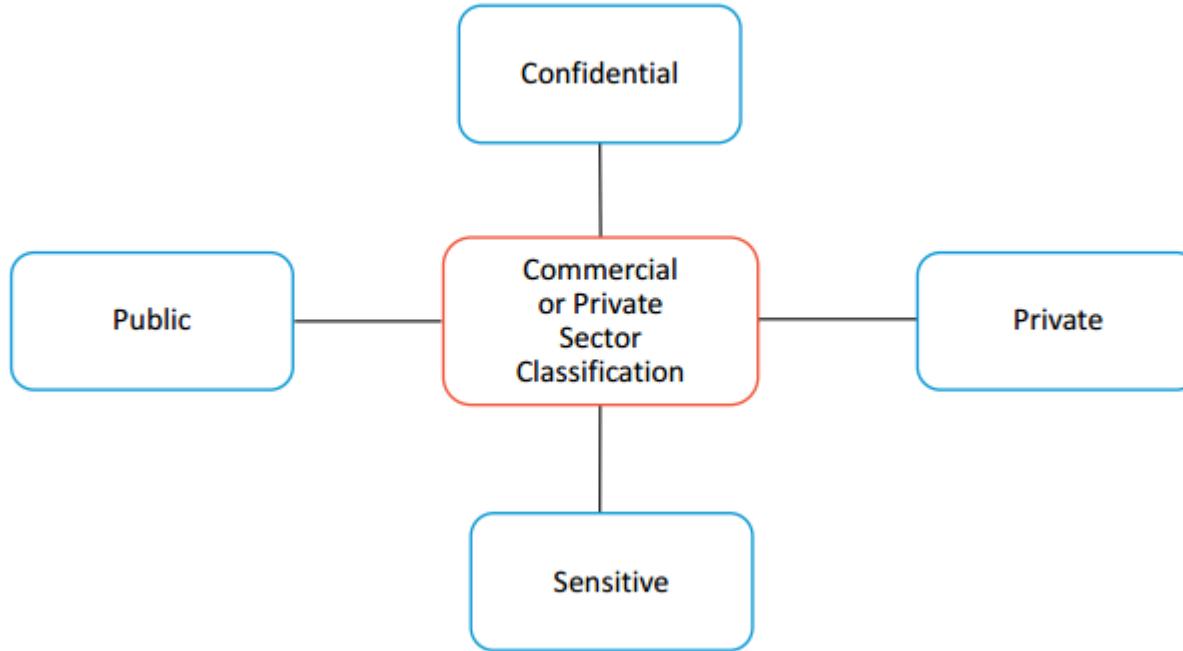
PROTECTING AND MAINTAINING
DATA COSTS MONEY, BUT IT IS
IMPORTANT TO SPEND THIS MONEY
FOR THE INFORMATION THAT
ACTUALLY REQUIRES PROTECTION.

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

Government or Military Sector
Classification



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.

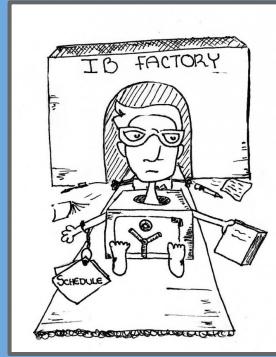
CLASSIFICATION	DEFINITION	EXAMPLES	ORGANIZATIONS THAT WOULD USE THIS
PUBLIC	LA DIVULGACIÓN NO ES BIENVENIDA, PERO NO CAUSARÍA UN IMPACTO ADVERSO PARA LA EMPRESA O EL PERSONAL.	CUÁNTAS PERSONAS ESTÁN TRABAJANDO EN UN PROYECTO ESPECÍFICO.	COMMERCIAL BUSINESS
SENSITIVE	REQUIERE PRECAUCIONES ESPECIALES PARA GARANTIZAR LA INTEGRIDAD Y CONFIDENCIALIDAD DE LOS DATOS, POR LOS QUE LO PROTEGE DE MODIFICACIÓN O ELIMINACIÓN NO AUTORIZADA.	INFORMACIÓN FINANCIERA.	COMMERCIAL BUSINESS

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

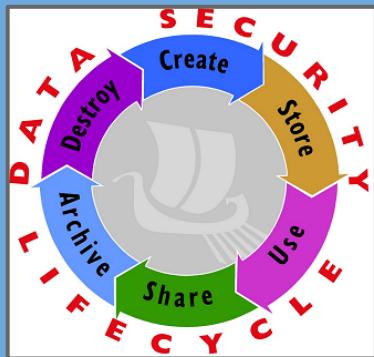
CLASSIFICATION	DEFINITION	EXAMPLES	ORGANIZATIONS THAT WOULD USE THIS
UNCLASSIFIED	LA INFORMACIÓN NO ES SENSIBLE O CLASIFICADA.	- MANUAL DEL COMPUTADOR Y GARANTÍA - INFORMACIÓN DE RECLUTAMIENTO.	MILITARY
SENSITIVE BUT UNCLASSIFIED (SBU)	SECRETO MENOR. SI SE DA A CONOCER, PUEDE QUE NO CAUSE DAÑOS GRAVES.	- DATOS MÉDICOS. - RESPUESTAS A LAS CALIFICACIONES DE LAS PRUEBAS	MILITARY

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

LAS CLASIFICACIONES NO DEBEN SER DEMASIADO RESTRICTIVAS.



CADA CLASIFICACIÓN DEBE SER ÚNICO Y SEPARADO DE LOS DEMÁS Y NO TIENE EFECTOS SUPERPUERTOS.



EL PROCESO DE CLASIFICACIÓN TAMBIÉN DEBE DELINEAR COMO LA INFORMACIÓN ES CONTROLADA Y MANEJADA A TRAVÉS DE SU CICLO DE VIDA.

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.

EFEKTOS 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.

LAS APLICACIONES QUE CONTIENEN Y PROCESAN
INFORMACIÓN CLASIFICADA DEBEN SER EVALUADOS PARA
EL NIVEL DE PROTECCIÓN QUE PROPORCIONAN.



APLICACIONES Y ALGUNAS VECES SISTEMAS ENTEROS
PUEDEN NECESSITAR SER CLASIFICADOS.

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 SUCEΣIVAMENTE.





<https://www.youtube.com/watch?v=7QEdAykXxoM>

<https://www.wikileaks.org>



<http://journalistsresource.org/wp-content/uploads/2011/09/Wikileaks-Case-Study.pdf>

http://www.argumentcritique.com/uploads/1/0/3/1/10317653/rees_dissent.pdf

<http://www.ruairi.info/ethics.pdf>

<http://www.cabrillo.edu/~cclose/docs/Case%20Study%202%20Sp13%20-%20Kant.pdf>

https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html

WIKILEAKS PROVES 911 WAS INSIDE JOB!

<https://www.youtube.com/watch?v=JdkXnOGhBp8>



Study Cases



Edward Snowden NBC Interview - I was Trained as a Spy

<https://www.youtube.com/watch?v=EiEpMUOA3J8>

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

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



http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

http://www.unirioja.es/servicios/si/seguridad/difusion/politica_contraseñas.pdf

[HTTP://WWW.SGP.GOV.AR/SITIO/PSI_MODELO-V1_200507.PDF](http://WWW.SGP.GOV.AR/SITIO/PSI_MODELO-V1_200507.PDF)



Payment Card Industry Data Security Standard (PCI DSS)

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



What Is It?

Payment Card Industry Data Security Standard (PCI DSS)

- The Standard: A proprietary information security standard for organizations that handle cardholder information

Payment Card Industry Security Standards Council (PCI SSC)

- The Council: Defined and created the standards to increase controls around cardholder data and reduce credit card fraud via its exposure



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

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?

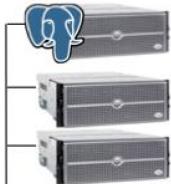
La aplicación opera en cualquier dispositivo electrónico de mano(handheld) que no es dedicado exclusivamente para el pago de alguna transacción?

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.

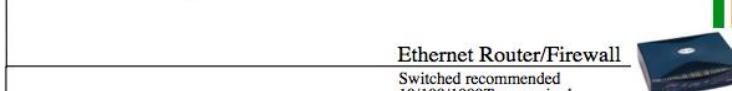
OFFICE LAN

Servers

All servers should be UPS protected.



Purpose	Operating System	Memory	Considerations
Database	PC: Windows Server OS-X 10.6.8+ Linux	8-16+ GB	250+Gb, SSD, Raid 1+0 or 5 external backup
Remote Box Office	Citrix/term. Services Or fast networks/ VPN	4+ GB	scalable
Web Services	PC: XP, Win 7, 8 OS-X 10.6.8+ Intel	4 GB	Multi core
Apache Web Server	PC: 2003/8, Win 7, 8 OS-X 10.6.8+ Intel Linux	2 GB	Standalone DMZ between firewalls mod-SSL



Admin
Ethernet Connected PC and/or Mac

Box Office
Ethernet Connected PC and/or Mac Restricted outbound access

Ticket Printers
Ethernet for shared Parallel (PC only) or Serial (PC or Mac)

VENUE



Laptop
Wireless access outside office LAN only

Access Mgt.
Wired (Desktop based)
Wireless (Handheld)
Bar code Scanners
At each entry location
Supports check in/check out



Wireless Access
WPA2 enabled
Hidden SSID
MAC secured
Outside firewall

DMZ



Powered by
APACHE
Router/Firewall
2.4
NAT/VPN Capable
IP to IP mapping

REMOTE



Remote Box Office
VPN Access Citrix/Terminal services internet connection Desktop/Countertop printers Supports work at home

INTERNET



Internet Ticketing
Any current web browser Mac, PC or tablet HTML 3.1 compliant



Veamos el siguiente caso:

1. Un hacker adivino fácilmente la contraseña del servidor de acceso remoto de una reconocida cadena de almacenes.
2. La aplicación le permita conectarse a todos los almacenes.
3. El hacker descargó e instaló "keyloggers" en todos los sistemas.
4. Los "keyloggers" capturaban todas las transacciones tecleadas manualmente y leídas por el lector de tarjetas de crédito.
5. El hacker se conectaba periódicamente para descargar los datos de tarjeta de crédito capturados por los Keyloggers.
6. El hacker utilizó esta información para hacer compras por todo el mundo robando a los dueños de las tarjetas.

CONSECUENCIAS

1. Realizar una Investigación Forense.
2. Reconstruir todos los sistemas siguiendo la norma PCI.
3. Actualizar o remplazar el Software de los puntos de venta.
4. Pagar las sanciones por no cumplir con la norma PCI.
5. Pagar la re-expedición de las tarjetas de crédito. Un comercio promedio puede tener almacenada la información de 130,000 tarjetas que multiplicadas por \$60,000 que vale re-expedir cada plástico, nos da un total de 8,000 Millones de pesos!

Acciones a tomar para un buen cumplimiento de seguridad.

Separación de funciones (Separation of duties)	Políticas de datos sensitivas (Sensitive data pol).
Rotación de trabajo (Rotation jobs).	Contraseñas y ID de usuarios (ID & Passwords).
Vacaciones obligatorias (Mandatory Vacations).	Licenciamiento de softwares (Licensing).
Menor privilegio (Least Privilege).	Destrucción de datos (Data Destruction).
Respuesta a incidentes (Incident Response).	Formalización y sensibilización (Training and awareness).
Tareas forense (Forensic Tasks).	
Requerimientos de auditorias (Auditing requirements).	
Responsabilidad de empleados (Employee resp).	
Necesidad de saber (Need to Know).	
Clasificación de la información (Data Classif).	
Uso aceptable (Acceptable use).	

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

