# METODOLOGIA PARA REALIZAR EL ANÁLISIS GAP PCI DSS

## (INFORMATION QUALITY)

## CONTROL DOCUMENTAL

### Historia

| Versión | Autor | Tipo de Revisión | Descripción | Aprobado por | **Fecha** |
|---|---|---|---|---|---|
| 1.0 | IQ | Creación | Proyecto | | |
| | | | | | |
| | | | | | |

### Distribución

| Copia | Destinatario | Destino / Dirección |
|---|---|---|
| Original | IQ | |
| Copia | IQ | |

### Referencias

| Ref. | Documento o ítem referenciado |
|---|---|
| | |
| | |

### Control de Acceso

| Sección | Disponibilidad |
|---|---|
| Todo | |
| | |

# TABLA DE CONTENIDO

## LISTADO DE ILUSTRACIONES



## LISTADO DE TABLAS

# 1 INTRODUCCION

La seguridad de la información debe ser un componente crítico dentro de la estrategia de seguridad de la información. El análisis de brecha es recomendable realizarlo para iniciar el establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI), ya que este análisis permite conocer el nivel de madurez con que se cuenta, para luego, proponer un plan de acción para la futura implementación del modelo de seguridad en una organización.

# 2 OBJETIVOS

## *2.1 Objetivo general*

Presentar la metodología recomendada con respecto a la norma PCI DSS V 3.21 con el fin de comprender el estado de madurez de la seguridad de la información.

## *2.2 Objetivo Específicos*

Detallar la metodología recomendada para:

1. Estimar Nivel de madurez por dominios
2. Estimar Nivel de madurez por control
3. Ayudar en el mejoramiento de la protección y seguridad de los datos de tarjetahabiente
4. Entender la situación actual en lo relacionado al cumplimiento PCI
5. Identificar las debilidades en los sistemas o componentes que conforman la infraestructura de la organización
6. Estimar el grado general de madurez anterior al proceso de certificación
7. Contar con recomendaciones para la implementación de los requerimientos y sub- requerimientos faltantes
8. Facilitar la realización de un plan de remediación

# 3 OBJETIVOS DE LA SEGURIDAD DE LA INFORMACION

Los objetivos son el soporte de la visión, la misión y la estrategia de la entidad desde el punto de vista de la seguridad de la información. Estos se exponen a continuación:


**Ilustración 1**. Objetivos de la Seguridad de la Información

- La información (los datos de tarjetahabiente) es uno de los activos más importantes de toda entidad, por lo tanto, se espera que sea utilizada acorde con los requerimientos y la clasificación definida por la entidad.
- La confidencialidad de la información de la entidad y de terceras partes debe ser mantenida y preservada.
- La información de la entidad debe preservar su integridad independientemente de su residencia temporal o permanente, o la forma en que sea transmitida.
- La información sensible (datos de tarjetahabiente) debe ser protegida durante la transmisión, el almacenamiento y el procesamiento (PCI DSS).

## 4 LA NORMA PCI DSS

La norma PCI DSS (Payment Card Industry Data Security Standard) fue desarrollada por un conjunto de compañías de tarjetas de débito y crédito en el año 2006 entre las que figuran: America Express, Discover, JCB, Mastercard y VISA. Esta norma procura que las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes protejan esta información con el fin de evitar fugas que involucren divulgación de información sensible. Este tipo de fugas podría afectar todo el ecosistema de tarjetas de pago incluyendo clientes, comercios e instituciones financieras. Estas entidades pierden credibilidad como consecuencias de fugas de información y quedarían expuestas a numerosas demandas económicas.

Los beneficios asociados de mantener el cumplimiento de PCI son fundamentales para el éxito a largo plazo de las entidades que procesan pagos con tarjeta. El cumplimiento involucra la identificación continua de

amenazas y vulnerabilidades que podrían potencialmente afectar a dichas organizaciones. La mayoría de empresas nunca se recuperan totalmente de una infracción o fuga de sus datos ya que la pérdida o el impacto es mayor que los datos en sí mismos. Seguir la norma PCI es una gran oportunidad para los negocios. Por medio de ella se logra asegurar la salud y confianza en las transacciones de pago para cientos de millones de personas en el mundo que utilizan sus tarjetas día tras día.

Las compañías autorizadas por el Concilio (PCI SSC) para realizar la validación de cumplimiento de la norma PCI DSS se conocen como QSA (Qualified Security Assessor), las cuales deben cumplir una serie de requisitos como empresa y sus ingenieros son entrenados directamente por esta asociación. La norma PCI es una de las normas más exigentes a nivel mundial en lo relacionado con la protección de la información sensible debido al énfasis que ella pone en los controles de tipo tecnológicos y la rigurosidad que exige en el proceso de evaluación para otorgar la certificación de cumplimiento.

## 5 MODELO DE SEGURIDAD RECOMENDADO PARA PCI DSS

En el ámbito de la seguridad de la información de PCI DSS, los componentes del modelo de seguridad se ubican en diferentes niveles de acuerdo a su importancia. Este modelo permite la implementación efectiva y eficiente de la norma. Por esta razón se sugiere su utilización en comercios, pasarelas de pago e instituciones financieras para la mejora continua de la seguridad de la información:

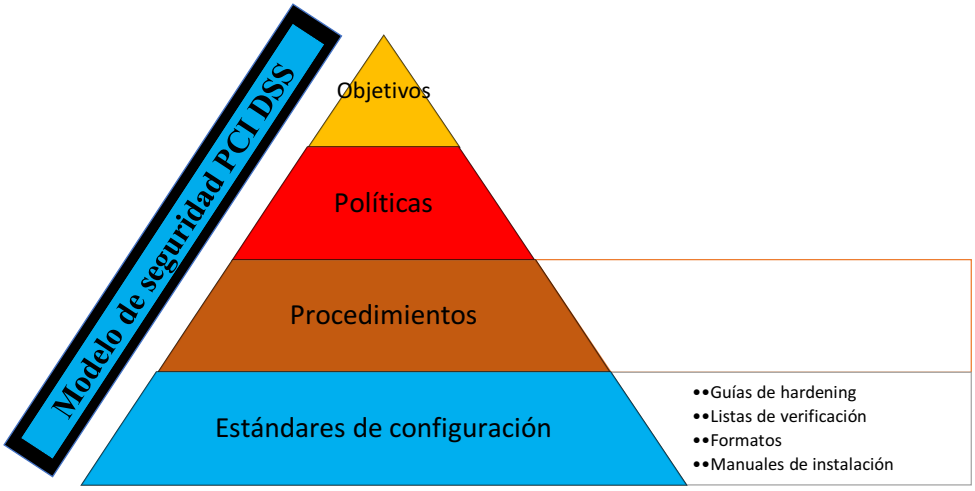


**Ilustración 2.** Componentes del modelo PCI DSS.

## 6 ALCANCE DEL GAP PCI DSS

El alcance de las actividades del GAP considera los componentes (hardware y software, procedimientos, estándares de configuración, personas, tecnologías, procesos, entre otros) definidos en el alcance según los lineamientos estipulados por PCI DSS V.3.21:

> The PCI DSS security requirements apply to all systems components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data (PCI DSS 3.21, p. 10).

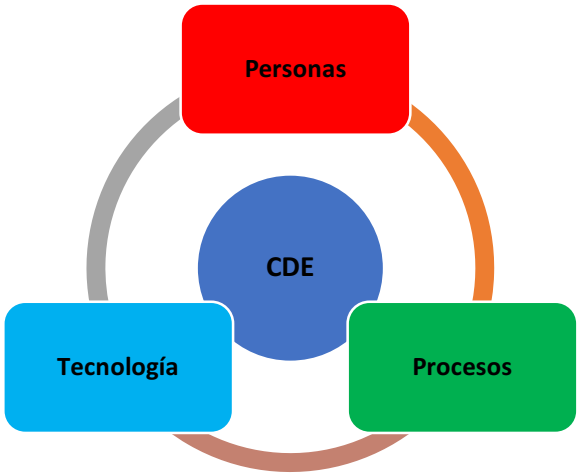


**Ilustración 3**. Componentes del alcance del GAP PCI DSS.

## 7 CONCEPTOS FUNDAMENTALES DEL GAP

El cuidado de la información es importante para el funcionamiento para que las organizaciones logren la consecución de su misión. Contar con una serie de controles para mitigar el riesgo según PCI DSS V 3.21 ayuda a gestionar y proteger la información.

El marco teórico propio de este documento está basado con la norma PCI DSS V 3.21 y el Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL y la norma ISO 27032:2009. Estas recomendaciones se establecen para contar con una guía para el establecimiento, implementación, operación, seguimiento, revisión y mejora de un (SGSI).

**PCI Data Security Standard – High Level Overview**

| | |
|---|---|
| **Build and Maintain a Secure Network and Systems** | 1. Install and maintain a firewall configuration to protect cardholder data<br>2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | 3. Protect stored cardholder data<br>4. Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | 5. Protect all systems against malware and regularly update anti-virus software or programs<br>6. Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | 7. Restrict access to cardholder data by business need to know<br>8. Identify and authenticate access to system components<br>9. Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | 10. Track and monitor all access to network resources and cardholder data<br>11. Regularly test security systems and processes |
| **Maintain an Information Security Policy** | 12. Maintain a policy that addresses information security for all personnel |

**Tabla 1.** Dominios de la norma PCI DSS

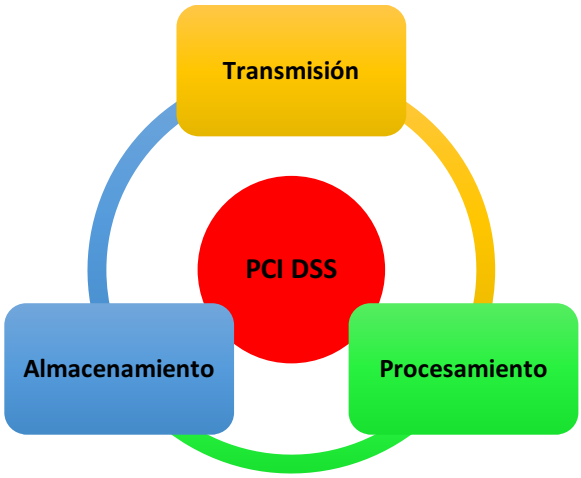


**Ilustración 4**. Seguridad en PCI DSS.

## 8 GLOSARIO

- **Actividades críticas**: Operaciones críticas y/o actividades que soportan los objetivos de la Entidad.
- **Activo:** Cualquier cosa que tenga valor para la organización.
- **Activos de información:** Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos del negocio, servicio y soporte. Se pueden clasificar de la siguiente manera:
    - Personas: Incluyendo sus calificaciones, competencias y experiencia.
    - Intangibles: Ideas, conocimiento, conversaciones.
    - Electrónicos: Bases de datos, archivos, registros de auditoria, aplicaciones, herramientas de desarrollo y utilidades.
    - Físicos: Documentos impresos, manuscritos y hardware.
    - Servicios: Servicios computacionales y de comunicaciones.
- **Análisis de riesgo**: Uso sistemático de la información para identificar las fuentes y estimar el riesgo
- **Área IT**: Es el área encargada de soportar, diseñar y mantener los activos electrónicos y el hardware propiedad de la Entidad.
- **Confidencialidad:** Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Contratistas:** Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una Entidad.
- **Custodio:** Encargado de proteger la información por delegación del propietario. Generalmente este rol es ejecutado por el Área IT.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una Entidad autorizada.
- **Estándares:** Un producto o mecanismo especifico el cual es seleccionado desde un punto de vista universal, para su uso a lo largo de toda la organización, con el objetivo fundamental de soportar una política ya aceptada y aprobada por las directivas de la Entidad.
- **Falla:** Daño o afectación de un dispositivo por un periodo determinado

- **Incidente:** Un evento o una serie de eventos no deseados o inesperados que tienen una posibilidad significativa de comprometer las operaciones del servicio y amenazar la continuidad del Sistema.
- **Información:** Entendemos por INFORMACIÓN cualquier manifestación (ya sea visual, auditiva, escrita, electrónica, óptica, magnética, táctil...) de un conjunto de conocimientos. Por ejemplo:
    - Una noticia que escuchamos por la radio.
    - Una señal de tráfico que advierte un peligro.

La información se representa mediante conjuntos de símbolos, que pueden ser de diferente naturaleza:

- Textuales o numéricos, como las letras y números que usamos al escribir.
- Sonoros, como los fonemas, las notas musicales...
- Cromáticos, como los colores de los semáforos.

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Lista de verificación:** Herramienta para recordar y/o validar que tareas tienen que ser cumplidas y que recursos están disponibles en una etapa de recuperación.
- **Procedimientos:** Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.
- **Propietario:** Es el responsable y dueño del activo de información. Define también sus niveles de clasificación.
- **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información.

## 9 BIBLIOGRAFÍA

Business Continuity Institute (2013) *Good Practice Guidelines: A guide to global good practice in business continuity*, Business Continuity Institute, Caversham.

ISO 22301 (2012) – Societal security – Business continuity management systems – Requirements

ISO 27001:2013 Information security.

PCI DSS V 3.21