PCI Resources - Modelo y enfoque del alcance de PCI DSS

Fuente: http://www.pciresources.com/pci-dss-scoping-model-and-approach/

El enfoque y el modelo que se describen aquí se extraen del Volumen 2 (Alcance del PCI DSS) de la serie de libros de PCI Resources que cubre el PCI DSS. Los detalles del análisis que condujeron a este modelo, y de otros detalles de alcance relevantes, se pueden encontrar en ese volumen (principalmente en la sección 2.5). Mientras que el alcance de PCI DSS cubre las personas, los procesos y las tecnologías (PPT), este modelo detallará principalmente la parte tecnológica, los componentes del sistema de TI. Las personas y los procesos involucrados también deberían estar cubiertos por las organizaciones.

 Este enfoque modelo es el resultado del pensamiento y la experiencia de Yves Desharnais con PCI DSS desde 2012 (versión 2.0). Este modelo no está respaldado ni aprobado por el PCI SSC ni por nadie más.

Espero que la apertura de este modelo ayude a todos a ponerse de acuerdo sobre lo que debería estar dentro del alcance, o al menos tener una base razonable para la clasificación y el debate. Creo que este modelo también podría aplicarse a otros datos que requieren protección, por ejemplo, información de la salud del paciente (PHI) o información de identificación personal (PII). La actualización de diciembre de 2017 de la versión 1.2 de este modelo se alinea con el Suplemento informativo PCI DSS de diciembre de 2016 del PCI SSC y se denomina "Guía para el alcance y segmentación de la red PCI DSS" (este suplemento se denominará "Guía de diciembre de 2016" ". No se realizaron cambios, solo se agregaron aclaraciones.

Acrónimos

En este modelo y enfoque, me verán usar muchos acrónimos (en su versión original inglesa), que defino aquí:

- CHD = Siglas del ingl. "Cardholder Data" ('datos del titular de la tarjeta'); consiste del PAN, el nombre del titular de la tarjeta, la fecha de vencimiento de la tarjeta y, a veces, el código de servicio.
- PAN = Acrónimo de "Primary Account Number" ('número de cuenta principal'); el número impreso en el frente de la tarjeta de pago.
- SAD = Acrónimo de "Sensitive Authentication Data" ('datos de autenticación confidenciales'), incluye la información de la cinta magnética, el PIN (NIP) o el bloque PIN (NIP), así como el valor de autorización de Tarjeta-no-presente al cual nos referiremos como CVV2 pero puede tomar cualquiera de los siguientes acrónimos : CAV2/CVC2/CVV2/CID.
- SPT = Siglas del Ingl. "Store, Process, or Transmit" ('almacenar, procesar o transmitir'), lo que significa que un sistema o proceso entra en contacto con CHD y / o SAD y, por lo tanto, está automáticamente dentro del alcance.
- CDE = Siglas del ingl. "Cardholder Data Environment" ('entorno de datos del titular de la tarjeta'), básicamente lo que estamos tratando de proteger, que comienza con los sistemas que SPT CHD o SAD pero no se limita a estos.
- Aislamiento = No hay acceso posible entre sistemas.
- Acceso controlado = Hay comunicaciones limitadas (restringidas) posibles entre los sistemas.

- RoC = Informe de cumplimiento (inglés: Report on Compliance); Informe que documenta los resultados detallados de la evaluación PCI DSS de una entidad.
- Entidad = Una entidad es cualquier organización que tiene la responsabilidad de proteger los datos de la tarjeta; para el cumplimiento de PCI DSS, una entidad se definirá como un comerciante o un proveedor de servicios.
- DESV = Validación suplementaria de entidades designadas PCI DSS para PCI DSS 3.1, un nuevo estándar PCI lanzado en junio de 2015 que ahora está integrado como apéndice A3 desde PCI DSS 3.2

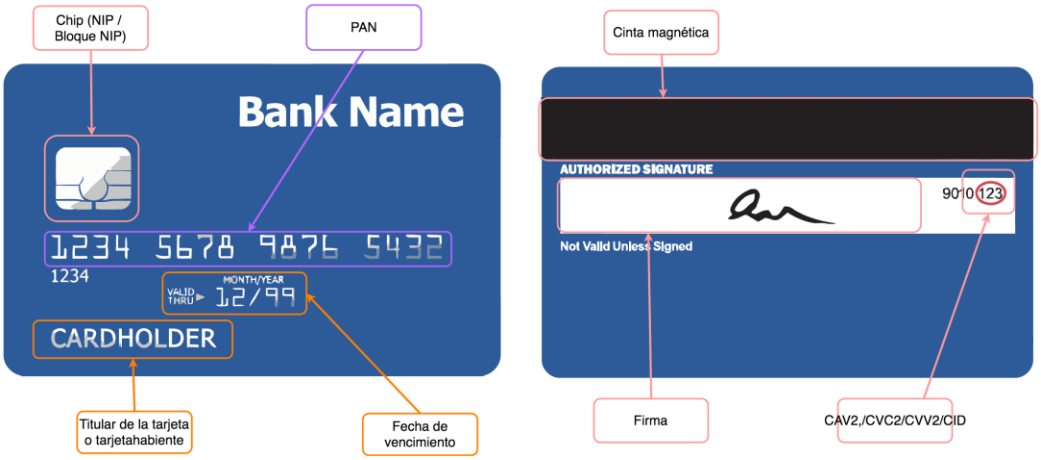

Figura 1 - Representación de la tarjeta de crédito (anverso y reverso) que muestra CHD y SAD

Categorías del alcance

Mi enfoque del alcance, como lo hacen otros enfoques, se usa para categorizar sistemas. Inicialmente definí tres (3) categorías básicas que se derivan directamente del lenguaje del estándar PCI DSS: CDE, conectado ("connected") y fuera del alcance ("out-of-scope"). Un problema que tengo con la Guía del PCI SSC sobre el alcance se refiere a si los dispositivos de segmentación (o combinaciones de los mismos) constituyen sistemas CDE (mi posición inicial) o sistemas conectados (PCI SSC y OPST); Por lo tanto, he decidido tratar los dispositivos de segmentación como su propia categoría, que explicaré en el modelo revisado. Esto no tiene ningún efecto en el alcance, simplemente en la claridad. Describiré estos uno por uno, comenzando desde el núcleo interno que estamos tratando de proteger: el área donde tenemos CHD y / o SAD, el CDE.

Primera Categoría: Sistemas CDE

Todos los sistemas CDE a menudo se llaman dispositivos de categoría 1 o tipo 1. Hay dos subcategorías diferentes en el CDE, pero todos los requisitos atribuibles se aplicarán a todos los subtipos de CDE por igual. La pregunta frecuente (FAQ) #1252 responde a la pregunta "*¿Se aplican todos los requisitos de PCI DSS a todos los componentes del sistema?*" empezando con "*Los requisitos del PCI DSS se aplican a todos los componentes del sistema, a menos que se haya verificado que un requisito particular no es aplicable para un sistema en particular."* Nos referiremos a esta pregunta frecuente en el volumen 3 cuando analicemos cómo abordar cada uno de los requisitos. En general, los sistemas CDE están representados en ***rojo***.

CDE/CHD

El alcance de PCI DSS se presenta en la página 10 de la versión 3.2 del estándar. El primer párrafo dice:

> *Los requisitos de seguridad del PCI DSS se aplican a todos los componentes del sistema incluidos o conectados al entorno de datos del titular de la tarjeta. El entorno de datos del titular de la tarjeta (CDE) está compuesto por personas, procesos y tecnologías que almacenan, procesan o transmiten datos de titulares de tarjetas (CHD) o datos confidenciales de autenticación (SAD). Los "componentes del sistema" incluyen dispositivos de red, servidores, dispositivos informáticos y aplicaciones.*

Vamos a dividir este párrafo en sus aspectos importantes.

- "*aplica a todos **los componentes del sistema***"- agregando que "*incluyen dispositivos de red, servidores, dispositivos informáticos y aplicaciones.* " - así que básicamente, cualquier tipo de sistema informático (hardware, sistema operativo, software, aplicaciones) está sujeto a los requisitos.
- "*(CDE) está integrado de personas, procesos y tecnologías*" - entonces, mientras que el PCI DSS se aplica a los sistemas informáticos, las personas y los procesos también son fundamentales (y recomiendo, al igual que muchos otros, adoptar primero un enfoque de proceso de negocio).
- "*que almacena, procesa o transmite datos del titular de la tarjeta o datos de autenticación confidenciales*" - lo que a menudo se referirá como SPT CHD/SAD para resumir. Los sistemas que entran en contacto con CHD o SAD son los principales que estamos tratando de proteger, desde que almacenan o permiten acceso a la información (los bienes) que estamos obligados a proteger.

Todos estos sistemas que SPT CHD/SAD son parte, o forman las bases, de su CDE (Cardholder Data Environment - el entorno dentro del alcance para PCI). Nos referiremos a estos como sistemas CDE/CHD. La Guía de diciembre de 2016 se refiere a estos como "componentes del sistema almacena, procesa o transmite CHD/SAD". El OPST llama a estos tipos "1a".

CDE/Contaminated

En la sección de segmentación de red, el estándar establece que *"la segmentación de red de o el aislamiento (segmentación) del entorno de datos del titular de la tarjeta del resto de la red de una entidad no es un requisito de PCI DSS"*. Por lo tanto, no se requiere segmentación de red más que en el perímetro externo de la red. El estándar también agrega: "sin una adecuada segmentación de red (a veces llamada una 'red plana'), toda la red está dentro del alcance de la evaluación PCI DSS". Si usted no usa la segmentación, todo está sujeto a los requisitos de PCI DSS. Básicamente, su CDE se expande a todos los sistemas que están en la misma red que sus sistemas CDE/CHD dentro del alcance descrito anteriormente hasta que alguna segmentación lo impida.

Llamaremos a estos sistemas en las mismas zonas de red como CDE/contaminated (contaminados) ya que fácilmente podría haber una transferencia de información entre sistemas que no están restringidos de otra manera (generalmente mediante un firewall u otro dispositivo). La Guía de diciembre de 2016 se refiere a estos sistemas como *"componente del sistema está en el mismo segmento de red (por ejemplo, en la misma subred o VLAN) que el sistema (s) que almacena, procesa o transmite datos del titular de la tarjeta"*.

Segunda categoría: Segmenting (previamente llamada CDE/Segmenting)

La segunda categoría principal son los sistemas que proporcionan la segmentación (generalmente de red) y previenen la "contaminación" de los sistemas CDE. Típicamente, estos son dispositivos de firewall, pero no están limitados a esos. Estos dispositivos se llaman sistemas Segmenting. La definición del alcance incluye una instrucción a tal efecto (presente en versiones previas de PCI DSS): "Si existe una segmentación de la red y se usa para reducir el alcance de la evaluación PCI DSS, el asesor debe verificar que la segmentación sea adecuada para reducir el alcance de la evaluación".

Tenga en cuenta que esta función se puede lograr mediante una combinación de dispositivos y sistemas, pero cuanto más compleja sea, mejor será la documentación que necesitará su asesor.

En el OPST, estos serían "1b": o "2a", lo que podría generar confusión. Sin sistemas de segmentación, no podemos tener sistemas conectados. Por lo tanto, lo que la guía PCI SSC de diciembre de 2016 se refiere a estos como "El componente del sistema segmenta los sistemas CDE de sistemas y redes fuera del alcance", pero lo coloca en la categoría de sistemas conectados ("Sistemas conectados a o sistemas que impactan la seguridad") voy a marcarlo en su propia categoría para evitar cualquier confusión (este punto es mi único desacuerdo con el documento PCI SSC, pero esta diferencia es más estilística que cualquier otra cosa).

Además, esta segunda categoría está justificada por la inclusión de un nuevo requisito desde PCI DSS 3.0 con respecto a la prueba de segmentación durante las pruebas anuales de penetración interna requeridas (#11.3.4). La sección 3.3 (Segmentación de red) de la plantilla RoC PCI DSS 3.2 agrega documentación de que esta validación de segmentación adecuada sea realizada. Tenga en cuenta que las reglas de firewall que no están relacionadas con el entorno CDE estarían fuera del alcance. Esto podría suceder si el firewall administra el punto de conexión entre el CDE y varios otros segmentos de red. En ese caso, solo las reglas que pertenecen al acceso al CDE están dentro del alcance (para revisión), aunque sería una buena idea tratarlas a todas de la misma manera.

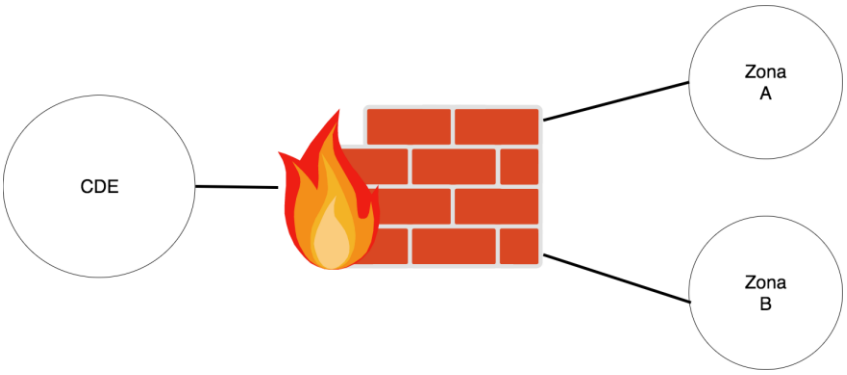

Figura 2 - Imagen del firewall y 3 zonas de red (incluyendo el CDE)

Por ejemplo, en el diagrama anterior, las reglas que limitan las conexiones entre la zona A y la zona B estarían fuera del alcance.

En última instancia, a menos que se utilice un dispositivo de segmentación sencillo como un firewall físico, las entidades deben proporcionar una evaluación que cubra el requisito #11.3.4 exigiendo pruebas de penetración de segmentación de red.

Los sistemas Segmenting generalmente están representados en naranja.

Segmentación en virtualización e informática en la nube

El suplemento "Guía de Informática en la nube de PCI DSS" cubre la segmentación en las secciones 4.4 a 4.4.3. Establece claramente: "La segmentación en una infraestructura de computación en la nube debe proporcionar un nivel equivalente de aislamiento como el que se puede lograr a través de la separación física de la red". Aunque se menciona la informática en la nube, esta es también la prueba de fuego para cualquier entorno virtual. Por lo tanto, una entidad debe "garantizar que su entorno esté adecuadamente aislado de los otros entornos de clientes". En términos de nubes o proveedores de alojamiento, el proveedor hace esa garantía, mientras que en los entornos internos esto sería validado por la entidad. Sin embargo, en última instancia, la responsabilidad de que la validación haya sido realizada (por alguien) depende de la entidad.

En la sección 4.4.1, se recomienda utilizar un "hipervisor de CDE dedicado" para simplificar el problema de la segmentación (el cual se hace más complejo en entornos de nube que en el alojamiento privado). Dedicar el hipervisor a los sistemas CDE (sin modo mixto) es también lo que muchos QSAs con los que he hablado usan como lineamientos mínimos.

Para obtener más detalles, consulte la sección 2.7 del volumen 2.

Tercera categoría: Sistemas connected (conectados)

Entonces, ¿cuándo un sistema CDE contamina a otro? Algunos casos son más fáciles de entender que otros. Por ejemplo, si dos sistemas están en el mismo segmento de red y pueden comunicarse más o menos libremente (dependiendo de los servicios abiertos), entonces está claro que puede haber contaminación (tenga en cuenta que la posibilidad es suficiente para garantizar la inclusión). Pero, ¿qué se requiere para que un sistema connected no se contamine? Vamos a separarlo en partes para resolverlo.

Sabemos que la comunicación entre los sistemas debe restringirse solo a los servicios requeridos para las operaciones comerciales (lo que se conoce como "acceso controlado") de acuerdo con el requisito #1.2.1. Ahora, no siempre podemos mantener todos los sistemas que necesitamos dentro de una sola zona, o estaríamos derrotando los objetivos de reducción de alcance a los que deberíamos aspirar. Entonces, ¿qué vamos a hacer en estos casos?

El estándar establece que cualquier dispositivo que esté "conectado al entorno de datos del titular de la tarjeta" (CDE) está dentro del alcance dado que no está completamente aislado. El estándar incluye en su alcance cualquier "sistema que pueda afectar la seguridad del CDE (por ejemplo, resolución de nombres o servidores de redirección web) ". Esta es probablemente una de las líneas más importantes escritas sobre el alcance en el estándar. Esto fue tratado en múltiples ocasiones en la presentación de RSA de 2013 y en la presentación de las reuniones de la comunidad de PCI (PCI community meetings) de 2013:

Si puede afectar la seguridad del CDE, está dentro del alcance
Recuerde que los sistemas que no son CHD también pueden estar dentro del alcance

y

Si un sistema "fuera del alcance" pudiera generar un compromiso del CDE, no debería haberse considerado fuera del alcance

Por lo tanto, si no estamos seguros de si un sistema está o no en el alcance (como un sistema "conectado"), debemos ver si un compromiso del sistema podría llevar a un ataque en un sistema CDE sin necesidad de comprometer primero otro sistema. Si es el caso, entonces este sistema está dentro del alcance. El segundo subtipo de sistemas conectados también abordará esto parcialmente.

En esta metodología, usamos aislado para indicar que dos sistemas no se pueden comunicar en absoluto el uno con el otro. Si la comunicación es limitada (nota: el uso de las reglas ANY - "cualquier" - o "genéricas" están prohibidas en PCI DSS), lo llamamos acceso controlado. Las presentaciones de la conferencia RSA confirman esto:

- *Para estar fuera del alcance: segmentación = aislamiento = sin acceso*
- *Acceso controlado ≠ aislamiento*
- *Acceso controlado:*
    - *Sigue siendo acceso*
    - *Es un requisito de PCI DSS*
    - *No aísla un sistema / red de otro*
    - *Proporciona un punto de entrada al CDE*
    - *Está dentro del alcance de PCI DSS*
        - *Verificar que los controles de acceso estén funcionando*
        - *Verificar que la conexión / punto de entrada sea seguro*

Los sistemas conectados a menudo se conocen como dispositivos de categoría 2 o tipo 2. Al igual que en el caso de CDE, existen diferentes tipos de dispositivos "conectados" que presentan un nivel de riesgo diferente. Los sistemas conectados generalmente están representados en **amarillo**. Examinemos esos tres subtipos.

Connected/Security

Existen sistemas tales como directorios de usuarios (Active Directory, LDAP), sistemas de administración de parches, sistemas de administración de vulnerabilidades, así como varios otros (esto no es una lista completa) que brindan 'servicios de seguridad'. En nuestras analogías físicas, estos serían guardias de seguridad que pueden emitir las llaves de la habitación, o podría ser el personal de limpieza que brinde servicios para esa habitación. Podemos llamar a estos sistemas connected/security.

La guía de diciembre de 2016 de la PCI DSS para el Alcance y Segmentación de red crea 3 categorías de sistemas que considero como Connected/Security en una sección que denominan "Sistemas conectados a o sistemas de seguridad que impactan la seguridad":

- El componente del sistema afecta la configuración o seguridad del CDE
- El componente del sistema proporciona servicios de seguridad al CDE
- El componente del sistema sostiene requisitos de PCI DSS

Considero que todos estos tipos de sistemas fueron incluidos inicialmente por mi modelo, pero la aclaración adicional del consejo PCI es bienvenida.

El OPST llama a estos tipo "2a".

Connected/Communicating Systems

Cualquier sistema que esté 'conectado' al CDE (a los sistemas CDE) se considera un sistema 'conectado'. La excepción son los sistemas que están en el "exterior" de los sistemas de segmentación, por ejemplo, cuando un elemento de segmentación también afecta el tráfico no relacionado con el CDE, como el descrito en la sección Segmenting y presentado en la Figura 2.

Algunos sistemas conectados (que tienen una conexión con sistemas CDE) pueden eventualmente ser excluidos del alcance, pero la entidad debe documentar formalmente una evaluación para determinar si se aplica PCI DSS. Podría ser un sistema que recibe información fuera del CDE sin posibilidad de reingreso. Por ejemplo, supongamos que tenemos un sistema conectado que recibe transferencias de información periódicas iniciadas desde un sistema CDE y que hemos asegurado que no se transmite CHD/SAD. El protocolo utilizado para la transferencia de datos es sftp (parte del conjunto de aplicaciones SSH). El tráfico se inicia desde el CDE, se carga un archivo al sistema conectado y después se cierra la conexión. A parte de devolver los mensajes de estado como parte del protocolo, no hay información que regrese al sistema CDE. Yo diría que el sistema conectado como se describe aquí podría descartarse fuera del alcance, ya que no puede tener un impacto en la seguridad del CDE (aunque puede estar justificada alguna herramienta DLP para evitar que se filtré información). La documentación del proceso de evaluación debe ser creada, mantenida y conservada, para ser presentada a su asesor. La Guía de diciembre de 2016 llama a estos sistemas "componente del sistema se conecta directamente con CDE". El OPST llama a estos "2b" o "2c"; No hago la distinción basada en la dirección del flujo, sino en los detalles de la comunicación.

Connected/Indirectly

También hay sistemas que no tienen acceso directo a los sistemas CDE (están aislados del CDE) que aún están dentro del alcance. En cambio, generalmente tendrían acceso a otros sistemas connected o segmenting y, a través de estos, podría afectar la seguridad del CDE. Un ejemplo clásico sería el de una estación de trabajo de administrador que puede administrar un dispositivo de seguridad (directorio de usuario, etc.) o información de alimentación ascendente del sistema a los sistemas conectados (por ejemplo, sistema de parchado, o una conexión http como se describió anteriormente). En el caso de un directorio de usuarios, un administrador podría potencialmente otorgarse a sí mismo (u otros) derechos a sistemas en el CDE e infringir la seguridad del CDE.

De hecho, el estándar establece que cualquier sistema que "pueda afectar la seguridad del CDE" está dentro del alcance. Podemos referirnos a estos sistemas como connected/indirectly. La Guía de diciembre de 2016 designa a estos sistemas "componente del sistema se conecta indirectamente a CDE". El OPST llama a este tipo "2x".

Cuarta categoría: sistemas out-of-scope (fuera del alcance)

Finalmente, cualquier sistema que no sea ni un sistema CDE ni connected se considera fuera del alcance del cumplimiento de PCI. Ese sistema debe estar completamente aislado (sin conexiones de ningún tipo) de los sistemas CDE, aunque puede interactuar con sistemas connected (e incluso puede residir en la misma zona de red con sistemas connected). Recuerde, sin embargo, que, si puede afectar la seguridad del CDE indirectamente a través de otro sistema connected, que es un sistema connected/indirectly y, por lo tanto, está dentro del alcance.

Los sistemas fuera del alcance generalmente están representados en **verde**. La Guía de diciembre de 2016 para el Alcance de PCI DSS y Segmentación de red proporciona 4 pruebas que deben aprobarse para

confirmar que un sistema está fuera del alcance (lo que equivale a garantizar que el sistema no caiga dentro de las categorías definidas previamente):

- El componente del sistema NO almacena, procesa o transmite CHD/SAD => de lo contrario sería un sistema CDE/CHD.
- El componente del sistema NO se encuentra en el mismo segmento de red o en la misma subred o VLAN que los sistemas que almacenan, procesan o transmiten CHD => de lo contrario, sería un sistema CDE/contaminated.
- El componente del sistema no se puede conectar o acceder a ningún sistema en el CDE => de lo contrario sería un sistema connected/communicating (aunque todavía sostengo que algunas conexiones podrían considerarse fuera del alcance si se puede demostrar que no representan ningún riesgo, como pings).
- El componente del sistema no puede obtener acceso al CDE ni afectar un control de seguridad del CDE a través de un sistema dentro del alcance => de lo contrario, este es un sistema connected/security o connected/indirectly.

El OPST llama a esta categoría "3".

Resumen de categorías

En resumen, existen cuatro tipos básicos de sistemas para propósitos de PCI DSS. El primer grupo es el entorno de datos del titular de la tarjeta (CDE). El segundo grupo es la segmentación de sistemas, que se requieren para habilitar a los otros grupos. El tercer grupo son los sistemas connected, aquellos sistemas que tienen alguna conexión directa o indirecta con el CDE (que la guía de diciembre de 2016 denomina "Sistemas conectados a o sistemas que impactan la seguridad"). El cuarto son sistemas fuera del alcance completamente aislados de los sistemas CDE. Para estos, siempre recuerde que "los sistemas que pueden afectar la seguridad del CDE (por ejemplo, resolución de nombres o servidores de redirección web)" siempre están dentro del alcance o, para decirlo en otras palabras: "Si puede afectar la seguridad del CDE, está dentro del alcance".

La clasificación es la clave para que no tengamos que aplicar los requisitos de PCI DSS a todos los sistemas.

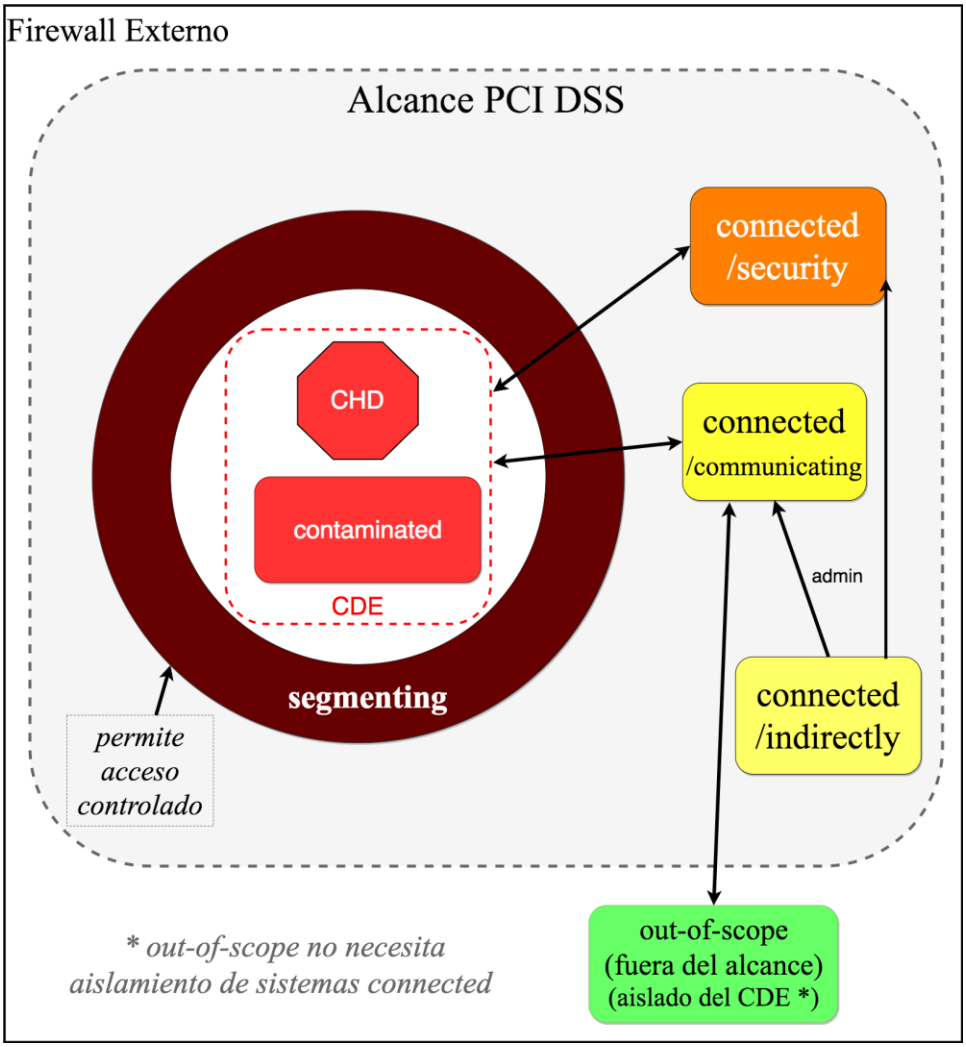

Figura 3 - Diagrama de los tipos de categorías del alcance PCI DSS

Tipo	Subtipo	Segmentación	CHD/SAD	Dentro del alcance
CDE	CHD	Ninguna	Si	Si
CDE	Contaminated	Ninguna	No	Si
Segmenting		Proporciona segmentación	No	Si
Connected	Communicating	Acceso controlado	No	Si
Connected	Security	Acceso controlado	No	Si
Connected	Indirectly	Aceso indirecto	No	Si
Out-of-scope		Aislamiento	No	No

Tabla 1 - Resumen de categorías de clasificación

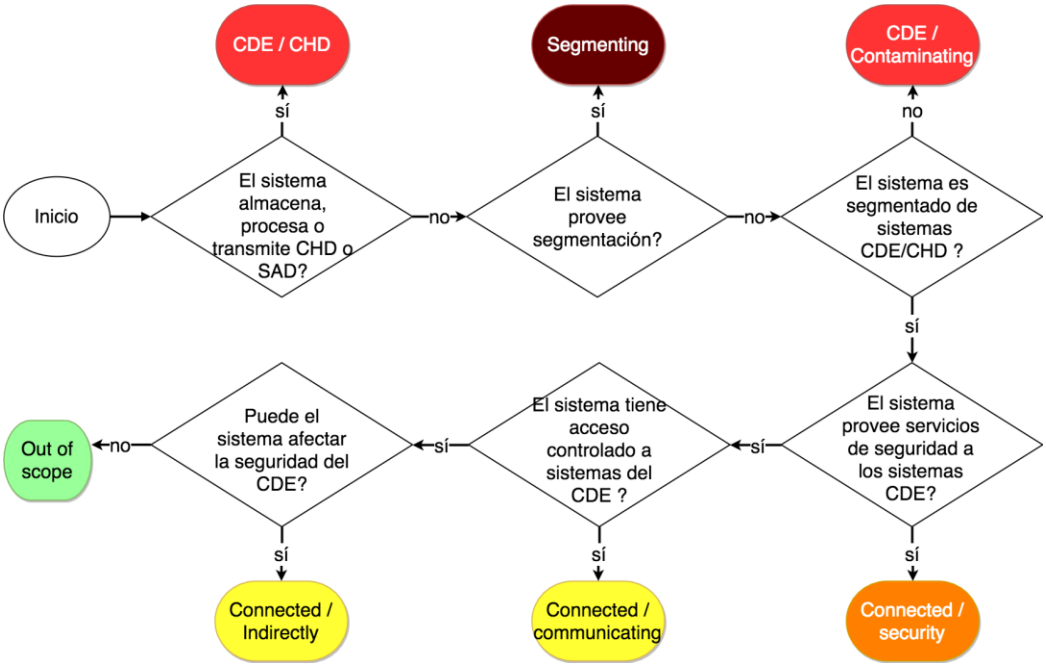

Figura 4 - Árbol de decisión del tipo de categorías del alcance PCI DSS

Enfoque de identificación de alcance y documentación de alcance

Ahora que hemos descrito el modelo de clasificación del alcance, tenemos que ver cómo debemos documentar adecuadamente el alcance. El enfoque sigue de cerca el modelo, con algunos elementos de validación agregados. Una vez más, las páginas 10 y 11 de la norma nos brindan el enfoque general, mientras que el Apéndice A3 (DESV) agregó más dirección de esta definición en los requisitos #A3.2.* (DE.2.* en DESV). Como tenemos 2 tipos de sistemas dentro del alcance (CDE y connected), dividiremos el proceso en dos partes, una para cada tipo.

Parte 1 - Identificación del CDE (un proceso de cuatro pasos)

Paso 1.1: Identificar todos los sistemas que almacenan, procesan o transmiten CHD o SAD (sistemas CDE/CHD). Estos incluyen servidores, estaciones de trabajo, dispositivos, equipos de red. El flujo de CHD debe documentarse en diagramas (#1.1.3) y se deben producir descripciones textuales detalladas (RoC #4.2). Los flujos de datos y la descripción deben cubrir captura, autorización, liquidación y reembolsos.

Paso 1.2 - Identificar dónde ocurre la segmentación (sistemas Segmenting). Los sistemas de segmentación previenen la contaminación y limitan el alcance del CDE. Las zonas CDE segmentadas e identificadas generalmente se representan en rojo en los diagramas de red.

Nota: Cada vez que implemente un nuevo tipo de segmentación, debe realizar pruebas de segmentación según lo exige el requisito #11.3.4 y confirmar su eficacia (y corregir problemas identificados) antes de implementar la nueva tecnología en la producción (también requerido en #A3.2.4).

Paso 1.3 - Identificar todos los otros sistemas dentro del CDE que son sistemas contaminados (CDE/contaminated). Este debería usar el inventario actual mantenido (requerido por #2.4) pero también incluir un descubrimiento de sistemas usando herramientas de escaneo (los barridos ping son típicos aquí). Cualquier diferencia con el inventario debe ser un indicio de un proceso de inventario fallando y se usa para revisar y corregir ese proceso. Los sistemas cubiertos incluyen servidores, estaciones de trabajo, dispositivos, equipos de red en las mismas zonas de red segmentadas o que se ejecutan bajo los mismos hipervisores de segmentación (más sobre hipervisores en la sección 2.7.1 del volumen 2 que cubre virtualización).

Nota: Dado que los sistemas CDE/contaminated brindan oportunidades potenciales de reducción de alcance, este paso puede usarse para revisar si tiene sentido mover el sistema fuera del CDE. Más sobre esto en el volumen 3 sobre TCO (Costo total de propiedad).

Paso 1.4 - Por último, validar que no tenemos otros PAN en otros sistemas (#A3.2.5) o ubicaciones. Este "descubrimiento de datos" generalmente se realiza utilizando herramientas especializadas (Data Loss Prevention, DLP) pero también funciona el simple 'grep' en Unix/Linux. Estas búsquedas generalmente usan expresiones regulares, pero el descubrimiento manual puede ser aplicable cuando se deben revisar pocos sistemas o en sistemas donde tales herramientas pueden no existir (por ejemplo, mainframes). Para aquellos que tienen recursos limitados, existen opciones económicas o incluso gratuitas.

El "descubrimiento de datos" debe realizarse en cualquier sistema con el potencial de almacenar PAN; como mínimo, esto debería cubrir todos los sistemas en el CDE y todos los sistemas connected (pero realmente debería incluir todos los servidores, computadoras de escritorio y computadoras portátiles). Si cualquier sistema está identificado con PAN, entonces las siguientes remediaciones son posibles:

- Considere el sistema como un sistema CDE/CHD y realice nuevamente los pasos de identificación previos
- Migre el sistema al CDE y vuelva a realizar los pasos anteriores
- Elimine de forma segura la CHD y determine por qué y cómo se transfirió el PAN al sistema o la ubicación para impedir una mayor expansión del alcance

En todos los casos, esto debe tratarse como un incidente de seguridad según los requisitos #12.10.*.

Nota 1: La versión 3.2 del PCI DSS aclaró el alcance de lo que se debe verificar cuando agrega la siguiente línea: "*Todos los tipos de sistemas y ubicaciones se deben considerar como parte del proceso de definición de alcance, incluidos los sitios de respaldo/recuperación y los sistemas de conmutación por error.* "

Nota 2: Este es también un momento apropiado para revisar el requisito #3.1 y el procedimiento de prueba #3.1.b para asegurar que los CHD se destruyan después del período de retención aprobado.

Parte 2: identifique los sistemas connected (un proceso de cinco pasos)

Una vez que el CDE ha sido debidamente validado, llega el momento de identificar los sistemas restantes dentro del alcance.

Paso 2.1: Revisar todas las reglas del firewall dentro del alcance (o el equipo equivalente que implementa las ACLs) de los sistemas de segmentación para identificar la lista de todos los sistemas que pueden conectarse al CDE. Si las reglas son para rangos de red en lugar de sistemas individuales, entonces será necesario usar una herramienta de descubrimiento del sistema para todo el rango (vea el paso 1.3 de la identificación de CDE). Tenga en cuenta que si una regla implica un sistema que ya no existe, entonces esa regla debe eliminarse según lo requerido por #1.1.7. El hecho de que un desmantelamiento no elimine un sistema de un conjunto de reglas de firewall debe tratarse como un incidente y solicitar una revisión del proceso de control de cambios. Con la lista completa, procederemos a clasificar estos sistemas de acuerdo con el modelo.

Paso 2.2 - Identificar cualquier sistema que proporcione servicios de seguridad o servicios que puedan afectar la seguridad del CDE y que se clasificarán como sistemas connected/security. Estos incluyen, como mínimo:

- Servicios de identidad y directorio (Active Directory, LDAP)
- Sistemas de nombres de dominio (DNS), sistemas de tiempo de red (NTP)
- Sistemas de gestión de parches
- Sistemas de gestión de vulnerabilidades
- Sistemas de gestión de antivirus
- Sistemas de gestión de integridad de archivos (FIM) o detección de cambios
- Sistemas de monitoreo de rendimiento
- Sistemas de gestión de claves de cifrado
- Sistemas de acceso remoto (VPN)
- Sistemas de autenticación multi-factor
- Sistemas para la gestión de registros y soluciones de monitoreo (SIEM, syslog, etc)
- Sistemas de Detección de Intrusos / Sistemas de Prevención de Intrusos (IDS/IPS)

Paso 2.3 - Identificar sistemas de terceros que pueden estar conectados al CDE a través de algún tipo de enlace de Internet o privado. Estos sistemas que están fuera de su control también están fuera del alcance, pero los proveedores externos deben ser controlados según lo establecido por los requisitos #12.8.*. Recuerde que si las conexiones pasan por equipos de red interna, como ruteadores, entonces estos equipos seguirán dentro del alcance.

Paso 2.4 - Identificar sistemas conectados que solo reciben información y que pueden (a través del análisis) considerarse fuera del alcance si no representan "ningún riesgo" para el CDE. Estos sistemas generalmente no pueden iniciar una conexión con el CDE y no tienen un reingreso al sistema iniciador (ping, o protocolo ICMP, puede ser una excepción). Este podría ser el caso de una conexión sftp, como se describió anteriormente. Tenga en cuenta que algunos protocolos (DNS, NTP) que podrían haberse considerado como fuera del alcance se han utilizado en brechas previas para filtrar la información. Sin embargo, en estos casos, IDS/IPS, DLP u otros controles en los puntos de conexión del CDE o en el sistema iniciador pueden ser más apropiados para monitorear la seguridad. El análisis debe documentarse exhaustivamente y esta documentación debe conservarse para su revisión por parte de su asesor (QSA, ISA, etc.).

Los sistemas restantes de la lista identificada en el primer paso son simplemente sistemas connected/communicating.

Paso 2.5 - Finalmente, identificar sistemas que están aislados del CDE pero que aún podrían afectar su seguridad, indirectamente a través de algún otro sistema conectado. Estos son obviamente clasificados como connected/indirectly. A menudo, estos son consolas administrativas o computadoras de escritorio/portátiles de administrador.

Guía adicional
La plantilla de informe RoC nos da más detalles sobre lo que debemos documentar. Nuestra documentación debe incluir la información en las siguientes subsecciones de las secciones 2, 3 y 4 de la plantilla de informes de RoC. Los que están marcados como "asesor" son para uso del asesor, no de la entidad, aunque el asesor podría ser interno, ya sea un ISA o alguien que produce un cuestionario de autoevaluación (SAQ).

Sección		**Detalle**
2	Resumen general	Título
2.1	Descripción del negocio de tarjetas de pago de la entidad	
2.2	Diagramas de red de alto nivel	PCI DSS 1.1.2
3	Descripción del alcance del trabajo y el enfoque adoptado	Título
3.1	Validación del asesor del entorno de datos del titular de la tarjeta (CDE) y precisión del alcance	Asesor
3.2	Visión general del entorno de datos del titular de la tarjeta (CDE)	Personas, Proceso, Tecnología
3.3	Segmentación de red	Cómo se implementa la segmentación
3.4	Detalles de los segmentos de red	Todas las zonas del CDE que contienen los sistemas que SPT CHD/SAD
3.5	Entidades conectadas para el procesamiento	PCI DSS 12.8.*
3.6	Otras entidades comerciales que requieren el cumplimiento de PCI DSS	
3.7	Resumen de redes inalámbricas	
3.8	Detalles de redes inalámbricas	
4	Detalles sobre el entorno revisado	Título
4.1	Diagramas de red detallados	PCI DSS 1.1.2
4.2	Descripción de los flujos de datos del titular de la tarjeta	PCI DSS 1.1.3
4.3	Almacenamiento de datos del titular de la tarjeta	Un subconjunto de sistemas CDE/CHD
4.4	Hardware crítico en uso en el entorno de datos del titular de la tarjeta	Sistemas CDE y connected/security
4.5	Software crítico en uso en el entorno de datos del titular de la tarjeta	Sistemas CDE y connected/security
4.6	Muestreo	Asesor
4.7	Conjuntos de muestra del informe	Asesor
4.8	Proveedores de servicios y otros terceros con los que la entidad comparte datos de titulares de tarjetas	PCI DSS 12.8.*
4.9	Aplicaciones / soluciones de pago de terceros	PA-DSS
4.1	Documentación revisada	Asesor
4.11	Individuos entrevistados	Asesor
4.12	Proveedores de servicios administrados	Incluido dentro del alcance o PCI DSS 12.8. *
4.13	Resumen de divulgación para respuestas "En el lugar con control de compensación" (Sí con CCW)	Asesor
4.14	Resumen de divulgación para respuestas "No probadas"	Asesor

Tabla 2 - Secciones de plantillas de informes RoC para la documentación del alcance

Las subsecciones marcadas como "Asesor" serían llenados por el asesor durante la evaluación de cumplimiento (RoC o SAQ). Los marcados como "Título" son simplemente encabezados.

Referencias:

Este modelo se basa en las páginas 10 y 11 del estándar y en algunos otros documentos:

- Una presentación del PCI SSC en la conferencia pública de RSA en 2013 [1] y una serie de diapositivas similares de las reuniones de la comunidad PCI (PCI community meetings) de 2013 (disponible para los evaluadores de PCI: QSA, ISA, PCIP)
- Respuestas del PCI SSC a las preguntas más frecuentes (FAQ) [2]
- Certificación suplementaria de entidades designadas para PCI DSS 3.1 (DESV, lanzado en junio de 2015) - Un conjunto de requisitos nuevos para aumentar la seguridad de que una entidad mantiene el cumplimiento de PCI DSS a lo largo del tiempo, y ese incumplimiento es detectado por un proceso continuo (incluso automatizado) de auditoría; este conjunto de requisitos se aplica a entidades designadas por las marcas de tarjetas o adquirentes que se encuentran en un alto nivel de riesgo para la industria. DESV ahora está integrado como Anexo A3 en PCI DSS 3.2. [3]
- Plantilla de informe RoC [4]
- Suplementos de información:
    - Mejores prácticas para mantener el cumplimiento de PCI DSS (publicado en agosto de 2014 pero actualizado en marzo de 2016) [5] (que es en muchos sentidos reemplazado por el DESV)
    - Protección de los datos de la tarjeta de pago a través del teléfono (Marzo de 2011) [6]
    - Garantía de Seguridad de Terceros [7] (Agosto de 2014)
    - Guía de informática en la nube PCI DSS 3.0 [8] (Abril de 2018)
    - Guía de virtualización PCI DSS v2.0 [9] (Junio de 2011)
    - Guía para el alcance del PCI DSS y la segmentación de la red [10] (Diciembre de 2016)

[1] (Alcance PCI DSS en conferencia RSA, 2013). menos es más - desmitificando el alcance de PCI DSS - Conferencia RSA. Obtenido el 2 de julio de 2015, de https://www.rsaconference.com/writable/presentations/file_upload/dsp-w21.pdf.
[2] (Preguntas frecuentes al PCI SSC). Preguntas frecuentes - PCI Security Standards Council. Obtenido el 2 de julio de 2015, de https://www.pcisecuritystandards.org/faq/.
[3] PCI DSS 3.2.1. Obtenido el 1 de julio de 2018, de https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.
[4] Plantilla de informe RoC. Obtenido el 1 de julio de 2018, de https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-ROC-Reporting-Template.pdf.
[5] (2014). Mejores prácticas para mantener el cumplimiento de PCI DSS. Obtenido el 2 de julio de 2015, de https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf.
[6] (2011). Proteger los datos de la tarjeta de pago a través del teléfono - PCI ... Obtenido el 2 de julio de 2015, de https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf.
[7] (2016) Garantía de seguridad de terceros v1.1 - PCI... Obtenido el 31 de mayo de 2016, de https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf.
[8] (2013) Guía de informática en la nube PCI DSS 3.0 - PCI Security... Obtenido el 1 de julio de 2018, de https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf.
[9] (2011) Guía de virtualización - PCI Security Standards Council. Obtenido el 13 de julio de 2015, de https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.
[10] (2017) Guía del alcance del consejo PCI - PCI Security Standards Council. Obtenido el 16 de enero de 2017, de https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf.

Historia de las versiones

Versión	Autor	Descripción	Fecha
1.0	Yves Desharnais	Versión inicial	Julio de 2015
1.1	Yves Desharnais	Aclaraciones, Formateo y Actualización a PCI DSS 3.2 y otros documentos actualizados del PCI SSC	Julio de 2016
1.2	Yves Desharnais	Aclaraciones y cambios relacionados al documento Guía del alcance del consejo PCI	Diciembre de 2017
1.2.1	Yves Desharnais	Cambios menores para PCI DSS 3.2.1, y versión inicial en español y francés	Julio de 2018

Autor:

Yves Desharnais, 8850895 CANADA INC.
Email: info@pciresources.com
Website: www.pciresources.com