Security Standards Council®

Estándar: Estándar de Seguridad de Datos PCI (PCI DSS)

Fecha: Mayo de 2017

Autor: PCI Security Standards Council

Información Complementaria:

Guía sobre el Alcance PCI DSS y Segmentación de la Red

Cambios en el Documento

Fecha	Versión del Documento	Descripción	Páginas
Diciembre de 2016	1.0	Versión inicial	Todas
Mayo de 2017	1.1	Corrección de errores tipográficos menores, aclaración menor de redacción (se agregó una nota al pie) en la Sección 3 y una corrección de errores en los diagramas de Flujo de Datos Lógicos del Escenario 1 y del Escenario 2 (en la leyenda, y en el diagrama y leyenda, respectivamente).	5, 10, 11, 17, 22

Tabla de Contenido

1 Introducción

Muchas organizaciones luchan por comprender dónde se requieren controles PCI DSS y qué sistemas deben protegerse. Este documento proporciona orientación para ayudar a las organizaciones a identificar los sistemas que, como mínimo, deben ser incluidos en el alcance PCI DSS. Además, el documento proporciona la guía sobre cómo puede utilizarse la segmentación para ayudar a reducir la cantidad de sistemas que requieren controles PCI DSS.

Cuando se trata de determinar el alcance PCI DSS, el enfoque más práctico es comenzar con la suposición de que todo está dentro del alcance hasta que se verifique lo contrario. Cuando se implementa correctamente, la segmentación de la red es *un método* que puede ayudar a reducir la cantidad de componentes del sistema dentro del alcance PCI DSS. Otros métodos también pueden ser efectivos para reducir el número de sistemas en los que se aplican los controles PCI DSS y/o el tamaño del CDE (como la subcontratación de un proveedor de servicios de terceros o el uso de una solución P2PE indicada en la lista PCI). *No obstante, estos métodos no son el tema de este documento.*

En la Sección 4 se incluyen ejemplos ilustrativos de algunos enfoques de segmentación comunes. Estos ejemplos resaltan los impactos y consideraciones del alcance PCI DSS en torno a los servicios compartidos (como los servicios de directorio) y brindan una guía para un alcance y una protección consistentes de CHD. Los ejemplos de este documento no representan la única forma en que puede utilizarse la segmentación para que tenga un impacto en el alcance PCI DSS y, de hecho podrán no ser efectivos para un sistema o una configuración de red determinados.

Solo porque un sistema no esté dentro del alcance PCI DSS no significa que la entidad deba dejar el sistema desprotegido, ya que podría representar un riesgo para la red y para la actividad comercial de la entidad. Un patrón común observado en las vulneraciones de datos ocurre cuando el atacante apunta a sistemas que la entidad considera fuera del alcance PCI DSS, y luego el atacante aprovecha esos sistemas para obtener acceso a más sistemas, lo que eventualmente proporcionan una ruta de acceso a los sistemas donde se pueden encontrar los datos CHD. Aunque la segmentación puede ayudar a reducir la cantidad de puntos de exposición al entorno de datos de tarjetahabientes (CDE), no es una solución milagrosa; la implementación de la segmentación no reemplaza el enfoque holístico que asegura la infraestructura de una organización.

1.1 Uso Previsto y Público Objetivo

Esta guía está destinada a cualquier entidad que busque comprender los principios del alcance y segmentación al aplicar PCI DSS a su entorno. Las recomendaciones proporcionadas en este documento pueden ser utilizadas por entidades grandes y pequeñas para evaluar qué componentes del sistema deben estar cubiertos por los requisitos PCI DSS. La guía no aborda la conformidad con PCI DSS. Las entidades deben ponerse en contacto directamente con su entidad adquirente (banco comercial) o con la marca de la tarjeta de pago, según corresponda, para obtener información sobre los programas de conformidad con la norma PCI DSS.

Esta guía también proporciona un método para facilitar debates eficaces sobre el alcance entre las entidades y es útil para:

- Comerciantes, adquirientes, emisores, proveedores de servicio - por ejemplo, procesadores de emisores y Proveedores de Servicios de Tokens (TSPs) y otros responsables de cumplir con los requisitos PCI DSS de su empresa
- Evaluadores (como los Evaluadores de Seguridad Calificados o los Evaluadores de Seguridad Internos) encargados de realizar las evaluaciones PCI DSS
- Adquirentes que evalúan los Informes PCI DSS de Conformidad de comerciantes o proveedores de servicios o Cuestionarios de Autoevaluación

- Investigadores Forenses de PCI (PFIs) responsables de determinar el alcance PCI DSS como parte de una investigación.

Esta guía está prevista para que sea utilizada como complemento de PCI DSS pero no anula ni reemplaza los requisitos PCI DSS. Aclara los principios del alcance y proporciona una guía que puede aplicarse a una variedad de situaciones.

En última instancia, cada entidad es responsable de tomar sus propias decisiones sobre el alcance PCI DSS, de diseñar una segmentación efectiva (si se utiliza) y de garantizar la conformidad de sus propias PCI DSS y los requisitos de validación relacionados. Seguir esta guía no garantiza que se haya implementado una segmentación efectiva, ni tampoco la conformidad con PCI DSS.

1.2 Terminología

A lo largo de este documento se utilizan los siguientes términos y acrónimos:

- CDE - Entorno de Datos de Tarjetahabientes
- CHD - Datos de Tarjetahabientes
- SAD - Datos Sensibles de Autenticación
- Datos de Tarjetahabientes - Datos del titular de la tarjeta y/o datos sensibles de autenticación

Las definiciones de estos términos se proporcionan en el Glosario de Términos, Abreviaturas y Acrónimos de PCI DSS y PA-DSS.

2 Cómo Entender el Alcance y la Segmentación para el PCI DSS

En un nivel alto, el alcance implica la identificación de personas, procesos y tecnologías que interactúan con la seguridad de CHD o que de otro modo podrían afectarla. La segmentación involucra la implementación de otros controles para separar los sistemas con diferentes necesidades de seguridad. Por ejemplo, con el fin de reducir la cantidad de sistemas dentro del alcance PCI DSS, se puede utilizar la segmentación para mantener los sistemas que están dentro del alcance separados de los sistemas que están fuera del alcance. La segmentación puede consistir en controles lógicos, controles físicos o una combinación de ambos. Entre los ejemplos de métodos de segmentación utilizados habitualmente para reducir el alcance PCI DSS se incluyen los cortafuegos y las configuraciones de enrutadores para impedir el paso de tráfico entre las redes fuera del alcance y el CDE, las configuraciones de red que impiden las comunicaciones entre diferentes sistemas y/o subredes, y los controles de acceso físico.

Los tipos de tecnologías utilizadas para la segmentación generalmente se utilizan para gestionar el acceso entre sistemas o redes que están dentro del alcance. Por ejemplo:

> Para cumplir el Requisito 1.2.1 PCI DSS, una entidad puede instalar un cortafuegos de red entre el CDE y la red corporativa para garantizar que sólo los sistemas designados de la red corporativa puedan comunicarse, a través de puertos aprobados con los sistemas del CDE. Además, la entidad podrá utilizar el mismo cortafuegos u otro para bloquear todas las conexiones y evitar el acceso entre el CDE y una red fuera del alcance. De este modo, se está utilizando un cortafuegos para implementar un requisito PCI DSS para los sistemas y la red dentro del alcance, y también se utiliza para segmentar una red fuera del alcance.

Tenga en cuenta que cuando se utilizan tecnologías para gestionar el acceso entre sistemas y redes con el fin de cumplir los requisitos PCI DSS, esto no se considera una segmentación que reduzca el alcance PCI DSS. Mientras que continúan estando dentro del alcance PCI DSS, estas comunicaciones son potencialmente más seguras que los canales de comunicación no controlados.

Los principios de alcance y segmentación se describen en la sección "Alcance de los Requisitos PCI DSS" de PCI DSS. A continuación se proporcionan algunos extractos de esta sección con guías adicionales.

Alcance de los Requisitos PCI DSS

> *Los requisitos de seguridad PCI DSS se aplican a todos los componentes del sistema incluidos o conectados al entorno de datos de tarjetahabientes. El entorno de datos de tarjetahabientes (CDE) está compuesto por personas, procesos y tecnologías que almacenan, procesan, o transmiten datos de tarjetahabiente o datos de autenticación sensibles.*[1]

El CDE de una organización es solo el punto de inicio para determinar el alcance general PCI DSS. Un alcance preciso PCI DSS implica una evaluación crítica de los flujos CDE y CHD, así como de todos los componentes del sistema conectados y de soporte para determinar la cobertura necesaria de los requisitos PCI DSS. Los sistemas con conectividad o acceso a o del CDE son considerados “conectados a” los sistemas. Estos sistemas tienen una vía de comunicación a uno o más componentes del sistema en el CDE. La conectividad puede ocurrir en varias tecnologías, que incluyen físicas, inalámbricas y de virtualización.

- La conectividad física puede ser a través de una red tradicional (por ejemplo, Ethernet o comunicación por cable eléctrico) o por una conexión directa de un sistema a otro (por ejemplo, USB, componente, etc.).

[1] PCI DSS v3.2, página 10

- La conectividad inalámbrica utiliza diferentes ondas y frecuencias de radio como su mecanismo de transporte (por ejemplo, LANs inalámbricas, GPRS, Bluetooth y tecnologías celulares). Las tecnologías inalámbricas generalmente están conectadas a una red física.
- La conectividad de virtualización incluye el uso de redes virtuales, máquinas virtuales, cortafuegos virtuales, interruptores virtuales, etc. Los dispositivos virtuales generalmente comparten recursos comunes, como un sistema host o hipervisor subyacente, que podría ser utilizado para conectar una partición lógica a otra.

La implementación de estas tecnologías puede ser muy compleja. Por lo tanto es muy importante que alguien que entienda la tecnología en uso evalúe el impacto de estas tecnologías en el alcance.

Es importante comprender los riesgos e impactos si los componentes del sistema conectados quedan excluidos o pasados por alto del alcance PCI DSS. Los compromisos de los componentes del sistema conectados a menudo conducen al compromiso del CDE y al robo del CHD.

Siempre se aplican los siguientes conceptos de alcance:

- Los sistemas ubicados dentro del CDE están dentro del alcance, al margen de su funcionalidad o el motivo por el que se encuentran en el CDE.
- Del mismo modo, los sistemas que se conectan a un sistema del CDE están dentro del alcance, independientemente de su funcionalidad o de la razón por la que tienen conectividad con el CDE.
- En una red plana, todos los sistemas están dentro del alcance si alguno de ellos almacena, procesa o transmite datos de tarjetahabientes.

Tenga en cuenta que las redes públicas, no confiables (por ejemplo, Internet), no están dentro del alcance PCI DSS. Sin embargo, se deben implementar los requisitos PCI DSS para proteger los sistemas y datos dentro del alcance de redes no confiables de la entidad.

Segmentación de la Red

La segmentación de la red o el aislamiento (segmentación) del entorno de datos de tarjetahabientes del resto de la red de una entidad no es un requisito PCI DSS. Sin embargo, se recomienda encarecidamente como método que puede reducir:

- *El alcance de la evaluación PCI DSS*
- *El costo de la evaluación PCI DSS*
- *El costo y la dificultad de implementar y mantener controles PCI DSS*
- *El riesgo de la organización (se reduce consolidando los datos del titular de la tarjeta en menos ubicaciones más controladas)*

Sin una segmentación adecuada de la red (a veces denominada una «red plana»), toda la red está dentro del alcance de la evaluación PCI DSS.[2]

La intención de la segmentación es evitar que los sistemas fuera del alcance puedan comunicarse con los sistemas del CDE o afectar a la seguridad del CDE. La segmentación generalmente se logra con tecnologías y controles de procesos que implementan una separación entre el CDE y los sistemas que están fuera del alcance. Cuando se implementa correctamente, un componente del sistema segmentado (fuera del alcance) no podría afectar a la seguridad del CDE, incluso si un atacante obtuviera acceso administrativo en ese sistema fuera del alcance.

[2] PCI DSS v3.2, página 11

Tenga en cuenta que está permitida la conectividad o el acceso al CDE desde sistemas que están fuera del CDE. Sin embargo, toda esa conectividad está dentro del alcance PCI DSS y se aplican todos los requisitos PCI DSS correspondientes para asegurar esa conexión o acceso.

La existencia de segmentos de red separados por sí solos no crea automáticamente la segmentación PCI DSS. La segmentación se logra a través de controles diseñados específicamente para crear y hacer cumplir la separación y para evitar que los compromisos que se originan en la(s) red(es) fuera del alcance lleguen a CHD.

Es importante señalar que no existe ninguna solución o tecnología que elimine todos los requisitos PCI DSS. Las herramientas y tecnologías (como el cifrado o la tokenización) pueden ayudar a reducir el riesgo, reducir la aplicación de algunos requisitos PCI DSS, reducir el tamaño del CDE o ayudar a cumplir los requisitos PCI DSS con mayor facilidad.

Para poder apoyar la seguridad continua, dichas tecnologías deben implementarse adecuadamente con ajustes de configuración y procesos específicos que garanticen una gerencia segura y continua de la tecnología. Estos controles deben formar parte de la verificación y las pruebas anuales para confirmar que funcionan efectivamente

2.1 Proveedores de Servicios y otros Terceros

Además de incluir sistemas y redes internos en el alcance, todas las conexiones de entidades de terceros (por ejemplo, socios comerciales, entidades que brindan servicios de apoyo remoto y otros proveedores de servicios) deben identificarse para determinar la inclusión en el alcance PCI DSS Una vez identificadas las conexiones dentro del alcance, deben implementarse los controles PCI DSS aplicables para reducir el riesgo de que se utilice una conexión de terceros que comprometa el CDE de una entidad.

Del mismo modo, si una entidad subcontrata funciones o instalaciones incluidas en el alcance a terceros, o utiliza un servicio de terceros que repercute en la forma en que cumple los requisitos PCI DSS, la entidad tendrá que trabajar con los terceros para garantizar que los aspectos aplicables del servicio se incluyen en el alcance PCI DSS, ya sea para la entidad o para el proveedor del servicio. También es importante que ambas partes entiendan claramente qué requisitos PCI DSS proporciona el proveedor de servicios y cuáles son responsabilidad de la entidad que utiliza el servicio. Véase el Requisito 12.8 PCI DSS.

Consulte la Información Complementaria PCI SSC: Garantías de Seguridad de Terceros[3] para obtener una guía sobre la gestión de relaciones con terceros.

2.2 Responsabilidad de Confirmar el Alcance

Es importante comprender la naturaleza compartida de la confirmación de que el alcance PCI DSS se ha definido con precisión. PCI DSS indica lo siguiente:

La entidad es la responsable de asegurar que su alcance se mantenga correctamente de forma continua.

> *Por lo menos una vez al año y antes de la evaluación anual, la entidad evaluada debe confirmar la precisión de su alcance PCI DSS, mediante la identificación de todas las ubicaciones y flujos de datos de tarjetahabientes, e identificar todos los sistemas que están conectados o que, en caso de verse comprometidos, podrían afectar al CDE (por ejemplo, los servidores de autenticación), para asegurarse de que ellos se han incluido en el alcance PCI DSS.*

[3] Disponible en el Sitio Web PCI SSC: https://www.pcisecuritystandards.org/document_library

> *La entidad conserva la documentación que muestra cómo se determinó el alcance PCI DSS. La documentación se conserva para la revisión del evaluador y/o como referencia durante la próxima confirmación anual del alcance PCI DSS. Para cada evaluación PCI DSS, el evaluador debe validar que el alcance de la evaluación esté definido y documentado con precisión*.[4]

Esto significa que, si bien la entidad evaluada es responsable de determinar anualmente el alcance PCI DSS y confirmar su exactitud, el evaluador que realiza la validación PCI DSS es responsable de confirmar que el alcance se ha definido y documentado adecuadamente. El evaluador deberá cuestionar las decisiones sobre el alcance si alguna no está clara en la documentación de la entidad evaluada. En estos casos, el evaluador deberá trabajar de forma colaborativa con la entidad para comprender la decisión tomada sobre el alcance.

> *Si la segmentación de la red está implementada y se utiliza para reducir el alcance de la evaluación PCI DSS, el evaluador debe verificar que la segmentación sea adecuada para reducir el alcance de la evaluación.*[5]

Todos los controles de segmentación también deben someterse a pruebas de penetración al menos una vez al año según el Requisito 11.3.4 PCI DSS[6], para garantizar que los controles implementados continúen proporcionando una segmentación efectiva.

[4] PCI DSS v3.2, página 10
[5] PCI DSS v3.2, página 11
[6] A partir del 1 de febrero de 2018, los proveedores de servicios deberán realizar pruebas de penetración por lo menos cada seis meses para verificar los controles de la segmentación.

3 Definición del Alcance y Categorías

En el glosario de Términos, Abreviaturas y Acrónimos de PCI DSS y PA-DSS, el alcance se define como: "Proceso de identificación de todos los componentes, personas y procesos del sistema que se incluirán en una evaluación PCI DSS. El primer paso de una evaluación PCI DSS es determinar con precisión el alcance de la revisión."

Un alcance preciso implica evaluar críticamente el CDE y los componentes del sistema conectados para determinar la cobertura necesaria para los requisitos PCI DSS.

Un ejercicio típico de alcance puede incluir lo siguiente:

Actividad	Descripción
Identificar cómo y dónde la organización recibe CHD.	1. Identificar todos los canales y métodos de pago para aceptar CHD, desde el punto en el que los CHD son recibidos hasta el punto de su destrucción, eliminación o transferencia.
Localizar y documentar dónde se almacenan, procesan y transmiten datos de tarjetahabientes.	2. Documentar todos los flujos de CHD e identificar a las personas, procesos y las tecnologías involucrados en el almacenamiento, procesamiento y/o transmisión de CHD. Estas personas, procesos y tecnologías son todos parte del CDE[7].
Identificar todos los demás componentes del sistema, procesos y personal que estén dentro del alcance.	3. Identificar todos los procesos (tanto empresariales como técnicos), los componentes del sistema y el personal con capacidad para interactuar o influir en el CDE (tal y como se ha identificado en el punto 2, más arriba). Estas personas, procesos y tecnologías están dentro del alcance, ya que tienen conectividad al CDE o podrían tener algún impacto en la seguridad de los CHD de otra manera.
Implementar controles para minimizar el alcance a componentes, procesos y personal necesarios.	4. Implementar controles para limitar la conectividad entre el CDE y otros sistemas dentro del alcance a solo la necesaria. 5. Implementar controles para segmentar el CDE de personas, proceso y tecnologías que no necesitan interactuar con el CDE ni influir en él.
Implementar todos los requisitos PCI DSS aplicables.	6. Identificar e implemente los requisitos PCI DSS aplicables a los componentes del sistema, los procesos y el personal del alcance.
Mantener y monitorear.	7. Implementar procesos para garantizar que los controles de la PCI DSS sigan siendo efectivos día tras día. 8. Asegurarse de que las personas, los procesos y las tecnologías incluidos en el alcance se identifican con precisión cuando se realicen cambios.

[7] Aunque que las personas que participan en el almacenamiento, procesamiento o transmisión de datos de tarjetahabientes son parte del CDE, al implementar la segmentación para el alcance PCI DSS, estas personas no tienen que ser segmentadas o aisladas de las personas que están fuera del CDE. Esto se debe a que los procesos y tecnologías existentes implementados para mantener la segmentación también aseguran que las personas en el CDE sean las únicas con el acceso requerido.

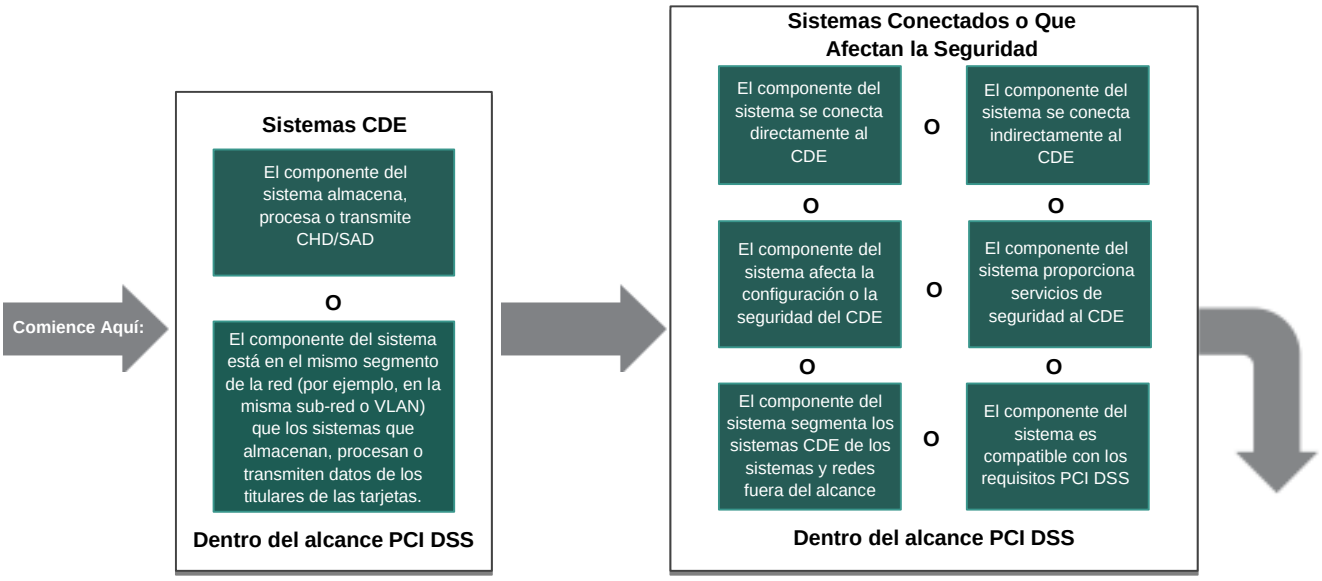
Tenga en cuenta que estar dentro del alcance no significa que todos los requisitos PCI DSS se apliquen a un determinado componente del sistema; los requisitos PCI DSS[8] aplicables dependen de la función y/o ubicación del componente del sistema.

El diagrama y la tabla de esta sección ilustran cómo pueden categorizarse los componentes del sistema utilizando varios factores:

- Si se están almacenando, procesando o transmitiendo datos de tarjetahabientes (CHD/SAD).
- La conectividad entre el componente del sistema y el CDE.
- Si un componente del sistema impacta la seguridad del CDE.

Las categorías que aquí se proporcionan son sólo ejemplos e ilustran una forma de considerar los diferentes componentes y el impacto en el alcance PCI DSS. Las entidades pueden seguir este enfoque o utilizar otro proceso de evaluación, a su discreción. El uso de estas categorías no es obligatorio.

FIGURA 1 – Categorías del Alcances PCI DSS



En este enfoque, los componentes del sistema sólo pueden categorizarse *en una* de estas categorías. Estas categorías son jerárquicas, con los Sistemas CDE como la categoría más alta que debe considerarse en

[8] Las entidades elegibles para el SAQ que cumplan con todos los criterios para un SAQ en particular pueden considerar que los requisitos aplicables son aquellos identificados dentro de ese SAQ.

primer lugar; si un sistema cumple alguno de los criterios de los Sistemas CDE, es un sistema CDE independientemente de si también cumple la descripción de una categoría inferior. La siguiente categoría incluye sistemas conectados y que tienen un impacto en la seguridad; esta categoría tiene prioridad y se evalúa antes de que se considere la categoría de los sistemas fuera del alcance. Para ser considerado fuera de alcance, un sistema debe cumplir TODOS los criterios de la categoría fuera de alcance y NINGUNO de los criterios de una categoría superior.

La siguiente tabla contiene más detalles sobre cada categoría:

Tipo de Sistema	Descripción	Alcance y Aplicabilidad
Sistemas del CDE	• El componente del sistema almacena, procesa o transmite CHD/SAD. O • El componente del sistema se encuentra en el mismo segmento de red; por ejemplo, en la misma subred o VLAN que el sistema o sistemas que almacenan, procesan o transmiten CHD/SAD.	**Estos sistemas:** • Están dentro del alcance PCI DSS. • Deben ser evaluados para determinar la aplicabilidad de cada[9] requisito PCI DSS.
Sistemas Conectados y/o que Afectan la Seguridad	• El componente del sistema se encuentra en una red diferente (o subred o VLAN), pero puede conectarse o acceder al CDE (por ejemplo, a través de la conectividad de red interna). O • El componente del sistema puede conectarse o acceder al CDE a través de otro sistema (por ejemplo, mediante la conexión a un servidor de salto que proporcione acceso al CDE). O • El componente del sistema puede tener un impacto en la configuración o seguridad del CDE, o en la forma en que se manejan los CHD/SAD, por ejemplo, un servidor de redireccionamiento web o un servidor de resolución de nombres. O • El componente del sistema proporciona servicios de seguridad al CDE; por ejemplo, filtrado del tráfico de la red, distribución de parches o gestión de autenticaciones. O • El componente del sistema apoya los requisitos PCI DSS, tales como los servidores de tiempo y los servidores de almacenamiento de registros de auditoría. O ▪ El componente del sistema proporciona la segmentación del CDE de sistemas y redes fuera del alcance, por ejemplo, cortafuegos configurados para bloquear el tráfico de redes no confiables.	**Estos sistemas:** • Están dentro del alcance PCI DSS. Incluso cuando una conexión se limita a puertos o servicios específicos en sistemas determinados, dichos sistemas se incluyen en el alcance para verificar que se han implementado los controles de seguridad aplicables. • Deben evaluarse para determinar la aplicabilidad de cada requisito[9] PCI DSS. • No deben proporcionar una ruta de acceso entre sistemas del CDE y sistemas fuera del alcance.

[9] Las entidades elegibles para el SAQ que cumplan con todos los criterios de un SAQ en particular pueden considerar que los requisitos aplicables son aquellos identificados en ese SAQ.

Tipo de Sistema	Descripción	Alcance y Aplicabilidad
Sistemas Fuera del Alcance	• El componente del sistema NO almacena, procesa o transmite CHD/SAD. Y • El componente del sistema NO está en el mismo segmento de la red o en la misma subred o VLAN que los sistemas que almacenan, procesan o transmiten CHD. Y • El componente del sistema no puede conectarse o acceder a algún sistema del CDE. Y • El componente del sistema no puede obtener acceso al CDE ni puede tener un impacto en un control de seguridad del CDE a través de un sistema que está dentro del alcance. Y • El componente del sistema no cumple con ninguno de los criterios descritos para sistemas conectados o que tengan algún impacto en la seguridad, como se indica arriba. ***Nota:*** *Estos sistemas no están dentro del alcance PCI DSS, pero aún podrían representar un riesgo para el CDE si no se aseguran. Se recomienda enfáticamente que se implementen las mejores prácticas de seguridad para todos los sistemas/redes que están fuera del alcance.*	**Sistemas Fuera del Alcance:** • No están dentro del alcance PCI DSS; por lo tanto, no se requieren los controles PCI DSS. • No tienen acceso a ningún sistema del CDE; si hay algún acceso, el sistema está dentro del alcance. • Son considerados no confiables (o «públicos»): no hay garantías de que se hayan asegurado correctamente. • Si en la misma red (o subred o VLAN), que de cualquier modo tienen conectividad con un sistema conectado que afecte la seguridad, deben implementarse controles para evitar que el sistema que está fuera del alcance obtenga acceso al CDE a través de sistemas que están dentro del alcance. Estos controles deben validarse por lo menos una vez al año.

3.1 Verificación de la segmentación de sistemas que están fuera del alcance

Para que se considere fuera del alcance, un componente del sistema no debe tener acceso a ningún sistema del CDE. Es posible que un sistema fuera del alcance se encuentre en el mismo segmento de red o subred que un sistema conectado o que afecte a la seguridad, siempre y cuando el sistema fuera del alcance no pueda acceder al CDE, ni a través del sistema dentro del alcance ni a través de ningún otro método.

Para que un sistema se considere fuera del alcance, deben colocarse controles que proporcionen una garantía razonable de que el sistema fuera del alcance no puede utilizarse para comprometer un componente del sistema dentro del alcance, ya que el sistema dentro del alcance podría entonces utilizarse para obtener acceso al CDE o afectar a la seguridad del CDE. Ejemplos de controles que podrían aplicarse para evitar que los sistemas fuera de alcance comprometan un sistema conectado o que afecte la seguridad incluyen:

- Cortafuegos del servidor y/o sistema de detección y prevención de intrusiones (IDS/IPS) en sistemas que están dentro del alcance que bloquean intentos de conexión de sistemas que están fuera del alcance.
- Controles de acceso físico que permitan que solo usuarios designados accedan a sistemas que están dentro del alcance.
- Controles de acceso lógico que permiten que solo los usuarios designados inicien sesión en los sistemas dentro del alcance.
- Autenticación de múltiples factores en sistemas que están dentro del alcance.
- Restringir los privilegios de acceso administrativo a los usuarios y sistemas/redes designados.
- Monitorear activamente si hay comportamientos sospechosos en la red o en el sistema que pudieran indicar que un sistema fuera del alcance está intentando acceder a un componente del sistema dentro del alcance o al CDE.

Estos ejemplos no son exhaustivos ni pueden aplicarse a todos los escenarios. La intención de tales controles es proporcionar una garantía razonable de que un sistema fuera del alcance no puede aprovechar un componente del sistema dentro del alcance para obtener acceso al CDE o afectar a la seguridad del CDE. Los controles utilizados para proporcionar esta garantía forman parte de la verificación global de la segmentación. Una vez verificados todos los controles de la segmentación, los sistemas podrán ser considerados fuera del alcance PCI DSS.

Seguridad de Sistemas y Redes que están Fuera del Alcance

Aunque no es obligatorio implementar controles PCI DSS en los sistemas fuera del alcance, se recomienda encarecidamente como una buena práctica, evitar que los sistemas fuera del alcance se utilicen con fines maliciosos. Ejemplos de controles que pueden ayudar a reducir el riesgo incluyen minimizar el acceso entre sistemas que están fuera del alcance y redes públicas a solo lo necesario, manteniendo los sistemas hasta la fecha con parches de seguridad y software antivirus, utilizando mecanismos de detección de cambios (por ejemplo, software de monitoreo de integridad de los archivos) e implementando controles de acceso en base a una fuerte autenticación y a los menores privilegios.

Nota: *Proteger los sistemas/redes fuera del alcance no los coloca dentro del alcance de los requisitos de PCI DSS. No obstante, si esos controles además evitan que los sistemas que están fuera del alcance accedan al CDE, los controles deben incluirse en la verificación de la segmentación.*

4 Ejemplo de Implementaciones de Segmentación: Servicios Compartidos

Los ejemplos de esta sección ilustran solo dos tipos de situaciones; hay muchas otras opciones de implementación y configuración que podrían aplicarse para segmentar el CDE desde sistemas que están fuera del alcance. Una implementación determinada no tiene por qué cumplir los criterios expuestos en estos ejemplos: una implementación puede necesitar más o menos controles en función del entorno específico. Dado que todos los entornos y organizaciones son diferentes, estos ejemplos se han simplificado para proporcionar claridad en relación con el tema de los límites del alcance.

Los siguientes ejemplos no abordan el riesgo de que un atacante comprometa u obtenga acceso a una cuenta de administrador en la red fuera del alcance, y luego utilice esa cuenta para obtener acceso al CDE. Para mitigar el riesgo de este tipo de ataques, la capacidad de utilizar cuentas de administradores y usuarios debe limitarse a los sistemas y segmentos de la red para los cuales el personal administrador tiene un rol administrativo específico asignado. De esta manera, una cuenta comprometida en una red que está fuera del alcance no puede ser aprovechada para obtener acceso a otros sistemas, redes o al CDE.

Para que la segmentación de los sistemas fuera del alcance sea efectiva, deben implementarse controles rigurosos para monitorear y hacer cumplir la separación. El registro diligente y la supervisión de eventos son esenciales para detectar y responder a los fallos en los controles de segmentación que podrían dar lugar a un acceso no autorizado al CDE desde la red que está fuera del alcance.

Los siguientes principios aplican tanto al Ejemplo 1 (detallado en la Sección 5.1) como al Ejemplo 2 (Sección 5.2):

- Se definen tres zonas de red diferentes:
  - LAN Corporativa
  - Servicios Compartidos
  - CDE
- Las reglas para cortafuegos y enrutadores aseguran que:
  - Las únicas conexiones permitidas dentro y fuera del CDE son las de los Servicios Compartidos, a través de puertos y sistemas específicamente designados, y solo cuando existe una necesidad comercial documentada.
  - Todos los intentos de conexión entre la LAN Corporativa y el CDE se bloqueen activamente (no se permite la entrada en el CDE de tráfico originado en la LAN corporativa).
  - Las comunicaciones entre los Servicios Compartidos y la LAN Corporativa:
    - Sólo se permiten entre sistemas, puertos, servicios, etc. designados, y se bloquean todos los demás intentos de conexión.
    - Están limitados por las necesidades de la empresa; por ejemplo, la conectividad entre las estaciones de trabajo y un Servidor de Directorio se limita únicamente al tráfico de autenticación de red.
- Los CHD no se almacenan, procesan ni transmiten fuera del CDE excepto a través de conexiones de red seguras con el banco/procesador adquirente (no se muestra en los diagramas).
- Se aplican todos los requisitos PCI DSS correspondientes:
  - A las redes y componentes del sistema del CDE y de los Servicios Compartidos
  - Para administrar y asegurar la conectividad entre el CDE y los Servicios Compartidos, incluyendo cortafuegos, ACLs, IDS/IPS, antimalware y otras herramientas y técnicas de defensa de amenazas
  - Para administrar y asegurar el tráfico entrante/saliente entre los Servicios Compartidos y la LAN Corporativa.

- El acceso físico al CDE y a la red de Servicios Compartidos se restringen al personal designado específicamente, como lo defina la necesidad comercial.
- Todos los controles que establecen la segmentación se incluyen en cada evaluación PCI DSS para validar su efectividad, incluidos los que limitan las conexiones a puertos o servicios específicos en sistemas específicos.
- Se monitorean e inspeccionan activamente el tráfico y la actividad entre Servicios Compartidos y el CDE y dentro del CDE, para detectar anomalías y reducir el riesgo de que un compromiso de los Servicios Compartidos lleve a un riesgo del CDE.

4.1 Ejemplo 1: "Conectado a" Servicios Compartidos

Nota: *Este ejemplo y los diagramas relacionados son únicamente para propósitos ilustrativos. Cada red es diferente y las técnicas de segmentación que funcionan bien en una red podrán no funcionar en otra. Por lo tanto, cualquier método de segmentación utilizado deberá probarse minuciosamente según los requisitos PCI DSS para confirmar que funciona de la forma esperada y continúe proporcionando una segmentación efectiva en ese entorno. Del mismo modo, los controles aquí señalados son adicionales a PCI DSS y pueden no ser obligatorios o necesarios para todos los entornos.*

Los "Servicios Compartidos" son componentes comunes del sistema que proporcionan servicios, tales como la autenticación y el apoyo administrativo en los componentes del sistema de organización de toda la empresa, incluyendo tanto los sistemas de CDE y los sistemas que están fuera del alcance.

Los servicios compartidos comunes incluyen, de forma enunciativa más no limitativa:

- Directorio y autenticación (ej. Directorio Activo, LDAP/ AAA)
- NTP - Protocolo de Tiempo de la Red
- DNS - Servicio de Nombres de Dominio
- SMTP - Protocolo de Transferencia de Correo Simple
- Herramientas de monitoreo y escaneo
- Herramientas de copia de seguridad
- Servidores antivirus y de despliegue de parches

Para este ejemplo, los Servicios Compartidos se encuentran ubicados fuera de un CDE segmentado, pero proporcionan servicios al CDE. Los Servicios Compartidos además proporcionan funciones de autenticación y/u otras funciones de apoyo operativo a otros sistemas corporativos considerados fuera del alcance. Como estos Servicios Compartidos se conectan y brindan servicios al CDE, están dentro del alcance de PCI DSS.

La pregunta en este escenario es cómo implementar la segmentación de forma que los sistemas de la LAN Corporativa puedan conectarse a los Servicios Compartidos pero estar efectivamente segmentados desde el CDE de forma que no puedan acceder al CDE. En otras palabras, cómo establecer Servicios Compartidos que apoyen tanto al CDE como a la LAN Corporativa manteniendo al mismo tiempo los sistemas de la LAN corporativa fuera del alcance PCI DSS.

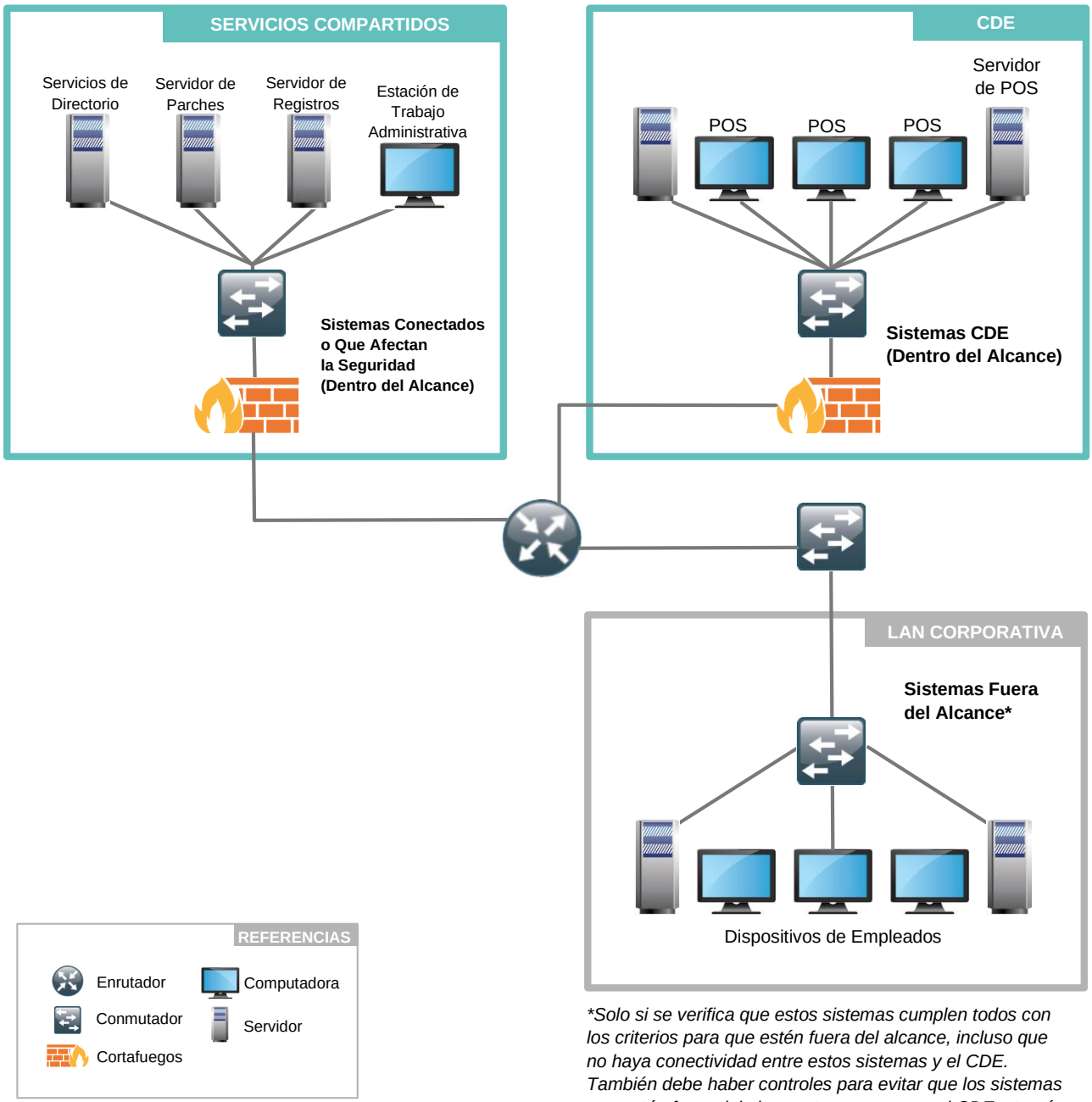
Los siguientes principios se aplican además de los definidos anteriormente. Véanse las Figuras 2 y 3.

- El acceso administrativo a sistemas de Servicios Compartidos se permite únicamente desde dentro de la red de los Servicios Compartidos y todo acceso de este tipo se registra y monitorea.
- El acceso administrativo a los sistemas del CDE se permite únicamente desde sistemas que están dentro del CDE o desde sistemas designados en la red de los Servicios Compartidos.

- Se utiliza una autenticación de múltiples factores para todo el acceso administrativo desde sistemas de Servicios Compartidos hacia el CDE. Todo el acceso administrativo al CDE se registra y se monitorea.
- Las cuentas utilizadas para acceder a Servicios Compartidos desde la LAN Corporativa no tienen acceso al CDE.
- Todos los controles de acceso se establecen y se gestionan en los cortafuegos en las zonas de Servicios Compartidos y del CDE.

FIGURA 2 – Ejemplo de Ilustración de Segmentación: "Conectado a" Servicios Compartidos

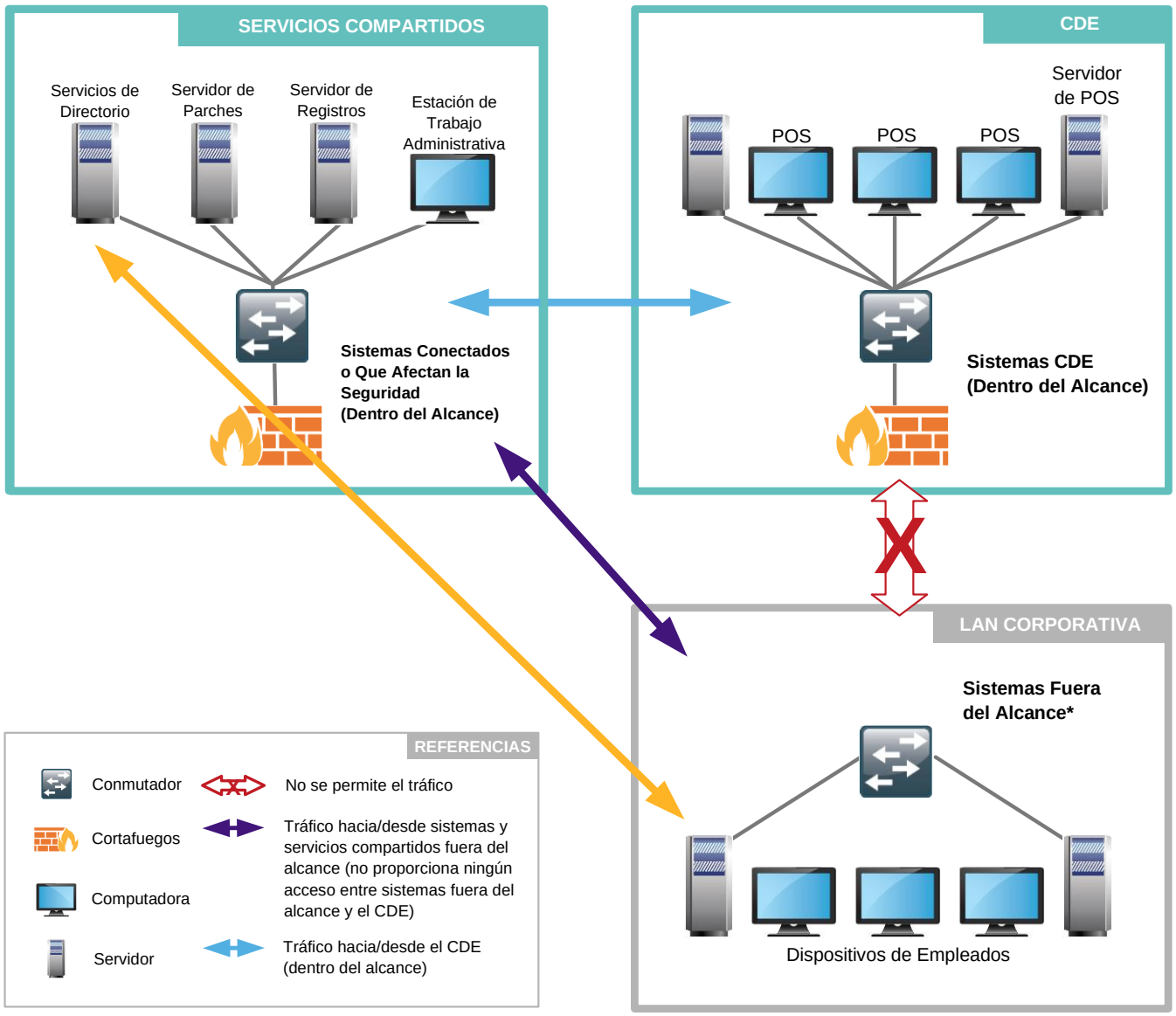
Escenario 1:



**Solo si se verifica que estos sistemas cumplen todos con los criterios para que estén fuera del alcance, incluso que no haya conectividad entre estos sistemas y el CDE. También debe haber controles para evitar que los sistemas que están fuera del alcance tengan acceso al CDE a través de sistemas de la red de Servicios Compartidos.*

FIGURA 3 – Flujo de Datos Lógicos para «Conectados a» Servicios Compartidos

Escenario 1: Flujo de Datos Lógicos



**Solo si se verifica que estos sistemas cumplen todos con los criterios para que estén fuera del alcance, incluso que no haya conectividad entre estos sistemas y el CDE. También debe haber controles para evitar que los sistemas que están fuera del alcance tengan acceso al CDE a través de sistemas de la red de Servicios Compartidos.*

La siguiente tabla resume las zonas de la red ilustradas en las Figuras 2 y 3 de arriba y el potencial impacto en el alcance PCI DSS.

Zonas de la Red	Categoría	Impacto en el Alcance PCI DSS
CDE	Sistemas del CDE	Completamente dentro del alcance de todos los requisitos PCI DSS aplicables
Servicios Compartidos	Sistemas Conectados y/o que Afectan la Seguridad	Completamente dentro del alcance de todos los requisitos PCI DSS aplicables
LAN Corporativa	Sistemas Fuera del Entorno	No está en el alcance *Los controles de la segmentación deben probarse y verificarse completamente antes de que pueda determinarse si los sistemas de la LAN Corporativa están fuera del alcance. Los sistemas y el personal de la LAN Corporativa que acceden a Servicios Compartidos no deben poder tener acceso al CDE a través de los Servicios Compartidos. Los controles de la segmentación deben verificarse por lo menos una vez al año.*

4.2 Ejemplo 2: Estación de Trabajo de la Administración del CDE fuera del CDE

Nota: *Este ejemplo y los diagramas relacionados son únicamente para propósitos ilustrativos. Cada red es diferente y las técnicas de segmentación que funcionan bien en una red podrán no funcionar en otra. Por lo tanto, cualquier método de segmentación utilizado deberá probarse minuciosamente según los requisitos PCI DSS para confirmar que funciona de la forma esperada y continúe proporcionando una segmentación efectiva en ese entorno. Del mismo modo, los controles aquí señalados son adicionales a PCI DSS y pueden no ser obligatorios o necesarios para todos los entornos.*

Un administrador de sistemas suele tener responsabilidades sobre los sistemas de toda la empresa, que pueden incluir sistemas CDE, sistemas conectados y que afectan a la seguridad, así como sistemas fuera del alcance. Las cuentas de administrador son cuentas privilegiadas que deben gestionarse y supervisarse con mucho cuidado, ya que las personas con estos privilegios superiores pueden conceder privilegios elevados a otros usuarios, y pueden acceder, añadir, eliminar y cambiar varios (si no todos) los archivos y ajustes de configuración y del sistema, cambiar o eliminar datos del registro de auditoría y acceder a CHD.

En este ejemplo, un administrador del sistema es responsable de los Sistemas del CDE, de los sistemas de los Servicios Compartidos y de los sistemas que están fuera del alcance en la LAN Corporativa. La estación de trabajo del administrador se encuentra ubicada en la LAN Corporativa y fuera del CDE. Por lo tanto, la administración del sistema del CDE se origina desde afuera, pero requiere conectividad con los dispositivos que se encuentran dentro del CDE.

Este ejemplo se basa en la red de Servicios Compartidos del ejemplo anterior, con el agregado de:

1) La estación de trabajo de un administrador de la LAN Corporativa y
2) Una caja de salto dentro de la red de Servicios Compartidos para gestionar y controlar el acceso administrativo en el CDE.

La pregunta clave para este ejemplo es cómo implementar una segmentación que permita la administración segura de los sistemas CDE desde un sistema que afecte la seguridad ubicado en la LAN corporativa, y que también mantenga al resto de los sistemas de la LAN corporativa fuera del alcance.

El enfoque tomado en este ejemplo es similar al de un escenario de acceso remoto, en el que un administrador se conecta remotamente al CDE desde su red doméstica:

- La LAN Corporativa es una red no confiable similar a lo que sería una red doméstica.
- La zona de la red de Servicios Compartidos actúa como una DMZ, proporcionando servicios tanto a computadoras que no son de confianza como a un usuario de confianza con acceso al CDE.
- La estación de trabajo del administrador está protegida del mismo modo que debe estarlo un computador remoto, con software de cortafuegos personal, autenticación multifactor y todos los demás requisitos PCI DSS aplicables implementados.
- El acceso al CDE desde redes no confiables es gestionado y controlado por sistemas específicos de la red de Servicios Compartidos.

Todos los controles que aplican al Ejemplo 1 también aplican a este ejemplo, excepto que el acceso administrativo al CDE se permite desde una estación de trabajo administrativo designada en la LAN Corporativa. Además de los controles definidos arriba, aplican a este ejemplo los siguientes principios de segmentación. (Véanse las Figuras 4 y 5)

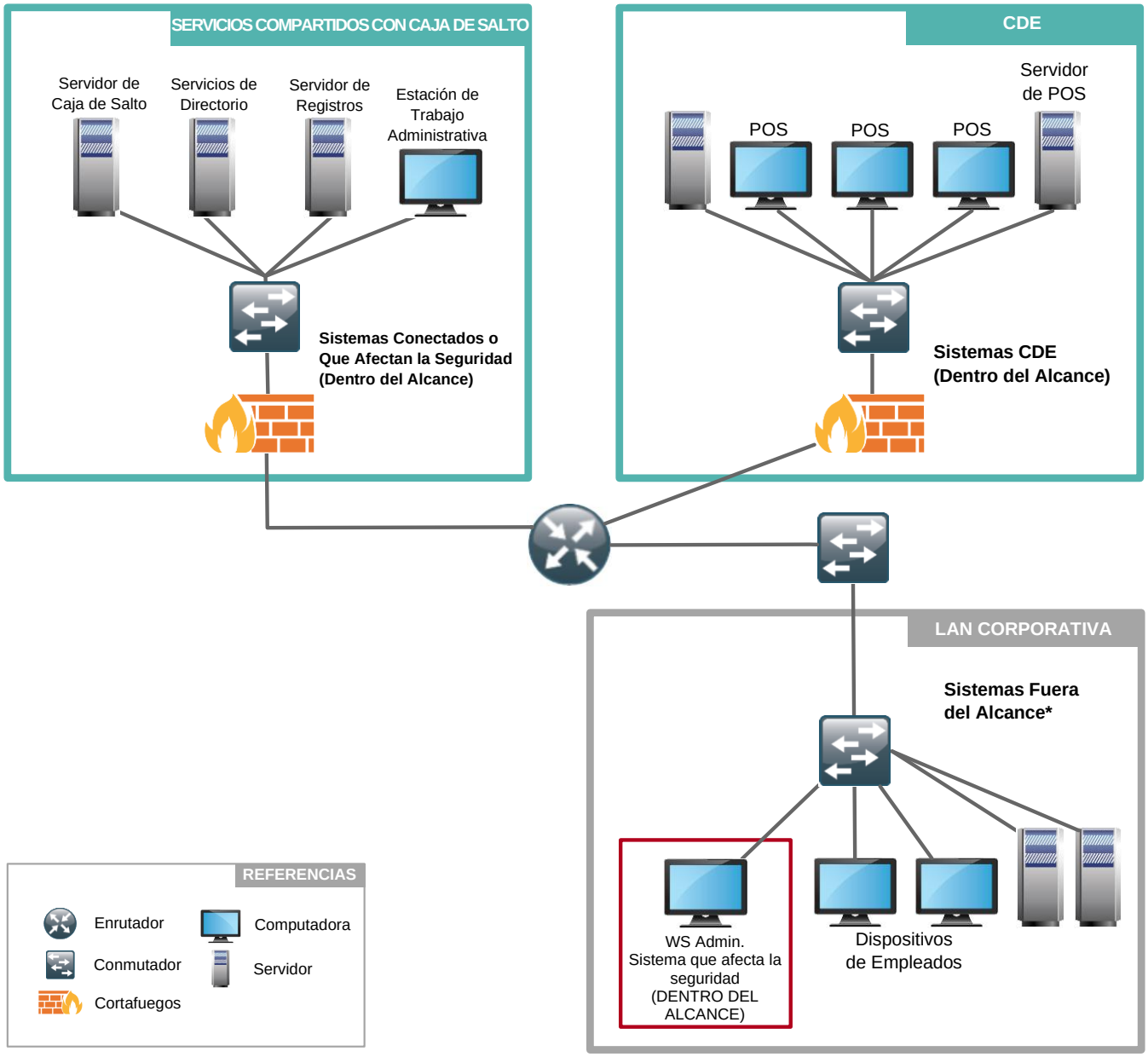
- Hay una “caja de salto” (Host Bastión[10]) instalada en la red de Servicios Compartidos.
- Las reglas del cortafuegos y del enrutador aseguran que
  - Las conexiones a la caja de salto desde la LAN Corporativa estén restringidas únicamente al personal designado de la estación de trabajo del Administrador y todos los demás intentos de conexión están bloqueados.
  - La estación de trabajo del Administrador no pueda acceder al CDE directamente y deba pasar por la Caja de Salto para todo el acceso al CDE.
- Se han implementado herramientas activas de monitoreo y prevención de pérdida de datos (DLP) para garantizar que los datos de los tarjetahabiente no puedan transferirse del CDE a la caja de salto.
- La administración de la caja de salto en sí se realiza a través de una consola local únicamente y no hay una gestión remota de este dispositivo.
- La estación de trabajo del Administrador en sí misma no almacena, procesa o transmite CHD.
- La estación de trabajo del Administrador está completamente dentro del alcance PCI DSS y se aplican todos los requisitos PCI DSS correspondientes.
- La estación de trabajo del Administrador (que se encuentra esencialmente en una red no confiable) está protegida de Internet mediante la funcionalidad de cortafuegos personal, tal y como se define en el Requisito 1.4 PCI DSS.
- El uso de la Estación de Trabajo del Administrador está restringido al personal administrativo designado.
- El acceso a la caja de salto desde la estación de trabajo del Administrador ocurre a través de una cuenta de usuario diferente a la que se utiliza para administrar el CDE. La cuenta utilizada para acceder a la caja de salto no tiene privilegios elevados en la Caja de Salto.

[10] Una computadora diseñada y configurada específicamente para soportar ataques. (Fuente: wikipedia.org)

- El acceso a la caja de salto desde la estación de trabajo del Administrador requiere la autenticación de múltiples factores para personas individuales. Por lo menos uno de los métodos de autenticación de múltiples factores es independiente de la estación de trabajo del Administrador y está «en manos» del personal administrador designado (por ejemplo, se utiliza una tarjeta inteligente física o un token como autenticación de «algo que tiene»).
- Todos los requisitos PCI DSS aplicables están implementados para administrar y proteger la conectividad entre la estación de trabajo del Administrador y la caja de saltos, incluidos el cortafuegos, IDS/IPS, antimalware y otras herramientas y técnicas de defensa contra amenazas.
- Todos los requisitos aplicables de la PCI DSS están implementados para gestionar y asegurar la conectividad entre la caja de salto y el CDE, incluidos cortafuegos, IDS/IPS, antimalware y otras herramientas y técnicas de defensa contra amenazas.

FIGURA 4 – Ejemplo de Ilustración de Segmentación: Administración de Sistemas del CDE desde un Sistema que Afecta la Seguridad en la LAN Corporativa

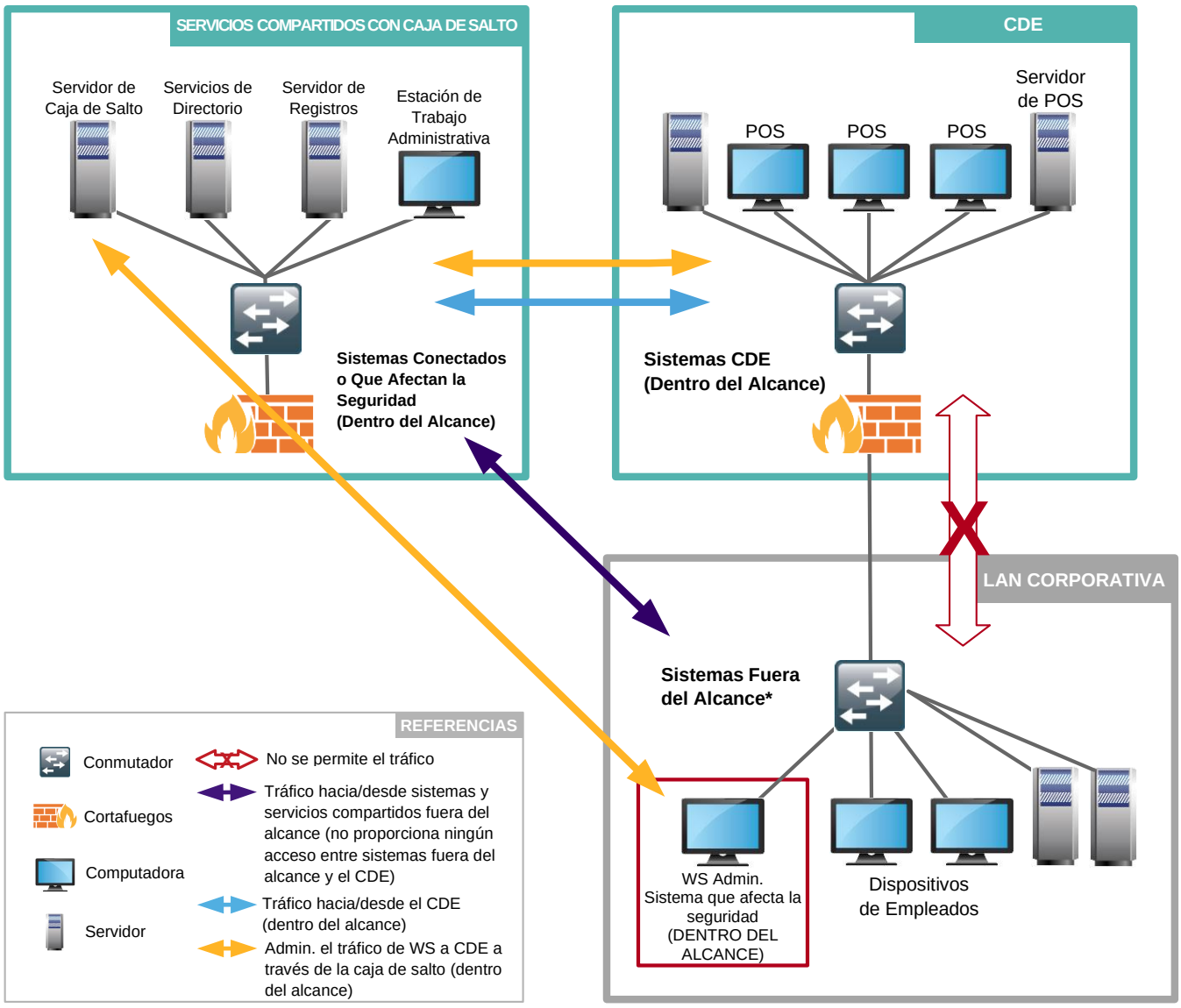
Escenario 2:



**Solo si se verifica que estos sistemas cumplen todos con los criterios para que estén fuera del alcance, incluso que no haya conectividad entre estos sistemas y el CDE. También debe haber controles para evitar que los sistemas que están fuera del alcance tengan acceso al CDE a través de sistemas de la red de Servicios Compartidos.*

FIGURA 5 – Flujo de Datos Lógicos: Administración de Sistemas del CDE desde un Sistema que Afecta la Seguridad en la LAN Corporativa

Escenario 2: Flujo de Datos Lógicos



Solo si se verifica que estos sistemas cumplen todos con los criterios para que estén fuera del alcance, incluso que no haya conectividad entre estos sistemas y el CDE. También debe haber controles para evitar que los sistemas que están fuera del alcance tengan acceso al CDE a través de sistemas de la red de Servicios Compartidos.

La tabla siguiente resume las zonas de la red ilustradas en las figuras 4 y 5 anteriores, y el impacto potencial en el alcance PCI DSS.

Zonas/Sistemas de la Red	Categoría	Impacto en el Alcance PCI DSS
CDE	Sistemas del CDE	Completamente dentro del alcance de todos los requisitos PCI DSS aplicables
Servicios Compartidos (incluyendo la Caja de Salto)	Sistema Conectado y/o que Afecta a la Seguridad	Completamente dentro del alcance de todos los requisitos PCI DSS aplicables
Estación de Trabajo del Administrador en la LAN Corporativa	Sistema que Afecta la Seguridad	Completamente dentro del alcance de todos los requisitos PCI DSS aplicables
Otros sistemas en la LAN Corporativa	Sistemas Fuera del Entorno	No está en el alcance *Los controles de la segmentación deben probarse y verificarse por completo antes de que pueda determinarse que otros sistemas de la LAN corporativa están fuera de alcance. Los sistemas y el personal de la LAN Corporativa que acceden a Servicios Compartidos no deben poder tener acceso al CDE a través de los Servicios Compartidos. Los controles de la segmentación deben verificarse por lo menos una vez al año.*

5 Conclusión

Al delimitar el alcance de un entorno para PCI DSS, es importante partir siempre del supuesto de que todo está dentro del alcance hasta que se verifique que todos los controles necesarios están implementados y proporcionan realmente una segmentación efectiva. La segmentación efectiva puede reducir ampliamente el riesgo de que los sistemas del CDE se vean impactados por debilidades o compromisos de seguridad que se originen en sistemas que están fuera del alcance.

Recuerde que establecer mal el alcance (decidir que algo está fuera de alcance sin la verificación apropiada) puede poner a una empresa en riesgo. Para ser efectivos, el alcance y la segmentación requieren una cuidadosa planificación, diseño, implementación y monitoreo. Muchas infracciones se han producido a través de sistemas y redes determinados incorrectamente como fuera de alcance, en los que la entidad vulnerada implementó una falsa confianza en la segmentación, para descubrir después que la vulnerabilidad de esos controles no permitía la protección efectiva sus redes. Por lo tanto, es fundamental que las entidades se enfoquen en la seguridad de todo su entorno en lugar de centrarse únicamente en lo que exige PCI DSS para minimizar los riesgos para sus organizaciones.

Acerca del PCI Security Standards Council

El PCI Security Standards Council es un foro mundial abierto responsable del desarrollo, gestión, educación y concientización del Estándar de Seguridad de Datos (PCI DSS) y otros estándares que aumentan la seguridad de los datos de pagos. Creado en 2006 por las marcas de tarjetas de pago fundadoras American Express, Discover Financial Services, JCB International, Mastercard y Visa Inc., el Consejo cuenta con más de 650 Organizaciones Participantes que representan a comerciantes, bancos, procesadores y proveedores de todo el mundo. Para obtener más información sobre cómo contribuir a proteger los datos de las tarjetas de pago a nivel mundial, visite: pcisecuritystandards.org.