BANCO CENTRAL DE COSTA RICA

Políticas Específicas de Ciberseguridad del Ambiente PCI-DSS

HISTÓRICO DE VERSIONES Y CONTROL DE CAMBIOS A LA POLÍTICA

Versión:	Fecha de creación:	Aprobado por:	Cambios realizados:
3.0	7 de octubre de 2024	Gerencia	Cambios en los nombres de las dependencias de conformidad con la estructura organizativa vigente. Mejora en la redacción de políticas, controles y lineamientos existentes, así como inclusión de nuevos términos al glosario. Inclusión de las políticas P-8, P-9, P-12 Modificación de numeración después de la política P.8 Inclusión de las secciones Gestión Documental, Gestión de Acceso a Contratistas, Pruebas de Penetración y Segmentación, Definición de la Periodicidad de Ejecución de Controles y Parchado de sistemas con sus políticas, controles y lineamientos.
2.0	2 de septiembre de 2022	Director División Servicios Tecnológicos	Cambios en los nombres de las dependencias de conformidad con la estructura organizativa vigente. Inclusión de la política P-9. Se cambio la numeración a partir de la P-9. Se agregó el apartado Seguridad en la Operativa, con las políticas P-11. Y P-12.
1.0	3 de febrero de 2022	Director División Servicios Tecnológicos	Emisión de políticas

Contenido

POLÍTICAS ESPECIFICAS DE CIBERSEGURIDAD DEL AMBIENTE PCI-DSS 4
Consideraciones que sustentan la emisión de estas políticas específicas. 4
I. ASPECTOS GENERALES 5
II. ASPECTOS OPERATIVOS 7
ASEGURAMIENTO O ENDURECIMIENTO DE LA PLATAFORMA 7
BITÁCORAS Y AUDITORÍA 7
MONITOREO DE EVENTOS DE CIBERSEGURIDAD 8
ANÁLISIS DE VULNERABILIDADES 9
PROTECCIÓN DE LOS DATOS DEL TITULAR DE LA TARJETA 9
SEGURIDAD EN LA OPERATIVA 11
GESTIÓN DOCUMENTAL 13
GESTIÓN DE ACCESO A CONTRATISTAS 13
PRUEBAS DE PENETRACIÓN Y SEGMENTACIÓN 13
DEFINICIÓN DE LA PERIODICIDAD DE EJECUCIÓN DE CONTROLES 14
PARCHADO DE SISTEMAS 14

POLÍTICAS ESPECIFICAS DE CIBERSEGURIDAD DEL AMBIENTE PCI-DSS

Consideraciones que sustentan la emisión de estas políticas específicas.

A. La Junta Directiva del BCCR aprobó en agosto del 2017 el proyecto Pago Electrónico en el Transporte Público, para diseñar el Sistema de Pago Electrónico y construir el Sistema Central de Recaudo como un servicio integrado a la plataforma tecnológica del Sistema Nacional de Pagos Electrónicos (SINPE).

B. Mediante el Convenio para el diseño y construcción del sistema de pago electrónico en el trasporte público, celebrado entre el Ministerio de Obras Públicas y Transportes, el Consejo de Transporte Público, el Instituto Costarricense de Ferrocarriles, la Autoridad Reguladora de los Servicios Públicos, los representantes de la industria del transporte público remunerado de personas y el Banco Central de Costa Rica, firmado el 11 de enero del año 2018, se delega en el Banco Central de Costa Rica la responsabilidad de construir, implementar y gestionar el Sistema de Pago Electrónico en Transporte Público. En ese sentido como responsable de la gestión de información relacionada a dispositivos de pago electrónico, el BCCR acoge lo solicitado por los estándares internacionales de la industria, para proveer una infraestructura tecnológica que permita el aseguramiento adecuado de dicha información.

C. Este documento de políticas busca atender temas específicos, normados en el estándar internacional PCI-DSS[1].

D. Las políticas específicas aquí contenidas han sido revisadas y aprobadas por sus responsables; satisfacen el esquema definido para la creación de políticas específicas, controles y lineamientos y cuentan con el visto bueno de la División Transformación y Estrategia.

[1]Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (Payment Card Industry Security Standards Council – PCI SSC)

I. ASPECTOS GENERALES

P-1. El Banco Central de Costa Rica establece que la infraestructura para el ambiente de seguridad PCI-DSS sujeto a certificación; en primera instancia, se encuentra normada por las Políticas Específicas de Seguridad Tecnológica y las Políticas Específicas de Seguridad de la Información, lo anterior en cumplimiento al estándar.

P-2. El Banco Central de Costa Rica establece como alcance de las Políticas Específicas de Ciberseguridad del Ambiente PCI-DSS, los servicios brindados por la División Servicios Tecnológicos (DST) del Banco Central de Costa Rica (BCCR) para soportar la gestión del ambiente sujeto a cumplimiento de dicha certificación.

P-3. El Banco Central de Costa Rica establece como alcance para las políticas presentadas en este documento las siguientes certificaciones externas:

a) Certificación PCI Council PCI-DSS

P-4. Con el fin de procurar la adecuada interpretación de los aspectos relacionados con la seguridad tecnológica para efecto de la certificación PCI-DSS, se definen los siguientes términos:

a) Acceso no autorizado	Acceder de manera indebida, sin autorización o contra derecho a un sistema de gestión de información.
b) Ambiente	Combinación de hardware y software para realizar una tarea o una serie de tareas específicas. Generalmente existen ambientes de pruebas, ambientes de desarrollo, ambientes de capacitación, ambientes de preproducción y ambientes de producción.
c) Análisis de vulnerabilidades	Es el proceso para definir, identificar, clasificar y priorizar las debilidades del sistema para proporcionar una evaluación de las amenazas previsibles y reaccionar de manera apropiada.
d) Autenticación	Es el acto o proceso de confirmar que algo o alguien es quien dice ser.
e) Aseguramiento, endurecimiento o hardening	Es una buena práctica de seguridad que se aplica sobre elementos de la infraestructura con el fin de reducir la superficie de vulnerabilidad, evitando así posibles ataques.
f) Cambio significativo	Según la normativa PCI se considera cambio significativo lo siguiente: a. Nuevo hardware, software o equipo de red añadido al CDE. b. Cualquier sustitución o actualización importante de hardware y software en el CDE. c. Cualquier cambio en el flujo o almacenamiento de datos de cuentas. d. Cualquier cambio en los límites del CDE y/o en el alcance de la evaluación PCI DSS. e. Cualquier cambio en la infraestructura de apoyo subyacente del CDE (incluidos, pero sin limitarse a, los cambios en los servicios de directorio, los servidores de tiempo, el registro y la supervisión).

	f. Cualquier cambio en los vendedores/proveedores de servicios (o servicios prestados) que apoyen el CDE o cumplan los requisitos de PCI DSS en nombre de la entidad. g. Cualquier cambio que se presente en la estructura organizacional.
g) CDE	CardHolder Data Enviroment, por sus siglas en ingles. Se refiere al ambiente de datos de tarjetahabiente, definido como: Las personas, procesos y tecnologías donde se almacenan, procesan o trasmiten datos de tarjeta.
h) Cifrado	Proceso de codificación o encriptación de datos para que solo pueda leerlo alguien con los medios para devolverlo a su estado original.
i) Contratista (TPSP Third Party Service Provider)	Persona que tiene a su cargo, en virtud de un contrato, la ejecución de una actividad o servicio. Se excluye de esta definición el personal de Outtasking. Se incluye en esta categoría al personal de cualquier entidad comercial que no es una marca de pago, que participa directamente en el procesamiento, almacenamiento o transmisión de datos de titulares de tarjetas en nombre de otra entidad. Esto también incluye al personal de las empresas que brindan servicios que controlan o podrían afectar la seguridad de los datos de los titulares de tarjetas. Como, por ejemplo, entidades que: • Almacenan, procesan o transmiten datos de cuentas en nombre de la entidad. • Gestionan los componentes del sistema incluidos en la evaluación PCI DSS de la entidad. • Podría afectar la seguridad del CDE de la entidad.
j) Datos confidenciales de autenticación	Información necesaria para autenticar al dueño de la tarjeta en entornos de pago presenciales y no presenciales, según la clasificación indicada por PCI-DSS.
k) Datos del titular de la tarjeta.	Información que identifica al titular o dueño de la tarjeta, según la clasificación indicada por PCI-DSS.
l) Infraestructura	Es el conjunto de elementos físicos y virtuales que soportan las aplicaciones.
m) Mecanismo de autenticación multifactor (MFA)	Los mecanismos de autenticación multifactor o MFA por sus siglas en inglés, comprueban múltiples aspectos de la identidad de un usuario antes de permitir el inicio de sesión a un dispositivo, aplicación o base de datos. Los mecanismos de autenticación multifactor requieren de al menos dos de los siguientes métodos: 1. Algo que el usuario conoce: Este método verifica la información que un usuario ingrese, por ejemplo, una contraseña, una frase, un PIN o la respuesta a una pregunta secreta. 2. Algo que el usuario tiene: Este método involucra validar algo que el usuario tenga en su posesión, por ejemplo, token físico o digital, un OTP (One Time Password por sus siglas en ingles), una tarjeta de acceso, la firma digital, entre otros.

	3. Algo que el usuario es: Este método involucra validar datos biométricos del usuario como, por ejemplo, huella digital, reconocimiento facial, reconocimiento de voz, entre otros.
n) PCI-DSS	Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard).
o) Rol	Conjunto de privilegios de acceso a la información en los diferentes sistemas o dispositivo en la que esta se almacene.
p) Sistema	Un sistema informático es el conjunto de partes interrelacionadas tanto de hardware como de software; que permite almacenar y procesar la información.
q) Cuenta de servicio	Una cuenta de servicios es una cuenta que no utilizan los usuarios, sino que son utilizadas como identidad por los sistemas para ejecutar aplicaciones.
r) Vulnerabilidad	Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información.

II. ASPECTOS OPERATIVOS

ASEGURAMIENTO O ENDURECIMIENTO DE LA PLATAFORMA

P-5. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, establece los mecanismos de aseguramiento o endurecimiento para la infraestructura sujeta al cumplimiento de la certificación PCI-DSS.

C-5.1. La División Servicios Tecnológicos es responsable de implementar los mecanismos para que la infraestructura que soporta el ambiente sujeto a cumplimiento de la certificación PCI-DSS sea asegurada (hardening).

L-5.1.1. Todo elemento de infraestructura que se implemente en el ambiente tecnológico sujeto a la certificación PCI-DSS, deberá ser asegurado (hardening) según una buena práctica de la industria, avalada por el estándar PCI-DSS.

L-5.1.2. Cuando alguna de las configuraciones recomendadas no pueda ser aplicada, deberá documentarse en un repositorio institucional, previa autorización del Departamento de Ciberseguridad.

BITÁCORAS Y AUDITORÍA

P-6. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, implementa los mecanismos y controles adecuados para gestionar los registros de auditoría, que permitan vincular los accesos de los usuarios a los componentes que se incluyen dentro del alcance de certificación PCI-DSS.

C-6.1. La División Servicios Tecnológicos, por medio del Departamento de Infraestructura Tecnológica; con asesoría del Departamento de Ciberseguridad, es responsable de configurar el registro de eventos y el envío de las bitácoras correspondientes para los accesos a los componentes que se incluyen dentro del alcance de certificación PCI-DSS.

L-6.1.1. Se deberán registrar los accesos a los componentes que se incluyen dentro del alcance de certificación PCI-DSS, donde se gestionen, almacenen o procesen datos del titular de la tarjeta.

C-6.2. La División Servicios Tecnológicos, por medio del Departamento de Ciberseguridad, es responsable de implementar las soluciones apropiadas para gestionar las bitácoras recopiladas de los accesos a los componentes que se incluyen dentro del alcance de certificación PCI-DSS.

L-6.2.1. Se deberá conservar el historial de las bitácoras durante al menos un año, con un mínimo de disponibilidad para análisis de 90 días.

L-6.2.2. Se deberá limitar el acceso a la información de las bitácoras únicamente a los roles que por sus funciones están autorizados para ello.

L-6.2.3. Se deberá registrar cualquier intento de borrado, detención o pausa de estas bitácoras, así como su inicialización.

MONITOREO DE EVENTOS DE CIBERSEGURIDAD

P-7. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, implementa los mecanismos y controles adecuados para monitorear los eventos de ciberseguridad.

C-7.1. La División Servicios Tecnológicos, por medio del Departamento de Ciberseguridad, es responsable de implementar mecanismos apropiados para monitorear eventos de ciberseguridad de los componentes que forman parte del ambiente PCI-DSS.

L-7.1.1 Se deberá analizar al menos una vez al día las siguientes alertas:

a) Todos los eventos de ciberseguridad.
b) Registros de todos los componentes del sistema que almacenan, procesan o transmiten datos del titular de la tarjeta y/o datos de autenticación confidenciales.
c) Registros de todos los componentes críticos del sistema.
d) Registros de todos los componentes del sistema que realizan funciones de seguridad.

L-7.1.2 Se deberá analizar de manera inmediata cualquier falla en un control de ciberseguridad dentro del alcance PCI-DSS, para ello el proceso de monitoreo deberá generar una alerta la cual deberá ser atendida en la brevedad siguiendo los procedimientos de atención previamente establecidos por el Departamento de Ciberseguridad.

C-7.2. La División de Servicios Tecnológicos, por medio del Departamento de Ciberseguridad deberá atender cualquier incidente de ciberseguridad que se presente en el ambiente PCI-DSS siguiendo los pasos establecidos en el procedimiento correspondiente.

P-8. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, implementa los mecanismos y controles adecuados para monitorear y detectar los puntos de acceso inalámbricos autorizados y no autorizados.

C-8.1. La División Servicios Tecnológicos, por medio del Departamento de Infraestructura Tecnológica, es responsable de realizar una revisión de los puntos de acceso inalámbricos para detectar aquellos no autorizados y tomar las medidas pertinentes de mitigación.

L-8.1.1 La periodicidad de ejecución de esta revisión deberá ser cada 90 días.

P-9. El Banco Central de Costa Rica, por medio de la División de Sistemas de Pago, implementa los mecanismos y controles adecuados para verificar el cumplimiento del marco normativo institucional aplicable al ambiente PCI-DSS.

C-9.1 La División Sistemas de Pago, por medio del Departamento Sistema de Pagos Electrónicos en el Transporte Público, es responsable de verificar que el personal está realizando sus tareas de acuerdo con el marco normativo institucional aplicable al ambiente PCI-DSS.

L-9.1.1 La periodicidad de ejecución de esta revisión deberá ser cada 90 días.

ANÁLISIS DE VULNERABILIDADES

P-10. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, implementa evaluaciones periódicas de posibles vulnerabilidades en los sistemas.

C-10.1. La División Servicios Tecnológicos, por medio del Departamento de Ciberseguridad, es responsable de realizar análisis de vulnerabilidades internos de manera periódica, con el fin de detectar posibles brechas o debilidades de la infraestructura tecnológica.

L-10.1.1. Se deberá ejecutar un análisis de vulnerabilidades por trimestre sobre la plataforma que soporta los servicios.

L-10.1.2. Cuando se realicen cambios mayores en la infraestructura contenida en el alcance de PCI-DSS, deberán ejecutarse análisis de vulnerabilidades internos para evaluar el estado de los componentes.

L-10.1.3. Se deberá realizar un análisis de vulnerabilidades para confirmar que se realizaron las correcciones respectivas al menos cada 30 días.

PROTECCIÓN DE LOS DATOS DEL TITULAR DE LA TARJETA

P-11. El Banco Central de Costa Rica, protege y restringe el acceso a los datos del titular de la tarjeta.

C-11.1. Con el fin de proteger y restringir el acceso a los datos del titular de la tarjeta, los usuarios con acceso al Ambiente de Datos de Tarjetahabientes (CardHolder Data Enviroment, CDE) deberán cumplir con los siguientes lineamientos:

L-11.1.1. Se prohíbe la copia, transferencia o almacenamiento de la información de los datos del titular de la tarjeta en unidades de discos locales y dispositivos

electrónicos extraíbles al acceder dichos datos a través de tecnologías de acceso remoto.

L-11.1.2. La transmisión del PAN (número de cuenta principal) no protegido no se debe realizar por medio de tecnologías de usuario final.

L-11.1.3. Cuando se requiera la transmisión del PAN, por canales no aprobados previamente como parte del ambiente PCI-DSS, es responsabilidad del Departamento Sistema de Pagos Electrónicos en el Transporte Público, solicitar asesoría especializada en el Departamento de Ciberseguridad para la debida protección de la información.

L-11.1.4 El acceso al ambiente PCI-DSS deberá realizarse utilizando un mecanismo de autenticación multifactor (MFA), el cual es de carácter individual y se prohíbe compartirlo con terceros.

P-12. El Banco Central de Costa Rica, por medio de la División Sistemas de Pago, documenta y mantiene debidamente actualizados los flujos de datos del titular de la tarjeta.

C-12.1. La División Sistemas de Pago, por medio del Departamento Sistema de Pagos Electrónicos en el Transporte Público, es responsable de documentar los flujos de datos del titular de la tarjeta.

L-12.1.1. Se deberán mantener actualizados; y debidamente documentados, los flujos de datos del titular de la tarjeta. Esta revisión deberá realizarse al menos una vez al año o después de cualquier cambio significativo.

P-13. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, establece los mecanismos apropiados de aseguramiento de los datos del titular de la tarjeta en reposo, durante su procesamiento, y durante o previo a su transmisión.

C-13.1. La División Servicios Tecnológicos, por medio del Departamento de TI de Sistemas de Pago; con asesoría del Departamento de Ciberseguridad, es responsable de implementar mecanismos robustos y apropiados para que la información de los datos del titular de la tarjeta se encuentre protegida previo a su transmisión, procesamiento y almacenamiento.

L-13.1.1. Para la transmisión de los datos del titular de la tarjeta se debe garantizar el cifrado de la información antes de enviarla por el canal de comunicación, según una buena práctica de la industria avalada por el estándar PCI-DSS o en su defecto, justificar y escalar la situación cuando no se pueda implementar, con el fin de tomar las medidas adecuadas.

L-13.1.2. Durante el procesamiento de la información de los datos del titular de la tarjeta se deberá implementar los mecanismos necesarios a nivel de aplicación para prevenir modificaciones o alteraciones de los datos.

L-13.1.3. No se deberán almacenar de ninguna manera los datos confidenciales de autenticación, necesarios para autenticar al dueño de la tarjeta en entornos de pago presenciales y no presenciales.

C-13.2. La División Servicios Tecnológicos, por medio del Departamento Infraestructura Tecnológica; con asesoría del Departamento de Ciberseguridad, es responsable de implementar mecanismos robustos y apropiados para que la información de los datos del titular de la tarjeta se encuentre protegida durante su transmisión, procesamiento y almacenamiento.

L-13.2.1. Para la transmisión de los datos del titular de la tarjeta, se deberá garantizar el cifrado del canal de comunicación, según una buena práctica de la industria avalada por el estándar PCI-DSS o en su defecto, justificar y escalar la situación cuando no se pueda implementar, con el fin de tomar las medidas adecuadas.

L-13.2.2. Durante el procesamiento de la información de los datos del titular de la tarjeta se deberá implementar los mecanismos necesarios a nivel de infraestructura tecnológica para prevenir accesos no autorizados.

L-13.2.3. La información de los datos del titular de la tarjeta que se encuentre en reposo; en cualquier medio de almacenamiento gestionado por el Departamento de Infraestructura Tecnológica, deberá protegerse mediante mecanismos de cifrado aceptados por la industria como robustos y apropiados, según una buena práctica avalada por el estándar PCI-DSS.

C-13.3. La División Servicios Tecnológicos, por medio del Departamento de Ciencia e Ingeniería de Datos, con asesoría del Departamento de Ciberseguridad, es responsable de implementar mecanismos robustos y apropiados para que la información de los datos del titular de la tarjeta se encuentre protegida durante su acceso y almacenamiento.

L-13.3.1. La información de los datos del titular de la tarjeta que se encuentre en reposo; en cualquier medio de almacenamiento gestionado por el Departamento de Ciencia e Ingeniería de Datos, deberá protegerse mediante mecanismos de cifrado aceptados por la industria como robustos y apropiados, según una buena práctica avalada por el estándar PCI-DSS.

SEGURIDAD EN LA OPERATIVA

P-14. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, concientiza en temas de ciberseguridad al personal con acceso al ambiente PCI-DSS.

C-14.1. El Departamento de TI de Sistemas de Pago, coordina sesiones de entrenamiento, de forma anual o cuando se determine la necesidad debido a una nueva amenaza o vulnerabilidad, actualizadas y de participación obligatoria, dirigidas a los desarrolladores designados al ambiente PCI-DSS, basadas en técnicas de codificación segura, según las guías y las mejores prácticas de la industria.

C-14.2. El Departamento de Ciberseguridad, deberá concientizar a los usuarios con acceso al ambiente PCI-DSS, en temas relacionados a la ciberseguridad, quienes deberán participar de manera obligatoria. El material utilizado deberá ser actualizado al menos de manera anual o cuando se determine la necesidad debido a una nueva amenaza o vulnerabilidad y estar a disposición de los usuarios en cualquier momento que requieran revisarlo.

P-15. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos establece un inventario con los dispositivos críticos del Ambiente de Datos de Tarjetahabientes (CardHolder Data Enviroment, CDE) junto con el personal autorizado de su uso, con el fin de mantener adecuados niveles de seguridad y auditoría.

C-15.1. La División de Servicios Tecnológicos, con el propósito de proteger los dispositivos críticos del Ambiente de Datos de Tarjetahabientes (CardHolder Data Enviroment, CDE), determina el inventario de Equipos Críticos del CDE y el personal autorizado de su uso.

La División de Servicios Tecnológicos vela por el cumplimiento de los siguientes lineamientos:

L-15.1.1. El inventario de Equipos Críticos del CDE y la Matriz de roles y responsabilidades; donde se incluye el personal autorizado a acceder los componentes del ambiente PCI-DSS, están publicados en la Intranet.

L-15.1.2. El inventario de Equipos Críticos del CDE y la Matriz de roles y responsabilidades puede sufrir variaciones en cuanto a agregar, eliminar o actualizar elementos.

L-15.1.3. Cualquier modificación que sufra el inventario de Equipos Críticos del CDE y la Matriz de roles y responsabilidades, deberá ser autorizada por el Director del Departamento de Ciberseguridad, o por quien éste designe como encargado de dicha labor.

L-15.1.4. El inventario de Equipos Críticos del CDE y la Matriz de roles y responsabilidades se deberán revisar y actualizar al menos una vez al año o después de cualquier cambio significativo.

P-16. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos establece un inventario de las cuentas de servicio con el fin de mantener adecuados niveles de seguridad y auditoría.

C-16.1. El Departamento de Infraestructura Tecnológica y el Departamento de TI de Sistemas de Pago son responsables de notificar al Departamento de Ciberseguridad sobre la creación, modificación o eliminación de cuentas de servicio de las que son responsables para el ambiente PCI-DSS, para su debido registro.

L-16.1.1. La notificación relacionada con la creación o modificación de una cuenta de servicio deberá incluir los roles asignados y el nombre del responsable de la cuenta.

GESTIÓN DOCUMENTAL

P-17. El Banco Central de Costa Rica establece los procesos para la gestión adecuada de todos los documentos formales que gobiernan el aseguramiento de los datos de tarjetas en el ambiente PCI-DSS.

C-17.1. De acuerdo con lo solicitado por la norma PCI-DSS, es responsabilidad de los dueños de los distintos documentos formales que gobiernan el aseguramiento de los datos de tarjetas en el ambiente PCI-DSS, realizar una revisión al menos de forma anual o cuando ocurra un cambio significativo; adicionalmente, se debe agregar un registro en el histórico de versiones y control de cambios, así como solicitar las aprobaciones formales cuando se requiera.

GESTIÓN DE ACCESO A CONTRATISTAS

P-18. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, realiza las acciones adecuadas para asegurarse que los accesos generados para contratistas al ambiente PCI-DSS, se habilitan únicamente en el horario definido y son monitoreados para garantizar la seguridad del ambiente PCI-DSS.

C-18.1. El Departamento responsable del contratista, definirá los horarios en los cuales el contratista podrá realizar sus labores dentro del ambiente PCI-DSS.

C-18.2. El Departamento responsable del contratista verificará que las actividades realizadas **por el contratista en el ambiente PCI-DSS, estén acorde al servicio solicitado.**

PRUEBAS DE PENETRACIÓN Y SEGMENTACIÓN

P-19. El Banco Central de Costa Rica, por medio de la División Sistemas de Pago, realiza las acciones adecuadas para asegurarse la ejecución periódica de pruebas de penetración y segmentación en el ambiente PCI-DSS.

C-19.1. La División Sistemas de Pago, por medio del Departamento Sistema de Pagos Electrónicos en el Transporte Público, es responsable de coordinar la ejecución de pruebas de penetración y segmentación en el ambiente PCI-DSS.

L-19.1.1. Se debe validar que el evaluador que realiza las pruebas de penetración y segmentación cuenta con la experiencia suficiente, está calificado para ejecutar este tipo de pruebas y cuenta con independencia organizacional.

L-19.1.2. Todos los componentes del ambiente PCI-DSS, deben formar parte del alcance de las pruebas de penetración y segmentación.

L-19.1.3. Se debe ejecutar las pruebas de penetración al menos una vez cada 12 meses, después de cualquier cambio significativo en la infraestructura o las aplicaciones.

L-19.1.4. Se debe ejecutar las pruebas de segmentación al menos una vez cada 6 meses, después de cualquier cambio significativo en la infraestructura o las aplicaciones.

P-20. El Banco Central de Costa Rica, por medio de la División Servicios Tecnológicos, colabora en la ejecución periódica de las pruebas de penetración y segmentación para el ambiente PCI-DSS.

C-20.1. La División Servicios Tecnológicos, por medio del Departamento de Ciberseguridad, es responsable de apoyar en la ejecución de las pruebas de penetración y segmentación para el ambiente PCI-DSS.

DEFINICIÓN DE LA PERIODICIDAD DE EJECUCIÓN DE CONTROLES

P-21. El Banco Central de Costa Rica, por medio de la División Sistemas de Pago, realiza las acciones adecuadas para determinar la periodicidad de la ejecución de los controles establecidos, para la protección del ambiente PCI-DSS.

C-21.1. La División Sistemas de Pago, por medio del Departamento Sistema de Pagos Electrónicos en el Transporte Público, es responsable de coordinar la ejecución de los análisis de riesgos, que permitan determinar la adecuada periodicidad de la ejecución de los controles establecidos, para la protección del ambiente PCI-DSS.

L-21.1.1 Los requisitos que deben cumplir con el análisis de riesgos para definir su periodicidad son los siguientes:

a. Revisión del acceso de aplicaciones y cuentas de servicio y los privilegios de acceso relacionados.
b. Cambio de contraseña a las cuentas de servicio.
c. Frecuencia de inspección a los dispositivos POI y el tipo de inspección.
d. Gestión de vulnerabilidades no críticas ni de alto riesgo.
e. Frecuencia de la capacitación del personal de respuesta a incidentes.

L-21.1.2. Los análisis de riesgos que se ejecuten deben considerar:

a. Los activos para proteger
b. Las amenazas que busca mitigar o prevenir el control que se está analizando
c. Los factores que contribuyen a la probabilidad y/o impacto de que se materialice las amenazas identificadas
d. Incluir la justificación de la frecuencia seleccionada

L-21.1.3. Se debe ejecutar y documentar la revisión de los análisis de riesgos, al menos una vez cada 12 meses, con el fin de validar la periodicidad definida para cada control o si es necesario ejecutar nuevamente el ejercicio.

PARCHADO DE SISTEMAS

P-22. El Banco Central de Costa Rica por medio de la División Servicios Tecnológicos realiza el proceso de parchado del ambiente PCI-DSS, para mantener un adecuado nivel de seguridad.

C-22.1. La División Servicios Tecnológicos, a través de los departamentos correspondientes, es responsable de aplicar el proceso de parchado del software, aplicaciones de escritorio y los sistemas que forman parte del ambiente PCI-DSS.

L-22.1.1. Esta actividad deberá ejecutarse al menos cada 30 días.