Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI)

Versión 1.1

Publicada Septiembre del 2006

Desarrollar y Mantener una Red Segura

Requisito 1:	Instalar y mantener una configuración de cortafuegos para proteger los datos de los tarjetahabientes.
Requisito 2:	No usar contraseñas del sistema y otros parámetros de seguridad provistos por los suplidores.

Proteger los Datos de los Tarjetahabientes

Requisito 3:	Proteger los datos de los tarjetahabientes que estén almacenados.
Requisito 4:	Encriptar los datos de los tarjetahabientes e información confidencial transmitida a través de redes públicas abiertas.

Mantener un Programa de Manejo de Vulnerabilidad

Requisito 5:	Usar y actualizar regularmente el software antivirus.
Requisito 6:	Desarrollar y mantener sistemas y aplicaciones seguras.

Implementar Medidas Sólidas de Control de Acceso

Requisito 7:	Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información.
Requisito 8:	Asignar una Identificación única a cada persona que tenga acceso a un computador.
Requisito 9:	Restringir el acceso físico a los datos de los tarjetahabientes.

Monitorear y Probar Regularmente las Redes

Requisito 10:	Rastrear y monitorear todo el acceso a los recursos de la red y datos de los tarjetahabientes.
Requisito 11:	Probar regularmente los sistemas y procesos de seguridad.

Mantener una Política de Seguridad de la Información

Requisito 12:	Mantener una política que contemple la seguridad de la información

Prefacio

El presente documento describe los doce requisitos de las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI). Estos requisitos están organizados en 6 grupos que tienen relación lógica, que son los “objetivos de control”.

La tabla siguiente ilustra los elementos de datos confidenciales de los tarjetahabientes y de autenticación que normalmente se usan; establece si se permite o se prohíbe **guardar** cada elemento de datos y **si se requiere proteger cada elemento de datos**. Esta tabla no es exhaustiva, pero se presenta para ilustrar los distintos tipos de requisitos que se aplican a cada elemento de datos.

Los requisitos establecidos en las Normas de Seguridad de Datos de la Industria de Tarjeta de Pago (PCI DSS) son aplicables si se guarda, procesa o transmite un número de cuenta primario (PAN). Si el número de cuenta primario (PAN) no se guarda, procesa o transmite, no se aplican estos requisitos.

	Elemento de Datos	Se permite guardar	Protección requerida	PCI DSS Req. 3.4
Datos de los Tarjetahabientes	Número de Cuenta Primario (PAN)*	SÍ	SÍ	SÍ
	Nombre del Tarjetahabiente*	SÍ	SÍ*	NO
	Código de Servicio*	SÍ	SÍ*	NO
	Fecha de Vencimiento*	SÍ	SÍ*	NO
Datos Confidenciales de Autenticación **	Contenido de la banda magnética	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / Bloque de PIN	NO	N/A	N/A

** Se requiere proteger estos elementos de datos si se guardan junto con el Número de Cuenta Primario (PAN). Esta protección debe cumplir con los requisitos establecidos en las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) para la protección general del ambiente de tarjetahabientes. Además, otras leyes (por ejemplo, las relacionadas con la protección de los datos personales de los consumidores, el robo de identidad o la seguridad de datos) pueden requerir protecciones específicas para estos datos o la divulgación apropiada de las prácticas de privacidad de la empresa si se recopilan datos personales de los consumidores en el curso del negocio. Sin embargo, las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) no se aplican si no se guardan, procesan o transmiten números de cuenta primarios (PAN).*

*** Los datos de autenticación confidenciales, que tienen alta sensitividad, no deberán guardarse después de la autorización (aunque estén encriptados).*

Estos requisitos de seguridad se aplican a todos los “componentes de sistemas”. Los componentes de sistemas se definen como cualquier componente de red, servidor o aplicación incluido o conectado al ambiente de datos de los tarjetahabientes. El ambiente de datos de los tarjetahabientes es la parte de la red que procesa los datos de los tarjetahabientes o los datos confidenciales de autenticación. Una segmentación adecuada de la red, que aísla los sistemas que guardan, procesan o transmiten datos de

los tarjetahabientes de aquellos que no realizan estas funciones, podría reducir el alcance del ambiente de datos de los tarjetahabientes. Los componentes de red incluyen, sin limitación, cortafuegos, switches, ruteadores, puntos de acceso inalámbrico, aparatos conectados a la red y otros aparatos y dispositivos de seguridad. Los tipos de servidores incluyen, sin limitación, los siguientes: Web, base de datos, autenticación, correo, proxy, Network Time Protocol (NTP) y servidores de nombre de dominio (DNS). Las aplicaciones incluyen todas las aplicaciones adquiridas comercialmente o individualmente desarrolladas, incluyendo aplicaciones internas y externas (Internet).

Desarrollar y Mantener una Red Segura

Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos.

Los cortafuegos son dispositivos computarizados que controlan el tráfico permitido a y desde una red de computadores de una compañía, así como el tráfico a áreas sensibles de la red interna de una compañía. El cortafuego examina todo el tráfico de la red y bloquea las transmisiones que no cumplen con los criterios de seguridad especificados.

Es necesario proteger todos los sistemas contra el acceso no autorizado desde Internet, sea para fines de comercio electrónico, acceso basado en Internet de los empleados a través de los navegadores de los computadores de escritorio o acceso al correo electrónico de los empleados. Con frecuencia algunas vías de conexión hacia y desde la Internet aparentemente insignificantes pueden proporcionar un acceso sin protección a sistemas clave. Los cortafuegos son un mecanismo de protección esencial para cualquier red de computadores.

1.1 Establecer normas de configuración de cortafuegos que incluyan lo siguiente:

- **1.1.1** Un proceso formal para aprobar y probar todas las conexiones externas de la red y los cambios a la configuración de cortafuegos.
- **1.1.2** Un diagrama actualizado con todas las conexiones a los datos de los tarjetahabientes, incluyendo cualquier red inalámbrica.
- **1.1.3** Requisitos para tener un cortafuego en cada conexión a Internet y entre cualquier DMZ y la zona interna de la red.
- **1.1.4** Descripción de grupos, papeles y responsabilidades para una administración lógica de los componentes de la red.
- **1.1.5** Lista documentada de servicios y puertos necesarios para las actividades del negocio.
- **1.1.6** Justificación y documentación de cualquier protocolo disponible aparte de Hypertext Transfer Protocol (HTTP) y Secure Sockets Layer (SSL), Secure Shell (SSH) y Virtual Private Network (VPN).
- **1.1.7** Justificación y documentación de cualquier protocolo riesgoso permitido (por ejemplo, File Transfer Protocol (FTP), que incluya la razón para usar el protocolo y las funciones de seguridad implementadas.
- **1.1.8** Revisión trimestral del conjunto de reglas de cortafuegos y ruteadores.
- **1.1.9** Normas de configuración para ruteadores.

1.2 Desarrollar una configuración de cortafuegos que bloquee todo el tráfico de redes y hosts “no confiables”, exceptuados los protocolos necesarios para el ambiente de datos de los tarjetahabientes.

1.3 Desarrollar una configuración de cortafuegos que restrinja las conexiones entre los servidores públicamente accesibles y cualquier componente de sistema que guarde datos de los tarjetahabientes, incluyendo cualquier conexión de redes inalámbricas. Esta configuración de cortafuegos debe incluir lo siguiente:

- **1.3.1** Restringir el tráfico entrante de Internet a las direcciones de Internet (IP) dentro del DMZ (filtros de ingreso).
- **1.3.2** No permitir que las direcciones internas pasen de Internet al DMZ (filtros de egreso)
- **1.3.3** Implementar inspección completa, también conocida como filtrado dinámico de paquetes (es decir, permitir solamente la entrada a la red desde conexiones “establecidas”).
- **1.3.4** Colocar la base de datos en una zona interna de la red, segregada del DMZ.

1.3.5 Restringir el tráfico entrante y saliente a aquel que sea necesario para el ambiente de datos de los tarjetahabientes.

1.3.6 Asegurar y sincronizar los archivos de configuración de ruteador. Por ejemplo, los archivos de configuración de ejecución (utilizados para la ejecución normal de los ruteadores), y archivos de configuración de inicio de operaciones (utilizados cuando se hace un *re-booting* de las máquinas), deben tener la misma configuración segura).

1.3.7 Rechazar todo otro tráfico entrante y saliente que no esté específicamente permitido.

1.3.8 Instalar cortafuegos perimétricos entre cualquier red inalámbrica y el ambiente de datos de los tarjetahabientes, y configurar estos cortafuegos para rechazar o controlar (si dicho tráfico es necesario para los fines del negocio) todo el tráfico desde el ambiente inalámbrico.

1.3.9 Instalar software de cortafuego personal en cualquier computador móvil y/o de propiedad de los empleados con conectividad directa a Internet (por ejemplo, laptops utilizados por los empleados) mediante los cuales se acceda a la red de la organización.

1.4 Prohibir el acceso público directo entre redes externas y cualquier componente de sistema que guarde datos de los tarjetahabientes (por ejemplo, bases de datos, bitácoras, archivos de rastreo).

1.4.1 Implementar un DMZ para filtrar y controlar todo el tráfico, a fin de prohibir las rutas directas del tráfico entrante y saliente de Internet.

1.4.2 Restringir el tráfico saliente de las aplicaciones de tarjetas de pago a las direcciones de Internet (IP) dentro del DMZ.

1.5 Implementar máscaras de IP para prevenir que las direcciones internas se traduzcan y revelen en Internet. Usar tecnologías que implementan el espacio de dirección RFC 1918 tales como Port Address Translation (PAT) o Network Address Translation (NAT).

Requisito 2: No usar contraseñas de sistemas y otros parámetros de seguridad provistos por los suplidores.

Los delincuentes que roban datos de los computadores (comúnmente llamados "hackers", que pueden ser externos o internos en una compañía) a menudo usan las contraseñas y otras opciones automáticamente programadas por los suplidores y proveedores para comprometer la seguridad de los sistemas. Estas contraseñas y opciones son bien conocidas entre los delincuentes y fácilmente se determinan por medio de información pública.

2.1 Cambiar siempre los valores por defecto provistos por los suplidores **antes** de instalar un sistema en la red (por ejemplo, incluir contraseñas, Protocolo de Manejo de Red Simple (SNMP), cadenas comunitarias y eliminación de cuentas innecesarias).

2.1.1 En los **ambientes inalámbricos**, cambiar los valores por defecto programados por los vendedores del equipo inalámbrico, incluyendo, sin limitación, claves WEP (Wired Equivalent Privacy), SSID (Service Set Identifier) de selección automática, contraseñas y cadenas comunitarias SNMP. Deshabilitar transmisiones SSID. Habilitar la tecnología Wi-Fi Protected Access (WPA y WPA2) para la encriptación y la autenticación cuando exista capacidad WPA.

2.2 Desarrollar normas de configuración para todos los componentes de sistemas. Asegurar que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y sean coherentes con las normas de más alta seguridad aceptadas en la industria según han sido definidas por ejemplo, por SysAdmin Audit Network Security Network (SANS), el National Institute of Standards Technology (NIST), y el Center for Internet Security (CIS).

2.2.1 Implementar solamente una función primaria por servidor (por ejemplo, los servidores de Web, servidores de base de datos y servidores de nombre de dominio (DNS) se deben implementar en servidores separados).

2.2.2 Deshabilitar todos los servicios y protocolos innecesarios (servicios y protocolos que no sean directamente necesarios para realizar la función especificada de los dispositivos).

2.2.3 Configurar los parámetros de seguridad del sistema para prevenir el uso indebido.

2.2.4 Eliminar todas las funcionalidades innecesarias, tales como archivos de comandos (scripts), accionadores, funciones, subsistemas, sistemas de archivo y servidores de Web innecesarios.

2.3 Encriptar todo el acceso administrativo que no sea de consola. Usar tecnologías como SSH, VPN, o SSL/TLS para la administración basada en Web y otros tipos de acceso administrativo sin consola.

2.4 Los proveedores de servicios de hospedaje en redes deben proteger el ambiente y los datos de cada entidad. Estos proveedores deben cumplir con los requisitos específicos detallados en el Apéndice A: “Normas de Seguridad de Datos de la Industria de Tarjeta de Pago: Aplicabilidad para Proveedores de Servicio de Hospedaje en Redes”.

Proteger los Datos de los Tarjetahabientes

Requisito 3: Proteger los Datos de los Tarjetahabientes.

La encriptación es un componente crítico en la protección de los datos de los tarjetahabientes. En el caso de que un intruso lograra penetrar los controles de seguridad de otras redes y acceder a los datos encriptados, si no tiene las claves criptográficas apropiadas no podrá leer los datos ni podrá usarlos. Otros métodos eficaces para proteger los datos almacenados deben considerarse como oportunidades potenciales para mitigar los riesgos. Por ejemplo, los métodos para minimizar los riesgos incluyen no almacenar datos de los tarjetahabientes a menos que sea absolutamente necesario, truncar los datos de los tarjetahabientes si no se necesita el Número de Cuenta Primario (PAN), y no enviar el número de cuenta en correos electrónicos no encriptados.

3.1 Mantener el mínimo de datos de tarjetahabientes almacenados. Desarrollar una política de retención y eliminación de los datos. Limitar la cantidad de datos almacenados y el tiempo de retención a los que se requieren para fines comerciales, legales y/o regulatorios, según se haya documentado en la política de retención de datos

3.2 No almacenar datos de autenticación confidenciales después de la autorización (ni siquiera en forma encriptada). Los datos confidenciales de autenticación incluyen los citados en los siguientes Requisitos 3.2.1 a 3.2.3*:*

3.2.1 No guardar el contenido íntegro de ninguna pista de la banda magnética (en el reverso de una tarjeta, en un chip o en algún otro lugar). Estos datos se conocen alternativamente como “full track”, “track (pista)”, “track (pista) 1”, “track (pista) 2” y datos de la banda magnética.

En el curso normal del negocio podría surgir la necesidad de retener los siguientes elementos de datos de la banda magnética: el nombre del titular de la cuenta, el número de cuenta primario o PAN, la fecha de vencimiento y el código de servicio. A fin de minimizar el riesgo, almacene solamente aquellos elementos de datos necesarios para la conducción de los negocios. NUNCA guarde el código de verificación de la tarjeta o el valor de verificación del número de identificación personal (PIN). Nota: Vea el “Glosario” para obtener información más detallada.

3.2.2 No guardar el código de validación de la tarjeta (el código de tres o cuatro dígitos impreso en el frente o en el reverso de una tarjeta de pago) que se utiliza para verificar las transacciones de tarjeta ausente.

Nota: Ver el “Glosario” para obtener información más detallada.

3.2.3 No guardar el Número de Identificación Personal (PIN) ni el bloque de PIN encriptado.

3.3 Enmascarar el número de cuenta primario (PAN) cuando se despliegue el mismo (los primeros seis y los últimos cuatro dígitos son el número máximo de dígitos que se puede desplegar).

Note: Este requisito no se aplica a los empleados y otras entidades que necesiten específicamente ver los números de cuenta completos, ni tampoco sobresee los requisitos más estrictos establecidos para el despliegue de los datos de los tarjetahabientes (por ejemplo, en los recibos de punto de venta).

3.4 Asegurar que, como mínimo, el número de cuenta primario sea ilegible en cualquier lugar donde esté guardado (incluyendo datos en medios digitales portátiles, medios de respaldo, registros o bitácoras, y datos recibidos de redes inalámbricas o guardados en las mismas) utilizando los siguientes métodos:

- Valores de control de alta seguridad de una sola vía (“hashed indexes”)
- Números truncados

- Tokens de índice y PAD guardado bajo seguridad
- Criptografía de alta seguridad con procesos y procedimientos de administración de claves asociados.

La información MÍNIMA sobre las cuentas que necesita estar en forma ilegible es el número de cuenta de la tarjeta de pago (PAN).

Si por algún motivo una compañía no puede encriptar los datos de los tarjetahabientes, consulte el Apéndice B: "Controles de Compensación para Encriptación de Datos Almacenados".

3.4.1 Si se usa la encriptación de disco (en lugar de la encriptación a nivel de archivo o columna de base de datos), el acceso lógico deberá administrarse en forma independiente de los mecanismos de control de acceso del sistema operativo nativo (por ejemplo, no usando las cuentas del sistema local o del Directorio Activo). Las claves de decriptación no deberán estar vinculadas a cuentas de usuarios.

3.5 Proteger las claves (o llaves) de encriptación contra la divulgación y el uso indebido.

3.5.1 Restringir el acceso a las claves y llaves al número mínimo de custodios necesarios.

3.5.2 Guardar las claves en forma segura en el mínimo número de ubicaciones y formatos posibles.

3.6 Documentar e implementar totalmente todos los procesos y procedimientos de administración de claves, incluyendo:

3.6.1 Generación de claves de alta seguridad

3.6.2 Distribución segura de claves

3.6.3 Almacenaje seguro de claves

3.6.4 Cambio periódico de las claves

- Según se considere necesario y recomiende la aplicación asociada (por ejemplo, volver a digitar la clave); preferiblemente en forma automática.
- Al menos anualmente.

3.6.1 Destrucción de claves viejas

3.6.2 Conocimiento no compartido y control dual de las claves (de forma que se requiera a dos o tres personas, cada una de las cuales conozca solamente una parte de la clave, para reconstruir la clave completa)

3.6.3 Prevención de la sustitución no autorizada de claves

3.6.4 Reemplazo de claves cuando se sepa o sospeche que su seguridad ha sido comprometida

3.6.5 Revocación de las claves viejas o inválidas

3.6.6 Requisito de que los custodios de claves firmen un formulario especificando que comprenden y aceptan su responsabilidad como custodios de las claves.

Requisito 4: Encriptar la información de los tarjetahabientes e información confidencial transmitida a través de redes públicas abiertas.

La información confidencial debe encriptarse durante su transmisión a través de las redes, ya que es fácil y común que un defraudador intercepte y/o redirija los datos mientras se encuentran en tránsito.

4.1 Usar criptografía y protocolos de alta seguridad como Secure Sockets Layer (SSL) / Transport Layer Security (TLS) e Internet Protocol Security (IPSEC) para salvaguardar los datos confidenciales de los tarjetahabientes durante su transmisión a través de redes públicas abiertas.

Ejemplos de redes públicas abiertas que caen bajo el alcance de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI) son Internet, WiFi (IEEE 802.11x), sistema global para comunicaciones móviles (GSM), y servicio general de paquete de radio (GPRS).

4.1.1 **En el caso de las redes inalámbricas que transmitan datos de los tarjetahabientes,** encriptar las transmisiones usando las tecnologías WiFi Protected Access (WPA o WPA2), IPSEC VPN, o SSL/TLS. No depender nunca exclusivamente del protocolo Wired Equivalent Privacy (WEP) para proteger la confidencialidad y el acceso a una red de acceso local (LAN) inalámbrica. Si se usa el protocolo WEP, hacer lo siguiente:

- Usar con una clave de encriptación que tenga un mínimo de 104 bits y un valor de inicialización de 24 bits
- Usar SOLAMENTE en conjunción con WiFi Protected Access (WPA o WPA2), VPN, o SSL/TLS.
- Rotar las claves WEP compartidas trimestralmente (o en forma automática) si la tecnología lo permite.
- Rotar las claves WEP compartidas siempre que haya cambios en el personal con acceso a las claves.
- Restringir el acceso basándose en la dirección de código de acceso de medios (MAC).

4.2 No enviar nunca números de cuenta de tarjetahabientes (PAN) por correo electrónico sin encriptar.

Mantener un Programa de Manejo de Vulnerabilidad

Requisito 5: Usar y actualizar regularmente el software antivirus.

Muchas vulnerabilidades y virus maliciosos y destructivos entran al sistema a través de la actividad de correo electrónico de los empleados. El software antivirus deberá utilizarse en todos los sistemas de correo electrónico y computadores de escritorio para proteger los sistemas de cualquier programación destructiva.

5.1 Implementar mecanismos antivirus en todos los sistemas comúnmente afectados por virus (por ejemplo, computadores y servidores).

Nota: Los sistemas comúnmente afectados por virus típicamente no incluyen sistemas operativos basados en UNIX ni mainframes.

5.1.1 Asegurar que los programas antivirus sean capaces de detectar, eliminar y proteger contra otros tipos de softwares dañinos, incluyendo spyware y adware.

5.2 Asegurar que todos los mecanismos antivirus estén actualizados, estén funcionando activamente y sean capaces de generar registros de auditoría

Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguras.

Las personas sin escrúpulos utilizan las vulnerabilidades en la seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades se pueden subsanar mediante parches de seguridad desarrollados por los proveedores y todos los sistemas deben contar con las actualizaciones y parches de seguridad más recientes de software para estar protegidos contra la explotación por parte de empleados, delincuentes externos y virus. Nota: Los parches de software apropiados son los que han sido evaluados y probados suficientemente para determinar que los parches no causan conflicto con las configuraciones de seguridad existentes. En el caso de las aplicaciones desarrolladas internamente por

la institución es posible evitar numerosas vulnerabilidades utilizando estándares reconocidos para desarrollo de sistemas y técnicas de codificación de seguridad.

6.1 Asegurar que todos los componentes de sistemas y software tengan instalados los parches de seguridad más recientes proporcionados por los proveedores dentro de un plazo de un mes de la fecha en que sean dados a conocer.

6.2 Establecer un proceso para identificar las vulnerabilidades de seguridad recientemente descubiertas (por ejemplo, suscribirse a los servicios de alerta disponibles en forma gratuita a través de Internet). Actualizar sus normas para subsanar cualquier nuevo problema de vulnerabilidad que pudiera surgir.

6.3 Desarrollar aplicaciones de software basadas en las mejores prácticas de la industria e incorporar la seguridad de la información a través de todo el ciclo de desarrollo de software.

- **6.3.1** Hacer pruebas de todos los parches de seguridad y cambios de configuración de software y sistema antes de implementarlos.
- **6.3.2** Mantener ambientes separados de desarrollo/prueba y producción.
- **6.3.3** Separar las responsabilidades entre los ambientes de desarrollo y prueba y producción
- **6.3.4** Los datos de producción (números reales de cuentas de tarjetas) no se usan para fines de prueba y desarrollo.
- **6.3.5** Eliminar todos los datos y cuentas de prueba antes de activar los sistemas de producción.
- **6.3.6** Eliminar las cuentas, nombres de usuarios y contraseñas de aplicaciones individuales antes que las aplicaciones se activen o se pongan a disposición de los clientes.
- **6.3.7** Revisar los códigos individuales antes de ponerlos en producción o a disposición de los clientes, a fin de identificar cualquier vulnerabilidad relacionada con la codificación

6.4 Seguir procedimientos de control de cambios para todas las modificaciones de configuración de sistemas y software. Los procedimientos deben incluir lo siguiente:

- **6.4.1** Documentación del impacto
- **6.4.2** Aprobación final por escrito (con firma) de los funcionarios apropiados
- **6.4.3** Pruebas que verifiquen la funcionalidad operativa
- **6.4.4** Procedimientos de cancelación

6.5 Desarrollar todas las aplicaciones Web basadas en directrices de codificación segura como Open Web Application Security Project. Revisar el código de aplicación individual para identificar vulnerabilidades en la codificación. Contemplar la prevención de vulnerabilidades comunes de codificación en los procesos de desarrollo de software, que incluyen:

- **6.5.1** Ingreso de datos sin validar
- **6.5.2** Control de acceso interrumpido (por ejemplo, uso malicioso de las identificaciones de usuarios)
- **6.5.3** Interrupción de la autenticación o administración de sesiones (uso de credenciales de cuenta y cookies de sesión)
- **6.5.4** Ataques con inyección de códigos en ventanas pertenecientes a diferentes dominios (el llamado Cross-Site Scripting o XSS)
- **6.5.5** Ataques de buffer overflow
- **6.5.6** Defectos de inyección (por ejemplo, inyección de SQL)
- **6.5.7** Manejo inapropiado de errores
- **6.5.8** Almacenaje sin la debida seguridad
- **6.5.9** Negación de servicio

6.5.10 Administración no segura de configuraciones

6.6 Asegurar que todas las aplicaciones hacia la Web estén protegidas contra ataques conocidos mediante la aplicación de cualquiera de los siguientes métodos:

- Hacer revisar el código de aplicación para detectar vulnerabilidades comunes por una organización especializada en la seguridad de las aplicaciones.
- Instalar un cortafuego de capa de aplicación frente a todas las aplicaciones con conexión de salida a la Web.

Nota: Este método se considera parte de las mejores prácticas hasta el 30 de junio de 2008, fecha en que se convertirá en un requisito.

Implementar Medidas Sólidas de Control de Acceso

Requisito 7: Restringir el acceso a los datos de los tarjetahabientes tomando como base la necesidad del funcionario de conocer la información.

Este requisito asegura que solamente el personal autorizado tenga acceso a los datos.

7.1 Limitar el acceso a los recursos de computación y a la información de los tarjetahabientes exclusivamente a aquellas personas que por necesidad de su trabajo requieran dicho acceso.

7.2 Establecer un mecanismo para los sistemas de múltiples usuarios que restrinja el acceso tomando como base la necesidad del usuario de conocer la información y esté programado para negar el acceso a todo el mundo, a menos que se permita específicamente el mismo.

Requisito 8: Asignar una identificación única a cada persona que tenga acceso a un computador.

Asignar una identificación (ID) única a cada persona que tenga acceso asegura que todas las acciones que impliquen datos y sistemas críticos sean realizadas por usuarios conocidos y autorizados y se puedan rastrear a los mismos.

8.1 Identificar a todos los usuarios mediante un nombre de usuario único antes de permitirles el acceso a los componentes de sistemas y datos de los tarjetahabientes.

8.2 Emplear al menos uno de los métodos enumerados a continuación además de la identificación única para autenticar a todos los usuarios:

- Contraseña
- Dispositivos de token (por ejemplo, SecureID, certificados o clave pública)
- Biométrica.

8.3 Implementar la autenticación de dos factores para el acceso remoto al sistema por parte de los empleados, administradores y terceros. Usar tecnologías como Remote Authentication and Dial-In Service (RADIUS) o Terminal Access Controller Access Control System (TACACS) con tokens, o VPN (basada en SSL/TLS o IPSEC) con certificados individuales.

8.4 Encriptar todas las contraseñas durante la transmisión y el almacenaje, en todos los componentes de sistemas.

8.5 Asegurar la autenticación y la administración apropiadas de las contraseñas de todos los usuarios no consumidores y administradores en todos los componentes de sistemas, de la manera siguiente:

8.5.1 Controlar la adición, eliminación y modificación de las identificaciones de usuarios, credenciales y otros objetos de identificación.

8.5.2 Verificar la identidad del usuario antes de reprogramar (reset) las contraseñas.

8.5.3 Programar la primera contraseña de un usuario a un valor único para dicho usuario y cambiarla inmediatamente después del primer uso.

8.5.4 Revocar inmediatamente el acceso de todo usuario que ya no sea un empleado o no lo requiera.

8.5.5 Eliminar las cuentas de usuarios inactivos al menos después de 90 días.

8.5.6 Habilitar cuentas para uso de los proveedores de mantenimiento remoto solamente durante el tiempo necesario.

8.5.7 Comunicar los procedimientos y políticas relacionadas con las contraseñas a todos los usuarios que tengan acceso a la información de los tarjetahabientes.

8.5.8 No usar cuentas o contraseñas grupales, compartidas o genéricas.

8.5.9 Cambiar la contraseña de los usuarios al menos cada 90 días.

8.5.10 Requerir una longitud mínima de contraseña de al menos siete caracteres.

8.5.11 Usar contraseñas que contengan tanto caracteres numéricos como alfabéticos.

8.5.12 No permitir a ninguna persona que presente una nueva contraseña que sea igual a cualquiera de las últimas cuatro que ha utilizado.

8.5.13 Limitar los intentos repetidos de lograr acceso bloqueando la ID del usuario después de un máximo de seis intentos.

8.5.14 Programar la duración de este bloqueo a treinta minutos o hasta que el administrador del sistema habilite la ID del usuario.

8.5.15 Si no ha habido actividad en una sesión durante más de 15 minutos, requerir que el usuario vuelva a ingresar la contraseña para reactivar el terminal.

8.5.4 Autenticar todos los accesos a cualquier base de datos que contenga información de los tarjetahabientes. Esto incluye acceso por parte de las aplicaciones, los administradores y todos los demás usuarios.

Requisito 9: Restringir el acceso físico a los datos de los tarjetahabientes.

Cualquier acceso físico a los datos o sistemas que contienen datos de los tarjetahabiente brinda una oportunidad para acceder a dispositivos o datos y eliminar sistemas o copias impresas, y debe ser restringido de forma apropiada.

9.1 Usar controles apropiados de entrada a las instalaciones para limitar y monitorear el acceso a los sistemas que almacenan, procesan o transmiten datos de los tarjetahabientes.

9.1.1 Usar cámaras para vigilar las áreas vulnerables. Auditar estos datos y correlacionar con otros. Guardar durante al menos tres meses, a menos que existan otras restricciones impuestas por la ley.

9.1.2 Restringir el acceso físico a los conectores de redes (network jacks) que estén accesibles al público.

9.1.3 Restringir el acceso físico a los puntos de acceso inalámbrico, puentes y pasarelas de conexión y dispositivos de mano (handheld).

9.2 Desarrollar procedimientos para ayudar al personal a distinguir fácilmente a los empleados de los visitantes en las áreas en que la información de los tarjetahabientes está accesible.

"Empleado" se refiere a los funcionarios que laboran a jornada completa o parcial, empleados y personal temporal y consultores "residentes" en la ubicación. Un "visitante" es un proveedor, invitado de un funcionario o cualquier otra persona que entre a las instalaciones durante un período breve, normalmente no más de un día.

9.3 Asegurar que todos los visitantes:

- **9.3.1** Sean autorizados antes de entrar a las áreas donde se procesa o mantiene la información de los tarjetahabientes.
- **9.3.2** Reciban una identificación física (gafete o dispositivo de acceso) que caduque y que los identifique como personas que no son empleados.
- **9.3.3** Entreguen su identificación física antes de salir de las instalaciones o en la fecha en que caduque la misma.

9.4 Usar un registro de visitantes para mantener una bitácora física de auditoría sobre la actividad de visitas. Retener este registro por un mínimo de tres meses, a menos que existan otras restricciones impuestas por la ley.

9.5 Guardar las copias de respaldo en un lugar seguro fuera de las instalaciones, que puede ser las instalaciones de un tercero o un almacenaje comercial.

9.6 Asegurar físicamente todos los medios electrónicos y en papel (es decir, computadores, medios electrónicos y hardware de redes y comunicaciones, líneas de telecomunicaciones, recibos en papel, reportes impresos y telefacsímiles) que contengan información de los tarjetahabientes.

9.7 Mantener un control estricto de la distribución interna o externa de cualquier tipo de medio que contenga información de los tarjetahabientes.

- **9.7.1** Marcar los medios con una etiqueta para que puedan ser identificados como confidenciales.
- **9.7.2** Enviar los medios a través de un servicio de mensajería o mecanismo de entrega seguro que pueda trazarse en forma precisa.

9.8 Asegurar que la administración apruebe todos los medios que se trasladen desde áreas seguras (particularmente cuando estos medios se distribuyan a personas).

9.9 Mantener un control estricto del almacenaje y accesibilidad de los medios que contengan información de los tarjetahabientes.

- **9.9.1** Mantener un inventario apropiado de todos los medios y asegurar que los mismos estén almacenados en forma segura.

9.10 Destruir los medios que contengan información de los tarjetahabientes cuando ya no sean necesarios para el negocio o por razones legales:

- **9.10.1** Pasar los materiales impresos por una trituradora que corte en zig zag o reducirlos a pulpa.
- **9.10.2** Purgar, borrar electrónicamente, triturar o de otra manera destruir físicamente los medios electrónicos para que los datos de los tarjetahabientes no se puedan reconstruir.

Monitorear y Probar Regularmente las Redes

Requisito 10: Rastrear y monitorear todo el acceso a los recursos de la red y datos de los tarjetahabientes.

Los mecanismos de registro y la capacidad de rastrear las actividades de los usuarios son factores críticos. La presencia de registros o bitácoras en todos los ambientes permite un rastreo y análisis detallados cuando algo marcha mal. Determinar la causa de un compromiso de seguridad es una tarea muy difícil cuando el sistema no cuenta con registros de actividad.

10.1 Establecer un proceso para vincular todos los accesos a componentes del sistema (particularmente aquellos realizados con privilegios administrativos - root) a un usuario individual.

10.2 Implementar pistas de auditoría automatizadas para reconstruir los siguientes eventos en todos los componentes de sistemas:

- **10.2.1** Todos los accesos individuales a los datos de los tarjetahabientes
- **10.2.2** Todas las acciones de cada persona con privilegios root o administrativos
- **10.2.3** Acceso a todas las bitácoras de auditoría
- **10.2.4** Intentos inválidos para lograr un acceso lógico
- **10.2 5** Uso de mecanismos de identificación y autenticación
- **10.2.6** Inicialización de los registros o bitácoras de auditoría
- **10.2.7** Creación y eliminación de todos los objetos a nivel de sistema

10.3 Registrar al menos los siguientes eventos en las bitácoras de auditoría en todos los componentes de sistemas:

- **10.3.1** Identificación de usuario
- **10.3.2** Tipo de evento
- **10.3.3** Fecha y hora
- **10.3.4** Indicación de éxito o fallo
- **10.3.5** Origen del evento
- **10.3.6** Identidad o nombre de los datos, componente de sistema o recurso afectado

10.4 Sincronizar todos los relojes y horas de todos los sistemas críticos.

10.5 Asegurar las bitácoras de auditoría para que no se puedan alterar, incluyendo las siguientes:

- **10.5.1** Limitar la visualización de las pistas de auditoría a las personas que tengan necesidad de verlas por razones de su trabajo.
- **10.5.2** Proteger los archivos de pistas de auditoría de las modificaciones no autorizadas.
- **10.5.3** Respaldar rápidamente los archivos de pistas de auditoría a un servidor centralizado o medio de respaldo que sea difícil de alterar.
- **10.5.4** Copiar los registros o bitácoras de las redes inalámbricas a un servidor de la red de acceso local (LAN).
- **10.5.5** Usar software de detección para monitorear la integridad y detectar cualquier cambio en las bitácoras a fin de asegurar que los datos existentes en dichos registros no se puedan cambiar sin generar un alerta (aunque al agregar nuevos datos no se deberá generar un alerta).

10.6 Revisar los registros y bitácoras de todos los componentes de sistemas al menos diariamente. Estas revisiones deben incluir todos los servidores que realicen funciones de seguridad como los servidores IDS (Intrusion Detection System) y de autenticación, autorización y contabilidad (AAA), como por ejemplo, RADIUS.

Nota: Se pueden usar herramientas de cosecha, "parsing" y alerta para cumplir con el Requisito 10.6.

10.7 Retener el historial de pistas de auditoría durante un mínimo de un año, con un mínimo de tres meses de disponibilidad en línea.

Requisito 11: Probar regularmente los sistemas y procesos de seguridad.

Los delincuentes que roban datos de los computadores e investigadores continuamente descubren nuevas vulnerabilidades que se introducen a través de nuevos softwares. Los sistemas, procesos y programas deben probarse frecuentemente para garantizar que los mismos mantengan su seguridad a través del tiempo y los cambios.

11.1 Probar anualmente los controles de seguridad, limitaciones, conexiones de redes y restricciones para asegurar que puedan identificar o detener en forma apropiada cualquier intento de uso no autorizado. Usar un analizador inalámbrico al menos trimestralmente para identificar todos los dispositivos inalámbricos en uso.

11.2 Realizar escanes de vulnerabilidad de redes internas y externas al menos trimestralmente y después de cualquier cambio significativo en la red (por ejemplo, instalación de nuevos componentes de sistemas, cambios en la topología de red, modificación de reglas de cortafuegos, mejora de productos).

Nota: Los escanes trimestrales de vulnerabilidades externas deberá realizarlos un proveedor calificado por la industria de tarjetas de pago. El personal interno de la empresa deberá realizar los escanes después de implementar cambios de sistemas.

11.3 Realizar pruebas de penetración de la infraestructura de la red y aplicaciones al menos una vez al año y después de actualizar o mejorar significativamente la infraestructura o cualquier aplicación (por ejemplo, actualización del sistema operativo, adición de una subred al ambiente, adición de un servidor de Web al ambiente). Estas pruebas de penetración deberán incluir lo siguiente:

11.3.1 Pruebas de penetración de capas de red

11.3.2 Pruebas de penetración de capas de aplicaciones.

11.4 Usar sistemas de detección de intrusiones en la red, sistemas de detección de intrusiones basados en host y/o sistemas de prevención de intrusiones para monitorear todo el tráfico de la red y alertar al personal sobre cualquier sospecha de compromiso de seguridad. Mantener al día todos los motores de detección y prevención de intrusiones.

11.5 Implementar monitoreo de la integridad de los archivos para alertar al personal sobre cualquier modificación no autorizada de un sistema o contenido de un archivo crítico y configurar el software para realizar comparaciones de archivos críticos al menos semanalmente.

Los archivos críticos no son necesariamente o únicamente aquellos que contienen datos de los tarjetahabientes. Para fines de monitoreo de integridad de archivos, los archivos críticos son normalmente aquellos que no cambian regularmente, pero cuya modificación podría indicar un compromiso o riesgo de compromiso de seguridad del sistema. Los productos para monitorear la integridad de los archivos normalmente vienen pre-configurados con los archivos críticos para el sistema operativo relacionado. Otros archivos críticos tales como los de aplicaciones individuales, deben ser evaluados y definidos por el comercio o proveedor de servicio.

Mantener una Política de Seguridad de la Información

Requisito 12: Mantener una política que contemple la seguridad de la información para los empleados y contratistas.

Una política sólida de alta seguridad establece la pauta de la seguridad en toda la compañía y hace a los empleados tomar conciencia de lo que se espera de ellos. Todos los empleados deben estar conscientes del carácter confidencial de los datos y de su responsabilidad de protegerlos.

12.1 Establecer, mantener y diseminar una política de seguridad que logre lo siguiente:

- **12.1.1** Contemple todos los requisitos de esta especificación.
- **12.1.2** Incluya un proceso anual para identificar amenazas y vulnerabilidades y traiga como resultado una evaluación formal de los riesgos.
- **12.1.3** Incluya una revisión al menos una vez al año y una actualización cuando el ambiente cambie.

12.2 Desarrollar procedimientos diarios de seguridad operativa que sean congruentes con los requisitos establecidos en esta especificación (por ejemplo, procedimientos de mantenimiento de cuentas, procedimientos de revisión de registros y bitácoras).

12.3 Desarrollar políticas de uso para tecnologías críticas que usan los empleados (como módems y dispositivos inalámbricos), a fin de definir el uso apropiado de estas tecnologías por parte de todos los empleados y contratistas. Asegurar que estas políticas de uso requieran lo siguiente:

- **12.3.1** Aprobación explícita de la administración
- **12.3.2** Autenticación para el uso de la tecnología
- **12.3.3** Una lista de todos los dispositivos y personal que tiene acceso a ellos
- **12.3.4** Etiquetas en los dispositivos que indiquen su dueño, información de contacto y propósito
- **12.3.5** Usos aceptables de la tecnología
- **12.3.6** Ubicaciones aceptables en la red para estas tecnologías
- **12.3.7** Una lista de los productos aprobados por la empresa
- **12.3.8** Desconexión automática de las sesiones de módem después de un período específico de inactividad
- **12.3.9** Activación de módems por parte del proveedor solamente cuando sea necesario, con desactivación inmediata después del uso.
- **12.3.10** Al acceder datos de los tarjetahabientes en forma remota por módem, deshabilitar el almacenaje de dichos datos en discos duros locales, disquetes y otros medios externos. Deshabilitar igualmente las funciones que permiten cortar y pegar e imprimir datos durante el acceso remoto.

12.4 Garantizar que la política y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información en el caso de todos los empleados y contratistas.

12.5 Asignar a una persona o equipo las siguientes responsabilidades de administración de seguridad de la información:

- **12.5.1** Establecer, documentar y distribuir las políticas y los procedimientos de seguridad.
- **12.5.2** Monitorear y analizar los alertas y la información de seguridad y distribuirlos al personal apropiado.

12.5.3 Establecer, documentar y distribuir procedimientos de respuesta a incidentes y procedimientos para acudir a una autoridad superior a fin de asegurar un manejo oportuno y eficaz en todas las situaciones.

12.5.4 Administrar las cuentas de usuarios incluyendo la adición, eliminación y modificación de información.

12.5.5 Monitorear y controlar todo el acceso a los datos.

12.6 Implementar un programa formal para promover la conciencia sobre la seguridad a fin de que que todos los empleados cobren conciencia de la importancia que tiene la seguridad de los datos de los tarjetahabientes.

12.6.1 Educar a los empleados en el momento de su contratación y al menos anualmente por medio de afiches, cartas, memorandos, reuniones y promociones.

12.6.2 Requerir a los empleados que hagan constar por escrito que han leído y comprenden la política y los procedimientos de seguridad de la compañía.

12.7 Hacer una investigación de antecedentes de los candidatos a empleo para minimizar el riesgo de ataques procedentes de fuentes internas.

En el caso de los empleados que sólo tengan acceso a un número de tarjeta en un momento dado para facilitar una transacción, este requisito es solamente una recomendación.

12.8 Si los datos de los tarjetahabientes se comparten con proveedores de servicio, requerir contractualmente lo siguiente:

12.8.1 Que los proveedores de servicio deben adherirse a los requisitos establecidos en las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS).

12.8.2 Un acuerdo que incluya el reconocimiento de que el proveedor de servicio es responsable por la seguridad de los datos de los tarjetahabientes que dicho proveedor posea.

12.9 Implementar un plan de respuesta a incidentes. Estar preparado para responder inmediatamente a una violación del sistema.

12.9.1 Crear un plan de respuesta a incidentes, el cual se implementará en caso de un compromiso de la seguridad del sistema. Asegurar que el plan contemple, como mínimo, procedimientos específicos de respuesta a incidentes, recuperación comercial y reanudación de actividades comerciales, procesos de respaldo de datos, papeles y responsabilidades y estrategias de comunicación y contacto (por ejemplo, informar a los Adquirentes y a las asociaciones de tarjetas de pago).

12.9.2 Probar el plan al menos una vez al año.

12.9.3 Designar a miembros específicos del personal que estén disponibles 24 horas al día los 7 días de la semana para responder a los alertas.

12.9.4 Proporcionar capacitación apropiada al personal que tenga la responsabilidad de responder a una violación de la seguridad.

12.9.5 Incluir alertas de sistemas de detección de intrusiones, prevención de intrusiones y monitoreo de la integridad de los archivos.

12.9.6 Desarrollar un proceso para modificar y mejorar el plan de respuesta a incidentes según las lecciones aprendidas de la experiencia e incorporar los desarrollos en la industria.

12.10 Todos los procesadores y proveedores de servicio deberán mantener e implementar políticas y procedimientos para administrar a las entidades conectadas, que incluyan lo siguiente:

12.10.1. Mantener una lista de las entidades conectadas.

12.10.2. Asegurar que se proceda con la debida diligencia antes de conectar a una entidad.

12.10.3. Asegurar que la entidad cumpla con las Normas de Seguridad de Datos de la Industria de Tarjetas de Ppago (PCI DSS).

12.10.4. Conectar y desconectar a las entidades siguiendo un proceso establecido.

Apéndice A: Aplicabilidad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) para Proveedores de Servicios de Hospedaje en Redes

Requisito A.1: El proveedor del servicio de hospedaje en redes protegerá el ambiente de datos de los tarjetahabientes.

Según se menciona en el Requisito 12.8, se requiere que todos los proveedores de servicio que tengan acceso a los datos de los tarjetahabientes (incluidos los proveedores de servicios de hospedaje en redes) se adhieran a los requisitos establecidos en las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Además, el Requisito 2.4 estipula que todos los proveedores de servicios de hospedaje en redes deberán proteger el ambiente y los datos hospedados de cada entidad. Por consiguiente, los proveedores de servicios de hospedaje en redes deberán dar especial consideración a lo siguiente:

A.1 Proteger el ambiente y los datos hospedados de cada entidad (es decir, del comercio, del proveedor de servicio o de otra entidad) según se indica en los puntos A.1.1 a A.1.4:

- **A.1.1** Asegurar que cada entidad tenga acceso únicamente a su propio ambiente de datos de tarjetahabientes.
- **A.1.2** Restringir el acceso y los privilegios de cada entidad solamente a su propio ambiente de datos de tarjetahabientes.
- **A.1.3** Asegurar que estén habilitadas las bitácoras y pistas de auditoría y que sean únicas para el ambiente de datos de tarjetahabientes de cada entidad y cumplan con el Requisito 10 de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS).
- **A.1.4** Habilitar procesos que aseguren la investigación forense oportuna en caso de un compromiso de la seguridad de cualquier comercio hospedado o proveedor de servicios.

El proveedor de servicios de hospedaje en redes deberá cumplir con estos requisitos, así como con otras secciones relevantes de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS).
Nota: Aunque el proveedor del servicio de hospedaje cumpla con estos requisitos, el cumplimiento de la entidad que utiliza los servicios de hospedaje de dicho proveedor no está necesariamente garantizado. Cada entidad deberá cumplir individualmente con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) y validar su cumplimiento en la forma que sea aplicable.

Apéndice B: Controles Compensatorios

Controles Compensatorios – Generalidades

Podrían considerarse controles compensatorios para la mayoría de los requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) cuando una entidad no pueda cumplir con una especificación técnica de un requisito pero tenga suficientemente mitigado el riesgo asociado con la misma. Véase el Glosario de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) para obtener una definición completa de los controles compensatorios.

La eficacia de un control compensatorio depende de las características específicas del ambiente en el cual se implemente el control, los controles de seguridad que lo rodeen y la configuración del control. Las empresas deben estar conscientes de que un control compensatorio en particular no será eficaz en todos los ambientes. Cada control compensatorio deberá evaluarse en forma exhaustiva después de su implementación para garantizar su eficacia.

Las siguientes orientaciones proporcionan controles compensatorios cuando las compañías no puedan lograr que los datos de los tarjetahabientes sean ilegibles, según dicta el requisito 3.4.

Controles Compensatorios para el Requisito 3.4

En el caso de las empresas que no puedan lograr que los datos de los tarjetahabientes sean ilegibles (por ejemplo, por encriptación) debido a restricciones técnicas o limitaciones comerciales, podrían considerarse controles compensatorios. *Únicamente las compañías que hayan pasado por un análisis de riesgo y tengan restricciones tecnológicas o comerciales documentadas y legítimas pueden considerar el uso de controles compensatorios para cumplir con los requisitos.*

Las empresas que consideren controles compensatorios para hacer ilegibles los datos de los tarjetahabientes deben estar conscientes del riesgo que corren al mantener estos datos en forma legible. Generalmente los controles deben proporcionar protección adicional para mitigar cualquier riesgo adicional que corran los datos legibles de los tarjetahabientes. Los controles considerados deberán ser adicionales a los controles requeridos en las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) y deben satisfacer la definición de “Controles Compensatorios” que se da en el Glosario de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Los controles compensatorios pueden consistir en un dispositivo o conjunto de dispositivos, aplicaciones y controles que cumplan con **todas** las condiciones siguientes:

1. Proporcionar segmentación/abstracción adicional (Por ejemplo, en la capa de red)
2. Proporcionar la capacidad de restringir el acceso a los datos de los tarjetahabientes o bases de datos basándose en los siguientes criterios:
   - Dirección IP /dirección Mac
   - Aplicación/servicio
   - Cuentas/grupos de usuarios
   - Tipo de datos (filtrado de paquete)
3. Restringir el acceso lógico a la base de datos
   - Controlar el acceso lógico a la base de datos en forma independiente al Directorio Activo o Lightweight Directory Access Protocol (LDAP)
4. Prevenir/detectar ataques comunes a las aplicaciones o bases de datos (por ejemplo, inyección de SQL).