PPCIDSS-00 Política de seguridad de datos de tarjetas de pago y cumplimiento PCIDSS

25 AGOSTO 2025. – V2.2

Índice

Control documental

Control de cambios

VERSIÓN	FECHA	ANOTACIONES/CAMBIOS	AUTOR	CARGO
1.0	06/06/2019	Edición Inicial	MMG	Resp. Infraestructura
1.1	10/05/2020	Revisión. Sin cambios.	MMG	Resp. Infraestructura
1.2	16/09/2020	Revisión. Sin cambios.	MMG	Resp. Infraestructura
1.3	27/01/2021	Incumplimiento de la política. Definición de PCIDSS. Documentación de referencia.	MMG	Resp. Infraestructura
1.4	31/01/2022	Revisión. Sin cambios.	MMG	Resp. Infraestructura
1.5	31/05/2023	Actualización domicilio fiscal y logos de certificación	618	Ingeniero de procesos
1.6	06/02/2024	Integración contenido PR-29. Cambio de nombre a Política de Seguridad para la protección de datos de tarjetas de pago	618	Ingeniero de procesos
2.0	02/10/2024	Adecuación a PCIDSS V4.0 Inclusión Matriz RACI de responsabilidades PCIDSS	386	Resp. SIG
2.1	17/03/2025	Aptdo 4.1 : Se incluye la prohibición explícita de guardar cualquier tipo de Dato de Cuenta (CHD o SAD) Se incluye "Los datos de cuenta (CHD o SAD) no serán almacenados una vez se haya realizado la autorización" Aptdo. 4.2.5 Se incluye la obligación de revisar el alcance cuando se produzcan cambios organizativos.	386	Resp. SIG
2.2	25/08/2025	Actualización Imagen Gráfica Eliminación de enlace a Informe de Seguimiento tareas BAU	386	Resp. SIG

Revisión

FECHA	NOMBRE	ÁREA	CARGO
17/03/25	YF 386	Ciberseguridad Calidad	Ing. Ciberseguridad Resp. SIG

Aprobación

FECHA	NOMBRE	ÁREA	CARGO
03/04/2025	Comité SGSI	-	-

Distribución

DESTINATARIOS	CANAL DE COMUNICACIÓN
Plantilla	Intranet/Together
Partes interesadas Externas	Web

Glosario de términos

TÉRMINO	DEFINICIÓN

Documentación de referencia

TIPO	CÓDIGO	DESCRIPCIÓN
MANUAL	MPCIDSS	MPCIDSS – MANUAL DE OPERACIONES CON DATOS DE TARJETA EN OMNICHANNEL PAYMENTS. PCI DSS. ALCANCE OPERACIONES CON TARJETAS DE PAGO.
MANUAL	MSGSI	MANUAL DE SEGURIDAD DE LA INFORMACIÓN
POLÍTICA	PRH-03	POLÍTICA DE USO ACEPTABLE Y RESPONSABILIDAD DEL USUARIO
POLÍTICA	PRH-02	POLÍTICA DE PROCESO DISCIPLINARIO
POLÍTICA	PSGSI-00	POLÍTICA DE SEGURIDAD
POLÍTICA	PPCIDSS-02	POLÍTICA DE BASTIONADO DE SISTEMAS

TIPO	CÓDIGO	DESCRIPCIÓN
POLÍTICA	PPCIDSS-05	POLÍTICA DE ANTIVIRUS
POLÍTICA	PPCIDSS-08	POLÍTICA PARA LA CONFIGURACIÓN DE DISPOSITIVOS DE RED
POLÍTICA	PSGSI-11	POLÍTICA DE DESARROLLO SEGURO
POLÍTICA	PSGSI-14	POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
POLÍTICA	PSGSI-17	POLÍTICA DE AUTORIZACIONES DE ACCESO
REGISTRO	R-PCIDSS-00	BAU: PROGRAMA DE TAREAS PERIÓDICAS
PROCEDIMIENTO	PR-09	CONTROL DE ACCESO
PROCEDIMIENTO	PR-31	MONITORIZACIÓN Y RESPUESTA ANTE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

1 Objeto

El objetivo de esta política es:

- Evitar los accesos no autorizados, daños e interferencias de la información relativa a datos de tarjetas de pago
- Evitar pérdidas, daños, robos, interrupciones de servicio
- Evitar cualquiera otra circunstancia, que pongan en peligro los activos que conforman el entorno de datos de tarjetahabiente (CDE o Cardholder Data Environment) de Alisys Digital S.L.U. (en adelante, Alisys) en los que se **adquieren, almacenan, procesan y transmiten** información de **tarjetas de pago**.
- Garantizar el cumplimiento de la Norma PCIDSS de aplicación en Alisys

2 Campo de aplicación

Las disposiciones definidas en este documento aplican a todo el personal de Alisys para el desarrollo de sus actividades, así como para otras entidades colaboradoras o terceros involucrados, en las que se adquieren, almacenan, procesan y transmiten información de tarjetas de pago para la realización de sus actividades de negocio.

3 Requisitos para la protección de datos de tarjetas de pago

Alisys Digital, en el ámbito de su solución **OMNICHANNEL PAYMENTS**, gestiona información relacionada con **datos de tarjetas de pago**.

La protección de los datos de tarjetas de pago, se gestiona en Alisys de acuerdo con los requisitos exigidos en el **Estándar de Seguridad de Datos de Payment Card Industry (PCI DSS), en su versión 4.0.**

Este Estándar se desarrolló para fomentar y mejorar la seguridad de los datos del tarjetahabiente y para facilitar la adopción generalizada de medidas de seguridad de datos consistentes a nivel mundial. PCI DSS proporciona una base de requisitos técnicos y operativos diseñados para proteger los datos del tarjetahabiente. Si bien está diseñado específicamente para enfocarse en entornos con datos de cuentas de tarjetas de pago, PCI DSS también se pueden utilizar para proteger de amenazas y asegurar otros elementos en el ecosistema de pagos.

En esta norma se especifican 12 requisitos para el cumplimiento, organizados en 6 secciones relacionadas lógicamente. Dichos requisitos son también llamadas "**OBJETIVOS DE CONTROL**" y son los siguientes:

Estándar de Seguridad de Datos PCI: Descripción General de Alto Nivel	
Construya y Mantenga Redes y Sistemas Protegidos	**1.** Instale y Mantenga Controles de Seguridad en la Red. **2.** Aplique Configuraciones Protegidas para Todos los Componentes del Sistema
Proteja los Datos del tarjetahabiente	**3.** Proteja los Datos de Cuenta Almacenados. **4.** Proteja los Datos del Titular de la Tarjeta con una Sólida Criptografía Durante la Transmisión a Través de Redes Públicas Abiertas.
Mantenga un Programa de Gestión de Vulnerabilidades	**5.** Proteja Todos los Sistemas y Redes de Software Malintencionado. **6.** Desarrolle y Mantenga Sistemas y Softwares Protegidos.
Implemente Medidas Sólidas de Control de Acceso	**7.** Restrinja el Acceso a los Componentes del Sistema y a los Datos del Titular de la Tarjeta Según las Necesidades Comerciales. **8.** Identifique a los Usuarios y Autentique el Acceso a los Componentes del Sistema **9.** Restrinja el Acceso Físico a los Datos del Titular de la Tarjeta
Monitorear y Verificar las Redes Regularmente.	**10.** Registre y Monitorear Todo el Acceso a los Componentes del Sistema y a los Datos del Titular de la Tarjeta. **11.** Verifique la Seguridad de los Sistemas y Redes Regularmente.
Mantenga una Política de Protección Informática	**12.** Respalde la Protección Informática con Políticas y Programas Organizacionales.

4 Principios generales de actuación

La Dirección establece los siguientes principios que deben cumplirse obligatoriamente dentro del entorno de comunicaciones e infraestructura propia o relacionada con datos de tarjeta.

4.1. Prohibiciones

- Se prohíbe el acceso, copia, transmisión o cualquier tipo de gestión sobre los datos de tarjeta.
- Se prohíbe el uso de cualquier medio removible para el almacenamiento de datos de tarjeta.
- Se prohíbe guardar cualquier tipo de Dato de cuenta (CHD o SAD).
- Los datos de cuenta (CHD o SAD) no serán almacenados una vez se haya realizado la autorización
- Una vez finalizada la llamada, los únicos datos almacenados relevantes serán el código de la operación de cobro, el importe, el teléfono y el resultado de la operación, así como los datos de referencia, relativos al resultado de la operación de cobro del TPV virtual de los proveedores en caso de que el resultado haya sido satisfactorio. En ningún caso se almacenarán datos de tarjeta.

4.2. Obligaciones

4.2.1. Borrado de datos de tarjeta:

- Es obligatorio el borrado de datos de tarjeta al finalizar la llamada, así como mantener una tarea programada de borrado automático diario como sistema de backup.
- El equipo de Explotación, con la pertinente autorización, debe establecer y mantener una vigilancia activa sobre los procesos de **borrado automático y programado de los datos de tarjeta.**

4.2.2. Comunicaciones

- Todas las **comunicaciones** entre el entorno securizado de IVR de Pago y el exterior deben ir sobre canal cifrado TLS igual a 1.3 y se deben inhabilitar las versiones 1.0 y

1.1 por ser vulnerables.

4.2.3. Pruebas de Seguridad

- Mantener un histórico de **registros de auditoría** como mínimo de 1 año y con un mínimo de disponibilidad en línea de 3 meses.
- Deben establecerse y mantenerse mecanismos de vigilancia y alerta detallada de control de seguridad sobre el entorno.
- Se debe realizar **análisis trimestrales internos de vulnerabilidades** conocidas, lo gestiona el personal cualificado del Departamento de Ciberseguridad.
- Realizar **análisis trimestrales externo**, conocido como **ASV**, por proveedor externo certificado por el PCI SSC (Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago).
- Se deben realizar **PRUEBAS DE PENETRACIÓN INTERNAS Y EXTERNAS** al menos una vez al año o bien después de un cambio significativo.

4.2.4. Software antivirus:

- Debe cumplirse con las políticas establecidas en el documento interno denominado: **PPCIDSS-05 POLÍTICA ANTIVIRUS** dónde se especifica la normativa en su uso y mantenimiento.
- **Actualizaciones de Seguridad**: debe cumplirse con las políticas establecidas en el documento interno denominado: **PPCIDSS-01 POLÍTICA DE APLICACIÓN DE PARCHES DE SEGURIDAD** dónde se especifica la normativa en su uso y mantenimiento

4.2.5. Cambios

- Implementar mecanismos de **control de cambios** no autorizados sobre archivos críticos del sistema.
- Cuando se produzcan cambios en la estructura organizacional de Alisys, se revisará el alcance PCI DSS para analizar si será afectado o no.

4.3. Seguridad en otras aplicaciones web de Alisys relacionada con operaciones bajo el alcance de PCI DSS:

- Deben adherirse a las mismas medidas de seguridad descritas en la sección Ciclo de vida del desarrollo, también se deben revisar y probar vulnerabilidades adicionales.

- Anualmente, o siempre que se hayan producido modificaciones, las aplicaciones web expuestas a internet deben someterse a **pruebas de penetración** realizadas por un proveedor externo o haber implementado soluciones técnicas automatizadas que detecten e impidan continuamente los ataques basados en la web, como los firewalls de aplicaciones web (WAF) y tecnologías de Autoprotección de Aplicaciones en Tiempo de Ejecución (RASP).

  .

5 Desarrollo y mantenimiento de una red segura

5.1. Firewall

Cada plataforma relacionada con los servicios de adquisición, almacenamiento, procesamiento y/o transmisión de información de tarjetas de pago se encontrarán en entornos completamente protegidos al exterior y segmentados.

Asimismo, se mantendrá una **única puerta de enlace hacia el exterior** alojada en el firewall perimetral.

5.2. Uso de contraseñas

Los requisitos establecidos para el uso de contraseñas se encuentran definidos en el procedimiento **PR-09 CONTROL DE ACCESO**.

6 Protección de los datos de tarjeta

6.1. Visualización de datos de tarjeta

Se debe garantizar la protección de los números de tarjetas de pago a medida que se muestran.

En consecuencia, se establecen las siguientes reglas:

- Ningún empleado/a de Alisys Digital tendrá visibilidad del PAN completo, excepto aquellos que tengan una necesidad de negocio legítima de ver el PAN completo.
- Mostrar PAN completo en pantallas de computadora, recibos, faxes o cualquier tipo de medio de copia impresa está en contra de la presente política y de LA **PSGSI-00 POLÍTICA DE SEGURIDAD** de Alisys.
- Se puede mostrar un máximo de los primeros seis y los últimos cuatro dígitos del PAN. Todos los demás dígitos deben estar enmascarados.
- Cualquier aplicación utilizada por Alisys que muestre información de la tarjeta de crédito debe configurarse para ocultar o enmascarar esos datos sensibles o confidenciales (si es posible). Si el propósito de la aplicación implica mostrar el número completo de la tarjeta de crédito u otros datos personales, el Responsable de Seguridad debe aprobar su uso. En todos los casos, este tipo de aplicación debe limitarse al menor número posible de usuarios requeridos.

6.2. Transmisión segura de datos

6.2.1. Transmisión a través de redes no confiables

Para evitar la interceptación o el uso indebido de los datos, cualquier información confidencial o sensible que se transmita a través de redes públicas debe protegerse mediante fuertes técnicas de cifrado, como:

- Capa de conexión segura (SSL) o TLS
- Seguridad de protocolo de Internet (IPSEC)

6.2.2. Tecnologías de mensajería para el usuario final

No está permitido que los empleados envíen por correo electrónico información confidencial o sensible no cifrada, como el PAN de tarjetas de crédito.

Si existe una justificación comercial válida, el Departamento de sistemas proporcionará software de correo electrónico cifrado a dicho empleado.

Además, no está permitido que los empleados envíen PAN sin protección a través de otras tecnologías de mensajería como mensajería instantánea, chat o texto.

7 Programa de gestión de vulnerabilidades

Se define y aplica un conjunto de métodos para prevenir o mitigar los ataques de software más comunes y las vulnerabilidades relacionadas, como ataques de inyección, manipulación de datos y estructuras de datos, explotación de la criptografía, ataques a la lógica del negocio y mecanismos de control de acceso.

7.1. Uso y mantenimiento de software antivirus

Se emplearán aplicaciones contra software malicioso, con el objetivo de detectar y eliminar estas amenazas de acuerdo con las disposiciones establecidas en la **PPCIDSS-05 Política de antivirus**.

7.2. Análisis de vulnerabilidades internas

Las evaluaciones de vulnerabilidades internas se efectúan trimestralmente, utilizando para ello la herramienta Nessus Professional, la cual debe estar constantemente actualizada con los últimos datos sobre vulnerabilidades. Dichos análisis son ejecutados por personal cualificado del Departamento de Ciberseguridad. Tras cada evaluación, se elabora un informe técnico detallado que incluye, como mínimo, la identificación de cada vulnerabilidad con su correspondiente clasificación de riesgo, los activos comprometidos, el software involucrado, un plan de remediación específico para cada vulnerabilidad identificada y una fecha límite para su resolución. La implementación de medidas correctivas está a cargo del equipo del Departamento de Ciberseguridad, en colaboración con los miembros del proyecto afectado. Las vulnerabilidades categorizadas como críticas y de alto riesgo recibirán atención prioritaria para minimizar el periodo de exposición al riesgo; las demás vulnerabilidades se tratarán de acuerdo con el nivel de riesgo asignado en el análisis de riesgo corporativo.

7.3. Análisis de vulnerabilidades externas (ASV)

Las evaluaciones de vulnerabilidad externa, conocidas como ASV (por sus siglas en inglés, Approved Scanning Vendor), se realizan cada trimestre y son llevadas a cabo por un proveedor certificado por el PCI SSC (Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago).

El equipo del Departamento de Ciberseguridad es responsable de gestionar las

vulnerabilidades identificadas, trabajando en estrecha colaboración con los integrantes de los proyectos implicados. Es requisito que, antes de finalizar el trimestre en curso dentro del ciclo programado para las evaluaciones ASV, el proveedor externo realice un nuevo escaneo para verificar la corrección de las vulnerabilidades previamente detectadas; limitando así el período disponible para la resolución de vulnerabilidades a este marco temporal.

La gestión de los análisis de vulnerabilidades se gestionará de acuerdo con lo especificado en el **PR-38 GESTIÓN DE VULNERABILIDADES**

8 Desarrollo Seguro

El proceso de desarrollo seguido en Alisys debe considerar las pautas de **OWASP**. Estas pautas están disponibles en el siguiente sitio web:

OWASP Foundation, la fundación de código abierto para la seguridad de aplicaciones | Fundación OWASP

8.1. Capacitación en Codificación Segura

La capacitación en codificación segura es obligatoria, con carácter anual, para todos los desarrolladores de Alisys Digital y el contenido de los cursos incluirán temáticas que ayuden a responder al menos las siguientes preguntas:

- ¿cuáles son las diferentes vulnerabilidades y ataques potenciales?
- ¿cómo adoptar estrategias de mitigación durante el proceso de desarrollo para prevenir vectores de ataque?

8.2. Revisiones del Código

Se efectúan revisiones del código para asegurar su desarrollo conforme a las pautas de codificación segura, buscando activamente tanto vulnerabilidades existentes como emergentes.

En las revisiones se buscarán elementos claves como características ocultas, uso seguro de componentes externos, manejo adecuado del registro, análisis de estructuras de código inseguras, detección de vulnerabilidades lógicas y revisión por pares.

La dirección debe revisar y aprobar el código antes de su lanzamiento, garantizando la adherencia a los estándares de seguridad establecidos y limitando la posibilidad de omitir el proceso de revisión.

8.2.1. Pruebas del Código

Durante la fase de revisión y prueba del código, se deben verificar obligatoriamente las siguientes vulnerabilidades:

- Gestión de configuración insegura
- Entrada no validada

- Negación de servicio
- Uso malicioso de ID de usuario
- Almacenamiento inseguro
- Uso malicioso de credenciales de cuenta y cookies de sesión
- Errores de manejo de errores
- Secuencias de comandos entre sitios
- Inyección SQL y otras fallas de inyección de comandos
- Desbordamientos de búfer

Las disposiciones sobre desarrollo seguro se establecen y desarrollan en la **PSGSI-11 POLÍTICA DE DESARROLLO SEGURO** y en el **PR-20 DESARROLLO POR RELEASE**

9 Medidas de control de acceso

- Todo el personal de Alisys dispondrá de una **identificación única de acceso.**
- El control de acceso se hará por usuarios autorizados en el Directorio Activo (LDAP), configurándose el factor de autenticación múltiple (MFA) para cada uno de ellos.
- A nivel de acceso al servicio, todo acceso se canalizará a través del **SSO** de la compañía.
- La habilitación de accesos siempre seguirá los **principios de mínimo privilegio y necesidad de conocer.**
- Para la concesión de permisos de acceso a recursos compartidos se establecen roles de usuario que marcan el derecho de acceso en función del departamento y el puesto ostentado por cada trabajador/a. Cada rol solamente tendrá acceso a los recursos que sean estrictamente necesarios para el desarrollo adecuado de sus funciones.
- Solo se accederá a entornos de producción en caso de intervenciones operativas y resolución de emergencias.

9.1. Aprobación y/o Autorización de acceso

- Todos los accesos deben ser aprobados por el Comité de Seguridad de la Información.
- Todo acceso se incorporará al registro de habilitaciones de seguridad.

9.2. Revisión de accesos concedidos

- Todos los accesos se revisarán con una periodicidad fija con el objetivo de mantener, reducir o ampliar los permisos existentes.

Estas disposiciones también serán aplicables a cada uno de los proveedores o socios de negocio que necesiten tecnologías de acceso remoto.

Las medidas expuestas se desarrollan con mayor nivel de detalle en el procedimiento **PR-09 CONTROL DE ACCESO**.

10 Monitorizar y probar regularmente la redes

10.1. Rastreo y monitorización de acceso

La monitorización de los accesos se realizará en tiempo real utilizando un SIEM y sus agentes de control de eventos instalados en los elementos operativos del entorno en el que se gestionan datos de tarjeta.

10.1.1. Registros de auditoría (logs)

Los registros de auditoría se implementan para respaldar la detección de anomalías y actividades sospechosas, y el análisis forense de eventos.

Se capturará la siguiente información y/o datos:

- Se capturarán registros de todo acceso de usuarios individuales a los datos de titulares de tarjetas y todos los intentos de acceso lógico inválidos.
- Se capturarán registros de todas las acciones realizadas por personas con privilegios elevados.
- Se capturarán registros de todo el acceso a los registros de auditoría.
- Se capturarán registros de todos los cambios de identificación y credenciales de autenticación.
- Se capturarán los registros de alteraciones que indican que un sistema ha sido modificado con respecto a su funcionalidad original.

En general, los registros de auditoría guardan los siguientes detalles para cada evento auditable:

- Identificación del usuario
- Tipo de evento
- Fecha y hora
- Indicación de Exitoso o Fallido
- Origen del evento

- Identidad o nombre de los datos, componentes del sistema, recursos o servicios afectados (por ejemplo, nombre y protocolo).

Estos logs se almacenarán hasta un año para permitir el análisis y la correlación de datos.

Asimismo, diariamente se verificará que los usuarios sólo tienen acceso a los sistemas y datos que necesitan para realizar sus tareas y, a su vez, se tratará de detectar cualquier actividad sospechosa, para su posterior investigación y, si corresponde, la aplicación de las medidas de mitigación correspondientes.

11 Programa de cumplimiento de los servicios prestados por proveedores

Es necesario exigir a todos los proveedores externos de servicio en el entorno del CDE el mismo grado de seguridad que ALISYS aplica a sus sistemas de información.

Es indispensable que ALISYS mantenga el control sobre toda su seguridad, aun cuando esté siendo gestionada por terceros.

Para ello es necesario controlar que la relación con todos los proveedores con acceso al CDE está suficientemente protegida en base a los acuerdos y contratos correspondientes.

Se relacionan a continuación los controles que deben aplicarse a las relaciones mantenidas con cada uno de los proveedores de ALISYS:

CONTROL	DESCRIPCIÓN	PERIODICIDAD
Requisitos de seguridad en productos y servicios	Definir los requisitos mínimos de seguridad que deben cumplir los servicios que se contratan	Antes de la contratación del servicio
Definir cláusulas contractuales en materia de seguridad de la información	Elaborar y aceptar cláusulas contractuales rigurosas en cuanto a ciberseguridad	Antes de la contratación del servicio
Definir las responsabilidades concretas por ambas partes	Delimitar las responsabilidades de cada una de las partes	Antes de la contratación del servicio
Definir los acuerdos de Nivel de Servicio (SLA)	Definir los acuerdos de nivel de servicio que ALISYS somete a los servicios contratados	Antes de la contratación del servicio
Controles de Seguridad Obligatorios	Informar al proveedor, mediante una matriz de responsabilidades, de los requisitos de la normativa PCI de obligado cumplimiento por su parte y controlar periódicamente su cumplimiento	Antes de la contratación del servicio
Certificación de los servicios contratados	Exige a los proveedores evidencias de las certificaciones en materia de seguridad de la información, especialmente en los contratos de mayor criticidad	En la formalización del contrato
Auditoría y control de servicios contratados	En necesario supervisar que los productos y servicios contratados responden a lo acordado en materia de ciberseguridad	Antes y durante la contratación del servicio
Controlar la reputación de los proveedores	-	Permanentemente
Finalización de la relación contractual	Garantizar la seguridad de la información de ALISYS tras la finalización de un servicio.	A la finalización del servicio

Más información sobre compras y proveedores en el **PR-15 COMPRAS Y APROVISIONAMIENTOS.**

12 Funciones y responsabilidades del programa de cumplimiento de PCI

(Requisito 1.1 Norma PCIDSS V4.0)

Se definen a continuación las responsabilidades para cumplir el programa PCI

RESP. DE SEGURIDAD	Definido en el **MSGSI MANUAL DE SEGURIDAD DE LA INFORMACIÓN** de Alisys
RESP. GENERAL DE MANTENER EL CUMPLIMIENTO DE PCI DSS	Definido en el **MSGSI MANUAL DE SEGURIDAD DE LA INFORMACIÓN** de Alisys

12.1. Diagrama RACI del programa de cumplimiento pci

Atributos/Responsables	Responsable	Autorizante	Consultado	Informado
GESTIÓN DEL PROGRAMA PCI				
Políticas de Seguridad de la información	Comité SGSI			
Definición del proceso de gestión de riesgos	Resp. Seguridad REsp. Cumplimiento	Comité SGSI		
Evaluaciones anuales/periódicas de riesgos	Comité SGSI			
Ejecución del proceso de gestión de riesgos	Comité SGSI			
Política de uso aceptable	Comité SGSI			
Estado general de cumplimiento de del programa PCI	Resp. Cump PCI			
Definición y gestión del alcance de PCI	Resp. Seguridad REsp. Cumplimiento	Comité SGSI		
Comunicación del programa PCI a la dirección ejecutiva.	Resp. Cump PCI			
Programa de concientización sobre seguridad PCI	Resp. Cump PCI			
Verificaciones de antecedentes	RRHH			
Programa de gestión de riesgos de proveedores PCI	LEGAL			Comité SGSI
Matriz de responsabilidad de cara al cliente (solo SP)	Resp. Cump PCI			
Seguridad de red (Req. 1)				
Definición, implementación y mantenimiento del conjunto de reglas de control de seguridad de la red	Resp. Seguridad			Sistemas
Aprobaciones de cambios del NSC	Sistemas			
Mantenimiento del diagrama de red	Sistemas			
Mantenimiento del diagrama de flujo de datos	Sistemas			
Revisiones semestrales de configuración/conjunto de reglas del NSC	Sistemas			

Atributos/Responsables	Responsable	Autorizante	Consultado	Informado
Arquitectura de seguridad de red	Sistemas			
Seguridad de la red de dispositivos móviles	Sistemas			
Configuración segura de sistemas (Req. 2)				
Definiciones y aplicación de estándares de configuración segura de infraestructura	Sistemas			
Definiciones y aplicación de los estándares de configuración segura de las estaciones de trabajo	Sistemas			
Definiciones y aplicación de los estándares de configuración segura de aplicaciones/dispositivos	Sistemas			
Definiciones y aplicación de los estándares de configuración segura de contenedores	Sistemas			
Definiciones y aplicación de los estándares de configuración segura de plataformas en la nube	Sistemas			
Gestión de protocolos y servicios inseguros	Sistemas			
Definición y aplicación de los estándares de configuración segura de redes inalámbricas	Sistemas			Ciberseguridad Ingeniería
Seguridad del almacenamiento de datos (Req. 3)				
Definición y aplicación de la política de retención de datos	Ingeniería	Resp. Seguridad		Sistemas Ciberseguridad
Definición y aplicación de estándares de cifrado de datos	Ingeniería			Sistemas Ciberseguridad
Gestión de Acceso PAN/SAD	Ingeniería	Resp. Seguridad		Sistemas Ciberseguridad
Definición y aplicación de estándares de gestión de claves criptográficas	Ingeniería	Resp. Seguridad		Sistemas Ciberseguridad
Seguridad de la transmisión de datos (Req. 4)				
Definición y aplicación de estándares de seguridad de transmisión basados en Internet	Sistemas	Resp. Seguridad	Ingeniería	Ingeniería Ciberseguridad
Inventario de claves confiables y mantenimiento de certificados	Sistemas		Ingeniería	Ingeniería Ciberseguridad
Definición y aplicación de estándares de seguridad inalámbrica	Sistemas	Resp. Seguridad	Ingeniería	Ingeniería Ciberseguridad
Seguridad de comunicación/transmisión PAN del usuario final	Sistemas		Ingeniería	Ingeniería Ciberseguridad
Protección contra software malicioso (Req. 5)				
Definiciones, aplicación y supervisión de estándares antimalware	Ciberseguridad		Sistemas	Sistemas
Evaluación de riesgos y clasificación de sistemas que no corren riesgo de sufrir malware	Ciberseguridad		Sistemas	Sistemas
Definiciones, aplicación y supervisión de estándares antiphishing	Ciberseguridad		Sistemas	Sistemas
Desarrollo y mantenimiento de software seguro (Req. 6)				

Atributos/Responsables	Responsable	Autorizante	Consultado	Informado
Definición, aplicación y mantenimiento del estándar SSDLC	Ingeniería	Resp. Seguridad	Ciberseguridad	Ingeniería
Formación en codificación/desarrollo seguro	RRHH			
Aprobación final para implementaciones de código	Ingeniería			
Monitoreo e identificación de vulnerabilidades	Ingeniería			Ciberseguridad
Definición, aplicación y supervisión del estándar de gestión de vulnerabilidades	Ciberseguridad			
Gestión de parches de sistemas	Sistemas			
Definición, aplicación y supervisión del conjunto de reglas WAF	Ciberseguridad			
Definición, aplicación y seguimiento del proceso de gestión segura de cambios	Ingeniería			
Definición y aplicación de privilegios mínimos (Req. 7)				
Definición, aplicación y supervisión del modelo de control de acceso de usuarios	Sistemas			
Definición, aplicación y supervisión del modelo de control de acceso a cuentas de aplicaciones/sistemas	Sistemas			
Aprobaciones de solicitudes de acceso	Resp. Seguridad	Comité SGSI		
Revisión de acceso de usuarios	Sistemas			
Revisiones de acceso de cuenta de sistema/aplicación	Sistemas			
Definición, aplicación y supervisión de políticas de control de acceso	Sistemas			
Gestión de identificación y autenticación (Req. 8)				
Definición, aplicación y supervisión de políticas de identificación y autenticación	Sistemas	Comité SGSI		Sistemas Ingeniería Ciberseguridad
Definición, aplicación y seguimiento de estándares de gestión de cuentas de usuario	Sistemas	Comité SGSI		Sistemas Ingeniería Ciberseguridad
Definición y facilitación del proceso de restablecimiento de contraseña	Sistemas	Comité SGSI		Sistemas Ingeniería Ciberseguridad
Definición y facilitación del proceso de incorporación de usuarios	Sistemas	Comité SGSI		Sistemas Ingeniería Ciberseguridad
Definición y facilitación del proceso de terminación del usuario	Sistemas	Comité SGSI		Sistemas Ingeniería Ciberseguridad
Gestión de acceso remoto de terceros	Sistemas	Comité SGSI		Sistemas Ingeniería Ciberseguridad
Definición, aplicación y supervisión de estándares de autenticación	Sistemas	Comité SGSI		Sistemas Ingeniería Ciberseguridad
Definición, aplicación y seguimiento de estándares de gestión de cuentas de clientes	Sistemas	Comité SGSI		Sistemas Ingeniería Ciberseguridad

Atributos/Responsables	Responsable	Autorizante	Consultado	Informado
Definición, aplicación y seguimiento de directrices y estándares de autenticación de clientes	Sistemas	Comité SGSI		Sistemas Ingeniería Ciberseguridad
Definición, aplicación y supervisión de estándares de gestión de cuentas de sistema/aplicación	Sistemas	Comité SGSI		Sistemas Ingeniería Ciberseguridad
Seguridad Física (Req. 9)				
Definición, aplicación y monitoreo de políticas de seguridad física	Resp. Seguridad	Comité SGSI		Sistemas Ingeniería Ciberseguridad
Definición, aplicación y seguimiento del procedimiento de acceso de visitantes	Resp. Seguridad			Sistemas Ingeniería Ciberseguridad
Almacenamiento, distribución y destrucción seguros de CHD Media	Sistemas			Sistemas Ingeniería Ciberseguridad
Clasificación de medios CHD	Sistemas			Sistemas Ingeniería Ciberseguridad
Mantenimiento del inventario de medios electrónicos CHD	Sistemas			Sistemas Ingeniería Ciberseguridad
Definición, aplicación y seguimiento de la política y el procedimiento de protección de puntos de interés	N.A.	N.A.	N.A.	N.A.
Mantenimiento de inventario de puntos de interés	N.A.	N.A.	N.A.	N.A.
Inspección e informes de dispositivos POI	N.A.	N.A.	N.A.	N.A.
Formación en protección de POI	N.A.	N.A.	N.A.	N.A.
Registro y Monitorización (Req. 10)				
Definición, aplicación y supervisión de políticas de registro de eventos y monitoreo	Ciberseguridad		Sistemas	
Definición, aplicación y supervisión de estándares de registro de eventos de seguridad	Ciberseguridad	Resp. Seguridad	Sistemas	
Definición, aplicación y monitoreo de estándares de monitoreo de seguridad	Ciberseguridad	Resp. Seguridad	Sistemas	
Definición, aplicación y supervisión del estándar de protección de registros de eventos de seguridad	Ciberseguridad	Resp. Seguridad	Sistemas	
Mantenimiento y validación del modelo de orígenes y destinos de registros de seguridad PCI	Ciberseguridad		Sistemas	
Definición, aplicación y supervisión del manual de seguimiento de registros de seguridad	Ciberseguridad		Sistemas	
Monitoreo y clasificación de alertas de registros de seguridad	Ciberseguridad		Sistemas	
Definición, aplicación y seguimiento del proceso de respuesta a incidentes	Ciberseguridad	Resp. Seguridad	Sistemas	
Ejecución de respuesta a incidentes	Ciberseguridad	Resp. Seguridad	Sistemas	
Declaración de Incidencias	Ciberseguridad	Resp. Seguridad	Sistemas	
Formación del personal de respuesta a incidentes	Ciberseguridad		Sistemas	
Definición, aplicación y supervisión del estándar de gestión del tiempo del sistema	Ciberseguridad		Sistemas	

Atributos/Responsables	Responsable	Autorizante	Consultado	Informado
Monitoreo y respuesta del control de seguridad crítico	Ciberseguridad		Sistemas	
Pruebas de Seguridad (Req. 11)				
Definición, aplicación y supervisión de políticas de pruebas de seguridad	Ciberseguridad	Resp. Seguridad	Sistemas	Ingeniería
Monitoreo y respuesta de AP no autorizados + mantenimiento de inventario WAP	Ciberseguridad	Resp. Seguridad	Sistemas	Ingeniería
Ejecución y clasificación del análisis de vulnerabilidades internas	Ciberseguridad	Resp. Seguridad	Sistemas	Ingeniería
Ejecución y clasificación del análisis de vulnerabilidades externas	Ciberseguridad		Sistemas	Sistemas Ingeniería
Análisis de vulnerabilidades para encontrar soluciones	Ciberseguridad		Sistemas	Sistemas
Definición, aplicación y seguimiento de la metodología de pruebas de penetración (externas e internas)	Ciberseguridad	Resp. Seguridad	Sistemas	Ingeniería
Ejecución de pruebas de penetración interna	Ciberseguridad		Sistemas	Sistemas
Ejecución de pruebas de penetración externa	Ciberseguridad		Sistemas	Ingeniería
Prueba(s) de penetración Búsqueda de clasificación y remediación	Ciberseguridad		Sistemas	Sistemas
Ejecución de pruebas de segmentación	Ciberseguridad		Sistemas	Ingeniería
Prueba(s) de segmentación Clasificación y remediación	Ciberseguridad		Sistemas	Sistemas
Definición, aplicación y supervisión de la arquitectura de seguridad	Ciberseguridad	Resp. Seguridad	Sistemas	Ingeniería
Implementación y configuración de IDS/IPS	Ciberseguridad		Sistemas	Sistemas
Implementación, configuración y mantenimiento del monitoreo de integridad de archivos (FIM)	Ciberseguridad		Sistemas	Ingeniería
Gestión y seguimiento de la detección de cambios en la página de pago	Ciberseguridad		Sistemas	Sistemas

12.2. Comprobación periódica del cumplimiento

A través de reuniones periódicas se verificará que las tareas se están ejecutando en tiempo y forma establecido en el programa. En dichas reuniones se revisará también el resultado de cada tarea y los hallazgos surgidos en ellas.

13 Programa de tareas periódicas (BAU) como garantía de cumplimiento

13.1. Definición y responsabilidades sobre las tareas que componen el programa

La verificación del cumplimiento de PCIDSS se sustentará y comprobará a través de la implementación del Programa BAU de PCIDSS**: R-PCIDSS-00 BAU: PROGRAMA DE TAREAS PERIÓDICAS**

Se trata de un conjunto de tareas a realizar de forma periódica, cuya configuración y programación se realizará a través de la herramienta de ticketing de la compañía.

13.2. Requisitos de cumplimentación

La definición y cumplimentación/ejecución de todas las tareas BAU deberá cumplir con los siguientes requisitos:

- Definición y programación de las tareas periódicas:.
    - Cada tarea debe estar asignada a un departamento/área o grupo, que será el encargado de resolver la tarea directamente (bien directamente o coordinando su resolución con el equipo que corresponda)
- Cumplimentación e información en el ticket sobre la ejecución de la tarea:
    - El ticket se irá actualizando de manera progresiva, con los detalles de las tareas realizadas a medida que estas se vayan ejecutando.
    - En el cierre se incluirá el resultado obtenido de la tarea confirmando si el resultado ha sido el esperado o si, por el contrario, existe algún tipo de hallazgo que deba ser revisado.
    - Siempre que sea posible se incluirá en el ticket una evidencia de su realización (capturas de pantalla, enlace a los informes generados, etc..).
    - En el caso de que la tarea no haya podido completarse, se debe describir el motivo del bloqueo. Por ejemplo, dependencias de IOPs, de cliente, etc.

13.2.1. Plazos de resolución

Los plazos de resolución se establecen de acuerdo a la periodicidad con la que se debe ejecutar la tarea y a la normativa que resulte de aplicación a Alisys (en este caso concreto según norma **PCIDSS**)

Plazos en los Requisitos PCI DSS	Descripciones y ejemplos
Diario	Todos los días del año (no sólo los días laborables).
Semanalmente	Al menos una vez cada siete días.
Mensualmente	Al menos una vez cada 30 o 31 días, o el n° del día del mes.
Cada tres meses ("trimestral")	Al menos una vez cada 90 a 92 días, o el n° del día de cada tercer mes.
Cada seis meses	Al menos una vez cada 180 a 184 días, o el n° del día de cada sexto mes.
Cada 12 meses ("anualmente")	Al menos una vez cada 365 días (o 366 para los años bisiestos) o en la misma fecha cada año.
Periódicamente	La frecuencia de ocurrencia queda a discreción de la entidad y está documentada y respaldada por el análisis de riesgos de la entidad. La entidad debe demostrar que la frecuencia es adecuada para que la actividad sea efectiva y cumpla con la intención del requisito.
Inmediatamente	Sin demora. En tiempo real o casi en tiempo real.
Con prontitud	Tan pronto como sea razonablemente posible.

Plazos establecidos por la Norma PCIDSS V4.0 para la resolución de las tareas en función de su periodicidad

El mantenimiento de la certificación PCI DSS requiere que durante los procesos de auditoría se presenten evidencias generadas durante los tres meses anteriores. En consecuencia, será necesario programar las tareas trimestrales (del trimestre correspondiente), semestrales (del semestre correspondiente) y anuales teniendo en cuenta estos plazos.

La auditoría de renovación se realizan habitualmente a finales del mes de Octubre, por lo que las tareas anuales y una secuencia de las trimestrales, por ejemplo, deberán realizarse durante los tres meses anteriores (Agosto, septiembre y el propio mes de Octubre)

Es posible que algunas tareas presenten dependencias, por ejemplo, IOPs o dependencias de cliente. Sin embargo, no se debe cerrar ninguna tarea que no se haya resuelto. Esta permanecerá abierta hasta resolver la dependencia.

14 Auditorías, pruebas y comprobaciones periódicas

Para garantizar la seguridad y la privacidad de los datos de tarjeta de crédito, Alisys llevará a cabo auditorías periódicas.

El objetivo de estas pruebas será evaluar el cumplimiento de las políticas y procedimientos de acceso a dichos datos.

15 Revisión, actualización y mantenimiento de la normativa de seguridad aplicable

Toda la normativa interna que afecte o aplique a la gestión de datos de tarjetas de pago deberá ser actualizada, obligatoriamente, **con carácter anual**.

Dicha actualización se evidenciará generando una nueva versión de cada documento con carácter anual, indicando “sin cambios” en el control del versionado cuando en el proceso de actualización se determine que no es necesario aplicar ningún cambio.

El objetivo de esta actualización es garantizar la adecuación de las políticas, normativas y procedimientos a los requisitos de la norma y a los estándares internos de seguridad de la compañía.

Esta documentación también deberá ser actualizada y/o modificada como resultado de:

- Los análisis de riesgos
- Cambios significativos en la estructura organizativa, en los procesos de negocio o en los activos de la compañía
- Por correcciones derivadas de lecciones aprendidas y/o planes de tratamiento de riesgo

16 Concienciación y formación

Es necesario que el personal de ALISYS conozca y aplique buenas prácticas en el uso de todo tipo de dispositivos y soluciones tecnológicas, especialmente en todo lo relacionado con el entorno de OMNICHANNEL con el objetivo de prevenir cualquier tipo de incidente. Para alcanzar los objetivos de la **PSGSI00_POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN** y en especial de la **PPCIDSS00_POLÍTICA DE CUMPLIMIENTO PCIDSS** es necesario incidir en la concienciación y formación en materia de Ciberseguridad de todo el personal. Igualmente, necesario será advertirles de los riesgos que puede suponer el mal uso de los dispositivos y de todas las soluciones tecnológicas que ALISYS pone a su alcance.

16.1. Programa anual de concienciación al personal

Para asegurar que el personal conoce, entiende y cumple las normas y las medidas de protección en materia de ciberseguridad se ha definido un programa anual de concienciación.

INFORMACIÓN	Destinatario	Canal	Periodicidad
Política de Seguridad de la Información	Todo el personal	Correo electrónico Intranet Corporativa	Anual
Política de Cumplimiento PCIDSS	Todo el personal	Correo electrónico Intranet Corporativa	Anual
Plan de Formación	Todo el personal	Intranet Corporativa	Anual
Formación específica sobre PCIDSS	Personal con acceso al entorno del CDE	Repositorio interno de formación	Incorporación a la empresa
Formación específica sobre DESARROLLO SEGURO	Personal implicado en el desarrollo del software	Centro de formación externo	Incorporación a la empresa
Programas de formación específicos	Personal con necesidades específicas de formación	Centro de formación externo	Cuando surja la necesidad
Evaluación del aprendizaje	Todo el personal que recibe formación	Correo electrónico Encuesta	A la finalización de cada acción formativa
Evaluación de la eficacia de la formación	Responsables del personal que ha realizado la formación	Correo electrónico	Trimestralmente
Promover la cultura de seguridad de la empresa	Todo el personal	Intranet Corporativa Cartelería en las oficinas	Trimestralmente

17 Comunicación

Para garantizar que las políticas de seguridad y los procedimientos e instrucciones técnicas que componen el Sistema de Seguridad de la Información sean de conocimiento para todo el personal y partes interesadas se ha definido la **PR-27 POLÍTICA DE COMUNICACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.**

17.1. Solicitudes de información por parte de clientes en relación al certificado PCIDSS de Alisys

(Req. 12.9.2 Norma PCIDSS V4.0)

Se podrá proporcionar a cliente información relativa al cumplimiento de PCIDSS por parte de Alisys siempre y cuando sea el cliente quien lo solicite de manera expresa.

La documentación a aportar puede ser:

- Información sobre el estado de cumplimiento de PCI DSS para cualquier servicio que Alisys realice en nombre de los clientes (Requisito 12.8.4).
- Información sobre qué requisitos de PCI DSS son responsabilidad del Alisys y cuáles son responsabilidad del cliente, incluidas las responsabilidades compartidas (Requisito 12.8.5).

Dicha información es propiedad del área de Calidad y Cumplimiento y, para su envío a cliente, será necesario que el departamento/área interesada en su envío a cliente, solicite esta información a través del correspondiente ticket al grupo SGSI.

18 Validación periódica del alcance de PCIDSS

(Requisito 12.5.2 Norma PCIDSS V4.0)

Se deberá confirma, al menos con carácter anual, el alcance de PCIDSS que deberá incluir, al menos, los siguientes aspectos:

- Identificar todos los flujos de datos para las distintas etapas de pago (por ejemplo, autorización, liquidación de captura, contracargos y reembolsos) y canales de aceptación (por ejemplo, tarjeta presente, tarjeta no presente y comercio electrónico).
- Actualización de todos los diagramas de flujo de datos según el requisito 1.2.4. •
- Identificar todas las ubicaciones donde se almacenan, procesan y transmiten los datos de la cuenta, incluidas, entre otras:
    - Cualquier ubicación fuera del CDE definido actualmente
    - Aplicaciones que procesan CHD
    - Transmisiones entre sistemas y redes, y
    - Copias de seguridad de archivos.
- Identificar todos los componentes del sistema en el CDE, conectados al CDE, o que podrían afectar la seguridad del CDE.
- Identificar todos los controles de segmentación en uso y los entornos de los que se segmenta el CDE, incluida la justificación de los entornos que están fuera del alcance
- Identificar todas las conexiones de entidades de terceros con acceso al CDE
- Confirmar que todos los flujos de datos identificados, los datos de cuenta, los componentes del sistema, los controles de segmentación y las conexiones de terceros con acceso al CDE están incluidos en el alcance.

La validación del alcance se realizará en el **MPCIDSS – MANUAL DE OPERACIONES CON DATOS DE TARJETAS DE PAGO EN OMNICHANNEL PAYMENTS. ALCANCE PCIDSS.**

19 Incumplimiento de la política

Alisys hará responsable al usuario de las consecuencias derivadas por el incumplimiento de las políticas y normas establecidas en este documento.

Alisys se reserva el derecho de evaluar periódicamente el cumplimiento de esta normativa.

Cualquier acción disciplinaria derivada del incumplimiento de la misma será considerada de acuerdo a los procedimientos establecidos.

El incumplimiento de las disposiciones aquí presentes puede estar sujeta a la aplicación de medidas disciplinarias, de acuerdo con lo establecido en la **PRH-02 POLÍTICA DE PROCESO DISCIPLINARIO** y la legislación vigente.

alisys

Calle Cronos, Nº63, Planta 2ª, Local 4
28037 Madrid
+34 910 200 000

info@alisys.net
www.alisys.net