PPCIDSS-00 Política de seguridad para la protección de datos de tarjetas de pago

06. FEBRERO. 2024. – V1.6

618 | 622 | 386

ISO 9001 ISO 27001 ISO 14001 ISO 27018

PCI DSS COMPLIANCE

CNMC COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA

Índice

Control documental

Control de cambios

VERSIÓN	FECHA	ANOTACIONES/CAMBIOS	AUTOR	CARGO
1.0	06/06/2019	Edición Inicial	Mario Miguel	Resp. Infraestructura
1.1	10/05/2020	Revisión. Sin cambios.	Mario Miguel	Resp. Infraestructura
1.2	16/09/2020	Revisión. Sin cambios.	Mario Miguel	Resp. Infraestructura
1.3	27/01/2021	Incumplimiento de la política. Definición de PCIDSS. Documentación de referencia.	Mario Miguel	Resp. Infraestructura
1.4	31/01/2022	Revisión. Sin cambios.	Mario Miguel	Resp. Infraestructura
1.5	31/05/2023	Actualización domicilio fiscal y logos de certificación	Antonio Camacho	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	Antonio Camacho	Ingeniero de procesos

Revisión

FECHA	NOMBRE	ÁREA	CARGO
28/02/2024	Yohanner Fernández Irene Villar	Ciberseguridad Calidad	Ing. Ciberseguridad Resp. SIG

Aprobación

FECHA	NOMBRE	ÁREA	CARGO
15/04/2024	Irene Villar	Calidad	Resp. SIG

Distribución

NOMBRE	ÁREA	CARGO	EMAIL

Glosario de términos

TÉRMINO	DEFINICIÓN

Documentación de referencia

TIPO	CÓDIGO	DESCRIPCIÓN
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
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
MANUAL	MPCIDSS	MANUAL DE OPERACIONES PCIDSS
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, así como evitar pérdidas, daños, robos, interrupciones de servicio, o 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**.

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

La versión actual de la normativa específica 12 requisitos para el cumplimiento, organizados en 6 secciones relacionadas lógicamente, que son llamadas "objetivos de control" y sus requisitos son los siguientes:

- **Desarrollar y Mantener una Red Segura**
    - Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas.
    - Requisito 2: No usar contraseñas del sistema y otros parámetros de seguridad predeterminados provistos por los proveedores.
- **Proteger los Datos de los propietarios de tarjetas.**
    - Requisito 3: Proteger los datos almacenados de los propietarios de tarjetas.
    - Requisito 4: Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.
- **Mantener un Programa de Gestión de Vulnerabilidades**
    - Requisito 5: Usar y actualizar regularmente un 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 propietarios de tarjetas.
- **Monitorizar y probar regularmente las redes**
    - Requisito 10: Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los propietarios de tarjetas.

- 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

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.
- Los datos de autenticación 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

- 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.
- 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 versión 1.0 y 1.1 por ser vulnerables.
- 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.
- Implementar mecanismos de control de cambios no autorizados sobre archivos críticos del sistema.
- Cualquier aplicación 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).
- Debe cumplirse con las políticas establecidas en el documento interno denominado: **PPCIDSS-05 Política antivirus** dónde se especifica la normativa en el uso y mantenimiento del software antivirus.
- 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 el uso y mantenimiento de las actualizaciones de seguridad.

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

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

Los empleados nunca pueden enviar 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, los empleados nunca deberán enviar PAN sin protección a través de otras tecnologías de mensajería como mensajería instantánea, chat o texto.

7 Programa de gestión de vulnerabilidades

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**.

8 Desarrollo Seguro

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.

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.

La capacitación en codificación segura es obligatoria, con carácter anual, para todos los desarrolladores de Alisys Digital y el contenido de los cursos deben incluir temáticas que ayuden a responder al menos las siguientes preguntas: ¿cuáles son las diferentes vulnerabilidades y ataques potenciales? y ¿cómo adoptar estrategias de mitigación durante el proceso de desarrollo para prevenir vectores de ataque?

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

8.1. Revisión y Prueba 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**.

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

En general, los registros de auditoría guardan los siguientes detalles para cada evento auditable; identificación del usuario, tipo de evento, fecha y hora, origen del evento, identidad o nombre de los datos, componentes del sistema, recursos o servicios afectados (por ejemplo, nombre y protocolo).

Estos logs se almacenan 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 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 para evaluar el cumplimiento de las políticas y procedimientos de acceso a dichos datos, que se sustentan en el Programa BAU, definido para garantizar el cumplimiento de la normativa de seguridad, que se deberá implementar/programar en la herramienta de ticketing de la compañía.

Periodicidad	Tarea	Responsable
Semanalmente	BAU-S-02 Revisión de los registros de auditoría(logs).	Ciberseguridad
	BAU-S-04 Actualización de IDS/IPS (motores, líneas base y firmas).	Explotación
	BAU-S-05 Comprobación de archivos críticos (FIM).	Ciberseguridad
	BAU-S-06 Retiro o reemplazo de claves de cifrado.	Explotación
Mensualmente	BAU-M-03 Eliminación/inhabilitar cuentas de usuarios inactivas.	Explotación
	BAU-M-06 Comprobación mensual estado firewall y antivirus.	Infraestructura
Trimestralmente	BAU-T-01 Realización de análisis de vulnerabilidades internas.	Ciberseguridad
	BAU-T-02 Realización de análisis vulnerabilidades externas (ASV).	Ciberseguridad
	BAU-T-03 Revisión de las direcciones IP autorizadas.	Ciberseguridad
Semestral	BAU-SX-01 Revisión de conjunto de reglas de firewall y router ACL.	Infraestructura
Anualmente	BAU-A-09 Revisión de referencias del personal.	RRHH
	BAU-A-12 Revisión de matriz de responsabilidad.	Legal
	BAU-A-15 Revisar y probar el programa de respuesta a incidentes	Ciberseguridad

El programa BAU completo está definido en el **MPCIDSS - Manual de operaciones con datos de tarjetas de pago.**

12 Revisión, actualización y mantenimiento de la normativa de seguridad aplicable a la protección de datos de tarjetas de pago

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

13 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

P.º de la Habana 9, 11
28036 Madrid
+34 910 200 000

info@alisys.net
www.alisys.net