Las Cámaras de Compensación para Pagos con Tarjeta deben atender a las siguientes especificaciones en materia de seguridad de datos y telecomunicaciones para cumplir con las Condiciones de Intercambio entre Cámaras de Compensación, dichas especificaciones se actualizarán semestralmente.

1 Estándar de comunicación entre Cámaras de Compensación para el intercambio de archivos

Las Cámaras de Compensación deberán emplear alguno de los siguientes protocolos de comunicación para el intercambio de archivos: FTPS y HTTPS con los siguientes estándares de seguridad:

- Autenticación: Certificados (emitidos por una agencia certificadora reconocida), nombre de usuarios y contraseñas.
- Confidencialidad: TLS versión 1.2 o mayor.
- Integridad de los datos: Hash

2 Algoritmos para el cifrado e integridad de datos:

A continuación se listan algunos de los algoritmos recomendados actualmente por NIST (por sus siglas en inglés National Institute of Standards of Technology), ANSI (por sus siglas en inglés American National Standards Institute) y/o FIPS (por sus siglas en inglés Federal Information Processing Standard) para el cifrado e integridad de datos.

Algoritmo Simétricos	Tipo Algoritmo	Aplicaciones sugeridas	Longitudes sugeridas (bits)
AES (Advanced Encription Standard)	Cifrado Simétrico	- Almacenamiento - Transmisión de datos - Cifrado de Archivos	- 128 - 192 - 256
Triple DES	Cifrado Simétrico	- Almacenamiento - transmisión de datos - Cifrado de Archivos	- 256
IDEA	Cifrado Simétrico	- Almacenamiento - transmisión de datos - Cifrado de Archivos	- 128
RSA	Cifrado Asimétrico	- Repudio - Transmisión de datos - Autenticación	- 2048 - 4096

Diffie-Hellman	Cifrado Asimétrico	- Solo genera llaves asimétricas	- 2048 - 4096
Familia SHA-2	De Digestión	- Integridad - Firma	- 256 - 512

3 Seguridad en los enlaces de comunicación

A continuación se listan algunos de los mecanismos de seguridad recomendados actualmente por NIST, ANSI y/o FIPS para el cifrado en los medios de comunicación.

PARÁMETRO	DESCRIPCIÓN	OPCIONES estándares o protocolos
Autenticación	Autenticación de los equipos (peers) que protegerán los datos.	Pre-Shared Key
Cifrado	Protección de la negociación del canal entre los peers.	AES (128,192,256)
Función Hash	Integridad de los paquetes a través de una función especial para corroborar que estos no han sido alterados en tránsito.	Familia SHA-2
Diffie-Hellman	Protocolo que permite establecer llaves secretas sobre un medio inseguro.	De al menos 2048 bits
IKE - Renegociación SA Fase 1 (Lifetime)	Duración de la Asociación de Seguridad (SA) de IKE1.	86400 seg. Se elige el valor por omisión que, para el canal de seguridad expone las llaves una sola vez cada 24 horas.
IPSEC - Algoritmo de Cifrado	Protección el tráfico de datos del usuario.	AES (128,192,256)
Perfect Forward Secrecy	Característica de seguridad que genera nuevos elementos de seguridad de forma independiente.	N/A
IPSEC – Renegociación SA Fase 2	Duración de la Asociación de Seguridad (SA) de IKE2.	120seg – 86400seg