POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN - ANEXO "6" - Gestión de Proveedores desde el punto de vista de la Ciberseguridad

VERSIÓN

Versión	Fecha	Observaciones
1.0	29 de febrero 2024	Creación del documento.

REFERENCIA

- Política de Seguridad de la Información JetSmart Airlines
- ISO 27001:2022
- ISO 27002:2022
- ISO27701:2019
- Marco Jurídico

OBJETIVO

El objetivo de esta política de Gestión de Proveedores es asegurar que todas las interacciones y transacciones con proveedores se realicen de manera segura, protegiendo la integridad, confidencialidad y disponibilidad de la información de JetSmart Airlines (en adelante indistintamente “JetSmart”, la “Empresa”, la “Organización” o la “Compañía”). Se busca establecer un marco de trabajo claro para la evaluación y el manejo de riesgos relacionados con la ciberseguridad, garantizando que los proveedores cumplan con los estándares y requisitos de seguridad de la información establecidos por la organización.

Este enfoque integral pretende minimizar los riesgos de ciberseguridad asociados a la cadena de suministro, incluyendo el acceso no autorizado, la divulgación, alteración o destrucción de información confidencial, así como asegurar la continuidad y la calidad del servicio proporcionado por los proveedores, alineándose con los objetivos estratégicos y las regulaciones aplicables en materia de protección de datos y ciberseguridad.

ALCANCE

La presente política tendrá cobertura de aplicación a todos los empleados, colaboradores externos, empresas proveedoras de servicios u otras personas que interactúen directa o indirectamente, habitual u ocasionalmente con la infraestructura tecnológica y/o de la información, o que usen o den soporte a los sistemas de información y/o de negocios, perteneciente a JetSmart. Los sujetos obligados por la presente política deberán cumplir en todo momento con el marco jurídico vigente en cada uno de los países en los que la Compañía tenga operación de tecnología de la información.

DETALLE CLAÚSULAS

Claúsula 1. Todos los proveedores deben someterse a una evaluación de seguridad de la información y privacidad antes de su selección y contratación por parte de la Compañía, considerando su cumplimiento con las normativas aplicables y mejores prácticas de la industria en ciberseguridad.

Claúsula 2. Los proveedores deben cumplir con los estándares de seguridad de la información de la Organización, incluyendo la protección contra malware, acceso no autorizado, y pérdida o inutilización de datos.

Claúsula 3. Deben existir acuerdos de nivel de servicio (SLAs) específicos que incluyan requisitos de seguridad de la información, planes de contingencia y mecanismos de respuesta a incidentes.

Claúsula 4. Los proveedores deben adherirse a las leyes y regulaciones de protección de datos aplicables, como el GDPR o la Ley de Protección de Datos Personales vigente en cada legislación, en el tratamiento de cualquier dato personal proporcionado o accesible como parte de sus servicios.

Claúsula 5. Se identificará y documentará a los proveedores y los servicios de TI, las utilidades de logística, los servicios financieros, los componentes de la infraestructura de TI y a quiénes la Organización autorice para acceder a su información.

Claúsula 6. Deben implementarse cláusulas contractuales específicas en los contratos con proveedores que cumplan con el estándar de la Organización en materias de seguridad de la información y que, entre otras, obliguen a los proveedores a notificar sobre incidentes o brechas de ciberseguridad y cooperar en la protección y recuperación de datos.

Claúsula 7. Los proveedores deben garantizar la seguridad y resiliencia de su infraestructura IT, incluyendo la implementación de medidas de seguridad física y lógica, y la realización de pruebas de penetración periódicas.

Claúsula 8. Se requiere que los proveedores utilicen tecnologías de cifrado para proteger cualquier comunicación o dato almacenado y transmitido.

Claúsula 9. Los proveedores deben implementar controles internos robustos para prevenir y detectar fraudes. Para ello la Compañía realizará auditorías regulares y monitoreo de transacciones anómalas.

Claúsula 10. Se establecerán procedimientos claros para la notificación y gestión de incidentes. Este procedimiento incluirá la responsabilidad de los proveedores en caso de incidentes que provengan de acciones u omisiones cometidas por sus trabajadores, dependientes o sistemas, o de terceros respecto de los cuales el proveedor dependa.

Claúsula 11. La Organización se reserva el derecho de realizar auditorías de seguridad y privacidad, y/o revisar los controles de seguridad de los proveedores, con una periodicidad definida o ante la ocurrencia de incidentes de seguridad.

Claúsula 12. Los proveedores deben comprometerse a corregir cualquier deficiencia de seguridad identificada en un plazo acordado.

Claúsula 13. Los proveedores deben poseer certificaciones relevantes en ciberseguridad y gestión de la información, como ISO 27001, y mantenerse al día con las actualizaciones de estas certificaciones.

CLASIFICACIÓN: TLP VERDE

Claúsula 14. En caso de terminación del contrato, los proveedores deberán proceder a la devolución o destrucción segura de toda la información confidencial y datos personales proporcionados por la Organización mediante la firma de una declaración jurada que dé cuenta de dicha eliminación o devolución.

Claúsula 15. Se deben establecer mecanismos para la transición segura de los servicios y datos a otro proveedor. Organización Por lo que, en todo intercambio de información entre un proveedor y la Organización, se deberán implementar estándares y procedimientos formales que permitan garantizar razonablemente la seguridad en el acceso y la transferencia de información.

Claúsula 16. Se recopilarán los registros de proveedores de servicios, donde sea compatible. Las implementaciones de ejemplo incluyen la recopilación de eventos de autenticación y autorización, eventos de creación y eliminación de datos y eventos de gestión de usuarios.

Claúsula 17. Se establecerá y mantendrá un inventario actualizado de proveedores de servicios. El inventario debe enumerar todos los proveedores de servicios, incluir clasificaciones y designar un contacto empresarial para cada proveedor de servicios. La Compañía revisará y actualizará el inventario anualmente o cuando ocurran cambios importantes que puedan afectar este control.

Claúsula 18. Se deberá clasificar a los proveedores de servicios. La consideración de la clasificación puede incluir una o más características, como la naturaleza o categoría de datos que el proveedor trate, el volumen de datos, los requisitos de disponibilidad, las regulaciones aplicables, el riesgo inherente y el riesgo mitigado. Se deberá actualizar y revisar las clasificaciones anualmente, o cuando se produzcan cambios significativos en la empresa.

Claúsula 19. Se asegurará que los contratos del proveedor de servicios incluyan cláusulas de protección de datos personales, seguridad de la información y ciberseguridad. Los requisitos pueden incluir requisitos mínimos del programa de seguridad, notificación y respuesta de incidentes de seguridad y/o violación de datos, requisitos de cifrado de datos y obligaciones de eliminación de datos.

Claúsula 20. Se evaluará a los proveedores de servicios de acuerdo con la política de gestión de proveedores de servicios de la Empresa. El alcance de la evaluación puede variar según la (s) clasificación (es) y puede incluir la revisión de informes de evaluación estandarizados, como el Control de la Organización de servicio 2 (SOC 2) y la Certificación de cumplimiento (AoC) de la industria de tarjetas de pago (PCI), cuestionarios personalizados u otros procesos rigurosos.

Asimismo, se reevaluará a los proveedores de servicios anualmente, como mínimo, o con contratos nuevos y renovados

Claúsula 21. Se dará de baja de forma segura a los proveedores de servicios. Para ello se tendrá en consideración lo siguiente: la desactivación de cuentas de usuario y servicio, la terminación de flujos de datos y la eliminación segura de información dentro de los sistemas de proveedores de servicios, entre otros.

Claúsula 22. La Organización implementará un proceso integral de gestión de riesgos de la cadena de suministro cibernética, el cual será llevado a cabo en colaboración con todas las partes interesadas internas y externas relevantes.

Claúsula 23. Se debe capacitar y concientizar al personal de la Organización involucrado en la contratación de proveedores y que utiliza servicios de terceros sobre las políticas, procesos y procedimientos correspondientes según las directrices de la Organización.

Claúsula 24. En los casos en que se requiera entregar al proveedor información confidencial, o que producto de la prestación del servicio acceda a información de la Organización, se deberán aplicar acuerdos de confidencialidad y no divulgación.

Claúsula 25. Todo proveedor deberá suministrar a la Organización una lista detallada y actualizada del personal específicamente autorizado por ellos para acceder o recibir cualquier información relacionada con los procedimientos, condiciones, o datos confidenciales de la Organización. Este listado incluirá, pero no se limitará a, los nombres, cargos, y la justificación de la necesidad de acceso o recepción de dicha información por parte de cada miembro del personal autorizado. Asimismo, todo proveedor deberá notificar a la Organización de cualquier modificación que surja en el listado durante la relación contractual.

RESPONSABILIDADES ESPECIFICAS

C-Levels

La Alta Dirección asume una responsabilidad crucial en el respaldo y fomento de esta Política, así como de las normativas y procedimientos que de ella se deriven. Su papel no se limitará a un mero apoyo formal; sino que, se extiende a garantizar activamente su implementación efectiva y sostenible. Esto implica no solo la aprobación de la política, sino también la provisión de los recursos necesarios, tanto humanos como tecnológicos y financieros, para asegurar su cumplimiento y aplicación eficaz.

Gerente de Ciberseguridad:

El rol del Gerente de Seguridad de la Información es fundamental para la protección y gestión de la seguridad de la información dentro de la Organización. Sus responsabilidades incluyen:

- **Evaluación de Seguridad de Proveedores**: Supervisar y dirigir las evaluaciones de seguridad de la información y privacidad de todos los proveedores antes de su selección y durante la relación contractual, asegurando su cumplimiento con las normativas aplicables y las mejores prácticas en ciberseguridad.
- **Cumplimiento de Estándares de Seguridad:** Asegurar que los proveedores cumplan con los estándares de seguridad de la información de la Organización, incluyendo la protección contra malware, acceso no autorizado, y pérdida o inutilización de datos.

- **Gestión de SLAs y Respuesta a Incidentes:** Desarrollar y supervisar los acuerdos de nivel de servicio que incluyan requisitos de seguridad de la información y establecer mecanismos eficaces de respuesta a incidentes.
- **Adherencia a Regulaciones de Protección de Datos:** Garantizar que los proveedores se adhieran a las leyes y regulaciones de protección de datos aplicables, incluido el GDPR o la Ley de Protección de Datos Personales vigente en cada legislación.
- **Documentación y Autorización de Acceso:** Identificar y documentar a los proveedores, sus servicios y a quiénes la Organización autorizará para acceder a su información, asegurando un control efectivo sobre el acceso y la gestión de datos.
- **Notificación de Brechas de Datos:** Implementar cláusulas contractuales específicas en los contratos con proveedores que cumplan con el estándar de la Organización en materias de seguridad de la Organización y que, entre otras obliguen a los proveedores a notificar sobre brechas de datos y cooperar en la protección y recuperación de los mismos.
- **Auditorías y Revisiones de Seguridad:** Organizar y realizar auditorías de seguridad y privacidad o revisar los controles de seguridad de los proveedores según sea necesario, para asegurar la continuidad del cumplimiento de los estándares de seguridad.
- **Corrección de Deficiencias de Seguridad:** Coordinar con los proveedores para asegurar la corrección de cualquier deficiencia de seguridad identificada en un plazo acordado.
- **Certificaciones y Cumplimiento de Proveedores:** Verificar que los proveedores posean y mantengan certificaciones relevantes en ciberseguridad y gestión de la información, como ISO 27001, y que proporcionen prueba de su cumplimiento con las normativas aplicables.
- **Seguridad y Resiliencia de la Infraestructura IT de Proveedores:** Asegurar que los proveedores mantengan la seguridad y resiliencia de su infraestructura IT, incluyendo la implementación de medidas de seguridad física y lógica.
- **Cifrado de Comunicaciones y Datos:** Requerir el uso de tecnologías de cifrado por parte de los proveedores para proteger cualquier comunicación o dato almacenado y transmitido.
- **Gestión de Incidentes de Fraude:** Establecer procedimientos claros para la notificación y gestión de incidentes de fraude, definiendo la responsabilidad de los proveedores.
- **Mantenimiento de Inventarios y Clasificación de Proveedores:** Mantener un inventario actualizado de proveedores de servicios, clasificarlos según su relevancia y riesgo, y actualizar esta información periódicamente.
- **Transición Segura de Servicios y Datos:** Coordinar mecanismos para la transición segura de servicios y datos a otro proveedor Organización según lo establecido en la Cláusula 15 del presente documento.
- **Capacitación y Concienciación:** Desarrollar programas de capacitación y concienciación para el personal de la Organización involucrado en las adquisiciones y uso de servicios de terceros, enfocados en políticas, procesos y procedimientos de seguridad.

El Gerente de Operaciones IT

La Gerencia de Operaciones IT juega un papel clave en asegurar que las interacciones con los proveedores se manejen de manera segura y eficiente, protegiendo la integridad, disponibilidad y confidencialidad de la infraestructura de la Organización.

- **Evaluación de Seguridad y Privacidad:** Revisar y asegurar que todos los proveedores pasen por una rigurosa evaluación de seguridad de la información y privacidad antes de su contratación y durante toda la relación, en línea con las regulaciones y prácticas de ciberseguridad vigentes.
- **Cumplimiento de Estándares de Seguridad:** Verificar que los proveedores cumplan con los estándares de seguridad de la Organización, incluida la protección contra malware, acceso no autorizado y pérdida o inutilización de datos, e implementar acciones correctivas cuando sea necesario.
- **Gestión de SLAs y Respuesta a Incidentes:** Desarrollar y mantener acuerdos de nivel de servicio que integren requisitos de seguridad y establecer procesos efectivos de respuesta ante incidentes de seguridad relacionados con proveedores.
- **Documentación y Autorización de Acceso:** Identificar, documentar y autorizar el acceso de proveedores a la infraestructura y datos de IT, asegurando que solo personal autorizado tenga acceso a información crítica.
- **Mantenimiento de Inventarios de Proveedores:** Crear y mantener un inventario detallado de proveedores de servicios, asegurando que esté actualizado y refleje cualquier cambio significativo en la Organización o en las relaciones con los proveedores.
- **Desmantelamiento Seguro de Proveedores:** Gestionar el proceso de dada de baja de servicios de proveedores, asegurando la eliminación segura de datos y la desactivación adecuada de accesos.
- **Supervisión del Directorio de Personal de Proveedores**: Asegurar que los proveedores proporcionen un listado actualizado del personal autorizado para acceder a la información de la Organización, y supervisar el cumplimiento de los procedimientos de autorización y revocación de accesos. En ese sentido, verificar que todo proveedor notifique a la Organización de cualquier modificación que surja en el listado durante la relación contractual.

Oficial de Datos Personales

El Encargado de Tratamiento de Datos desempeña un papel crucial en la supervisión y gestión del tratamiento seguro y conforme de los datos personales dentro de la cadena de suministro y los proveedores, garantizando que las prácticas de privacidad y seguridad de la información se adhieran a las regulaciones aplicables y a los estándares de la Organización.

A continuación, se detallan las responsabilidades del Encargado del Tratamiento de Datos:

- **Evaluación de Cumplimiento:** Asegurar que todos los proveedores sean evaluados en términos de seguridad de la información y privacidad antes de su selección, considerando su adherencia a normativas aplicables y mejores prácticas de ciberseguridad.
- **Adherencia a Regulaciones de Protección de Datos:** Verificar que los proveedores cumplan con las leyes y regulaciones de protección de datos aplicables, supervisando el manejo seguro de datos personales.
- **Documentación y Autorización de Acceso:** Documentar los proveedores y servicios que tienen autorización para acceder a la información de la Organización, gestionando el acceso basado en la necesidad de conocer y cumplir con los procedimientos de seguridad.
- **Notificación de Brechas de Datos:** Establecer cláusulas contractuales que obliguen a los proveedores a informar de manera oportuna sobre cualquier brecha de datos, y a cooperar en las acciones de recuperación.
- **Cifrado de Datos:** Exigir a los proveedores el uso de tecnologías de cifrado para la protección de datos almacenados y en tránsito.
- **Prevención y Detección de Fraudes:** Asegurar que los proveedores implementen controles internos para prevenir y detectar fraudes, incluyendo auditorías y monitoreo de transacciones.
- **Seguridad en la Terminación del Contrato**: Garantizar la devolución o destrucción segura de toda información confidencial y datos personales al terminar el contrato con proveedores.
- **Transición Segura de Servicios:** Establecer mecanismos para una transición segura de servicios y datos hacia otro proveedor o de regreso a la Organización, sin comprometer la seguridad de los datos.
- **Directorio de Personal Autorizado:** Exigir y mantener un directorio actualizado de personal de proveedores autorizado para acceder o recibir datos, asegurando que este acceso sea debidamente justificado y gestionado.

Gerentes, jefaturas y personas que tengan a cargo directamente un proveedor

Las personas a cargo de proveedores son responsables directamente de la supervisión y gestión integral de las relaciones con los proveedores. Esto involucra desde la evaluación preliminar de ellos hasta la terminación del contrato, asegurando que todas las actividades se alineen con los requisitos de seguridad de la información, privacidad y ciberseguridad de la Organización.

A continuación, se detallan las responsabilidades de las personas que tengan a cargo directamente un proveedor:

- **Evaluación Preliminar:** Realizar una evaluación exhaustiva de seguridad de la información y privacidad de todos los potenciales proveedores antes de su selección y contratación, asegurando que cumplan con las normativas aplicables y las mejores prácticas de la industria en ciberseguridad.

- **Cumplimiento de Estándares de Seguridad:** Asegurar que los proveedores cumplan con los estándares de seguridad de la información establecidos por la Organización, incluyendo protección contra malware, prevención de acceso no autorizado y mitigación de pérdida o inutilización de datos.
- **Acuerdos de Nivel de Servicio (SLAs):** Desarrollar y mantener acuerdos de nivel de servicio que incorporen requisitos de seguridad de la información y establezcan mecanismos claros de respuesta ante incidentes.
- **Adherencia a la Legislación de Protección de Datos:** Garantizar que los proveedores se adhieran a las leyes y regulaciones de protección de datos aplicables, gestionando adecuadamente cualquier dato personal proporcionado o accesible como parte de sus servicios.
- **Documentación y Autorización de Acceso:** Identificar y documentar a los proveedores y los servicios autorizados para acceder a la información de la Organización, supervisando y controlando este acceso.
- **Notificaciones de Brechas de Datos**: Implementar cláusulas contractuales que obliguen a los proveedores a notificar cualquier brecha de datos y cooperar en las medidas de protección y recuperación de datos.
- **Auditorías y Revisiones de Seguridad:** Mantener el derecho de realizar auditorías de seguridad y privacidad, o revisar los controles de seguridad de los proveedores, estableciendo una periodicidad definida o en respuesta a incidentes de seguridad.
- **Uso de Cifrado:** Exigir que los proveedores empleen tecnologías de cifrado para proteger cualquier dato almacenado y transmitido.
- **Controles Internos contra Fraudes:** Verificar que los proveedores implementen controles internos robustos para prevenir y detectar fraudes, incluyendo auditorías regulares y monitoreo de transacciones anómalas.
- **Gestión de Incidentes de Fraude:** Establecer procedimientos claros para la notificación y gestión de incidentes de fraude, definiendo la responsabilidad de los proveedores.
- **Seguridad en Terminación de Contratos:** Gestionar la devolución o destrucción segura de toda información confidencial y datos personales al terminar el contrato.
- **Transición Segura de Servicios y Datos:** Establecer mecanismos para una transición segura de servicios y datos a otro proveedor o de vuelta a la Organización.
- **Inventario de Proveedores de Servicios:** Mantener un inventario actualizado de proveedores de servicios, revisándolo anualmente o ante cambios significativos en la empresa.
- **Clasificación y Evaluación de Proveedores:** Clasificar a los proveedores de servicios basándose en factores como sensibilidad de datos, volumen, requisitos de disponibilidad, y riesgo inherente. Evaluarlos de acuerdo con la política de gestión de proveedores de servicios de la empresa.

Área de People & Esg

Las responsabilidades subrayan la importancia de una gestión proactiva y centrada en la seguridad de los recursos humanos en lo que respecta a la información personal y sensible, en alineación con las políticas generales de seguridad de la información y protección de datos de la Organización. El detalle es el siguiente:

- **Capacitación y Concienciación:** Desarrollar y proveer programas de capacitación y concienciación para el personal involucrado en la gestión de proveedores, enfocándose en las políticas, procesos y procedimientos de seguridad de la información y privacidad.
- **Cumplimiento de Normativas y Sanciones:** Garantizar el cumplimiento de todas las políticas internas y las regulaciones aplicables en esta materia, preparando a la Organización para auditorías internas y externas y estableciendo sanciones administrativas para los casos de incumplimiento, según lo dispuesto en el reglamento interno del área de recursos humanos.

Área Legal

El área legal juega un papel crucial en la gestión de riesgos y la protección de la Organización frente a las amenazas y vulnerabilidades asociadas con los proveedores, asegurando el cumplimiento legal y la seguridad de la información a través de todas las etapas de la relación con los proveedores. El detalle es el siguiente:

- **Evaluación Legal de Proveedores**: Asegurar que todos los proveedores se sometan a una evaluación de seguridad de la información y privacidad antes de su selección y contratación, verificando su cumplimiento con las normativas aplicables y las mejores prácticas en ciberseguridad.
- **Acuerdos de Nivel de Servicio (SLAs):** Desarrollar SLAs que incluyan requisitos de seguridad de la información y mecanismos de respuesta a incidentes, asegurando que estos acuerdos estén alineados con las leyes y regulaciones aplicables.
- **Adherencia a las Leyes de Protección de Datos:** Asegurar que los proveedores cumplan con las leyes y regulaciones de protección de datos aplicables, como el GDPR o la Ley de Protección de Datos Personales, en el tratamiento de cualquier dato personal.
- **Cláusulas Contractuales sobre Brechas de Datos**: Implementar cláusulas contractuales que obliguen a los proveedores a notificar sobre brechas de datos y cooperar en la protección y recuperación de datos.
- **Auditorías de Seguridad y Privacidad:** Establecer el derecho de la Organización a realizar auditorías de seguridad y privacidad o revisar los controles de seguridad de los proveedores, incluyendo la frecuencia y las condiciones de estas auditorías.
- **Terminación de Contratos:** Gestionar los aspectos legales en caso de terminación del contrato con proveedores, incluyendo la devolución o destrucción segura de toda la información confidencial y datos personales.

- **Transición Segura de Servicios y Datos:** Asegurar legalmente la transición segura de los servicios y datos a otro proveedor o de vuelta a la Organización, incluyendo la protección de la información durante el proceso.
- **Gestión de Incidentes de Fraude:** Establecer procedimientos legales claros para la notificación y gestión de incidentes de fraude, definiendo la responsabilidad de los proveedores en caso de fraude cometido por sus empleados o sistemas.
- **Inventario y Clasificación de Proveedores:** Colaborar en el establecimiento y mantenimiento de un inventario de proveedores de servicios, asegurando que incluya clasificaciones y designe un contacto empresarial para cada proveedor. Además, participar en la revisión y actualización de las clasificaciones según las necesidades legales y de seguridad.
- **Requisitos de Seguridad en Contratos:** Garantizar que los contratos de proveedores de servicios incluyan requisitos de seguridad adecuados y detallados, y que estos contratos sean revisados y actualizados conforme a las necesidades legales y de seguridad.
- **Capacitación y Concienciación sobre Políticas y Procedimientos:** Coordinar la capacitación y concienciación del personal de la Organización involucrado en las adquisiciones y el uso de servicios de terceros sobre las políticas, procesos y procedimientos legales correspondientes.

Gerentes y jefaturas

Estas responsabilidades subrayan el papel crucial que desempeñan los gerentes y jefes en la protección de la información de la Organización, asegurando que las personas bajo su responsabilidad cumplan a cabalidad la presente política. El detalle es el siguiente:

- **Asegurar la Clasificación de la Información:** Garantizar que toda la información generada, almacenada y transferida dentro de su ámbito de responsabilidad se clasifique adecuadamente según el Protocolo Traffic Light Protocol (TLP), asegurando que se cumplan los principios de confidencialidad e integridad en todo momento.
- **Supervisión de Evaluaciones de Seguridad:** Asegurar que los proveedores se sometan a evaluaciones de seguridad de la información y privacidad antes de su selección y contratación, supervisando el proceso de evaluación para verificar el cumplimiento con las normativas aplicables y las mejores prácticas en ciberseguridad.
- **Verificación del Cumplimiento de Estándares:** Verificar que los proveedores cumplan con los estándares de seguridad de la información de la Organización, incluyendo la protección contra malware, acceso no autorizado y pérdida de datos.
- **Gestión de Acuerdos de Nivel de Servicio (SLAs):** Garantizar que se establezcan SLAs específicos que incluyan requisitos de seguridad de la información y mecanismos de respuesta a incidentes, revisando y aprobando dichos acuerdos.
- **Cumplimiento con la Legislación de Protección de Datos**: Asegurar que los proveedores cumplan con las leyes y regulaciones de protección de datos aplicables en el tratamiento de cualquier dato personal.
- **Comunicación de Brechas de Datos:** Asegurar que existan cláusulas contractuales que obliguen a los proveedores a notificar sobre brechas de datos y cooperar en la protección y recuperación de datos.

- **Auditorías de Seguridad:** Coordinar con el área de ciberseguridad para realizar auditorías de seguridad y privacidad o revisar los controles de seguridad de los proveedores según se establezca.
- **Certificaciones de Proveedores:** Verificar que los proveedores mantengan certificaciones relevantes en ciberseguridad y gestión de la información, como ISO 27001.
- **Gestión de la Terminación de Contratos:** Supervisar los procesos de terminación de contratos con proveedores, incluyendo la gestión de la devolución o destrucción segura de información confidencial y datos personales.
- **Transición de Servicios y Datos:** Supervisar la transición segura de servicios y datos a otro proveedor o de vuelta a la Organización, asegurando la protección de la información durante el proceso.
- **Gestión de Incidentes de Fraude:** Establecer procedimientos claros para la notificación y gestión de incidentes de fraude, incluyendo la definición de responsabilidades de los proveedores en caso de incidentes.
- **Inventario de Proveedores:** Colaborar en el establecimiento y mantenimiento de un inventario de proveedores de servicios, revisando y actualizando el inventario regularmente.
- **Evaluación y Reevaluación de Proveedores:** Participar en la evaluación y reevaluación periódica de los proveedores de servicios según la política de gestión de proveedores de servicios de la empresa.
- **Desmantelamiento Seguro de Proveedores:** Supervisar el desmantelamiento seguro de los proveedores de servicios, incluyendo la desactivación de cuentas y la eliminación segura de datos empresariales.
- **Capacitación y Concienciación:** Asegurar que el personal a su cargo esté debidamente capacitado y concienciado sobre las políticas, procesos y procedimientos correspondientes al manejo de proveedores.
- **Directorio de Personal de Proveedores**: Solicitar y mantener actualizado un directorio del personal de proveedores específicamente autorizado para acceder o recibir información de la Organización.

Los puntos descritos en este instrumento podrán ser modificados, unilateralmente y en cualquier momento por JetSmart Airlines, para adaptar o modificar su contenido, así como para cumplir con requisitos legales aplicables. Los cambios se publicarán en el sitio web o en boletines informativos previo a su entrada en vigencia.

Si algún punto no queda claro, le sugerimos que se ponga en contacto con el área de ciberseguridad mediante el correo ciberegurdad@jetsmart.com para aclarar sus dudas.