POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN - ANEXO "1" - Política de Clasificación de la Información y Protección de los Datos Personales

VERSIÓN

Versión	Fecha	Observaciones
3.0	28 de mayo de 2024	Actualización 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 la presente política es entregar los lineamientos, para clasificar y proteger la información generada, procesada, almacenada y trasferida, por JetSmart Airlines (en adelante indistintamente “JetSmart”, la “Empresa”, la “Organización” o la “Compañía”), cumpliendo con el marco jurídico vigente y con los principios básicos de la seguridad de la información, “Confidencialidad, Disponibilidad e Integridad”, con el fin de apoyar la concreción de los objetivos estratégicos de la organización.

ALCANCE

La presente política tendrá cobertura de aplicación a todos los empleados, colaboradores externos, empresas proveedoras de servicios u otras que interactúen con la infraestructura tecnológica y/o de la información, directa o indirectamente, habitual u ocasionalmente, o que usen o den soporte a los sistemas de información y/o de negocios, perteneciente a JetSmart Airlines. Cabe señalar, que estos, deberán cumplir el marco jurídico vigente correspondiente a los países, donde exista operación de tecnologías de la información de la compañía.

DEFINICIONES

Definición 1: Ciclo de vida del dato: modelo de gestión de la información que abarca desde que se crean y almacenan por primera vez hasta que se eliminan. En este sentido y de acuerdo a la trazabilidad se distinguen cinco etapas:

1) Obtención;

2) Seguridad, transmisión y almacenamiento;

3) Gestión

4) Análisis y explotación

5) Obsolescencia y eliminación.

Definición 2: Dato personal: cualquier información vinculada o referida a una persona natural (persona física) identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado. Por ejemplo, nombre, edad, estado civil, profesión, número de cédula de identidad, números telefónicos, casilla de correo electrónico, número de tarjetas bancarias, entre otros.

Definición 3: Dato sensible: Sólo tendrán esta condición aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, hábitos personales, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural (persona física) .

Definición 4: Titular de datos: es la persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.

Definición 5: Tratamiento de datos personales: es cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permite recolectar, procesar, almacenar, grabar, organizar, elaborar, seccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal o utilizarlos en cualquier otra forma.

Definición 6: Confidencialidad: Implica que la información sea accesible únicamente por las personas que se encuentran autorizadas a conocerla. Propiedad de que la información no se pone a disposición ni se revela a personas, entidades o procesos (ISO 27.000:2018).

Definición 7: Integridad: Propiedad de exactitud y completitud (ISO 27.000:2018).

Definición 8: Disponibilidad: Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada (ISO 27.000:2018).

DETALLE CLAÚSULAS

Claúsula 1. La información de la Compañía deberá ser generada, almacenada y transferida, tanto interna como externamente, para los objetivos definidos por la misma, cumpliendo con los principios de confidencialidad, disponibilidad e integridad. (Cláusula 1 PSI:2020 r1)

Claúsula 2. La información, deberá ser protegida, a través de la clasificación, durante todo su Ciclo de Vida, desde la generación, almacenamiento, transferencia y destrucción. (Control A.5.12 ISO 27002:2022)

Claúsula 3. El criterio de clasificación se basará en los siguientes requisitos (Control A.5.12 ISO 27002:2022):

- **Valor de la Información:** Este factor evalúa el impacto que tendría la pérdida, compromiso de disponibilidad o destrucción de la información en la organización.
- **Impacto:** Se determina en base a la posible afectación a la reputación o protección de la marca, considerando factores que puedan resultar en daños a la imagen corporativa.
- **Criticidad**: Mide la importancia de la información para la continuidad y eficacia de los procesos de negocio esenciales.
- **Obligaciones Legales y Contractuales:** Analiza las consecuencias que el acceso no autorizado o la divulgación de la información podrían tener en términos de incumplimiento de compromisos contractuales o infracciones a las leyes aplicables.

Claúsula 4. Los propietarios de los activos de información deberían ser responsables de su clasificación, a lo largo de todo el ciclo de vida del dato. (Control A.5.12 ISO 27002:2022)

Claúsula 5. Los procedimientos, para el etiquetado de la información deberán cubrir la información y sus activos relacionados en formatos físicos o electrónicos.

En formato digital, podrán ser archivos de todo tipo (texto, imagen, multimedia, bases de datos, etc.), programas, aplicativos, hasta los equipos y sistemas computacionales que soportan estos servicios. (Control A.5.13 ISO 27002:2022)

Claúsula 6. Todos los usuarios deben utilizar un etiquetado de información como requisito irrenunciable, antes de realizar cualquier acuerdo y para compartir información de la compañía. Dichas etiquetas, podrán ser físicas o gráficas. En el caso de ser digitales, se utilizarán metadatos como forma de etiquetado. (Control A.5.13 ISO 27002:2022)

Claúsula 7. La clasificación utilizará el Protocolo internacional Traffic Light Protocol (TLP)[1], y se la siguiente clasificación requisitos (Control A.5.13 ISO 27002:2022) (Control 3.7 CIS V 8.0 :2021):

Código	Cuando utilizarlo	Impacto	ACCESO
TLP: ROJO	Se debe utilizar **TLP: ROJO,** cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	El acceso no autorizado a la información podría dañar de forma catastrófica (irreparable) el negocio y/o la reputación de la organización.	Solo personal de JetSmart, con roles específicos.
TLP: AMBAR	Se debe utilizar **TLP: AMBAR,** cuando la información requiere ser distribuida, de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	El acceso no autorizado a la información, podría dañar considerablemente el negocio y/o la reputación de la organización.	La información está disponible, solamente para un grupo específico de empleados y de terceros autorizados.
TLP: VERDE	Se debe utilizar **TLP: VERDE,** cuando la información es útil, para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	El acceso no autorizado a la información, podría ocasionar daños y/o inconvenientes menores a la organización	La información está disponible para todos los empleados y terceros seleccionados.
TLP: BLANCO	Se debe utilizar **TLP:** BLANCO, cuando la información no supone ningún riesgo, dentro de las reglas y procedimientos, establecidos para su difusión pública.	Hacer pública la información, no puede dañar a la organización de ninguna forma.	La información está disponible, para todo el público.

Claúsula 8. Los activos de naturaleza pública “TLP: BLANCO” no necesitan ser etiquetados (sin importar el formato en el que se encuentren).

Claúsula 9. Se deberá etiquetar la información, en base al TLP, dependiendo de la aplicación identificada en la cláusula 3.

Para ello, se procederá de la siguiente manera (dependiendo del medio de almacenamiento): (Control A.8.2.2 ISO 27002:2013) (Control 3.7 CIS V 8.0 :2021)

[1] Traffic Light Protocol (TLP) es un esquema creado para fomentar un mejor intercambio de información sensible (pero no clasificada) en el ámbito de la seguridad de la información. A través de este esquema, de una forma ágil y sencilla, el autor de una información puede indicar hasta dónde puede circular la información más allá del receptor inmediato, y este debe consultar al autor original cuando la información necesite ser distribuida a terceros. Fuente: https://www.incibe-cert.es/tlp

Claúsula 10. Los activos con otros niveles de confidencialidad son etiquetados de la siguiente forma:

- **Documentos en papel:** Si el documento contiene información TLP: AMBAR o VERDE se debe indicar el nivel de clasificación al menos en la portada del documento; si contiene información TLP: ROJO, se debiera indicar el nivel de clasificación tanto en la portada como en cada una de las páginas o en el sobre que contiene dicho documento, como también en la carpeta de archivo en la que se guarda el documento.

- **Documentos electrónicos:** Si el documento contiene información "TLP: AMBAR o VERDE", se debe indicar el nivel de clasificación al menos en la portada del documento; si contiene información "TLP: ROJO", se debiera indicar dicho nivel de clasificación tanto en la portada como en cada una de las páginas.

- **Correo electrónico:** se indica el nivel de clasificación en la primera línea del cuerpo del correo electrónico o mediante un procedimiento propio de la plataforma.

- **Soporte de almacenamiento electrónico (discos, tarjetas de memoria, etc.):** se debe indicar el nivel de clasificación sobre la superficie de cada soporte.

- **Archivo Digital:** Se deberá implementar el procedimiento técnico, que corresponda a nivel de los metadatos u otras tecnologías de protección, para utilizar esta misma clasificación, y de esta manera identificar la información.

- **Información transmitida oralmente:** el nivel de clasificación de la información TLP: ROJO o AMBAR que se transmite a través de una comunicación cara a cara, por teléfono o por alguna otra vía de comunicación debe ser comunicado antes que la información propiamente dicha.

Claúsula 11. La información debe ser tratada de acuerdo con su clasificación.

Para lineamientos sobre las medidas de seguridad a aplicar en la generación, transmisión, recepción, procesamiento y almacenamiento de activos de información se debe consultar el Apéndice "A" "Tratamiento para información según su clasificación".

Claúsula 12. Se deberán proteger de manera especial los Datos sensibles, y Datos personales. Estos datos tienen reglas específicas y más estrictas, para su tratamiento.

Claúsula 13. Se implementará un control para el almacenamiento de todos los datos con TLP: ROJO, incluyendo datos personales o sensibles, que se utilicen en la organización (Control 3.2 CIS V 8.0:2021)

Claúsula 14. Deberá existir segregación en el acceso a los datos, especialmente los datos TLP: ROJO y AMBAR que sean utilizados en la organización. (Control 3.3 CIS V 8.0 :2021) (Control 3.12 CIS V 8.0 :2021).

Claúsula 15. Deberá existir un control del tiempo de retención de los datos, de acuerdo con el proceso de gestión de los datos de la empresa, en especial los datos sensibles o personales que sean utilizados en la organización. (Control 3.4 CIS V 8.0 :2021)

Claúsula 16. Deberá existir un proceso formal de destrucción o eliminación de los datos TLP: ROJO, AMBAR, sensibles o de carácter personal, que ya no sean necesarios, pertinentes, se haya cumplido con la finalidad para la cual fueron recopilados, cumplido los plazos legales de conservación sean obsoletos para el proceso de gestión de la organización, esto será auditado por el área de ciberseguridad de acuerdo con el Anexo "1". (Control 3.5 CIS V 8.0 :2021)

Claúsula 17. Se deberá cifrar los datos en dispositivos de usuario final, que contengan datos TLP: ROJO, AMBAR, datos sensibles o de carácter personal, esto será auditado, por el área de ciberseguridad. (Control 3.6 CIS V 8.0 :2021)

Claúsula 18. Los datos personales o sensibles que por razones contractuales o de alianzas comerciales, deban ser transferidos a terceros, serán clasificados con TLP: AMBAR. (Control 3.7 CIS V 8.0 :2021). Para la transferencia de datos personales o sensibles se requiere llevar a cabo un análisis interno respecto de la factibilidad de la transferencia de dicha información.

Claúsula 19. Debe existir un portafolio de todas las aplicaciones, que se integren a la infraestructura de TI de JetSmart, para acceder, transmitir o entregar datos, con el detalle de acceso. (Control 3.8 CIS V 8.0 :2021)

Claúsula 20. Para la transferencia de datos TLP: ROJO, AMBAR y VERDE, desde JetSmart. se establecerá un procedimiento automatizado de transmisión, cautelando los "Derechos Arco" de los titulares. Y esta transmisión, deberá guardar relación exclusivamente con las tareas y finalidades de los organismos participantes. Se deberá dejar constancia de quien lo requirió, la fecha, el motivo, el propósito del requerimiento, y que tipo de datos se transmitirán. (Artículo 5° Ley 19.628:2020 Chile) (Control 3.8 CIS V 8.0 :2021)

Claúsula 21. Todos los datos TLP: ROJO, AMBAR personales y sensibles serán protegidos, mientras estén en tránsito con la utilización de TLS o SSH. (Control 3.11 CIS V 8.0 :2021)

Claúsula 22. Deberá existir un proceso formal de destrucción o eliminación de los datos sensibles o de carácter personal, información de identificación personal (PII), que ya no sean necesarios, pertinentes o sean obsoletos para el proceso de gestión de la organización, esto será auditado por el área de ciberseguridad. (Control 3.5 CIS V 8.0 :2021)

Claúsula 23. Todos los datos TLP rojo, personales y sensibles serán protegidos, mientras estén en tránsito con la utilización de TLS[2] o SSH[3].(Control 3.11 CIS V 8.0 :2021)

Claúsula 24. Las bases de datos que contengan datos TLP: ROJO y AMBAR personales y sensibles deberán estar alojadas en la infraestructura de la compañía. Se deberá usar plantillas de endurecimiento y recomendaciones de seguridad, para su configuración y mitigar posibles vulnerabilidades. Además, se realizarán pruebas de seguridad y análisis de las mismas, de forma periódica. (Control 3.11 CIS V 8.0 :2021)

Claúsula 25. En los ambientes no productivos, deben utilizarse datos de pruebas y no reales. (Control 3.7 CIS V 8.0 :2021)

Claúsula 26. Las bases de datos que contengan datos TLP rojo datos personales y/o sensible, deberán considerar tecnologías de Data Loss Prevention[4], para protección de fugas de datos. (Control 3.13 CIS V 8.0 :2021)

Claúsula 27. Las bases de datos que contengan datos TLP rojo datos personales y/o sensibles deberán considerar que se registren todos los accesos de los datos sensibles, durante su ciclo de vida (creación, procesamiento, almacenamiento, trasferencia y eliminación).(Control 3.14 CIS V 8.0 :2021)

Claúsula 28. Todos los miembros de JetSmart, que trabajan o poseen acceso al tratamiento de datos personales, están obligadas a guardar secreto sobre los mismos**, aún luego de la desvinculación de la empresa**; cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como, asimismo, sobre los demás datos y antecedentes relacionados con el banco de datos(Artículo 5° Ley 19.628:2020 Chile)

Claúsula 29. Los usuarios que autorizan el uso de sus datos personales, deben ser informados respecto del propósito del almacenamiento y su posible comunicación al público, en la Política de Privacidad de Jetsmart. Por lo que la compañía, se compromete a proporcionar información a las personas, cuyos datos son recopilados, procesados y usados. (Artículo 4° Ley 19.628:2020 Chile, GDPR:2018 Unión Europea)

Claúsula 30. Todo tipo de aviso legales y políticas de privacidad, deberán ser más simples e inteligibles, facilitando su comprensión y deben requiere consentimiento expreso.

[2] El protocolo TLS (Transport Layer Security, seguridad de la capa de transporte) es el protocolo sucesor de SSL. TLS es una versión mejorada de SSL.

[3] SSH™ (o Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.

[4] Una solución de prevención de pérdida de datos es un sistema que está diseñado para detectar potenciales brechas de datos/ transmisiones de datos y prevenirlos a través de monitoreo, detección y bloqueo de información sensible mientras está en uso, en movimiento y en reposo.

Claúsula 31. Se debe designar por parte del comité de ciberseguridad a un miembro de JetSmart, como el responsable del tratamiento de datos y de ser el canal de comunicación, entre la empresa los titulares de los datos y la autoridad competente. (Artículo 5° número VIII LGPD:2018 Brasil, Artículo 33° número 1 GDPR:2016 Unión Europea, Articulo 2° letra n Ley 19.628:2020 Chile).

Claúsula 32. Toda la información utilizada, para procesos de selección de personal, será catalogada de como TLP: rojo, y cumplirá todos los puntos establecidos, en la presente normativa interna. (Control 3.7 CIS V 8.0 :2021)

Claúsula 33. Todos los softwares utilizados, para almacenar de forma temporal o permanente datos de los usuarios, con fines del negocio o de marketing, deberán cumplir con GDPR compliance. (Control 3.1 CIS V 8.0 :2021)

Claúsula 34. El no cumplimiento de la presente política llevará a las sanciones administrativas correspondientes, a lo dispuesto en el reglamento interno del área de recursos humanos. (Control A.7.2.3 ISO 27002:2013)

RESPONSABILIDADES ESPECIFICAS

Alta dirección

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 derivan. Su papel no se limita a un mero apoyo formal; 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:

- **Garantizar la Generación, Almacenamiento y Transferencia Segura de Información**: Asegurar que todos los datos de la compañía se manejen de acuerdo con los objetivos de la organización, respetando la confidencialidad e integridad. (Cláusula 1)

- **Supervisar la Clasificación de Información:** Dirigir la clasificación de la información a lo largo de su ciclo de vida, aplicando criterios como el valor, la sensibilidad, la criticidad, y las obligaciones legales y contractuales. (Cláusula 2 y 3)
- **Gestión de Etiquetado de Información:** Implementar y monitorear los procedimientos para el etiquetado de la información y sus activos relacionados, tanto en formatos físicos como electrónicos, asegurando el uso de metadatos para el etiquetado digital. (Cláusulas 5 y 6)
- **Protección de Datos Sensibles y Personales:** Establecer controles estrictos para el manejo de datos sensibles y personales, cumpliendo con regulaciones específicas y más estrictas para su tratamiento. (Cláusula 12)
- **Segregación de Acceso y Control de Retención de Datos**: Gestionar la segregación de acceso y establecer controles de retención de tiempo para datos sensibles y personales, incluyendo un proceso formal para su destrucción o eliminación. (Cláusulas 14 y 15)
- **Cifrado y Protección de Datos en Tránsito y en Reposo:** Supervisar el cifrado de datos en dispositivos de usuario final y la protección de datos sensibles mientras estén en tránsito. (Cláusulas 17 y 22)
- **Auditoría y Cumplimiento:** Realizar auditorías regulares para verificar la adherencia a esta política, y manejar las consecuencias del no cumplimiento, asegurando que todas las acciones estén documentadas y sean revisadas por el área de ciberseguridad.
- **Educación y Concienciación sobre Ciberseguridad:** Fomentar entre todos los miembros de JetSmart la importancia de la seguridad de la información, ofreciendo formación regular y asegurando que entiendan su rol en la protección de los datos, especialmente en lo que respecta al tratamiento de datos personales y sensibles.

El Gerente de Operaciones IT

Debe trabajar en estrecha colaboración con el Gerente de Ciberseguridad y otros departamentos para integrar la seguridad de la información en todas las actividades de IT y operaciones de la organización, asegurando un enfoque proactivo para proteger los activos de información y cumplir con las obligaciones legales y contractuales.

- **Implementación de la Política de Seguridad de la Información:** Asegurar que todos los procesos y sistemas de IT cumplan con los estándares definidos en la política de seguridad de la información, especialmente en lo que respecta a la generación, almacenamiento, transferencia y destrucción de datos.
- **Clasificación de Activos de Información:** Colaborar con el Gerente de Ciberseguridad para garantizar que todos los activos de información sean clasificados correctamente según su valor, sensibilidad, criticidad y obligaciones legales y contractuales, como se especifica en las cláusulas relacionadas.
- **Ciclo de Vida de la Información:** Administrar el ciclo de vida completo de los activos de información, desde su creación hasta su eliminación, asegurando que todos los procesos se alineen con las prácticas de seguridad y clasificación definidas.

- **Control de Acceso y Segregación de Datos:** Implementar y mantener controles de acceso rigurosos y mecanismos de segregación para los datos, particularmente para aquellos clasificados como TLP: ROJO y ÁMBAR, para prevenir el acceso no autorizado y garantizar la seguridad de los datos.
- **Mantenimiento de la Infraestructura de TI:** Asegurar que la infraestructura de TI, incluidos los sistemas y dispositivos de almacenamiento, esté configurada y mantenida de acuerdo con las plantillas de endurecimiento y las recomendaciones de seguridad para proteger los activos de información.
- **Protección de Datos en Tránsito y en Reposo:** Colaborar con el Gerente de Ciberseguridad para implementar soluciones de cifrado y otras medidas de seguridad para proteger los datos sensibles y personales, tanto en tránsito como en reposo.
- **Respuesta a Incidentes de IT:** Desarrollar y mantener un plan de respuesta a incidentes de IT en conjunto con la gerencia de ciberseguridad que se active en caso de una brecha de seguridad, trabajando estrechamente con el equipo de ciberseguridad para mitigar cualquier daño.
- **Auditoría y Cumplimiento:** Colaborar con el área de ciberseguridad para realizar auditorías regulares de los sistemas de IT y procesos de gestión de datos, asegurando el cumplimiento de la política y las regulaciones aplicables.

Oficial de Datos Personales

Es fundamental para asegurar la integridad, confidencialidad y disponibilidad de la información dentro de la organización. Este rol es crucial para la gestión de la información y la protección de datos en todos los niveles de la compañía.

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

- **Gestión de la Información:** Asegurar que toda la información generada, almacenada y transferida dentro y fuera de la organización cumpla con los objetivos definidos, manteniendo los principios de confidencialidad e integridad en todo momento.
- **Clasificación de la Información:** Implementar y mantener el sistema de clasificación de la información según los criterios establecidos (valor, sensibilidad, criticidad, y obligaciones legales y contractuales), asegurando que cada pieza de información sea correctamente clasificada y manejada a lo largo de su ciclo de vida.
- **Etiquetado de la Información:** Desarrollar y supervisar los procedimientos para el etiquetado efectivo de la información y sus activos relacionados, ya sea en formatos físicos o digitales, utilizando etiquetas físicas o gráficas y metadatos para los activos digitales, siguiendo el Protocolo internacional Traffic Light Protocol (TLP).
- **Protección de Datos Sensibles y Personales**: Establecer medidas especiales de protección para los datos sensibles y personales, incluyendo la implementación de controles para el almacenamiento, acceso, retención, y transferencia de estos datos (Tratamiento de datos en general), asegurando el cumplimiento de las leyes aplicables y las mejores prácticas de seguridad.

- **Gestión de la Transferencia de Datos:** Supervisar y facilitar la transferencia segura de datos sensibles y personales a terceros, asegurando que todas las transferencias cumplan con las clasificaciones TLP aplicables y las leyes de protección de datos vigentes.
- **Auditoría y Cumplimiento:** Colaborar con el área de ciberseguridad para realizar auditorías regulares de los sistemas de IT y procesos de gestión de datos, asegurando el cumplimiento de la política y las regulaciones aplicables.
- **Comunicación y Formación:** Actuar como el principal canal de comunicación entre la empresa, la autoridad competente y los titulares de los datos, informando a los usuarios sobre el propósito del almacenamiento de sus datos y cualquier posible comunicación al público. Además, deberá asegurar que todos los miembros de la organización estén adecuadamente informados y formados en las políticas de privacidad y el tratamiento y protección de datos personales.
- **Gestión de Incidentes:** Establecer y liderar el proceso de respuesta ante incidentes de seguridad que involucren datos personales o sensibles, asegurando una rápida actuación para mitigar cualquier impacto adverso.

Gerentes y jefaturas del Departamento TI

A continuación, se detallan las responsabilidades para los distintos roles dentro del área de TI:

- **Gestión de Accesos:** Controlar el acceso a los sistemas de información, asegurando que solo el personal autorizado tenga acceso a información sensible, conforme a la clasificación TLP.
- **Implementación de Políticas de Seguridad:** Asegurar que todos los sistemas operativos y plataformas de la compañía cumplan con las políticas de seguridad de la información establecidas.
- **Cumplimiento de Normativas:** Asegurar que todas las aplicaciones desarrolladas cumplan con los requisitos legales y las políticas de seguridad de datos de la compañía.
- **Auditoría y Cumplimiento:** Colaborar con el área de ciberseguridad para realizar auditorías regulares de los sistemas de IT y procesos de gestión de datos, asegurando el cumplimiento de la política y las regulaciones aplicables.
- **Diseño de la Arquitectura de TI:** Desarrollar y mantener un marco de arquitectura de TI que apoye los principios de confidencialidad e integridad de la información, asegurando que la infraestructura de TI esté alineada con los objetivos de la organización y las políticas de seguridad de la información.
- **Gobernanza de Datos:** Asegurar que las estructuras de datos y sistemas de información cumplan con los criterios de clasificación y manejo establecidos en las políticas, especialmente en lo que respecta al valor, sensibilidad, criticidad y obligaciones legales y contractuales de la información.
- **Estandarización y Compatibilidad:** Promover la estandarización y compatibilidad entre sistemas para facilitar la clasificación efectiva, el etiquetado, la transferencia segura y la destrucción de datos conforme a las cláusulas establecidas.

- **Seguridad en el Diseño:** Incorporar requerimientos de seguridad y protección de datos desde el inicio en el diseño de nuevos sistemas, aplicaciones y procesos de negocio, considerando la segregación del acceso y el cifrado de datos sensibles y personales.
- **Desarrollo Seguro de Aplicaciones:** Asegurar que el proceso de desarrollo de software cumpla con las normativas de seguridad desde la concepción hasta la implementación, incluyendo la realización de pruebas de seguridad y la aplicación de parches de seguridad.
- **Formación y Concienciación:** Proporcionar formación continua al equipo de desarrollo en prácticas de seguridad informática, programación segura y concienciación sobre ciberseguridad para prevenir brechas de seguridad.

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 el dato 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:

- **Gestión de la Confidencialidad en el Proceso de Contratación:** Asegurar que toda la información utilizada en los procesos de selección de personal esté clasificada TLP: ROJO, garantizando la máxima confidencialidad y cumpliendo con todas las normativas internas establecidas para la protección de datos personales y sensibles.
- **Formación y Concienciación en Seguridad de la Información:** Desarrollar e implementar programas de formación y concienciación para todos los empleados sobre la importancia de la clasificación de la información, el manejo seguro de los datos personales y sensibles, y las políticas de seguridad de la compañía, incluyendo la importancia de mantener la confidencialidad de la información incluso después de la desvinculación de la empresa.
- **Políticas de Privacidad y Avisos Legales:** Asegurar que todas las políticas de privacidad y avisos legales sean claros, sencillos e inteligibles, facilitando la comprensión por parte de los empleados y los usuarios cuyos datos personales son recopilados, procesados y utilizados por la compañía. Esto incluye informar a los usuarios sobre el propósito del almacenamiento de sus datos y su posible comunicación al público.
- **Designación del Responsable del Tratamiento de Datos:** En colaboración con el comité de ciberseguridad, designar a un miembro de la compañía como responsable del tratamiento de datos, quien actuará como el principal punto de comunicación entre la empresa, la autoridad competente y los titulares de los datos en lo referente a cualquier asunto relacionado con la privacidad y la protección de datos.
- **Seguridad en el Ciclo de Vida de los Datos del Empleado:** Implementar controles para el almacenamiento, acceso, retención y destrucción de datos personales de empleados, asegurando que se cumpla con los tiempos de retención establecidos y se apliquen los procedimientos formales de destrucción o eliminación de datos obsoletos o innecesarios, cuando se haya cumplido con la finalidad para la cual fueron recopilados o cumplido los plazos legales de conservación según lo auditado por el área de ciberseguridad.
- **Cumplimiento de Normativas y Sanciones:** Garantizar el cumplimiento de todas las políticas internas y las regulaciones aplicables en materia de protección de datos, preparando a la

organización para auditorías internas y externas y estableciendo efectivamente las sanciones administrativas para los casos de incumplimiento, según lo dispuesto en el reglamento interno del área de recursos humanos y Código de Conducta de la Compañía.

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 se maneje de manera eficiente y responsable a lo largo de todo su ciclo de vida, en conformidad con las políticas internas y las normativas aplicables. 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.
- **Implementar Procedimientos de Etiquetado**: Establecer y supervisar los procedimientos para el etiquetado de la información y sus activos relacionados, ya sean en formatos físicos o electrónicos, utilizando metadatos como forma de etiquetado para los digitales, y asegurando que todos los usuarios cumplan con estos procedimientos antes de compartir información de la compañía.
- **Protección Durante el Ciclo de Vida de la Información:** Asegurar la protección de la información a través de su clasificación durante todo su ciclo de vida, desde su generación hasta su destrucción, incluyendo la implementación de controles para el almacenamiento seguro y la transmisión protegida de datos personales y/o sensibles.
- **Gestión de Transferencias de Datos a Terceros:** Asegurar que cualquier transferencia de datos personales y/o sensibles a terceros, por razones contractuales o de alianzas comerciales, se realice de acuerdo con las clasificaciones establecidas, especialmente TLP: AMBAR, y que se establezcan procedimientos automatizados de transmisión que protejan los derechos de los titulares.
- **Cumplimiento de Normativas de Protección de Datos:** Garantizar el cumplimiento de todas las normativas aplicables en materia de protección de datos personales y asegurar que se informe adecuadamente a los usuarios sobre el propósito del almacenamiento de sus datos y su posible comunicación al público.
- **Auditorías y Cumplimiento de Políticas:** Supervisar y garantizar el cumplimiento de las políticas de seguridad de la información dentro de su área, preparando a su equipo para auditorías internas y externas, y asegurando que se adopten las medidas correctivas necesarias en caso de incumplimientos.
- **Formación y Sensibilización:** Promover la formación y sensibilización continua de su equipo respecto a las mejores prácticas de seguridad de la información, la importancia de la clasificación de datos y la protección de datos personales y sensibles.

Empleados y colaboradores

Empleados JetSmart Airlines y empleados externos tiempo completo y proveedores (empresas que prestan servicios). Se comprometerán a cumplir con este procedimiento adjunto, a la política de seguridad de la información de JetSmart Airlines, en lo que corresponde a sus diferentes perfiles de acceso, debiendo cumplir con lo siguiente:

- Leer esta política, cumpliendo cabalmente con las disposiciones y requerimientos, establecidos en presente procedimiento.
- Velar por la correcta implementación de las cláusulas, enfocadas en la clasificación de la información y protección de los datos personales, tanto de clientes, proveedores y cualquier persona dentro de sus áreas de responsabilidad, así como del cumplimiento, por parte de su equipo de trabajo.
- Informar de inmediato a la Gerencia de Seguridad de la Información, a través de los canales internos existentes al efecto, la existencia de cualquier brecha, incidente o violación a este procedimiento, como también acciones que pongan en riesgo la seguridad de la información de dominio de la compañía.
- Generar, almacenar y transferir información siguiendo los objetivos de la organización, respetando los principios de confidencialidad e integridad.
- Clasificar adecuadamente la información según su valor, sensibilidad, criticidad, y obligaciones legales y contractuales.

Proteger la información a lo largo de su ciclo de vida, incluyendo la generación, almacenamiento, transferencia, y destrucción de la misma.

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 cibereguridad@jetsmart.com para aclarar sus dudas.

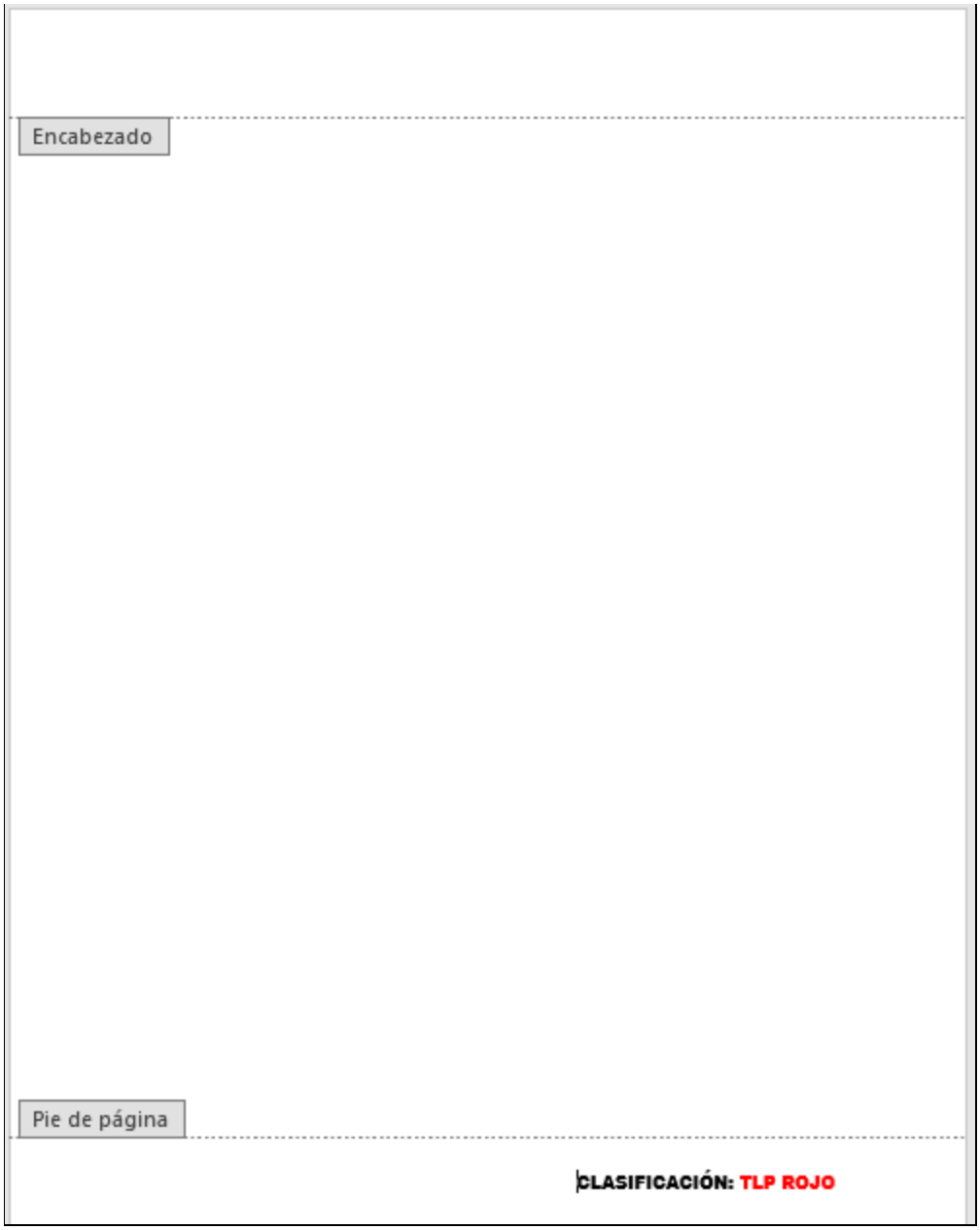
Apéndices

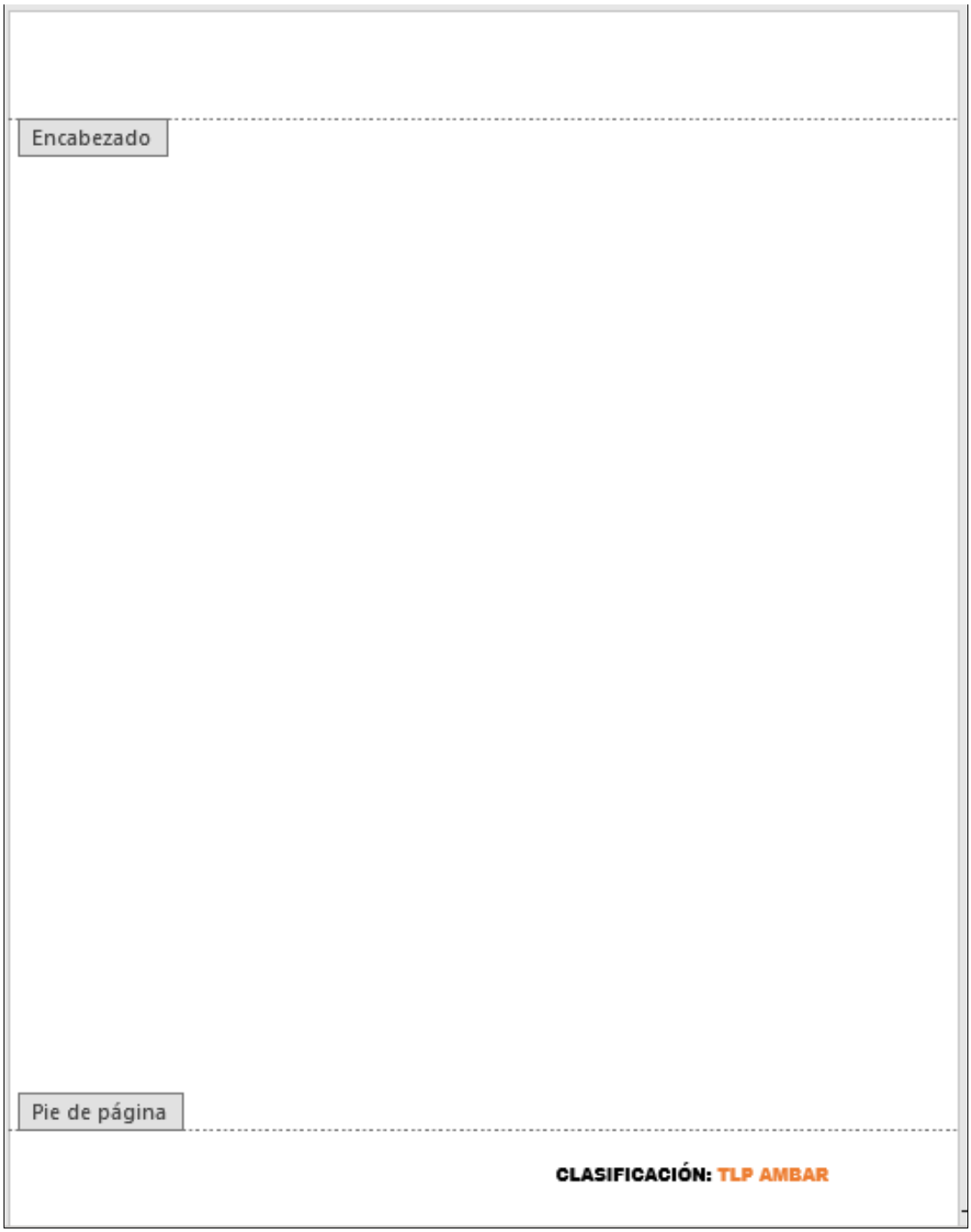
Apéndice "A" - Tratamiento para información según su clasificación
Apéndice "B" - Ejemplos de Etiquetado de documentos

Apéndice "A" Tratamiento para información según su clasificación

		CLASIFICACIÓN DE LA INFORMACIÓN			
PROCESAMIENTO DE LA INFORMACIÓN	MEDIDAS DE SEGURIDAD	TLP: ROJO	TLP: AMBAR	TLP: VERDE	TLP: BLANCO
Almacenamiento	Encriptación necesaria o control de acceso a medios de almacenamiento	X	X		
	Encriptación opcional			X	
	No se requiere encriptar				X
	Protección de DLP	X	X	X	
Copiado	Se requiere la aprobación del creador del documento	X	X		
	Se requiere firma digital para la no repudiación	X			
	Se requiere acuerdo de no divulgación (NDA)	X	X	X	
	No se restringe el uso				X
Transmisión de información externa	Encriptación necesaria	X	X		
	Encriptación opcional			X	
	No se requiere encriptar				X
	Registro de Logs de la Transferencia	X	X	X	
Transmisión de información Interna	Encriptación necesaria	X	X		
	Encriptación opcional			X	
	No se requiere encriptar				X
	Registro de Logs de la Transferencia	X	X		
Divulgación a terceros	Se requiere acuerdo de no divulgación (NDA)		X	X	
	No se puede entregar información a terceros	X			
	Se requiere la aprobación del creador del documento	X	X	X	
	No tiene restricción				X
Destrucción	Acta de destrucción	X	X	X	
	Trituración o eliminación segura	X	X	X	
	Método y equipamiento de eliminación avanzada	X	X	X	
	No requiere borrado seguro				X

Apéndice "A" Ejemplos de Etiquetado de documentos




Encabezado
Pie de página
CLASIFICACIÓN: TLP AMBAR


Encabezado
Pie de página
CLASIFICACIÓN: TLP VERDE