POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión	Fecha	Observaciones
3.0	28/05/2024	Actualización

REFERENCIAS

- Norma ISO 27001:2022, 27002:2022
- CIS Control v8.0:2021

OBJETIVO

El objetivo del presente documento es definir los lineamientos de alto nivel para proteger la información e infraestructura de tecnologías de la información que soportan los procesos de negocio de JetSmart Airlines (en adelante indistintamente "JetSmart", la "Empresa", la "Organización" o la "Compañía"), a través de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) acorde a las definiciones estratégicas, misión y objetivos estratégicos de la Compañía, con controles basados en los principios básicos de la seguridad de la información "confidencialidad, disponibilidad e integridad", que cumplan el marco regulatorio y jurídico vigente.

ALCANCE

La presente política tendrá cobertura 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 información de la Compañía, o bien usen o den soporte a los sistemas de información y/o de negocios de esta. 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 tecnologías de la información.

DEFINICIONES

Concepto	Definición
Ciberseguridad	Conservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio (4.20 ISO 27.032:2015).
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).
Incidente de seguridad de la información	Eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad de comprometer las operaciones comerciales y amenazar la seguridad de la información (ISO 27.000:2018).
Disponibilidad	Propiedad de ser accesible y utilizable bajo demanda por una entidad

	autorizada (ISO 27.000:2018).
Integridad	Propiedad de exactitud y completitud (ISO 27.000:2018).
Gestión de incidentes de seguridad de la información	Conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de incidentes de seguridad de la información (ISO 27.000:2018).

PRINCIPIOS DE SEGURIDAD DE LA INFORMACION

Principio 1: La información de la Compañía deberá solo ser generada, almacenada y transferida, tanto interna como externamente, para cumplir los fines de la organización bajo los principios de confidencialidad, disponibilidad e integridad (5.14: ISO 27002:2022)

Principio 2: Todas las acciones y controles implementados, para proteger la información corporativa, deberán estar alineados, con el establecimiento y mantenimiento de las operaciones de TI (5.2: ISO 27002:2022).

Principio 3: El Gerente de Seguridad de la Información, cumplirá el rol de oficial de seguridad de la información. Él es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas; procedimientos y acciones, con el fin de mejorar la seguridad de la información, enmarcada en sus pilares fundamentales de: confidencialidad, integridad y disponibilidad (5.2: ISO 27002:2022).

Principio 4: Se establecerá un proceso formal de gestión de Riesgos de TI, que los mantenga dentro de los niveles considerados como aceptables, por la organización y que ayuden a optimizar la contribución de la operación de TI a la organización y estén alineados con la "Matriz de Riesgos Corporativos" (5.2: ISO 27002:2022).

Principio 5: Existirá un proceso continuo de gestión de proveedores, los cuales acatarán los principios de esta política y procedimientos derivados de ella, a fin de salvaguardar la información de la Compañía (5.19: ISO 27002:2022).

Principio 6: La Ciberseguridad como concepto amplio de protección, será implementado como un proceso continuo en la organización y abarcará la protección a las operaciones de la Compañía en todas sus funciones relacionadas con el ciberespacio (5.3: ISO 27002:2022).

Principio 7: Se deberá implementar un procedimiento de control de cambios[1], en cualquier plataforma, tanto "on premise" como "Cloud", ya sea aplicación, dispositivo de red, EndPoint u otro, con el objetivo de mantener las relaciones entre los principales recursos y capacidades necesarios, para la prestación de servicios de TI. Este procedimiento incluirá la recopilación de información de configuración, el establecimiento de líneas base, verificación y auditoría (8.9: ISO 27002:2022).

Principio 8: El principio de disponibilidad de la información deberá estar presente en todos los proyectos y operaciones de TI de la Compañía, mediante una gestión de la continuidad operacional a fin de establecer medidas que permitan responder a incidentes e interrupción de las operaciones de los procesos críticos, manteniéndolos en un nivel considerado como aceptable (5.8: ISO 27002:2022).

[1] ES TE PROCEDIMIENTO PUEDE SER MANUAL, SEMI AUTOMÁTICO U AUTOMÁTICO.

Principio 9: Deben existir controles de acceso físico y lógicos a la infraestructura tecnológica de la Empresa y en oficinas administrativas, que permitan la identificación única de cualquier usuario, de forma personal e intransferible, permitiendo el no repudio como responsable de las acciones realizadas y la gestión de riesgos asociados. Es menester implementar un perfilamiento de usuarios en base a su nivel de responsabilidad y de acceso a la información, estableciendo medidas como la implementación de autenticación multifactorial, controles físicos y controles tecnológicos (5.16 ISO 27002:2022).

Principio 10: Respetar el marco jurídico vigente en todos los países en que la Compañía posea operaciones que sean soportadas por infraestructura de tecnologías de la información y comunicaciones. En especial se respetarán las normas de protección de datos personales (PII[2]) (5.31 y 5.34: ISO 27002:2022).

Principio 11: Todos los recursos tecnológicos entregados a los usuarios son de propiedad de la Compañía y su utilización está destinada principalmente a actividades profesionales, pudiendo usarse para fines personales las estaciones de trabajo, asignadas en forma individual (a excepción de los equipos bajo el alcance del entorno de PCI DSS), siempre que sea de forma responsable, cumpliendo la presente política y sus procedimientos derivados (incluyendo el monitoreo de acuerdo a las políticas y normas aplicables).

Principio 12: Todos los recursos tecnológicos entregados a los usuarios son de propiedad de la Compañía y su utilización se encuentra destinada principalmente a actividades profesionales, aunque excepcionalmente podrán usarse para fines personales previa autorización por escrito de la jefatura correspondiente y siempre que sea de forma responsable y cumpliendo la presente política y sus procedimientos derivados (incluyendo el monitoreo de acuerdo con las políticas y normas aplicables) (6.7: ISO 27002:2022).

Principio 13: Todos los dispositivos End point y servidores de ZOFRI S.A. deberán tener instalado el software con una versión actualizada, herramientas de prevención y detección de amenazas, de acuerdo con la línea de base que corresponda a su perfil dentro de JetSmart (8.8: ISO 27002:2022).

Principio 14: Todas las aplicaciones de terceros que necesiten integración con las aplicaciones de JetSmart deberán cumplir la actual política de seguridad de la información, documentación subsidiaria y la línea de base de seguridad, que corresponda al rol que necesita interactuar (5.19: ISO 27002:2022)

Principio 15: Se establecerá un modelo de clasificación de la información, a fin de protegerla a lo largo de su ciclo de vida desde su creación, almacenamiento, procesamiento, trasferencia y eliminación basada en estándares reconocidos internacionalmente (5.12:ISO 27002:2022).

Principio 16: Todos los usuarios deberán informar al área de IT la pérdida, hurto, robo o incidente que afecte cualquier estación de trabajo o recursos tecnológicos en un plazo máximo de 2 horas desde su ocurrencia o toma de conocimiento del hecho, con el objetivo de activar los procedimientos que permitan mitigar la pérdida y tomar los resguardos con la información corporativa alojada en aquellos.

Principio 17: El uso las cuentas de redes sociales corporativas para fines del negocio deberá proteger en todo momento la información confidencial y de propiedad de JetSmart, quedando prohibida toda publicación de información confidencial o reservada de la Compañía por cualquier persona (incluyendo empleados,

[2] La información de identificación personal (PII) es cualquier dato que podría identificar potencialmente a un individuo específico. Cualquier información que puede ser utilizada para distinguir una persona de otra, y que puede ser usada para quitarle el anonimato a los datos anónimos puede ser considerada PII.

exempleados, asesores externos, empresas que prestan servicios, etc) (5.10:ISO 27002:2022).

Principio 18: El uso de aplicaciones y servicios de cualquier tipo que no son de uso corporativo será restringido a menos que se realice una validación técnica de ciberseguridad que valide su nivel de riesgo como aceptable en relación con su necesidad de utilización (8.19:ISO 27002:2022).

Principio 19: Se realizarán auditorías a todos los equipos o recursos tecnológicos de la Compañía (8.16:ISO 27002:2022).

Principio 20: Todo nuevo proyecto o desarrollo de IT deberá poseer una componente de ciberseguridad, en virtud de la cual se validará técnicamente la robustez de la solución para asegurar que los riesgos son mitigados adecuadamente (5.8:ISO 27002:2022).

Principio 21: Respecto al uso de tecnologías actuales y emergentes como Inteligencia Artificial (IA), Machine Learning y otras similares, se establece la prohibición explícita de compartir información confidencial, datos personales o sensibles pertenecientes a JetSmart o que hayan sido recopilados por esta. Esta restricción se impone debido al potencial riesgo de que terceras partes hagan un uso indebido de dicha información, lo cual podría comprometer la confidencialidad, integridad y seguridad de los activos de la Compañía. Sin embargo, se contempla una excepción en casos donde la tecnología sea validada, previa y expresamente autorizada por escrito por parte del área de Tecnologías de la Información (IT), asegurando así el cumplimiento de los estándares de seguridad y privacidad establecido (5.12:ISO 27002:2022).

Principio 22: Todo nuevo proyecto o desarrollo de IT, deberá poseer una componente de ciberseguridad, la cual validará técnicamente la robustez de la solución para asegurar que los riesgos son mitigados adecuadamente (6.15:ISO 27002:2013).

Principio 23: Es obligatorio crear copias de respaldo de la información empresarial, estableciendo plazos de ejecución definidos. Esto se realiza con el propósito de resguardar la integridad de los datos corporativos y garantizar la continuidad operativa del negocio.

Principio 24: El acceso a las redes inalámbricas corporativas de las instalaciones físicas estará restringido para visitantes, salvo por una red especialmente diseñada y con restricciones específicas para su uso.

Principio 25: Es obligatorio reportar en tiempo y forma los ciberataques o incidentes de ciberseguridad que ocurran en JetSmart a las autoridades competentes y a los afectados en aquellos casos que la legislación vigente así lo establezca. En tales casos, JetSmart deberá aportar un plan de acción para mitigar los riesgos que hubiere causado el ciberataque o incidente de ciberseguridad.

Asimismo, es obligatorio para los trabajadores de JetSmart reportar a sus jefaturas tan pronto tengan conocimiento de cualquier circunstancia que pueda generar un ciberataque o incidentes de seguridad de la información. Lo anterior, con el objetivo que JetSmart puede llevar a cabo una adecuada gestión de incidentes de seguridad de la información.

Principio 26: 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.

Principio 27: Se contará con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciber higiene.

Principio 28: La Empresa contará con las certificaciones respecto de los planes de continuidad operacional o ciberseguridad, la medida que sea requerido por las autoridades o leyes de los países en los que la Compañía tenga operaciones.

RESPONSABILIDADES

C-Levels

Los C-levels asumen una responsabilidad crucial en el respaldo y fomento de esta Política de Seguridad de la Información, 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 Seguridad de la Información

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 clave incluyen:

- **Garantizar el Cumplimiento de la Política:** Asegurar que la Política de Seguridad de la Información se aplique efectivamente en todos los niveles operacionales de la organización. Esto implica no solo una supervisión constante, sino también la realización de evaluaciones periódicas para verificar el cumplimiento y la efectividad de la política.
- **Mantener la Política y Normativa Actualizada:** Responsabilizarse de la actualización regular de la Política de Seguridad de la Información y de la normativa de procedimientos específicos derivados de ella. Esta tarea es vital para adaptar y alinear la política con los cambios tecnológicos, las nuevas amenazas de seguridad y las regulaciones vigentes.
- **Coordinar con el área de People & ESG:** Colaborar estrechamente con el área de People & ESG para organizar y llevar a cabo charlas de inducción para todos los nuevos integrantes de la Compañía. El objetivo de estas charlas es garantizar que todos los empleados estén informados y comprendan la Política de Seguridad de la Información desde el inicio de su relación laboral.
- **Fomentar la Concienciación en Seguridad de la Información:** Más allá de las inducciones iniciales, el Gerente debe impulsar programas de formación y concienciación continuos sobre seguridad de la información para todos los empleados, asesores externos y empresas prestadoras de servicio, reforzando la importancia de seguir las políticas y procedimientos establecido.
- **Coordinar con el área de legal:** Colaborar estrechamente con el área legal para verificar que todas las políticas y procedimientos derivados están acordes al cumplimiento del marco jurídico vigente en todos los países donde exista algún tipo de operación de IT de la Compañía.

AREA LEGAL

El área legal desarrolla una estrecha colaboración con el área de ciberseguridad y seguridad de la información, para gestionar efectivamente los desafíos legales y riesgos asociados con la ciberseguridad. Las responsabilidades clave del área legal desde el ámbito de la ciberseguridad son las siguientes:

- **Asesoramiento sobre Cumplimiento Legal en Ciberseguridad**: Garantizar que la organización cumpla con todas las leyes, normativas y estándares relevantes en materia de ciberseguridad.
- **Desarrollo de Políticas y Procedimientos de Ciberseguridad**: Colaborar en la revisión y actualización de políticas y procedimientos internos relacionados con la ciberseguridad e infraestructura crítica de la información, asegurando su conformidad con los requisitos legales y reglamentarios.

- **Gestión de Contratos y Acuerdos con Terceros:** Revisar y negociar acuerdos con proveedores de servicios y otros terceros, incluyendo cláusulas específicas sobre ciberseguridad y protección de datos personales para mitigar riesgos.
- **Asesoramiento en Incidentes de Seguridad y Respuesta a Brechas de Datos:** Asesorar en la respuesta legal a incidentes de seguridad y violaciones de datos, incluyendo la notificación a las autoridades y a las partes afectadas según lo requieran las leyes de protección de datos.
- **Participar el Comité de Ciberseguridad:** Ser parte permanente del comité de ciberseguridad dando la asesoría a los proyectos e iniciativas desde el punto de vista legal.

ÁREA DE PEOPLE & ESG

El área de People & ESG de JetSmart tiene asignadas responsabilidades específicas para garantizar el cumplimiento de la política de seguridad de la información de la Compañía. Estas tareas son fundamentales para la protección de los activos informativos y para fomentar una cultura de seguridad en toda la organización. Las responsabilidades incluyen:

- **Establecimiento de Procedimientos y Controles de Contratación:** Desarrollar y aplicar procedimientos que aseguren que, desde la fase de contratación de personal y al formalizar relaciones laborales, servicios o asociaciones, se informe y conciencie a los involucrados sobre su responsabilidad en el cumplimiento de la política de seguridad de la información.
- **Comunicación con el Área de IT en Cambios de Empleo**: Informar de manera oportuna al área de IT sobre cualquier cambio relacionado con los empleados, como el término de su empleo, contrato o acuerdo. Esto es crucial para gestionar adecuadamente los derechos de acceso a la información de la Compañía, finalizándolos o modificándolos según corresponda.
- **Coordinación de Charlas de Inducción sobre Seguridad de la Información**: Colaborar estrechamente con el Gerente de Seguridad de la Información para organizar y ejecutar charlas de inducción para todos los nuevos integrantes de la Compañía. Estas charlas tienen como objetivo informar sobre la política de seguridad de la información, resaltando la importancia de su cumplimiento y las implicancias de no adherirse a ella.
- **Gestión del Ciclo de Vida del Empleado**: Asegurar que, durante todo el ciclo de vida laboral del empleado en la Empresa, desde la contratación hasta la finalización del contrato, se mantengan y actualicen los controles de seguridad pertinentes.
- **Promoción de una Cultura de Seguridad y Concienciación:** Fomentar una cultura organizacional donde la seguridad de la información sea una prioridad. Esto incluye la implementación de programas de formación continua y campañas de concienciación para mantener a los empleados informados sobre las mejores prácticas de seguridad.
- **Cumplimiento de la Normativa Laboral y de Privacidad:** Velar por que todos los procesos y procedimientos estén alineados con las leyes laborales y de protección de datos, evitando así riesgos legales y de privacidad para la Empresa.
- **Participar el Comité de Ciberseguridad:** Ser parte permanente del comité de ciberseguridad dando la asesoría a los proyectos e iniciativas desde el punto de vista de recursos humanos.

GERENTES Y JEFATURA

Todos los gerentes y jefaturas de la organización asumen responsabilidades adicionales en el marco de la Política de Seguridad de la Información, dada su posición de liderazgo y gestión. Estas responsabilidades son esenciales para asegurar el cumplimiento efectivo de la política y para fomentar una cultura de seguridad en toda la Empresa. Entre sus deberes clave se incluyen:

- **Cumplimiento Efectivo de la Política de Seguridad de la Información**: Asegurar que ellos mismos, así como sus equipos, adhieran a la Política de Seguridad de la Información. Esto implica comprender y aplicar las directrices establecidas, así como garantizar que todos los procedimientos y prácticas de seguridad se sigan consistentemente.
- **Comunicación con el Área de IT en Cambios de Empleo**: Informar de manera oportuna al área de IT sobre cualquier cambio relacionado con las empresas proveedoras o colaboradores externos, como el término de su empleo, contrato o acuerdo. Esto es crucial

para gestionar adecuadamente los derechos de acceso a la información de la Compañía, finalizándolos o modificándolos según corresponda.

- **Implementación de Procedimientos y Controles en la Gestión de Personal:** Durante la contratación de personal y la formalización de relaciones laborales o de prestación de servicios, es responsabilidad de los gerentes y jefaturas asegurarse de que sus subordinados directos estén conscientes y comprendan su responsabilidad en el cumplimiento de la política de seguridad. Esto incluye la inclusión de cláusulas de seguridad en los contratos y la realización de inducciones y capacitaciones necesarias, tanto para colaboradores externos como empresas proveedoras de servicios.
- **Monitoreo, Reporte y Respuesta a Incidentes de Seguridad:** Mantener una vigilancia constante sobre las actividades de seguridad de la información dentro de sus áreas de responsabilidad, incluyendo la identificación y el reporte oportuno de cualquier incidente de seguridad, desviación en la conducta o amenaza la organización.
- **Promoción de la Cultura de Seguridad**: Actuar como líderes en la promoción de una cultura de seguridad en la organización. Esto implica no solo el cumplimiento de las políticas, sino también el fomento activo de prácticas de seguridad entre los miembros de su equipo, a través de ejemplos positivos y la promoción de la concienciación en seguridad.
- **Formación Continua y Concienciación de su Equipo**: Asegurarse de que su equipo reciba la formación y actualizaciones necesarias en cuestiones de seguridad de la información, manteniendo un alto nivel de concienciación y preparación ante los riesgos de seguridad.

Empleados y colaboradores

Los empleados de JetSmart, tanto internos como externos a tiempo completo, proveedores (empresas que prestan servicios y requieren acceso a la red corporativa) y visitas (usuarios que, por una condición particular, deben acceder a la Red Wifi Corporativa) tienen la obligación de adherirse a la Política de Seguridad de la información de la Compañía. Sus obligaciones en relación con la seguridad de la información incluyen:

- **Cumplimiento de la Política de Seguridad de la Información:** Adherirse a los principios establecidos en esta política y cualquier procedimiento asociado.
- **Conocimiento de la Política y Directrices de Ciberseguridad**: Leer y esta Política y todos los procedimientos y directrices específicos relacionados con la ciberseguridad emitidos por la Empresa.
- **Reporte de Incidentes y Brechas de Seguridad:** Informar de manera inmediata a la Gerencia de Seguridad de la Información o a través de los canales internos designados sobre cualquier brecha, incidente o violación de esta política, así como de cualquier acción que pueda poner en riesgo la seguridad de la información de la Compañía.
- **Participación en Programas de Concientización y Capacitación:** Participar activamente en programas de concientización y entrenamiento en seguridad de la información proporcionados por la Empresa.
- **Adhesión a Procedimientos Técnicos de Seguridad:** Cumplir con todos los procedimientos técnicos de seguridad de la información desarrollados a partir de esta política.
- **Confidencialidad de la Información de Autenticación:** Mantener la confidencialidad de la información de autenticación, asegurando que no se divulgue a terceros.
- **Manejo Seguro de Información de Autenticación**: Evitar el registro de datos sensibles, a menos que pueda almacenarse de manera segura y el método de almacenamiento haya sido aprobado (por ejemplo, utilizando una bóvedas de contraseñas como 1Password).
- **Inducción sobre la Política de Seguridad de la Información**: Recibir una charla de inducción al ingresar a la Compañía, coordinada por el área de RRHH y el Gerente de Seguridad de la Información, para asegurar el conocimiento y entendimiento de la presente política.
- **Ser responsables de los accesos a redes de visitas**: Deberá coordinar a la gerencia de operaciones IT los accesos de visitas que estén bajo su supervisión.

El Comité de Ciberseguridad

El Comité de Ciberseguridad desempeña un papel crucial en asegurar que la organización esté protegida contra las amenazas cibernéticas y que pueda responder de manera efectiva en caso de un incidente, protegiendo así los activos críticos y manteniendo la confianza de clientes y socios.

Este sesionará de manera trimestral y se le presentarán los avances en la estrategia de ciberseguridad, incidentes u otras iniciativas relacionadas.

Estará conformado, por CEO, CFO, CCO, COO, directores de TI, People & ESG, E-commerce, Legal y el Gerente de Ciberseguridad; de forma estable. De manera circunstancial, por otros directores o gerentes adicionales, según las temáticas a tratar, por dicho comité. El Comité de Ciberseguridad juega un papel vital en la supervisión y dirección estratégica de las iniciativas de seguridad cibernética de la Compañía. A continuación, se presentan las responsabilidades de este comité:

- **Aprobación de la Estrategia de Ciberseguridad:** Establecer y revisar la estrategia global de ciberseguridad de la organización, asegurándose de que esté alineada con los objetivos empresariales y las tendencias actuales en seguridad de la información.
- **Supervisión de la Política de Ciberseguridad:** Supervisar el desarrollo, implementación y mantenimiento de políticas de ciberseguridad, garantizando que sean exhaustivas, actualizadas y efectivas.
- **Evaluación de Riesgos de Ciberseguridad**: Identificar, evaluar y priorizar los riesgos de ciberseguridad, y asegurarse de que existan planes y procedimientos adecuados para mitigarlos.
- **Gestión de Incidentes de Ciberseguridad:** Supervisar el proceso de gestión de incidentes de ciberseguridad, incluyendo la preparación, respuesta y recuperación ante incidentes.
- **Cumplimiento y Regulaciones:** Garantizar que la organización cumpla con las leyes, regulaciones y estándares relevantes en materia de ciberseguridad y protección de datos.
- **Comunicación y Reporte:** Facilitar la comunicación efectiva sobre ciberseguridad entre diferentes niveles de la organización, incluyendo la alta dirección. También es responsable de reportar el estado de la seguridad cibernética a los *stakeholders* clave.
- **Educación y Concienciación:** Promover programas de educación y concienciación sobre ciberseguridad para empleados a todos los niveles de la organización.
- **Presupuesto y Recursos:** Asegurarse de que la organización disponga de los recursos financieros y humanos necesarios para implementar eficazmente la estrategia de ciberseguridad.

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.