

Política de Seguridad de la Información para proveedores

GHSA-POL-06

Ed. 1 01/07/2026

Las copias impresas no tienen garantía de vigencia

Este documento es propiedad del Grupo Hispasat, no pudiendo ser usado con fines distintos de aquellos para los que ha sido entregado, ni reproducido, total o parcialmente, ni transmitido o comunicado a ninguna persona ajena a la organización sin autorización de Hispasat

hispasat.com

 **Hispasat** | A part of
INDRA GROUP

1. Objetivo

El objetivo principal de la Política de Seguridad de la Información para proveedores (en adelante la Política) es mitigar los posibles riesgos asociados al acceso a la información, sistemas de información o recursos del Grupo HispaSat (en adelante el Grupo o HispaSat) por parte de proveedores de servicios de información, independientemente del tipo de servicio proporcionado, o de relación que le una con HispaSat (legal, contractual o de cualquier otra índole no laboral), con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de HispaSat y sus clientes. Esta Política fue aprobada por el Consejo de Administración el 21 de julio de 2026, previo informe favorable de la Comisión de Auditoría. Cualquier modificación seguirá este mismo procedimiento.

HispaSat se reserva el derecho a modificar este documento cuando sea necesario. Los cambios realizados serán divulgados a todas las empresas proveedoras de servicios de información a las que les aplique utilizando los medios que HispaSat considere oportunos. Es responsabilidad de cada proveedor de servicios de información garantizar la lectura y conocimiento de la Políticas de seguridad más recientes de HispaSat por parte de su personal, así como de obtener su compromiso de cumplir y respetar dichas normas.

En caso de incumplimiento de cualquiera de estas obligaciones, HispaSat se reserva el derecho de adoptar, de acuerdo con la legislación vigente, las medidas sancionadoras que se consideren pertinentes y que podrían llegar a la resolución de los contratos que tenga vigentes con dicha empresa.

2. Principios generales de seguridad

Los proveedores de servicios de información proporcionarán a HispaSat siempre que se requiera, la relación de personas, perfiles, funciones y responsabilidades asociados al servicio prestado, e informará de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.

Los proveedores de servicios de información deberán asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo de la actividad contratada, tanto a nivel específico en las materias correspondientes a la misma relacionadas con el servicio prestado, como en materia de seguridad de la información.

Los proveedores de servicios de información deberán asegurarse, como mínimo que todo el personal asociado al mismo, sea propio o subcontratado, conoce y se compromete a cumplir lo recogido en esta Política. HispaSat podrá solicitar en cualquier momento evidencias del proceso de información.

Los proveedores de servicios de información deberán permitir que HispaSat lleve a cabo las auditorías de seguridad necesarias para asegurar presentación del servicio conforme a las directrices incluidas en esta Política debiendo colaborar con el equipo auditor y facilitar todas las evidencias y registros le sean requeridos.

El alcance y profundidad de cada auditoría será establecido expresamente por HispaSat en cada caso. Las auditorías se llevarán a cabo siguiendo la planificación que se acuerde en cada caso con el proveedor del servicio. HispaSat se reserva el derecho de realizar auditorías extraordinarias adicionales, en caso necesario.

2.1. Confidencialidad de la información

Toda información, documentación, programas y/o aplicaciones, métodos, organización, estrategias de negocio y actividades relacionadas con HispaSat o con su negocio, a las que tenga acceso los proveedores de servicios de información con objeto de la prestación del servicio contratado será considerada información confidencial. De acuerdo con esta consideración, el acceso, intercambio y tratamiento de esta se realizará siempre de acuerdo a las finalidades previstas descritas en el contrato de prestación de servicios. El proveedor de servicios de información mantendrá, en todo momento, el correspondiente deber de secreto durante la duración del servicio y después de que finalice la relación con HispaSat.

Todos los recursos e información a la que haya podido tener acceso o que haya sido necesaria elaborar, modificar o copiar para el correcto desempeño del servicio serán devueltos a la finalización de este. HispaSat podrá solicitar el borrado seguro de los dispositivos desde los que se haya tenido acceso a la Información de HispaSat.

2.2. Propiedad intelectual

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por la normativa de propiedad intelectual. Los proveedores de servicios de información únicamente podrán utilizar material autorizado por HispaSat para el desarrollo de sus funciones. Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los sistemas de información de HispaSat.

Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización por escrito.

HispaSat únicamente autorizará el uso de material producido por él mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

2.3. Protección de datos de carácter personal

Los proveedores de servicios de información que desarrollen actividades para HispaSat y que puedan, en el ejercicio de su actividad, tener acceso a datos de carácter personal según la definición recogida en la normativa específica vigente en la materia, deberán asegurar que cumplen, en lo que al tratamiento de dichos datos se refiere, con la normativa vigente y disponen de los Contratos de Encargado de Tratamiento exigidos.

Para preservar el cumplimiento de los derechos de privacidad HispaSat es responsable de operar, mantener y proteger las redes para sus comunicaciones electrónicas. El cumplimiento de estos objetivos implica interceptar y revelar dichas comunicaciones a través de sistemas automatizados de monitorización, registro de logs y otras herramientas de gestión. A través del uso de los sistemas y servicios de HispaSat el proveedor de servicios de información que los utilice consiente y permite la monitorización de su perfil y del de los profesionales involucrados en el desarrollo del proyecto contratado con el fin de proteger las comunicaciones, así como facilitar toda la información que se almacene en los recursos de HispaSat, cuando así sea requerido por orden judicial u otra instancia.

En el caso de que se trate de servicios relacionados con alojamientos en la nube (*cloud*), la ubicación de dicha infraestructura deberá mantenerse dentro de países miembros de la Unión Europea. En caso contrario, deberá solicitarse autorización a HispaSat.

En el caso de que por necesidades del servicio a prestar se realicen transferencias internacionales de datos fuera del espacio de la Unión Europea, dicha transferencia deberá contar con autorización expresa de HispaSat y documentarse adecuadamente conforme a la legislación vigente.

2.4. Intercambio de información

Cualquier tipo de intercambio de información que se produzca entre HispaSat y los proveedores de servicios de información se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios correspondiente, de modo que dicha información no podrá ser utilizada fuera de dicho marco ni para otros fines.

La distribución de información ya sea en formato electrónico o físico se realizará mediante los recursos determinados en el contrato de prestación de servicios para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato.

HispaSat se reserva, en función del riesgo identificado, la implantación de medidas de control, registro y auditoría sobre estos recursos de difusión. En relación con el intercambio de información dentro del marco del contrato de prestación de servicios, se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por los derechos de autor infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transmisión o recepción de información sensible, salvo que la comunicación electrónica esté cifrada y el envío esté autorizado por escrito.

- Transferencia de información protegida a terceras partes no autorizadas.
- Transmisión o recepción de aplicaciones no relacionadas con el negocio.
- Participación en actividades de Internet, como grupos de noticias, juegos u otras que no estén directamente relacionadas con la prestación del servicio.
- Todas las actividades que puedan dañar la imagen y reputación de HispaSat están prohibidas en Internet y en cualquier otro lugar.

2.5. Uso apropiado de los recursos corporativos

Los recursos corporativos de HispaSat a los que tengan acceso los proveedores de servicios de información serán utilizados exclusivamente para cumplir con las obligaciones y propósitos de la provisión del servicio. Bajo ningún concepto podrán ser utilizados para actividades no relacionadas con el propósito del servicio o para la comisión de actividades que pudieran ser consideradas ilícitas, como daños contra la propiedad intelectual de terceros, incumplimientos de la normativa de protección de datos etc.

Los proveedores de servicios de información se comprometen a utilizar los recursos corporativos de HispaSat a los que tenga acceso de acuerdo con las políticas de seguridad y directrices de HispaSat en la materia.

Con el fin de velar por el correcto uso de los mencionados recursos, HispaSat podrá implementar los mecanismos de control y auditoría que considere oportunos, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente.

En caso de apreciar que algún proveedor de servicios, o su personal, utiliza incorrectamente recursos o información de HispaSat, se le comunicará tal circunstancia al proveedor para que realice las acciones oportunas. HispaSat se reserva el derecho de ejercer las acciones que legalmente le amparen para la protección de sus derechos.

Cualquier fichero introducido en la red de HispaSat o en cualquier equipo conectado a ella a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal, y control de virus y programas malignos.

2.6. Responsabilidad del usuario

Los proveedores de servicios de información deberán asegurarse que todo el personal que desarrolle funciones para HispaSat, y que pueda tener acceso a la información, sistemas de información o recursos de HispaSat respete los siguientes principios básicos dentro de su actividad:

- Cada persona con acceso a información de HispaSat es responsable de la actividad desarrollada por su identificador de usuario y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo su control los sistemas de autenticación asociados a su identificador de usuario, garantizando que la clave asociada sea únicamente conocida por el propio usuario, no debiendo revelarse al resto del personal bajo ningún concepto.
- Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del propietario.
- HispaSat no autoriza el uso de contraseñas acordadas para uso de un grupo de personas como medio para facilitar el acceso a archivos, aplicaciones, bases de datos, ordenadores, redes u otros recursos.
- Los usuarios conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.
- Cualquier usuario con acceso a información de HispaSat deberá seleccionar contraseñas de calidad (al menos 12 caracteres, contener letras mayúsculas, minúsculas, dígitos y caracteres especiales, que no contengan ningún tipo de información fácilmente adivinable como por ejemplo nombres/apellidos de usuarios, etc).

Bajo ninguna circunstancia los usuarios guardarán sus credenciales en una forma legible en archivos locales de los equipos utilizados. Tampoco quedarán escritas en papel ni estarán en sitios donde puedan ser fácilmente accesibles. Si hay razones para creer que una contraseña ha quedado comprometida deberá comunicarlo al área de *Infrastructure & Software Adminsitration* y/o a *Local IT* inmediatamente.

- Cualquier usuario con acceso información de HispaSat deberá cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión, y como mínimo una vez cada 90 días y o cuando exista un posible indicio de conocimiento por parte de otros usuarios.
- Cualquier persona con acceso a información de HispaSat deberá velar por que los equipos queden protegidos cuando vayan a quedar desatendidos.
- Cualquier persona con acceso a información de HispaSat deberá respetar las normas de escritorio limpio, con el fin de proteger los documentos en papel, soportes informáticos y dispositivos portátiles de almacenamiento y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo. En este sentido deberán seguirse las prácticas de Almacenamiento bajo llave, bloqueo de equipos desatendidos, protección de los puntos de recepción y envío de información, destrucción segura, etc.
- La información de HispaSat necesaria para el desarrollo de las actividades contratadas debe estar almacenada en las ubicaciones autorizadas por HispaSat. En ningún caso debe estar almacenada localmente en los equipos informáticos puestos a disposición del personal del proveedor. HispaSat no autoriza ni el almacenamiento ni el tratamiento de su información corporativa en equipos de uso particular.
- Las personas que gestionen información que incluya datos de carácter personal y que no se encuentra recogida en un dispositivo de almacenamiento debe custodiarla e impedir, en todo momento, que pueda ser accesible por persona no autorizada. Asimismo, debe observar lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD).
- Las personas con acceso a sistemas de información de HispaSat nunca deberán, sin autorización por escrito, realizar pruebas para detectar y/o explotar una supuesta debilidad o incidencia de seguridad.
- No está permitido eludir la autenticación del usuario o la seguridad de cualquier sistema, revelar la identificación personal de acceso, permitir el uso de la cuenta asignada a otros usuarios, aunque sean de la misma empresa o departamento, o suplantar la personalidad de otro usuario accediendo o haciendo uso de los recursos informáticos.
- Ninguna persona con acceso a sistemas de información de HispaSat intentará, sin autorización expresa y por escrito, por ningún medio transgredir el sistema de seguridad y las autorizaciones. Se prohíbe expresamente la captura de tráfico de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría autorizadas por escrito.
- Queda expresamente prohibida cualquier conducta contraria al Código Ético y de Conducta de HispaSat ([303-codigo-etico-y-de-conducta-grupo-hispasat_2026-1.pdf](#))

2.7. Requisitos de seguridad para dispositivos

Todos los dispositivos con acceso a información de HispaSat, independientemente de la propiedad de estos, deberán cumplir con las políticas de seguridad establecidas por HispaSat, en especial se tendrán en cuenta las siguientes consideraciones:

- El acceso a los sistemas deberá realizarse siempre de forma autenticada, al menos mediante la utilización de un identificador personal y una contraseña asociada.
- Todo el software instalado o contenido en el dispositivo debe estar licenciado, dentro del ciclo de vida del producto y en un estado acorde a la licencia de uso.

- Los dispositivos deberán permanecer actualizados con la última versión disponible de parches de seguridad para el software y sistema operativo instalado.
- Los dispositivos deben contar con un sistema de protección anti-malware instalado, activo y actualizado a su última versión disponible, tanto del motor como del fichero de firmas.
- Debe activarse el bloqueo de pantalla para que este salte a los 15 minutos de inactividad. El desbloqueo deberá conllevar el uso de contraseñas, patrones de desbloqueo o mecanismos equivalentes, que garanticen que el dispositivo no podrá ser utilizado por un usuario no autorizado.
- Los dispositivos no dispondrán de ninguna herramienta o ficheros contrarios a la Política de Seguridad de HispaSat o que pueda interferir con el software corporativo. Este punto incluye, aquellos que traten de descubrir información distinta de la del propio usuario o realizar accesos no autorizados, como por ejemplo sniffers, herramientas de escaneo de redes, descubrimiento de contraseñas, etc.

2.8. Comunicación de incidentes de seguridad

Los proveedores de servicios de información se comprometen a comunicar tan pronto les sea posible y siempre en un plazo inferior a 24 horas a HispaSat cualquier incidente, debilidad o amenaza (observada o sospechada) que detecte en los sistemas de información de HispaSat o que haya podido afectar a información propiedad de HispaSat o de sus clientes. La comunicación habrá de realizarse al área de HispaSat responsable del servicio y al DPO, remitiendo un correo electrónico a protecciondedatos@hispasat.com.

Una vez el proveedor haya resuelto el incidente que haya podido comprometer a los sistemas o activos de HispaSat, el proveedor habrá de enviar un informe del mismo que incluya las causas de su generación, así como las medidas adoptadas para su resolución y la prevención de futuros eventos similares en el futuro.

En el caso de que el proveedor de servicios de información ostente la condición de Encargado de Tratamiento este habrá de seguir estas indicaciones junto con las que se hubieran indicado en el contrato suscrito para el acceso a datos por cuenta de terceros que se hubiera firmado entre HispaSat y dicho proveedor.

3. Principios específicos de seguridad

3.1. Seguridad física

Todos los proveedores de servicios de información cuyos servicios se presten desde sus propias sedes deberán tener en cuenta los aspectos que se recogen a continuación:

- Los edificios o instalaciones deben ser físicamente sólidos (por ejemplo: no deberían existir huecos en el perímetro o áreas dónde pudieran producirse rupturas fácilmente); los muros externos de las instalaciones deberían ser de construcción sólida.
- Todas las puertas externas deberían estar adecuadamente protegidas contra los accesos no autorizados a través de mecanismos de control, por ejemplo, barras, alarmas, cerraduras, tornos, cámaras de vigilancia etc.
- Cuando sea posible, se recomienda establecer barreras físicas que requieran la identificación del empleado mediante algún método de identificación y autenticación (tarjetas de identificación, tarjetas electrónicas, identificación biométrica, etc.) para prevenir los accesos físicos no autorizados.
- Los edificios o instalaciones deberían contar con sistemas automáticos de detección y respuesta automática ante condiciones ambientales adversas (fuego principalmente). Cuando no se pueda disponer de un sistema de extinción automática de incendios, deben contarse con medidas de extinción manual, que deben ser conocidas por todo el personal de la empresa.
- Se deben establecer las condiciones ambientales básicas de temperatura, higiene, aislamiento eléctrico y sonoro, y otras medidas similares de acuerdo con los requerimientos específicos del equipamiento informático.

- Si se mantiene algún tipo de copia de información responsabilidad de HispaSat, los sistemas que alberguen y/o procesen dicha información deberán estar ubicados en un área especialmente protegida, que incluya al menos las siguientes medidas de seguridad:
 - Tener un sistema de control de acceso independiente al de la sede.
 - Existirá un registro de acceso realizados.
 - El acceso por parte de personal externo se asignará únicamente cuando sea necesario y se encuentre autorizado, y siempre bajo la vigilancia de personal autorizado.
 - El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.
 - Contar con algún tipo de protección frente a fallos de alimentación.

3.2. Seguridad en el desarrollo

Será obligatorio para todos los proveedores de servicios de información que realicen trabajos de desarrollo y/o pruebas de aplicaciones para HispaSat cumplan con los aspectos que se recogen a continuación:

- Los entornos con los que se lleven a cabo dichas actividades deberán estar aislados entre sí y también aislados de los entornos de producción.
- Todos los accesos a los sistemas de información que alberguen o procesen información deberán estar protegidos, al menos, por un “cortafuegos”, que limite la capacidad de conexión a ellos.
- Todo el proceso de desarrollo de software externalizado será controlado y supervisado por HispaSat.
- Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.
- Se incorporarán los mecanismos de identificación, autenticación, control de acceso, auditoría e integridad en todo el ciclo de vida de diseño, desarrollo, implantación y operación de los aplicativos.
- Las aplicaciones que se desarrollen deberán incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.
- Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.
- Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.
- Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.
- El acceso al código fuente de los aplicativos deberá estar limitado al personal del servicio.
- En el entorno de pruebas sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.
- Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.
- Solo se transferirán al entorno de producción aquellos aplicativos que hayan sido expresamente aprobados.

3.3. Seguridad en sistemas

Todos los proveedores de servicios de información cuyos servicios se presten mediante el uso de sus infraestructuras TIC deberán tener en cuenta los aspectos que se recogen a continuación:

3.3.1. Acceso a recursos de red e intercambio de documentos

- HispaSat facilitará al personal de los proveedores de servicios de información acceso a sus recursos de red únicamente si es necesario para el desarrollo del trabajo encomendado y siempre y cuando este sea aprobado, en última instancia por el área de *Infrastructure & Software Administration*.
- Los intercambios de información no documental se gestionarán a través de los medios que establezca el área de *Infrastructure & Software Administration*. Dichos medios pueden variar en función del tipo de proyecto y del tipo de información a intercambiar con el proveedor de servicios de información.
- El acceso a la información y aplicativos de HispaSat por parte de un proveedor de servicios de información debe gestionarse según el procedimiento de Altas, Bajas y Modificación de Usuarios vigente en el que se detalla que los responsables de los activos respecto a los que deben concederse los accesos deben solicitar dichos accesos al área de *Infrastructure & Software Administration* mediante la herramienta corporativa de ticket, detallando en dicha solicitud los usuarios, grupos y permisos a conceder al proveedor de servicios de información.

3.3.2. Gestión de activos

- Los proveedores de servicios de información deberán contar con un registro de activos actualizado en el que se puedan identificar los activos utilizados para la prestación del servicio.
- Los proveedores de servicios de información deberán notificar a HispaSat las bajas de los activos utilizados para la prestación del servicio. Si dicho activo contiene otra propiedad de HispaSat (hardware, software u otro tipo de activos), deberá ser entregado a HispaSat previamente a llevar a cabo la baja para que HispaSat proceda a la retirada de los activos de su propiedad.
- Siempre que un activo haya contenido información considerada sensible, los proveedores de servicios de información deberá llevar a cabo las bajas de activos garantizando la eliminación segura de dicha información, aplicando funciones de borrado seguro o destruyendo físicamente el activo, para que la información que haya contenido no pueda ser recuperable.
- Todos los activos utilizados para la prestación del servicio deberán tener un responsable, que se deberá asegurar de que dichos activos incorporan las medidas de seguridad mínimas establecidas por HispaSat, y que al menos deben ser las especificadas en la presente normativa y, en particular:
 - Cumplir lo establecido en el punto Requisitos de seguridad para los dispositivos.
 - Deberán registrar los eventos más significativos en torno a su funcionamiento. Estos registros de actividad estarán contemplados dentro de la normativa de copias de seguridad del proveedor. En especial, se registrarán todos los eventos realizados con permisos privilegiados.
 - Deberá asegurar que los relojes de los sistemas estarán sincronizados entre sí y con la hora oficial.
 - Deberá garantizar que la capacidad de los sistemas se gestiona adecuadamente, evitando potenciales paradas o malos funcionamientos de dichos sistemas por saturación de recursos.

- Deberá garantizar que los componentes de software asociados a la protección contra intrusiones y código malicioso de los equipos se actualicen periódicamente según la distribución de firmas y actualizaciones del fabricante de dicho software. Asimismo, deberá garantizar que los equipos han sido actualizados con los últimos parches de seguridad y están configurados para que sean actualizados periódicamente, bien de manera automática o manual. Esta actualización debe realizarse al menos mensualmente.
- Se asegurará de que los errores y fallos registrados en la actividad de los sistemas se analizan, adoptándose las medidas necesarias para su subsanación.
- El proveedor de servicios de información establecerá una normativa de copias de seguridad que garantice la salvaguarda de cualquier dato o información relevante para el servicio prestado, con una periodicidad mensual.
- El proveedor de servicios de información deberá disponer de mecanismos seguros para la destrucción de cualquier soporte o documentación que pudiera incorporar información de HispaSat. Dichos mecanismos deberán garantizar la imposibilidad de recuperar cualquier archivo o dato que se hallara almacenado en los mismos. En caso de servirse de una tercera empresa para llevar a cabo la destrucción, el proveedor de servicios de información deberá haber suscrito los acuerdos oportunos, no sin antes haber realizado una evaluación previa de dicha empresa con la que pueda verificarse el cumplimiento de la normativa vigente en materia de protección de datos y de los estándares internacionales de Seguridad de la Información y Privacidad (p.e. ISO 27001).
- El proveedor de servicios de información cuenta con certificados de destrucción segura de soportes o información a disposición de HispaSat para su entrega una vez finalizada dicha destrucción.

3.3.3. Soporte informático

- El soporte informático del personal de los proveedores de servicios de información es responsabilidad de cada proveedor. *El área de Infrastructure & Software Administration* de HispaSat únicamente atiende:
 - Incidencias en los servicios informáticos facilitados por HispaSat e indicados en esta Política.
 - Incidencias o peticiones de servicio creadas por el empleado de HispaSat responsable del activo.

3.3.4. Gestión de la continuidad

- Los proveedores de servicios de información deberán contar con un plan de continuidad y un plan para la recuperación de TI en caso de desastre que permita la prestación del servicio aun en caso de contingencias. Este plan deberá ser desarrollado en función de una evaluación de riesgos (al menos una vez al año) para identificar los riesgos que podrían causar una interrupción de las operaciones y asegurarse de que se ponen en funcionamiento los controles apropiados para gestionarlos y controlarlos.
- Los proveedores de servicios de información pondrán a prueba el plan de continuidad y el plan de recuperación para confirmar que sirven para recuperar el servicio en los plazos de tiempo acordados. Estas pruebas se realizarán al menos anualmente o justo después de que se realicen cambios, mejoras o modificaciones importantes que afecten a los servicios.

3.3.5. Seguridad en red

- Todas las redes deberán estar adecuadamente gestionadas y controladas, asegurándose de que no existen accesos no controlados ni conexiones cuyos riesgos no estén apropiadamente gestionados por él, estableciéndose los oportunos sistemas de monitorización y auditoría de seguridad necesarios para garantizar la seguridad de las conexiones.
- Los servicios disponibles en las redes a través de las que circule la información deberán limitarse en la medida de lo posible.
- Las redes que permitan el acceso a la infraestructura de HispaSat deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:

- Deberán ser comunicadas y autorizadas por el área de *Infrastructure & Software Adminsitration*
- El acceso de usuarios remotos a la red de HispaSat estará sujeto al cumplimiento de procedimientos de autenticación previa y validación del acceso por el área de *Infrastructure & Software Adminsitration*.
- Estas conexiones se realizarán por tiempo limitado y mediante la utilización de redes privadas virtuales o líneas dedicadas.
- En estas conexiones no se permitirá ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas.

3.3.6. Gestión de cambios

- Los proveedores de servicios de información deberán garantizar que todos los cambios en la infraestructura TIC con la que prestan el servicio a HispaSat están controlados y autorizados, garantizándose que no forma parte de la infraestructura TIC ningún componente no controlado.
- Se deberán verificar que todos los nuevos componentes introducidos en la infraestructura TIC utilizada para la prestación del servicio funcionan adecuadamente y cumplen los propósitos para los que fueron incorporados.
- Todos los cambios que se lleven a cabo se deberán realizar siguiendo un procedimiento formalmente establecido y documentado, que garantice que se siguen los pasos apropiados para realizar el cambio.
- El procedimiento de gestión de cambios deberá garantizar que se minimizan los cambios sobre los componentes críticos, limitándose a los estrictamente imprescindibles.
- Se deberán verificar todos los cambios sobre los componentes críticos, para comprobar que no se producen efectos adversos colaterales o no previstos sobre el funcionamiento de dichos componentes o sobre su seguridad.
- Se deberán analizar las vulnerabilidades técnicas que presenten las infraestructuras utilizadas para la prestación del servicio, informando a HispaSat de todas aquellas asociadas a los componentes críticos, con el fin de gestionar conjuntamente dichas vulnerabilidades.

Trusted and Reliable Satellite Solutions

Avda. de Bruselas, 35
28108 Alcobendas
Madrid, Spain
T +34 91 710 25 40

hispasat.com

 **HispaSat** | A part of
INDRA GROUP