C/ Ourense. 24. Edificio Plaza | 36960 Sanxenxo (Pontevedra)
(+34) 902 400 320 (+34) 986 690 542 grupos@interrias.com
www.interrias.com

DATOS DEL PROVEEDOR

NOMBRE COMERCIAL:

NOMBRE FISCAL:

CIF/NIF:

% DE RETENCIÓN:

DIRECCIÓN FISCAL:

CÓDIGO POSTAL: POBLACIÓN:

PAÍS: PROVINCIA:

TELÉFONO ADMINISTRACIÓN:

EMAIL AMINISTRACIÓN:

DATOS BANCARIOS (**OBLIGATORIO ADJUNTAR CERTIFICADO BANCARIO ORIGINAL**)

IBAN:

SWIFT

FORMA DE PAGO: ☐ CRÉDITO DÍAS

EMAIL AVISO DE PAGOS:

PERSONA AUTORIZADA:

DNI:

Estimado proveedor:

VIAJES INTERRÍAS ha implantado un "Sistema de Gestión de Calidad" en base a la Norma ISO 9001:2015, en el que el control y seguimiento sobre el desempeño de los proveedores y subcontratas es un aspecto crítico para garantizar la calidad de nuestros servicios. Por ello, le comunicamos los requisitos básicos que hemos considerado para su selección y evaluación inicial.

Requisitos a considerar:

- Calidad de los servicios ofrecidos.
- Rapidez de respuesta ante solicitudes.
- Relación calidad/precio.

Valorando que el proveedor disponga de una Certificación o implantación de acciones de gestión de calidad, medio ambiente o responsabilidad social.

Evaluación inicial: Una vez verificado el cumplimiento de los requisitos establecidos, y tras un período de prueba, se procede a su inclusión como proveedor homologado de VIAJES INTERRÍAS.

Re-evaluación: En función de las incidencias ocasionadas y de su repercusión en los procesos o servicios de VIAJES INTERRÍAS se procederá a su reevaluación, pudiendo suponer su des-homologación como proveedor.

En caso de disponer de Certificado de Calidad, Medio Ambiente y/o Responsabilidad Social, les agradeceríamos que nos hicieran llegar copia de los mismos. Estamos a su disposición, para cualquier aclaración que necesite al respecto.

Aprovechamos para agradecerle su colaboración.

C/ Ourense, 24. Edificio Plaza | 36960 Sanxenxo (Pontevedra)
(+34) 902 400 320 (+34) 986 690 542 grupos@interrias.com
www.interrias.com

SERVICIO GRATUITO

FACTURACIÓN ELECTRÓNICA

El proveedor del servicio _____

con nombre fiscal _____ y con DNI/CIF _____

Solicita el envío de en formato electrónico de la facturación de Viajes Interrías

¿El proveedor dispone de integración con la plataforma VOXEL?

◯ Si ◯ No

En caso negativo, solicita credenciales a la plataforma de facturación electrónica de Viajes Interrías **e-factura** ¿El proveedor dispone de facturas en formato PDF con firma electrónica?

◯ Si ◯ No

En caso negativo, por favor indiquen un teléfono móvil válido y un correo electrónico con los cuales realizar la verificación manual:

- Teléfono móvil de verificación: _____
- Correo electrónico confirmaciones: _____

Nota Legal Fact Proforma.- Lo subido al sistema por la pestaña de Nueva Factura Proforma es meramente informativo y carece de validez legal alguna, nunca será utilizado para contabilizar ni será subido al SII de la Agencia Tributaria, únicamente se utilizará a efectos de Guía de Pago para el caso en que se necesite realizar el pago de un Pago Parcial/Total o un Deposito de Grupo con anterioridad a que el proveedor tenga emitida la Factura Oficial.

Nota Legal Fact Oficial.- Lo subido al sistema Interrias E-Factur@ por la pestaña de Nueva Factura será sometido cada día a las 18 horas a un proceso de Facturación automática contra las previsiones de Facturación de Viajes Interrias sin que medie supervisión alguna por nuestros Operadores, por lo que debe verificar de forma segura los datos Fiscales de Emisor / Receptor así como en Número y Fecha de Factura indicados. En caso de producirse algún tipo de error debe proceder al borrado de la misma antes de la hora indicada, momento en que será efectiva su contabilización con envío al SII de la Agencia Tributaria. Cualquier corrección que debe hacerse una vez contabilizada la Factura será ya mediante el Correspondiente Abono de la Factura anterior.

Fecha:

_____

Firmado:

CONFIALIS
protección de datos

- **AUTORIZACION CESION DATOS CONTACTO GUIAS EMPRESAS**

AUTORIZACIÓN PARA LA CESIÓN DE DATOS DE CONTACTO DE GUÍAS

D./Dña , con DNI , en nombre y representación de la empresa , con NIF autorizo a VIAJES FISTERRA, S.L.U. a la comunicación de los datos personales de contacto (nombre y teléfono de contacto) de los guías que prestan sus servicios en nuestra empresa, a las personas y entidades participantes en el desarrollo de un viaje (viajeros, otros guías, conductores, restaurantes, hoteles), para la adecuada coordinación del viaje.

En este mismo acto, la empresa a la que represento se compromete a disponer previamente de las autorizaciones necesarias en cumplimiento de la normativa de protección de datos, exonerando a VIAJES FISTERRA de toda responsabilidad en caso de reclamación por parte de un tercero.Para que conste, habiendo leído lo redactado anteriormente y dando mi total consentimiento firmo la presente a fecha de hoy.

En

- **AUTORIZACION CESION DATOS DE CV GUIAS EMPRESAS**

AUTORIZACIÓN PARA LA COMUNICACIÓN DE MI CV

D./Dña , con DNI , en nombre y representación de la empresa , con NIF autorizo a VIAJES FISTERRA, S.L.U. para la comunicación de los datos personales, contenidos en el CV de los guías que prestan sus servicios en la empresa a las Administraciones Públicas pertinentes, con la finalidad de participar en concursos públicos.

En este mismo acto, la empresa a la que represento se compromete a disponer previamente de las autorizaciones necesarias en cumplimiento de la normativa de protección de datos, exonerando a VIAJES FISTERRA de toda responsabilidad en caso de reclamación por parte de un tercero.

Para que conste, habiendo leído lo redactado anteriormente y dando mi total consentimiento firmo la presente a fecha de hoy.

En

PROTECCIÓN DE DATOS: Reglamento (UE) 2016/679 RGPD. VIAJES FISTERRA, S.L.U. como responsable del tratamiento, le informa que tratará sus datos para gestionar la relación contractual con nuestros proveedores. Podrá ejercitar los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento y a reclamar ante la Autoridad de Control, tal como se indica en la información adicional que podrá consultar en https://www.interrias.com/clausulado-rgpd/.

CONFIALIS
protección de datos

- **AUTORIZACION TOMA Y PUBLICACION DE IMAGENES**

AUTORIZACIÓN PARA LA TOMA Y PUBLICACION DE IMÁGENES

D./Dña , con DNI , autoriza a VIAJES FISTERRA, S.L.U. para latoma de sus imágenes y su posterior difusión y publicación en folletos publicitarios, página web de laentidad, blog, redes sociales, prensa y otros medios de comunicación, con el fin de promocionar ydar a conocer las actividades y eventos que organice la entidad.

PROTECCIÓN DE DATOS

VIAJES FISTERRA, S.L.U. le informa que se puede retirar el consentimiento en cualquier momento, dirigiéndose por escrito a Calle Orense, 24 Bajo 12, (Edificio Plaza), 36960, Sanxenxo (Pontevedra) España o a través del correo electrónico protecciondatos@interrias.com.

Que, si retira el consentimiento, los tratamientos que se hayan realizado antes continuarán siendo válidos.

Le informamos que la cesión a redes sociales implica una transferencia internacional de datos.

VIAJES FISTERRA, S.L.U., como responsable del tratamiento, tratará sus datos para llevar a cabo las actividades de promoción de la entidad. Podrá ejercitar los derechos de acceso, rectificación y supresión de los datos, a retirar el consentimiento, entre otros, tal y como se explica en la información adicional que está a su disposición en nuestras instalaciones o en https://www.interrias.com/clausulado-rgpd/.

En

FDO.: .....

En Sanxenxo, a

COMPARECEN

De una parte, Carlos Troncoso Gonzalo, con NIF 35307129J, en nombre y representación de VIAJES FISTERRA, S.L.U., con NIF B36050656 y domicilio en Calle Orense, 24 Bajo 12, (Edificio Plaza), 36960, Sanxenxo (Pontevedra) España. (En adelante el Encargado del tratamiento).

De la otra, con NIF y domicilio en (En adelante el Subencargado del tratamiento).En nombre de la sociedad con NIF . Las personas firmantes aseguran disponer de los poderes suficientes para firmar el presente contrato de subencargado de tratamiento y se hacen personalmente encargados de los perjuicios que puedan llegar a ocasionar en caso de no tener la capacidad de representación necesaria.

EXPONEN

1. OBJETO DEL SUBENCARGADO DE TRATAMIENTO

Mediante las presentes cláusulas se habilita al subencargado del tratamiento, para tratar por cuenta de VIAJES FISTERRA, S.L.U., encargado del tratamiento, los datos de carácter personal necesarios para prestar el servicio que tiene por objeto prestación de servicios de guía turístico.Concreción de los tratamientos a realizar:

- Comunicación
- Consulta

2. IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad VIAJES FISTERRA, S.L.U. encargado del tratamiento, pone a disposición de la entidad:

subencargado del tratamiento de datos del viajero.

3. DURACIÓN

El presente acuerdo tiene una duración igual a la del contrato principal de prestación de servicios.

4. OBLIGACIONES DEL SUBENCARGADO DE TRATAMIENTO

El subencargado del tratamiento y todo su personal se obliga a:

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para finespropios.

b. Tratar los datos de acuerdo con las instrucciones del encargado del tratamiento. Si el subencargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el subencargado informará inmediatamente al encargado.

c. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del encargado, que contenga:

1. El nombre y los datos de contacto del subencargado o subencargados y de cada encargado por cuenta del cual actúe el subencargado y, en su caso del representante del encargado o del subencargado y del delegado de protección de datos.

2. Las categorías de tratamientos efectuados por cuenta de cada encargado.

3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

a) La seudonimización y el cifrado de datos personales.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del encargado del tratamiento, en los supuestos legalmente admisibles. El subencargado puede comunicar los datos a otros subencargados del tratamiento del mismo encargado, de acuerdo con las instrucciones del encargado. En este caso, el encargado identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación. Si el subencargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al encargado de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e. Subcontratación.

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del subencargado.

Si fuera necesario subcontratar algún tratamiento, este

hecho se deberá comunicar previamente y por escrito al encargado, con una antelación de un mes indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el encargado no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de subencargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el subencargado del tratamiento y las instrucciones que dicte el encargado. Corresponde al subencargado inicial regular la nueva relación de forma que el nuevo subencargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subcontratista, el subencargado inicial seguirá siendo plenamente responsable ante el encargado en lo referente al cumplimiento de las obligaciones.

f. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondiente, de las que hay que informarles convenientemente.

h. Mantener a disposición del encargado la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j. Asistir al encargado del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición.
2. Limitación del tratamiento.
3. Portabilidad de datos.
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el subencargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección correo electrónico habitual. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k. Derecho de información.

Corresponde al encargado facilitar el derecho de información en el momento de la recogida de los datos.

l. Notificación de violaciones de la seguridad de los datos.

El subencargado del tratamiento notificará al encargado del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24-48 horas, y a través de correo electrónico habitual, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida. Corresponde al subencargado del tratamiento comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas. La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

a) Explicar la naturaleza de la violación de datos.

b) Indicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Describir las medidas adoptadas o propuestas por el encargado del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

m. Dar apoyo al encargado del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n. Dar apoyo al encargado del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o. Poner disposición del encargado toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el encargado u otro auditor autorizado por él.

p. Implantar las medidas de seguridad siguientes:

Las medidas de seguridad establecidas en el ANEXO I

MEDIDAS DE SEGURIDAD. En todo caso, deberá

implantar mecanismos para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d) Seudonimizar y cifrar los datos personales, en su caso.

q. Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al encargado cuando sea obligatoria su designación.

r. Destino de los datos.

Devolver al encargado de tratamiento los datos de carácter personal y suprimir cualquier copia que esté en su poder. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el subencargado.

El subencargado de tratamiento podrá conservar, debidamente bloqueados, una copia de los datos, en tanto pudieran derivarse responsabilidades de su relación con el encargado del tratamiento.

5. OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

Corresponde al encargado del tratamiento:

a) Entregar al subencargado los datos a los que se refiere la cláusula 2 de este documento.

b) Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el subencargado.

c) Realizar las consultas previas que corresponda.

d) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del subencargado.

e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

6. PROTECCIÓN DE DATOS

De acuerdo con el Reglamento (UE) 2016/679 RGPD y LOPDGDD 3/2018 le informamos que VIAJES FISTERRA, S.L.U. como responsable del tratamiento, tratará sus datos, los del firmante y/o representante, para gestionar adecuadamente la relación contractual como proveedor. Podrá ejercitar los derechos de acceso, rectificación y supresión de los datos, entre otros, tal y como se indica en la información adicional que puede solicitar en nuestras instalaciones o en protecciondatos@interrias.com.

EN ESTE MISMO ACTO SE OBLIGA A FACILITAR ESTA MISMA INFORMACIÓN A LAS PERSONAS CUYOS DATOS FACILITE.

7. LEGISLACIÓN APLICABLE Y RESOLUCIÓN DE CONFLICTOS

Todo litigio relativo al presente Acuerdo y a la relación entre las partes se regirá por la ley española, acordando las partes que se someterán a los Juzgados y Tribunales competentes conforme a derecho.

Y en prueba de conformidad y aceptación de todo lo anteriormente establecido, ambas partes firman el presente Acuerdo, en dos ejemplares y a un solo efecto, en el lugar y fecha indicados.

El Subencargado del Tratamiento

Marco organizativo Política de Seguridad

- ☐ **La política de seguridad (Debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige, en lo que corresponda)**

Normativa de seguridad

- ☐ **Se dispondrá de una serie de documentos que describan (El uso correcto de equipos, servicios e instalaciones; Lo que se considerará uso indebido; La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente)**

Procedimientos de seguridad

- ☐ **Se dispondrá de una serie de documentos que detallen de forma clara y precisa (Cómo llevar a cabo las tareas habituales; Quién debe hacer cada tarea; Cómo identificar comportamientos anómalos; Cómo reportar comportamientos anómalos)**

Marco operacional Planificación

- ☐ **Análisis de riesgos (Se identifican los activos más valiosos, las amenazas, salvaguardas y riesgos residuales)**
- ☐ **Arquitectura de seguridad (La seguridad del sistema será objeto de un planteamiento integral detallando)**
- ☐ **Adquisición de nuevos componentes (Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema)**

Control de acceso

- ☐ **Identificación (Se identifican todos los usuarios del sistema, procesos, datos gestionados)**
- ☐ **Requisitos de acceso (Los recursos del sistema se protegen ante un uso si autorización o privilegios, particularmente los ficheros de sistema y configuración)**
- ☐ **Segregación de funciones y tareas (Está separado configuración y mantenimiento de las de operación del sistema)**
- ☐ **Proceso de gestión de derechos de acceso (Están reducidos los privilegios al mínimo necesario)**
- ☐ **Mecanismo de autenticación (Se identifican y autentifican los usuarios mediante credenciales)**
- ☐ **Acceso local (Se limita la información de acceso, el número de intentos de acceso y se bloquearan cuando se supere el límite)**
- ☐ **Acceso remoto (Están asegurados los equipos cuando se accede remotamente y existe una política) Monitorización del sistema**
- ☐ **Detección de intrusión (Se dispone de herramientas de detección)**

Explotación

- ☐ **Existe inventario de activos (Información, servicios, aplicaciones, equipos, equipos móviles, comunicaciones, soportes, … y su responsable)**
- ☐ **Configuración de seguridad (Se realiza una configuración previa de los equipos antes de su puesta en servicio, limpiando toda la información, cuentas, servicios y comunicaciones antiguas)**
- ☐ **Gestión de la configuración (Se gestiona de forma continua la configuración de los equipos, previa autorización y gestionando las vulnerabilidades)**
- ☐ **Mantenimiento (Se prioriza y realiza el mantenimiento según lo especifica el fabricante)**
- ☐ **Gestión de cambios (Existe un control de actualizaciones y mantenimiento)**
- ☐ **Protección frente a código o SW dañino Gestión de incidentes (Existe un proceso de gestión de incidentes con asignación de recursos, análisis, prevención y optimización)**
- ☐ **Registro de la actividad de usuarios (Dispone de registro de actividad, se generan informes y se encuentra automatizado)**
- ☐ **Registro de la gestión de incidentes (Se registra la gestión realizada de los incidentes y se analiza)**
- ☐ **Protección de los registros de actividad (Se protegen los registros de actividad)**
- ☐ **Protección de claves criptográficas (Se utilizan programas evaluados o dispositivos criptográficos certificados con algoritmos certificados o acreditados)**

Servicios externos

- ☐ **Contratación y acuerdos de nivel de servicio (Se establece contractualmente las responsabilidades y características de los servicios externos)**
- ☐ **Gestión diaria (Existe un control diario, rutinario, coordinado y procidementado de los servicios externos)**
- ☐ **Medios alternativos (Existe una provisión de servicios alternativos con las mismas garantías)**
- ☐ **Continuidad del servicio**
- ☐ **Análisis de impacto (Se conocen los servicios críticos y el impacto en caso de interrupción)**
- ☐ **Plan de continuidad (Existe un plan de contingencia que dispone de servicios a ejecutar, previsión de medios, plan de recuperación y restitución de los servicios)**
- ☐ **Pruebas periódicas (Se realizan ensayos y pruebas periódicas regulares)**

Protección de las comunicaciones

- ☐ **Perímetro seguro (Se dispone de firewall, flujos autorizados y sistemas redundantes)**
- ☐ **Sistema de métricas (Se recopilarán datos suficientes para conocer el grado de implantación de las medidas de seguridad y elaborar los informes pertinentes)**

Medidas de protección Protección de instalaciones e infraestructuras

- ☐ **Áreas separadas y con control de acceso (Existen áreas separadas según su función y además se controla el acceso a las diferentes áreas)**
- ☐ **Identificación de personas (Se identifican a las personas que acceden a instalaciones y equipamiento)**
- ☐ **Acondicionamiento de los locales (Disponen de los elementos adecuados para el equipamiento y protección de los riesgos analizados)**
- ☐ **Energía eléctrica (Disponen de energía eléctrica y tomas suficientes. Luces de emergencia y sistemas de respaldo)**
- ☐ **Protección frente a incendios (Dispone de medios para protegerse frente al fuego)**
- ☐ **Dispone de protección frente a inundaciones Registro de entrada y salida de equipamiento**
- ☐ **(Se dispone de registro de entradas y salidas de las instalaciones)**
- ☐ **Instalaciones alternativas (Se garantiza y se dispone de instalaciones alternativas)**
- ☐ **Gestión del personal**
- ☐ **Caracterización del puesto de trabajo (Están definidas responsabilidades en materia de seguridad, inventariado de puestos, requisitos para el puesto y confidencialidad)**
- ☐ **Deberes y obligaciones (Informar de deberes y obligaciones del puesto, así como la confidencialidad)**
- ☐ **Concienciación (Se conciencia al personal sobre su papel en seguridad y confidencialidad, comportamientos sospechosos y actuación en caso de incidentes)**
- ☐ **Formación (Se forma al personal en configuración detección y reacción de incidentes y singularidades del sistema)**

Protección de los equipos

- ☐ **Puesto de trabajo despejado (Se encuentra despejado y el material no usado cerrado)**
- ☐ **Bloqueo del puesto de trabajo (Se bloquea al cabo de un tiempo y se bloquea la sesión al cabo de cierto tiempo de inactividad)**
- ☐ **Protección de equipos portátiles (Están inventariados, no contienen información sensible, se limita su acceso remoto, no contiene claves, se limita el acceso a redes básicas, protegido mediante contraseña y cifrado)**
- ☐ **Medios alternativos (Existen medios alternativos)**
- ☐ **Protección de la confidencialidad (Uso de VPN, Algoritmos acreditados por CCN)**
- ☐ **Protección de la autenticidad y de la integridad (Se asegura la autenticidad antes de realizar conexiones, sistemas de prevención activos, cifrados y encriptados)**
- ☐ **Segregación de redes (Control de entrada de usuarios, segregación de redes y monitorización)**
- ☐ **Medios alternativos (Existen medios alternativos para el servicio)**

Protección de soportes de información

- ☐ **Etiquetado (Sin revelar su contenido) Criptografía (Se aplican cifrados y encriptados) Custodia (Se garantiza el control de acceso) Transporte (Registro, cotejado y encriptado)**
- ☐ **Borrado y destrucción (Borrado y destrucción segura y certificada)**
- ☐ **Protección de aplicaciones informáticas Desarrollo de aplicaciones (En sistema diferente a sistema de producción)**
- ☐ **Aceptación y puesta en servicio (Análisis de vulnerabilidades y pruebas de penetración)**
- ☐ **Protección de la información Datos de carácter personal Calificación de la información**
- ☐ **Cifrado de información (En información sensible) Firma electrónica (Mediante sistemas seguros)**
- ☐ **Limpieza de documentos (Eliminación de información personal adicional en documentos y meta- datos)**
- ☐ **Copias de seguridad (backup) (De información, configuración y equipos. Cifrado, control y verificación de los respaldos. Procedimientos de respaldo)**

Protección de los servicios

- ☐ **Protección del correo electrónico (De la información mediante cifrado, antispam, limitaciones ante uso privado y código dañino)**
- ☐ **Protección de servicios y aplicaciones web Protección frente a denegación de servicios Medios alternativos personal alternativo**