# ANEXO 1 - REQUISITOS GENERALES

| | |
|---|---|
| **Nombre contacto:** | **0** |
| **Correo electrónico contacto:** | **0** |
| **Cargo:** | **0** |
| **Teléfono contacto:** | **0** |
| **Fecha:** | |

| CRITERIO | CÓDIGO | REQUERIMIENTO | CUMPLE | OBSERVACIONES DEL PROVEEDOR | EVIDENCIAS DEL PROVEEDOR | OBSERVACIONES ORGANIZACIÓN CONTRATANTE |
|---|---|---|---|---|---|---|
| | | | | | | |
| PRINCIPIOS DE SEGURIDAD | RG-PS-01 | ¿Están claramente definidos los roles y responsabilidades de Seguridad de la Información y Ciberseguridad dentro de la estructura de la organización? | | | | |
| | RG-PS-02 | Datos de contacto (nombre, apellidos, email y teléfono) del Responsable de Seguridad. Esta figura es obligatoria tal y como se establece en las normativas y estándares de seguridad como el ENS, la ISO27001 o la NIS2. | | | | |
| | RG-PS-03 | El proveedor debe informar a la organización contratante de la ubicación geográfica y de los países desde los que presta el Servicio y en los que puede almacenar y tratar la información de la misma, tanto durante la normal prestación del Servicio, como en caso de contingencia. Por otro lado, el proveedor deberá informar de cualquier cambio de ubicación. | | | | |
| | RG-PS-04 | ¿El proveedor dispone de Políticas de Seguridad de los Sistemas de Información establecidas en su empresa y de un marco normativo en materia de Seguridad de la Información? | | | | |
| | RG-PS-05 | ¿El proveedor ha llevado a cabo un análisis de riesgos del objeto del contrato? | | | | |
| | RG-PS-06 | ¿El proveedor es conocedor de las leyes de información que son de aplicación, tales como, si procede: la Ley de Protección de Infraestructuras Críticas, de 28 de abril y el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, el Esquema Nacional de Seguridad, el RGPD y la LOPDGDD? | | | | |
| | RG-PS-07 | ¿El proveedor dispone de un documento de arquitectura técnica que incluya todos los elementos tecnológicos relacionados con el servicio prestado (flujos de datos, sistemas, elementos de red, etc)? | | | | |
| | RG-PS-08 | ¿Cuenta con pólizas que cubran ataques cibernéticos? | | | | |
| | RG-PS-09 | ¿Las relaciones con terceros (subcontratistas) que intervienen en la prestación del servicio están reguladas por contrato? | | | | |
| | RG-PS-10 | En relación con la cuestión anterior, el proveedor debe especificar los servicios que se subcontratan y la empresa subcontratada. | | | | |
| | RG-PS-11 | ¿El proveedor verifica periódicamente el cumplimiento de las medidas de seguridad acordadas con cada proveedor? El subcontratista también cumplirá totalmente con las obligaciones existentes entre la empresa y el proveedor, incluidas las obligaciones contraídas a favor de las diferentes autoridades de control. | | | | |
| | | | | | | |
| CLASIFICACIÓN Y CONFIDENCIALIDAD | RG-CC-01 | ¿El proveedor realiza una clasificación de la información implementando controles asociados a la información clasificada en virtud de la confidencialidad? | | | | |
| | RG-CC-02 | ¿El proveedor lleva a cabo etiquetado de la información en base a la confidencialidad de la misma? | | | | |
| | RG-CC-03 | El proveedor debe indicar la clasificación de la información del objeto del contrato, las etiquetas establecidas para el proyecto, y los controles de seguridad que aplica en base a la clasificación realizada. | | | | |
| | RG-CC-04 | ¿El proveedor dispone de una política de manejo de información, política de puesto de trabajo despejado, pantalla limpia para los recursos de tratamiento de la información...? | | | | |
| | RG-CC-05 | El proveedor debe contemplar el compromiso de devolución/destrucción (a elección de la empresa contratante) de la información confidencial recabada durante la ejecución del servicio.<br>Si por la naturaleza del proyecto, la empresa contratante requiere del borrado y destrucción de cualquier soporte de información englobado al alcance del servicio prestado; el proveedor deberá aplicar un procedimiento seguro de borrado y destrucción, siguiendo lo indicado en el Esquema Nacional de Seguridad o en la legislación de ciberseguridad de aplicación correspondiente. | | | | |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **GESTIÓN DE INCIDENTES** | **RG-GI-01** | ¿El proveedor dispone de un procedimiento formal de gestión de incidentes de seguridad? | | | | |
| | **RG-GI-02** | En caso afirmativo, el proveedor debe indicar cómo llevará a cabo la comunicación de un incidente a la empresa contratante que pueda tener repercusión para la información o los sistemas de la misma. | | | | |
| | **RG-GI-03** | Adicionalmente, en caso de haber un incidente relacionado con el objeto del contrato deberá colaborar con la organización contratante en todo lo que esta requiera sin coste adicional alguno. | | | | |
| | | | | | | |
| **CUMPLIMIENTO NORMATIVO** | **RG-CN-01** | ¿El proveedor se encuentra certificado en algunos de los estándares de seguridad de la información tales como el Esquema Nacional de Seguridad, o la Norma ISO:27001:2022 para el alcance del proyecto/producto/servicio prestado? Indicar a continuación en cual o cuáles: | | | | |
| | | Norma ISO:27001:2022 | | | | |
| | | ENS- Nivel | | | | |
| | | Otros | | | | |
| | **RG-CN-02** | En caso de que la respuesta a la pregunta anterior sea “Si”, indicar cuales y aportar evidencia de la certificación. | | | | |
| | | | | | | |
| **SEGURIDAD DE LOS EQUIPOS** | **RG-SE-01** | ¿El proveedor va a tratar información de la empresa o va a conectarse a redes o sistemas de información de la empresa con sus propios equipos o va a tratar información de la empresa en sus equipos?<br>En caso de que la respuesta a esta cuestión no sea afirmativa, no será necesario contestar al resto de requerimientos de este bloque "Seguridad de los equipos". | | | | |
| | **RG-SE-02** | En caso afirmativo, ¿el proveedor dispone de un plan de no obsolescencia y tiene los equipos actualizados a la última versión de software disponible? | | | | |
| | **RG-SE-03** | ¿El proveedor dispone de un inventario actualizado de la totalidad de equipos, que contenga los siguientes campos?:<br>En caso afirmativo debe facilitar previamente al inicio del contrato dicho inventario. | | | | |
| | | a.Tipo de equipo | | | | |
| | | b.Dirección IP del equipo. | | | | |
| | | c.Nombre del equipo (hostname). | | | | |
| | | d.Dirección MAC del equipo | | | | |
| | | e.Inventario actualizado del Software instalado en cada equipo. | | | | |
| | | f.Modelo del equipo. | | | | |
| | | g.Versión del sistema operativo instalado. | | | | |
| | | h.Marca, modelo y Versión de antimalware instalado. | | | | |
| | **RG-SE-04** | ¿El proveedor dispone de un producto antimalware en sus equipos, y lleva a cabo el mantenimiento y actualización continua del mismo? | | | | |
| | **RG-SE-05** | El proveedor debe ejecutar el informe de cumplimiento en sus equipos con la herramienta CLARA del CCN, y obtener un porcentaje superior al 65% en categoría Media. Debe aportar dicho informe. | | | | |
| | **RG-SE-06** | ¿El proveedor dispone de controles para prevenir la fuga de datos en las estaciones de trabajo y/o en la red? - Por ejemplo, Bloqueo/desactivación de los medios extraíbles, cifrado del disco, herramienta de DLP, etc (ejemplo: uso Bitlocker, bloqueo USB, herramienta DLP e IRM...) | | | | |
| | **RG-SE-07** | ¿El proveedor dispone de procesos o procedimientos para controlar las condiciones de seguridad en situaciones de teletrabajo? | | | | |
| | **RG-SE-08** | ¿El proveedor dispone de un mecanismo seguro de acceso remoto a su infraestrucutra? | | | | |
| | **RG-SE-09** | ¿El mecanismo de acceso remoto cuenta con la posibilidad de permitir el acceso remoto segín cientas medidas de seguridad (SO actualizado, antivirus...etc) | | | | |
| | **RG-SE-10** | ¿El proveedor dispone de doble factor implantado y obligatorio para el acceso de los usuarios en remoto a los sistemas de su empresa? | | | | |
| | **RG-SE-11** | ¿El proveedor dispone de una Política de contraseñas implantada en su empresa que contemple normas de complejidad mínima y robustez frente a ataques de adivinación? Esta Política debe incluir, como mínimo, las siguientes medidas de seguridad en las contraseñas: | | | | |
| | | a.Longitud mínima: 12 caracteres | | | | |
| | | b.Nivel mínimo de complejidad:Números, mayúsculas, minúsculas, signos de puntuación y caracteres especiales (del tipo: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”). | | | | |
| | | c.Máximo número de intentos fallidos de autenticación: 5 | | | | |
| | | d.Prohibición de reutilizar contraseñas anteriores: 10 últimas contraseñas. | | | | |
| | | e.Se puede cambiar solo una vez al día (después de cambiar la contraseña, la función se inhabilita durante 24 horas) | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | f.Debe ser reemplazada cada 90 días | | | | |
| | | | | | | |
| **CONCIENCIACIÓN EN CIBERSEGURIDAD** | **RG-CO-01** | ¿El proveedor ha proporcionado la adecuada formación, concienciación y capacitación al personal involucrado en la prestación del servicio? Dicho personal deberá contar con formación y conocimientos específicos de las tecnologías involucradas en la prestación del servicio, Seguridad de la Información y la legislación aplicable en el contexto del servicio. | | | | |
| | | | | | | |
| **SEGURIDAD FÍSICA** | **RG-SF-01** | Si el servicio se presta desde instalaciones del proveedor, ¿cuenta un perímetro de seguridad física protegido (ej: control de acceso principal, acceso a planta y acceso a sala)? | | | | |
| | **RG-SF-02** | Si el servicio se presta desde las instalaciones del proveedor, ¿garantiza que dispone de personal de recepción 24x7? | | | | |
| | **RG-SF-03** | Si el servicio se presta desde las instalaciones del proveedor, ¿garantiza el uso de cámaras de video y/o mecanismos de control de acceso para monitorizar los accesos físicos individuales a zonas restringidas? | | | | |
| | **RG-SF-04** | Si el servicio se presta desde las instalaciones del proveedor, ¿garantiza la existencia de Sistema de Detección de Intrusos en el perímetro, conectado a un puesto de mando de seguridad? | | | | |
| | **RG-SF-05** | Si el servicio se presta desde las instalaciones del proveedor, ¿se garantiza la existencia de una lista de personas actualizada con acceso autorizado a la instalación, así como la realización del registro de las entradas y salidas de todos los visitantes? | | | | |
| | **RG-SF-06** | Si el servicio se presta desde las instalaciones del proveedor, su centro de procesamiento debe disponer de sistemas anti-incendios, protección para cambios de tensión, aire acondicionado, enfriador seco y de fluidos, bomba de agua instalados que deben revisarse periódicamente. | | | | |
| | | | | | | |
| **RECUPERACIÓN DE LA INFORMACIÓN** | **RG-RI-01** | Al servicio objeto del presente procedimiento de contratación le serán de aplicación los requisitos establecidos por ENS, RGPD Y LOPDGDD. Este nivel alto de exigencia, junto con el que la empresa se impone a sí misma, establece la necesidad de que el proveedor deba:<br>• Disponer de una o más localizaciones en las que poder mantener la provisión de servicios en caso de Contingencia, Crisis o Continuidad.<br>• Proveer a la plataforma o sistema de arquitecturas de seguridad redundadas y balanceadas.<br>• Contar con mecanismos de respaldo de la información adecuados y contrastados (procesos de backup, restauración, pruebas de restauración, etc.) para garantizar su correcta salvaguarda en caso de contingencia grave.<br>• Disponer de un Plan que permita disponer de un Plan de Continuidad de Negocio, para las contingencias que puedan producirse en la prestación de servicios al amparo del presente contrato. | | | | |
| | **RG-RI-02** | ¿El proveedor establece, documenta, aprueba, comunica, aplica, evalúa y mantiene políticas y procedimientos de gestión de la continuidad del negocio y resiliencia operativa? Debe revisar y actualizar las políticas y procedimientos al menos una vez al año. | | | | |
| | **RG-RI-03** | El proveedor debe aportar evidencia de un registro de pruebas de gestión de crisis que demuestren la participación del personal relevante de proveedores y prestadores de servicios en caso de contingencia o crisis. | | | | |
| | | | | | | |