Versión imprimible del documento. La integridad de este documento puede comprobarse en la sede electrónica del Gobierno de Cantabria, a través de https://verificacsv.cantabria.es/verificacsv?codigoVerificacion=A0600NbbQQ1bXa6Ow38hyX7ZduvTJLYdAU3n8j
Identificador de documento electrónico (ENI): ES_A06006299_2024_DOC_00N_0000000000000001464149

GOBIERNO de CANTABRIA
CONSEJERÍA DE PRESIDENCIA JUSTICIA SEGURIDAD Y SIMPLIFICACIÓN ADMINISTRATIVA
Dirección General de Informática
Centro de Proceso de Datos

AÑO JUBILAR LEBANIEGO 2023·2024

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU

SUMINISTRO DEL TERCER NODO DE LA SOLUCIÓN DE FIREWALL PARA EL CPD

PLIEGO DE PRESCRIPCIONES TÉCNICAS

DIRECCIÓN GENERAL DE INFORMÁTICA
CENTRO DE PROCESO DE DATOS

Firma 1: **26/04/2024 - OLGA ESTERAS HERNANDEZ**
COORDINADORA DE AREA TIC - D.G. DE INFORMATICA
Firma 2: **26/04/2024 - ALFREDO JAIME FERNANDEZ**
JEFE DE CENTRO PROCESO DE DATOS - D.G. DE INFORMATICA
CSV: A0600NbbQQ1bXa6Ow38hyX7ZduvTJLYdAU3n8j

*Este documento tiene carácter de copia electrónica auténtica con **validez y eficacia administrativa del documento ORIGINAL** (art. 27 Ley 39/2015)*

Versión imprimible del documento. La integridad de este documento puede comprobarse en la sede electrónica del Gobierno de Cantabria, a través de https://verificacsv.cantabria.es/verificacsv?codigoVerificacion=A0600NbbQQ1bXa6Ow38hyX7ZduvTJLYdAU3n8j
Identificador de documento electrónico (ENI): ES_A06006299_2024_DOC_00N_0000000000000001464149

1. OBJETO DEL CONTRATO

El objeto de este contrato es el suministro del tercer nodo de la solución firewall del Centro de Proceso de Datos, el cual es necesario para garantizar un adecuado nivel de seguridad en el centro de proceso de datos secundario del Gobierno de Cantabria. Este centro de proceso de datos secundario está situado en una ubicación diferente que el principal.

Este contrato permitirá dotar a las instalaciones del Centro de Proceso de Datos de redundancia en estos sistemas de seguridad perimetral, garantizando el rendimiento, la seguridad y la disponibilidad necesarias para que todos los servicios gestionados por el Centro de Proceso de Datos sigan manteniéndose en los niveles exigidos.

Este suministro se hace imprescindible para cumplir con las medidas de seguridad exigidas según el Esquena Nacional de Seguridad.

2. SITUACIÓN ACTUAL

Actualmente el Gobierno de Cantabria cuenta con una plataforma de firewalls del fabricante Fortinet en las instalaciones del centro de proceso de datos principal (CPD 1).

En el CPD 1 existen actualmente 3 clúster Fortigate de 2 nodos:

- FW-CPD: Es el firewall perimetral de la red corporativa, se protegen todas las conexiones desde y hacia el exterior.
- FW-Intranet: Firewall para los servicios internos de la red corporativa, se protegen todas las conexiones de los servidores internos.
- FW-Aplicaciones: Es el firewall para proteger las aplicaciones publicadas en Internet.

Estos sistemas actualmente están situados en el CPD principal, la ampliación de estos sistemas de seguridad perimetral al CPD secundario requiere de la utilización de equipos del mismo fabricante para garantizar la compatibilidad y que se puedan integrar de forma adecuada con la plataforma actualmente instalada.

Para poder formar este clúster extendido se necesita contar con los mismos equipos en el segundo CPD a nivel hardware, software y licenciamiento.

3. CARACTERÍSTICAS DEL OBJETO DEL CONTRATO

De acuerdo al equipamiento ya existente en las instalaciones del centro de proceso de datos principal (CPD 1), ya expuesto en el punto anterior, el detalle de los elementos a suministrar se muestra en la siguiente tabla:

Unidades	Código	Descripción
1	FG-2200E	FortiGate-2200E 4 x 40GE QSFP+ slots , 20 x 10GE SFP+ slots (including 18x ports, 2x HA ports), 14 x GE RJ45 ports (including 12 x ports, 2 x management ports), SPU NP6 and CP9 hardware accelerated, and dual AC power supplies.

Firma 1: 26/04/2024 - OLGA ESTERAS HERNANDEZ
COORDINADORA DE AREA TIC - D.G. DE INFORMATICA
Firma 2: 26/04/2024 - ALFREDO JAIME FERNANDEZ
JEFE DE CENTRO PROCESO DE DATOS - D.G. DE INFORMATICA
CSV: A0600NbbQQ1bXa6Ow38hyX7ZduvTJLYdAU3n8j

*Este documento tiene carácter de copia electrónica auténtica con **validez y eficacia administrativa del documento ORIGINAL** (art. 27 Ley 39/2015)*

Versión imprimible del documento. La integridad de este documento puede comprobarse en la sede electrónica del Gobierno de Cantabria, a través de https://verificacsv.cantabria.es/verificacsv?codigoVerificacion=A0600NbbQQ1bXa6Ow38hyX7ZduvTJLYdAU3n8j
Identificador de documento electrónico (ENI): ES_A06006299_2024_DOC_00N_00000000000000001464149

1	FC-10-F22HE-928-02-36	FortiGate-2200E Advanced Threat Protection (IPS, Advanced Malware Protection Service, Application Control, and FortiCare Premium)
1	FG-3301E-BDL-950-36	FortiGate-3301E Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP)
1	FWB-1000F-BDL-934-36	FortiWeb-1000F Hardware plus 3 Year FortiCare Premium and FortiWeb Standard Bundle
14	FG-TRAN-QSFP+SR-BIDI 40 GE QSFP+	FG-TRAN-QSFP+SR-BIDI 40 GE QSFP+ transceiver module, short range BiDi for systems with QSFP+ slots.
4	FN-TRAN-SFP28-SR 25 GE/10 GE dual rate SFP28 transceiver module, short range for systems with SFP28/SFP+ slots	
16	FN-TRAN-SFP+SR 10GE SFP+	
7	FN-TRAN-SX 1GE SFP SX	

El suministro deberá instalarse en el centro de proceso de datos secundario como tercer nodo de la solución en clúster de alta disponibilidad (Activo-Pasivo-Pasivo).

El adjudicatario durante el trascurso del contrato podrá evolucionar el hardware y software desplegado de los equipos anteriormente listados, sustituyéndolos por modelos más modernos, garantizando en todo momento que estos elementos se encuentran dentro del ciclo de vida recomendado por el fabricante y que son compatibles con los elementos del CPD 1. Además, los nuevos elementos deben respetar los requisitos de seguridad establecidos en este pliego.

En el caso de realizarse evoluciones hardware, con nuevos modelos lanzados previamente al despliegue inicial, el adjudicatario deberá contemplar, dentro del contrato, el cambio de los elementos. Dicho cambio incluirá el suministro y todas las tareas de instalación necesarias (análisis de la situación actual, revisión del diseño lógico y físico, migración, pruebas, documentación, formación y traspaso al servicio) para desplegar la solución. Siempre el adjudicatario deberá respetar los requisitos de seguridad establecidos en este pliego.

3.1 Garantía de la solución completa

El suministro debe contemplar una garantía de fabricante de 3 años.

Dada la criticidad de las instalaciones del Centro de Proceso de Datos del Gobierno de Cantabria, el recambio de un equipo averiado debe realizarse al siguiente día laboral, una vez que se haya producido y reportado el problema.

El Gobierno de Cantabria debe poder abrir casos de manera directa con el fabricante de la solución ofertada, estableciendo un cauce vía Web, email o incluso por teléfono o sesiones de tipo Comunicaciones Unificadas (Zoom, Teams o equivalente). Todos los casos deben estar perfectamente identificados y poder disponer de un mecanismo de seguimiento en la web del fabricante.

Firma 1: 26/04/2024 - OLGA ESTERAS HERNANDEZ
COORDINADORA DE AREA TIC - D.G. DE INFORMATICA
Firma 2: 26/04/2024 - ALFREDO JAIME FERNANDEZ
JEFE DE CENTRO PROCESO DE DATOS - D.G. DE INFORMATICA
CSV: A0600NbbQQ1bXa6Ow38hyX7ZduvTJLYdAU3n8j

*Este documento tiene carácter de copia electrónica auténtica con **validez y eficacia administrativa del documento ORIGINAL** (art. 27 Ley 39/2015)*

Versión imprimible del documento. La integridad de este documento puede comprobarse en la sede electrónica del Gobierno de Cantabria, a través de https://verificacsv.cantabria.es/verificacsv?codigoVerificacion=A0600NbbQQ1bXa6Ow38hyX7ZduvTJLYdAU3n8j
Identificador de documento electrónico (ENI): ES_A06006299_2024_DOC_00N_0000000000000001464149

Los equipos adquiridos se incluirán dentro de la cuenta de soporte global que Gobierno de Cantabria tiene contratada con el fabricante, beneficiándose así de las ventajas que esta cuenta posee a nivel de escalados, tiempos de respuesta, etc.

Toda la solución suministrada se instalará y configurará coexistiendo con la solución del CPD actual. Estas tareas no deben impactar en los horarios de servicio habitual que presta el CPD. Este hito debe ser proporcionado por personal cualificado y certificado por el fabricante.

Igualmente, se requiere de la transferencia de conocimiento completa de la nueva solución suministrada; dicho proceso debe estar realizado por el fabricante y los contenidos del mismo deben ser también los oficiales. Dicho proceso tendrá lugar en las oficinas del Gobierno de Cantabria en Santander y tendrá una duración mínima de al menos una semana (según los requerimientos del Gobierno de Cantabria). Se dará en idioma español, aunque la documentación puede estar en inglés.

4. CLÁUSULAS SOBRE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Las cláusulas de este apartado y sub-apartados incluyen obligaciones a cumplir por la entidad adjudicataria del contrato, complementarias a las del PCAP, sobre seguridad de la información y protección de datos personales.

Estas obligaciones específicas se suman y complementan al deber de cumplir con la legislación vigente en materia de seguridad de la información, particularmente el Esquema Nacional de Seguridad y su artículo 2, de protección de datos personales, y la política de seguridad de la información de la Administración de la Comunidad Autónoma de Cantabria, así como su normativa derivada, en el ámbito del cumplimiento del objeto del contrato.

La firma del contrato compromete a la entidad adjudicataria a dichos cumplimientos.

a. Categoría de seguridad del sistema de información.

Los elementos a suministrar para implantar el tercer nodo de la solución del firewall del CPD deberán estar certificados como “Categoría Alta” del Esquema Nacional de Seguridad y estar incluidos en el “Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)”.

Si algún elemento propuesto no está contenido en ese catálogo, pero está en proceso de validación para su inclusión, será admisible su suministro e instalación, si bien en caso de no superar tal proceso para “Categoría Alta”, deberá ser sustituido por otro equivalente que sí lo esté. Si existieran factores a tener en cuenta que pudieran desaconsejar ese reemplazo, la entidad adjudicataria deberá informar al Responsable del Contrato, quien tendrá la última palabra sobre la sustitución del elemento.

b. Cumplimiento y/o implementación de medidas de seguridad.

Los elementos suministrados deberán cumplir con lo señalado en el apartado “Categoría de seguridad del sistema de información” y los trabajos de configuración de los elementos no deben afectar negativamente a las medidas de seguridad correspondientes a su Categoría certificada.

En todo caso, tanto los elementos suministrados como los trabajos realizados deben ser compatibles con las medidas de seguridad ya implantadas en la Red Corporativa de la Administración de la Comunidad Autónoma de Cantabria.

En los trabajos de despliegue y configuración de los elementos suministrados, la entidad adjudicataria deberá configurar debidamente las medidas de seguridad del Anexo II del “Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad” según las indicaciones y decisiones del Responsable del Contrato o de la persona especialista en la materia por él designada.

c. Mecanismos de supervisión y seguimiento.

En cuanto a los elementos, se constatará su inclusión en el “Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)”.

Firma 1: 26/04/2024 - OLGA ESTERAS HERNANDEZ
COORDINADORA DE AREA TIC - D.G. DE INFORMATICA
Firma 2: 26/04/2024 - ALFREDO JAIME FERNANDEZ
JEFE DE CENTRO PROCESO DE DATOS - D.G. DE INFORMATICA
CSV: A0600NbbQQ1bXa6Ow38hyX7ZduvTJLYdAU3n8j

*Este documento tiene carácter de copia electrónica auténtica con **validez y eficacia administrativa del documento ORIGINAL** (art. 27 Ley 39/2015)*

En cuanto a la supervisión y seguimiento de la calidad de los trabajos realizados y el respeto a las medidas de seguridad, la entidad adjudicataria deberá entregar una documentación técnica detallada sobre los trabajos realizados, con especial mención a las configuraciones de seguridad realizadas. Si cualquier aspecto pudiera afectar a las medidas de seguridad propias de la Categoría certificada en los elementos suministrados, esta circunstancia deberá ser recogida en tal documentación.

Santander, a fecha de la firma electrónica

LA COORDINADORA DE ÁREA TIC	EL JEFE DE SERVICIO DEL CENTRO DE PROCESO DE DATOS
Fdo.: Olga Esteras Hernández	Fdo.: Alfredo Jaime Fernandez

Versión imprimible del documento. La integridad de este documento puede comprobarse en la sede electrónica del Gobierno de Cantabria, a través de https://verificacsv.cantabria.es/verificacsv?codigoVerificacion=A0600NbbQQ1bXa6Ow38hyX7ZduvTJLYdAU3n8j
Identificador de documento electrónico (ENI): ES_A06006299_2024_DOC_00N_00000000000000001464149

Firma 1: 26/04/2024 - OLGA ESTERAS HERNANDEZ
COORDINADORA DE AREA TIC - D.G. DE INFORMATICA
Firma 2: 26/04/2024 - ALFREDO JAIME FERNANDEZ
JEFE DE CENTRO PROCESO DE DATOS - D.G. DE INFORMATICA
CSV: A0600NbbQQ1bXa6Ow38hyX7ZduvTJLYdAU3n8j

*Este documento tiene carácter de copia electrónica auténtica con **validez y eficacia administrativa del documento ORIGINAL** (art. 27 Ley 39/2015)*