LMODIFICACIÓN MEMORIA TÉCNICA DEL PROYECTO “DESPLIEGUE DE SOC PARA EL AYUNTAMIENTO DE SANTIAGO DE COMPOSTELA”

ÍNDICE

DATOS DEL SOLICITANTE

Concello de Santiago de Compostela

Dirección: Praza do Obradoiro, 1, 15705 Santiago de Compostela, A Coruña

Teléfono: 981 54 23 00

Web: http://santiagodecompostela.gal

CIF: P1507900G

DATOS DEL PROYECTO

El proyecto con título “Despliegue de SOC para el Ayuntamiento de Santiago de Compostela compatible con herramientas del CCN, y actuaciones complementarias” fue presentado al amparo de la CONVOCATORIA DE PROYECTOS DE MODERNIZACIÓN Y DIGITALIZACIÓN EN EL ÁMBITO DE LAS ADMINISTRACIONES DE LAS ENTIDADES LOCALES (Convocatoria 2021), encuadrándose dentro de la Línea 5 para la puesta en marcha de un Centro de Operaciones de Ciberseguridad

Con fecha 18 de mayo de 2022, al mencionado proyecto le fue concedida una ayuda de 364.004,74 euros estableciéndose como fecha de finalización el próximo 20 de diciembre de 2022

Con fecha 6 de junio, el Ayuntamiento de Santiago de Compostela presentó la declaración responsable sobre los requisitos para obtener la condición de entidad beneficiaria y de compromiso en relación con la ejecución con las actuaciones del PRTR.

MOTIVACIÓN DE LA MODIFICACIÓN

Aunque el proyecto mantiene su esencia original en cuanto a su enfoque principal, los objetivos y los hitos reflejados en la memoria presentada, se considera necesario modificarlo con el objeto de atender los nuevos requisitos detectados y, a la vez, ampliar el espectro del mismo como consecuencia de las nuevas prestaciones que en el ámbito de la administración electrónica el Ayuntamiento de Santiago presta a sus funcionarios y a la ciudadanía en general.

Recopilando la memoria inicial a continuación se reflejan los aspectos más significativos del proyecto que se siguen manteniendo invariables con la modificación que ahora se propone:

- Enfoque
  - Centro de proceso de datos adaptado a las necesidades del proyecto
  - Gestión centralizada de los registros y eventos de seguridad generados por los sistemas.
  - Análisis o monitorización en tiempo real de los eventos de seguridad de múltiples fuentes.
  - Utilización de sistemas de gestión de bases de datos para consolidad la información.
  - Actualización del sistema y servicio de correo electrónico como para cumplir los estándares de seguridad definidos en el ENS y mejorar la infraestructura para todo el Ayuntamiento.

- Objetivos:
  - Tener una infraestructura acorde a las necesidades del proyecto
  - Disponer de un método efectivo para automatizar los procesos y centralizar la gestión de Seguridad de una forma que ayude a simplificar la difícil tarea de proteger la información que se maneja y el servicio que se prestan en la entidad.
  - Detectar patrones de distintos tipos de ataque y amenazas mediante el análisis del tráfico y sus flujos.
  - Facilitar un sistema de comunicación interna y externa adecuada y securizada para los peligros de la comunicación de hoy en día para el Ayuntamiento, modernizando los sistemas de correo electrónico.

- Hitos:
  - Hito 1: disponer de una infraestructura estable y actualizada, con redundancias que permita el despliegue de un SOC.
  - Hito 2: securización del correo electrónico y las comunicaciones del Ayuntamiento
  - Hito 3: despliegue de un SOC que permita:
    - Intercambio automático y fluido de ciberincidentes con la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes mediante la implantación y operación de la herramienta de gestión de incidentes LUCIA del CCN-CERT que operará en modo federado con el de la Plataforma Nacional.

- Implantación de las tecnologías necesarias que permitan la vigilancia del perímetro y de la red interna implantando las tecnologías disponibles en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CCN-STIC 105) o haciendo uso de los sistemas de alerta desplegados por el CCN-CERT.
- Despliegue de la herramienta microClaudia del CCN-CERT en toda la organización.
- Capacidad de recolección y correlación básica de los registros de trazabilidad (logs) necesarios para la vigilancia (Mediante productos recogidos en el catálogo CCN-STIC 105).

- Hito 4: Despliegue de tecnologías de detección y respuesta en el punto final, endpoint (EDR) implantando las tecnologías disponibles en el catálogo CCN-STIC 105.

Una vez referidos los principales descriptores del proyecto, que se mantienen invariables, se considera fundamental reorientarlos y modificarlos como consecuencia de los siguientes puntos:

- las consideraciones obtenidas de una auditoría de seguridad recientemente realizada
- las nuevas necesidades que han surgido y surgirán como consecuencia de nuevos servicios electrónicos
- los nuevos servicios derivados del proyecto Smartiago
- los nuevos dispositivos IoT implantados a raíz del proyecto Smartiago
- la futura ampliación de la red de voz y datos a 40 Centros Socio Culturales
- la implantación de oficinas virtuales de ayuda al ciudadano
- las previstas carencias del actual CPD en cuanto a capacidad y rendimiento una vez implantados los servicios del SOC
- la difícil gestión de los dispositivos hardware y software del CPD al comportarse de forma independiente según su aplicación

A modo de resumen, se muestra a continuación la redefinición de los aspectos clave del proyecto según su concepción inicial y la ahora planteada. Puede observarse que a nivel conceptual el proyecto sigue siendo el mismo y simplemente se plantea como más ambicioso y acorde a la realidad actual del Ayuntamiento:

Hito	Proyecto inicial	Modificación planteada
1	Ampliación del centro de Proceso de Datos	Implantación de una nueva estructura de CPD redefiniendo el actual como Centro de Respaldo (CPD de respaldo)
2	Actualización de los servidores de Correo Electrónico	Adquisición de un sistema de previsión y protección avanzada del correo electrónico en la nube
3	Creación de un SOC	Creación y despliegue de un SOC
4	Despliegue de tecnologías de detección y respuesta en el punto final, endpoint (EDR)	Despliegue de tecnologías de detección y respuesta en el punto final, endpoint (EDR)

DESCRIPCIÓN DE LA MODIFICACIÓN

A continuación, se reseñan los distintos hitos con los objetivos que se plantean en esta modificación para cada uno de ellos:

- Hito 1: Implantación de una nueva estructura de CPD redefiniendo el actual como Centro de Respaldo (CPD de respaldo)

  El nuevo planteamiento contempla el despliegue de una solución de hiperconvergencia que atienda de forma eficaz a los requerimientos actuales y futuros garantizando en todo momento la capacidad de almacenamiento y de cálculo. Se pretende, así mismo, que dicha solución aglutine todos los servicios ahora diseminados en distintos servidores o granjas y distintos sistemas de almacenamiento para así poder gestionar toda la infraestructura como un único elemento y poder aplicar de forma más efectiva todas las herramientas que el hito 3 (creación y despliegue del SOC) contempla.

  Se ha optado por una solución de hiperconvergencia, dada su capacidad y rendimiento en términos tecnológicos, su capacidad de crecer de forma horizontal y vertical y la posibilidad que plantea de aglutinar todos los ecosistemas actuales bajo un único hipervisor simplificando el rendimiento y aumentado considerablemente la seguridad del entorno. Otro de los hándicaps actuales que se solventaría es la velocidad de reloj de las actuales que no están certificadas por fabricantes de solucione software ya instaladas.

Esta nueva infraestructura permitirá también ofrecer de forma aislada y segura los servicios públicos en Internet del Ayuntamiento que en la actualidad también se encuentran diseminados en distintos entornos. Una vez más se cumplen los criterios de simplicidad y aumento considerable de la seguridad del entorno.

En términos técnicos la solución propuesta contempla la adquisición de:

- Clúster de cómputo basado en un mínimo de 6 servidores
- Clúster de almacenamiento de al menos 45 Tb netos (considerando el flujo masivo de información de nuevos proyectos BigData orientados a la ciudadanía)
- Interfaces de red duplicados con velocidades mínimas de 10 Gb
- Licenciamiento de hipervisor

Se plantea también la creación de un CPD de respaldo utilizando los sistemas actuales, cuyo rendimiento es inferior, para así garantizar la continuidad de los servicios en caso de contingencia e incluso tener un entorno de "test" donde realizar simulacros y pruebas de intrusión y hackeo de los servicios que se provean.

- Hito 2: Adquisición de un sistema de provisión y protección avanzada del correo electrónico en la nube

Teniendo en cuenta que el correo electrónico en la actualidad es una de las puertas de entrada de todo tipo de ataques que más compromete la seguridad de cualquier infraestructura, la cada vez más demandada movilidad de los usuarios y la necesidad de prestación de un servicio 24x7 sin fisuras, se ha optado por adquirir un nuevo sistema de correo electrónico que sustituya a la actual.

El sistema que se propone se soportará en una provisión y protección avanzada en la nube basado en múltiples capas contra el espectro completo de amenazas transmitidas por correo electrónico que ayude a prevenir, detectar y responder a amenazas correo no deseado, suplantación de identidad, malware, amenazas de día cero, suplantación y ataques de compromiso. Incluirá el soporte y gestión de 1.300 cuentas de correo electrónico (frente a las 700 inicialmente planteadas por motivos de crecimiento) que garantizarán en todo momento los siguientes aspectos:

- Cumplimiento de las necesidades y requisitos indicados en la normativa referente al Esquema Nacional de Seguridad.
- Implementación de una bandeja de entrada inteligente que asegura una mayor productividad y eficiencia a los empleados públicos
- Envío cifrado de mensajes, empleando los últimos algoritmos de encriptación y hashing, lo que incrementa la protección de los datos a un nivel adecuado para la nueva situación del Ayuntamiento en materia de ciberseguridad.
- Diferenciación entre tipos de usuarios mediante la creación de perfiles con diferentes niveles de seguridad
- Mejora de la gestión de las tareas rutinarias de filtrado, bloqueo de spam, listas negras, etc. Realizando esas acciones de modo mucho más sencillo y transparente para el usuario final y apoyadas en 2 fabricantes distintos.
- Compatibilidad con los sistemas de monitorización, y en particular con la aplicación SIEM que se pretende implantar
- Provisión de un sistema propio de backup en la nube así como métodos de prueba de respaldo granular o total.

- Hito 3: Creación y despliegue de un SOC

  Este hito mantiene los objetivos de la memoria inicial añadiendo otros nuevos como la implantación del software QRadar, la monitorización continua de la superficie de exposición (tanto a nivel de vulnerabilidades como en pruebas), al ampliación de la capacidad de correlación de EPS en 5.000 y un sistema integral especializado de respuesta a incidentes en modalidad 24x7. A estas nuevas funcionalidades se unirán las ya detalladas en la propuesta inicial que a modo de resumen son:
  - Servicio de monitorización
  - Implantación de un SIEM
  - Herramientas de Gestión de Incidencias e Inventariado, Monitorización y Cuadro de Mandos del Servicio
  - Alerta temprana
  - Despliegue de la herramienta microClaudia del CCN-CERT
  - Activación de la herramienta de gestión de incidentes LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) del CCN-CERT
  - Suministro e instalación de sonda SAT-INET

- Hito 4: Despliegue de tecnologías de detección y respuesta en el punto final, endpoint (EDR):

  En este hito se mantiene la definición del proyecto inicial con la única salvedad de aumentar a 850 las licencias de usuario a aplicar debido al constante crecimiento de necesidades y recursos demandado por los usuarios.

  Por tanto, el objetivo sigue siendo el incrementar la capacidad de respuesta ante incidentes y la provisión de una herramienta o servicio de remediación que ante un ataque de ramsomware desconocido por el antivirus, permita la rápida recuperación de los sistemas soportados (equipos de usuario o endpoints).

  También se pretende la implantación de otras tecnologías necesarias que permitan la vigilancia del perímetro y de la red interna implantando las tecnologías disponibles en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CCN-STIC 105) o haciendo uso de los sistemas de alerta desplegados por el CCN-CERT. Sin olvidar la capacidad de recolección y correlación básica de los registros de trazabilidad (logs) necesarios para la vigilancia (Mediante alguno de los productos recogidos en el catálogo CCN-STIC 105).

PRESUPUESTO

Con la modificación propuesta aumenta el presupuesto del proyecto de forma considerable entendiendo el Ayuntamiento que se le ha concedido una ayuda por un importe máximo de 364.004,74 euros y asumiendo el Ayuntamiento el compromiso de atender con fondos propios el importe restante de la totalidad del proyecto dada su especial relevancia.

Por tanto, el importe total del proyecto de despliegue de **“Despliegue de SOC para el Ayuntamiento de Santiago de Compostela compatible con herramientas del CCN, y actuaciones complementarias”** con las herramientas indicadas es el siguiente:

Hito	Proyecto inicial	Importe (sin iva)
1	Implantación de una nueva estructura de CPD redefiniendo el actual como Centro de Respaldo (CPD de respaldo)	280.000
2	Adquisición de un sistema de provisión y protección avanzada del correo electrónico en la nube	200.000
3	Creación y despliegue de un SOC	129.000
4	Despliegue de tecnologías de detección y respuesta en el punto final, endpoint (EDR)	40.000
	TOTAL PRESUPUESTO (sin iva)	649.000

Respecto a la financiación del proyecto se desglosa a continuación, tanto en términos netos como brutos:

- Financiación antes de impuestos (importes netos):

Financiación	Importe
Ayuda concedida	364.004,74
Aportación del Ayuntamiento	284.995,26
Total Financiación antes de impuestos	649.000,00

- Financiación después de impuestos (importes brutos):

Financiación	Importe
Ayuda concedida	364.004,74
Aportación del Ayuntamiento	284.995,26
Impuestos (aportación del Ayuntamiento)	136.290,00
Total Financiación después de impuestos	785.290,00

Santiago de Compostela, 28 de junio de 2022

MARCOS VALIÑO GARCÍA - 33308063S

Firmado digitalmente por MARCOS VALIÑO GARCÍA - 33308063S
Fecha: 2022.06.28 17:20:15 +02'00'

Director de área de Modernización, Innovación y Calidad de la Administración Local