serpa empresa pública Sociedad de Servicios del Principado de Asturias, S. A., M. P.

laboral ciudad de la cultura
C/ Luis Moya Blanco, 261
33203 Gijón. Asturias

T (+34) 985 133 316
F (+34) 985 338 374
T red IBERCOM 83222 - 3

serpa@serpasa.es
www.serpasa.es

Expediente: 024_03_ ENS

Título: PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR EL CONTRATO DE LOS SERVICIOS DE IMPLEMENTACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD EN LA EMPRESA PÚBLICA SOCIEDAD DE SERVICIOS DEL PRINCIPADO DE ASTURIAS, S. A., M. P.

09287620J JOSE ANGEL JODAR (R: A74061177)

Firmado digitalmente por 09287620J JOSE ANGEL JODAR (R: A74061177)
Fecha: 2024.02.20 14:42:49 +01'00'

Fdo.: D. José Ángel Jódar Pereña
Gerente de SERPA, S. A., M. P.

ÍNDICE

1 ANTECEDENTES

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito del sector público, fija los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

El Real Decreto se aplica a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

La Empresa Pública Sociedad de Servicios del Principado de Asturias, S, A, M.P, como integrante del sector público asturiano, se encuentra obligada a adaptarse al Esquema Nacional de Seguridad.

Se hace necesario por tanto tomar las acciones pertinentes y necesarias para la implantación de las medidas de seguridad aplicables que garanticen la protección y confidencialidad de sistemas y datos en cumplimiento de la mencionada norma.

2 OBJETO DEL CONTRATO

Este pliego de condiciones técnicas tiene como objetivo establecer las condiciones que regirán la contratación de los servicios de implementación efectiva de la adecuación al Esquema Nacional de Seguridad en la empresa pública Sociedad de Servicios del Principado de Asturias, S. A., M. P., y apoyo a la constitución de un Centro de Operaciones de Seguridad u Oficina de Ciberseguridad/ Comité de seguridad.

Para posibilitar el correcto dimensionamiento del alcance del contrato y de la oferta correlativa, se adjunta el Anexo I con el resultado de un GAP de cumplimiento de ENS previamente desarrollado por una empresa externa.

2.1 LÍNEAS DE ACTUACION

Constituye el objeto de la contratación las siguientes tareas:

- Implementación de la adecuación al ENS.
    - Puesta en marcha de las soluciones orientadas a la mejora de la ciberseguridad, incluyendo sistemas de monitorización, vigilancia del perímetro y red interna, superficie de exposición y gestión de incidentes de seguridad, utilizando productos y servicios del catálogo CPSTIC 105 del CCN.
    - Puesta en marcha de un servicio recurrente que permita evaluar la superficie de exposición, así como los principales servicios críticos (análisis de vulnerabilidades, servicios de hacking ético)

- Puesta en marcha de un servicio para la mejora de competencias digitales en ciberseguridad.
- Puesta en marcha en marcha las herramientas del CCN-CERT: INES, AMPARO, microCLAUDIA, y LUCIA.
- Mejoras en el sistema de gestión documental de distintos procesos, orientadas al cumplimiento normativo en materia de Esquema Nacional de Seguridad.

- Apoyo a la constitución de la Oficina de Ciberseguridad / Comité de seguridad.
- Definir instrumentos que permitan la posterior vigilancia y mejora continua en los ámbitos indicados.

3 TRABAJOS A REALIZAR

3.1 HERRAMIENTAS DE CIBERSEGURIDAD

- Implantación de las medidas técnicas de seguridad orientadas en la protección de instalaciones, infraestructuras, personal, equipamiento, comunicaciones, soportes aplicación, información y servicios:
- Puesta en marcha de soluciones para la vigilancia y control de la superficie de exposición (vigilancia de perímetro y red interna)
- Despliegue / puesta en marcha de soluciones específicas del CCN-CERT:
  - Lucia
  - microClaudia
  - Herramienta de Gobernanza CCN (Inés/Amparo)
- Bastionado de sistemas conforme a las guías CCN-STIC, tanto para sistemas on premise como para soluciones Cloud.
- Puesta en marcha de herramientas que permitan realizar auditorías técnicas de seguridad. En particular se realizarán los siguientes ejercicios
  - Hacking interno, analizando el estado actual de las vulnerabilidades de los servidores, debilidades en los protocolos de conexión (periodicidad trimestral), así como un test de intrusión, identificando el nivel de riesgo y plan de remediación

3.2 SOLUCIONES PARTICULARES DE SEGURIDAD

3.2.1.1 PROTECCIÓN ESPECÍFICA DEL DIRECTORIO ACTIVO Y DE SERVICIOS WEB

Siguiendo las guías de seguridad del CCN y mediante el SOC.
Implantación de un Web Application Firewall para servidores web IIS.

3.2.1.2 PUESTA EN MARCHA DE UNA SOLUCIÓN DE DOBLE FACTOR DE AUTENTICACIÓN.

La solución debe confirmar la identidad de sus usuarios con políticas de autenticación de dos factores y acceso contextual para usuarios. La solución debe verificar la identidad de los usuarios y proteger contra las

infracciones debidas al phishing y otros ataques con contraseña con una solución de autenticación de doble factor fácil de usar que agregue otra capa de seguridad a los inicios de sesión.

Las licencias necesarias serán asignadas a nivel de usuario, independientemente del número de dispositivos de los que disponga o de los servicios/aplicaciones en los que vaya a iniciar sesión.

La solución propuesta permitirá la flexibilidad para elegir qué método de inscripción más adecuado. Se podrá elegir el proceso de autoinscripción, que facilita a los usuarios el registro de su teléfono inteligente, teléfono celular, teléfono fijo o tableta, lo que reduce aún más los costes de soporte para la implementación.

La solución integrará sus logs en el SIEM propuesto.

La solución permitirá elegir autorizar, denegar o requerir la autenticación de dos factores para cada intento de autenticación, dependiendo de ciertas condiciones y cómo se configuran por aplicación y grupo de usuarios. Estos grupos de usuarios podrán ser definidos a nivel local de la herramienta o a nivel de directorio activo.

3.2.1.3 PUESTA EN MARCHA DE UN SERVICIO DE MONITORIZACIÓN

El adjudicatario pondrá en marcha y llevará a cabo el mantenimiento y soporte de las soluciones para la detección y prevención de incidentes de seguridad, incluyendo todo el equipamiento y licencias que sean necesarias para su funcionamiento.

La solución de monitorización contempladas deberá cumplir los siguientes requisitos generales:

- Detectar y prevenir intrusiones en cualquier protocolo y aplicación utilizados.
- No repercutir en una degradación del rendimiento de las aplicaciones y servicios.
- Monitorizar en tiempo real de los eventos de la organización 24x7.
- Detectar temprana y respuesta ante incidentes.
- Disponer de Honeypots a nivel de red y de usuarios.
- Analizar de eventos basado en firmas, comportamientos, logs, procesos e IOCs.
- Disponer de técnicas de IA para la detección de anomalías.
- Posibilidad de definir reglas de alerta adaptadas a la particularidad de la organización.
- Centralizar y salvaguardar y correlación de eventos multifuente.
- Disponer de Sistema de detección de intrusiones a nivel de red.
- Integrar de servicios externos vía syslog/api.
- Integrar /explotar de la solución EDR/XDR. Detección de anomalías en puesto de usuario.
- Contemplar soporte experto ante los incidentes notificados.
- Generar informes mensuales de estado con indicadores.

El adjudicatario proporcionará soporte en acciones necesarias para la contención o mitigación de los posibles ataques o incidencias de seguridad en los activos de la entidad. Para ello deberá analizar todas las alertas

generadas, descartando falsos positivos, transmitiendo el diagnóstico cuanto antes y aportando recomendaciones de forma proactiva que permita el bloqueo del ataque en caso de que se ponga en riesgo la seguridad de los activos o las infraestructuras que los soportan.

Asimismo, actuará como punto de contacto con la entidad para la operación de los servicios incluidos en el presente pliego, supervisará el estado de los activos y generará las alertas correspondientes en caso de eventos que puedan afectar a la seguridad de la información.

Para realizar las funciones referidas, el adjudicatario deberá implementar una solución SIEM; el contrato incluirá los costes de licenciamiento y despliegue de la solución SIEM, atendiendo al modelo de licencias y tipo de solución que mejor se adapte al cumplimiento de los requisitos recogidos en el presente contrato. Dicha solución SIEM debe cumplir los siguientes requisitos:

- Ser capaz de capturar y recopilar todos los eventos de seguridad que se producen en la red de forma centralizada, de recibir información desde una gran cantidad de fuentes, de correlacionar los datos recogidos y de mostrar una amplia variedad de información en paneles. La infraestructura que soporta la solución será proporcionada por el licitador en formato Cloud en alta disponibilidad.

- Capacidad de retención de eventos para su correlación. Se almacenará eventos durante 18 meses, de los cuales, al menos 3 meses deberán realizarse en caliente (para poder revisar la publicación de IOC en los 2 meses anteriores y saber si el Ayuntamiento se ha visto afectado).

- La solución propuesta deberá contar con una copia de seguridad diario del conjunto total de logs ingestados para asegurar su disponibilidad y cubrir posibles contingencias que pudieran suponer una pérdida de los registros. Dicha copia de seguridad deberá de estar alojada en una ubicación externa proporcionada por el licitador, diferente a la ubicación de la propia herramienta de SIEM, acreditando la seguridad de dicha ubicación. Las copias de seguridad deberán permitir una recuperación completa de los logs con un plazo de retención de 1 año.

REQUISITOS ADICIONALES PARA SU DESPLIEGUE Y EXPLOTACIÓN

- La empresa encargada de la explotación del sistema de monitorización deberá formar parte de CSIRT.es y ser miembro de la Red Nacional de SOC. Esta información será contrastada con el CCN.

- La capacidad de recolección y correlación de los registros de trazabilidad (SIEM) necesarios para la vigilancia por parte del SOC deberá realizarse mediante soluciones recogidas en el catálogo CCN-STIC 105 (CPSTIC) Esta información será contrastada con el organismo de certificación del Centro Criptológico Nacional.

- Se potenciará el uso de la herramienta de gestión de incidentes LUCIA del CCN-CERT, que operará en modo federado.

- Se potenciará el uso de productos, servicios y soluciones conformes al Esquema Nacional de Seguridad.

3.2.1.4 MODELO DE GOBERNANZA

Apoyo para la constitución de una oficina de ciberseguridad y cumplimiento normativo potenciando el uso de las herramientas específicas de gobernanza del CCN-CERT. Desde la oficina se realizarán se contemplarán las siguientes actuaciones:

- Coordinación y puesta en marcha de los servicios de ciberseguridad orientados a la supervisión / monitorización.
- Definición de indicadores asociados a los procesos de evaluación de riesgos, gestión y vigilancia de la seguridad.
- Adaptación al Esquema Nacional de Seguridad, prestando el asesoramiento normativo que sea demandado por parte de SERPA.
- Realización de los protocolos, procedimientos y la documentación necesaria para lograr el cumplimiento con el ENS.

Despliegue de herramientas para la mejora de la ciberseguridad y cumplimiento normativo, incluyendo tanto soluciones como la definición y carga documental.

3.3 HERRAMIENTAS PARA LA GESTIÓN DE LA GOBERNANZA

Se prestará especial atención en la puesta en marcha de un sistema de gestión de seguridad de la información que permita obtener la conformidad con el ENS, a través de las soluciones del CCN-CERT:

- Despliegue de las herramientas del CCN (INES y AMPARO) que permitan la carga de contenidos particularizados, incluyendo el Plan de Adecuación y el Sistema de Gestión de Seguridad de la Información.
- Puesta en marcha de soluciones que permitan la generación de todas las evidencias que serán necesarias para conseguir la conformidad con el ENS.
- Desarrollo de una auditoría interna previa a la certificación, incluyendo el soporte de acciones correctivas.

3.4 CONFORMIDAD ENS Y MEJORA CONTINUA

- Revisión del Modelo de Gobernanza.
- Actualización del análisis de riesgos (PILAR).
- Revisión de la Declaración de Aplicabilidad.
- Establecimiento de un Plan de Mejora, describiendo los principales hitos.
- Revisión de las medidas de seguridad.
- Revisión y actualización de procedimientos.
- Revisión del Estado de Seguridad.

3.5 REUNIONES DE SEGUIMIENTO

Se realizarán con periodicidad mínima quincenal reuniones de carácter presencial para evaluar el progreso en la implementación.

-NO MÁS CLÁUSULAS-