DIPUTACIÓN DE BADAJOZ
C/Felipe Checa, 23
06071, Badajoz
924 21 24 00

Candidatura Premios Socinfo Digital: EXTREMADURA TIC
Premio Seguridad y Protección del Dato
DIPUTACIÓN DE BADAJOZ

1. Descripción del proyecto

En un contexto de exposición cada vez más intenso a la materialización de amenazas del ciberespacio, las cuales siguen una pauta de crecimiento en frecuencia, sofisticación, alcance y severidad del impacto, resulta necesario implantar nuevos servicios y soluciones tanto tecnológicas como organizativas, que permitan a la Diputación de Badajoz alcanzar un adecuado nivel de madurez desde el punto de vista de la ciberseguridad y que le permita mejorar su nivel de cumplimiento del Esquema Nacional de Seguridad.

La Diputación de Badajoz dispone de diversos elementos para la protección de sus sistemas de información frente a ciberamenazas. Entre ellos se encuentran:

- Firewall perimetral
- EPDR y antivirus en equipos clientes y servidores
- Proxy para el control de la navegación web
- AntiSPAM para el servicio de correo

El creciente número de ciberataques, así como la complejidad de estos, hace necesario incrementar las medidas de vigilancia y protección de cara a evitar posibles incidentes de seguridad, así como a conseguir reducir los tiempos de recuperación en el caso en que alguna de las amenazas existentes se materialice.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en su Anexo II, indica lo siguiente:

"4.7.3 Vigilancia [op.mon.3]

Requisitos.

– [op.mon.3.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad.

Refuerzo R1-Correlación de eventos.

– [op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

Refuerzo R2-Análisis dinámico.

– [op.mon.3.r2.1] Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

Refuerzo R3-Ciberamenazas avanzadas.

– [op.mon.3.r3.1] Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos.

– [op.mon.3.r3.2] Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (Advanced Persistent Threat, APT) mediante la detección de anomalías significativas en el tráfico de la red.

Refuerzo R4-Observatorios digitales.

– [op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.

Refuerzo R5-Minería de datos.

Se aplicarán medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos:

– [op.mon.3.r5.1] Limitación de las consultas, monitorizando volumen y frecuencia.

– [op.mon.3.r5.2] Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.

Refuerzo R6-Inspecciones de seguridad.

Periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas, se realizarán las siguientes inspecciones:

– [op.mon.3.r6.1] Verificación de configuración.

– [op.mon.3.r6.2] Análisis de vulnerabilidades.

– [op.mon.3.r6.3] Pruebas de penetración.

Refuerzo R7-Interconexiones.

– [op.mon.3.r7.1] En las interconexiones que lo requieran se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.3.
– Categoría MEDIA: op.mon.3 + R1 + R2.
– Categoría ALTA: op.mon.3 + R1 + R2 + R3 + R4 + R5 + R6."

Los sistemas de información de Diputación de Badajoz categorizados según el ENS son como máximo de categoría MEDIA, por lo que cómo mínimo se han de cumplir los Refuerzos R1 y R2.

Diputación de Badajoz carecía de un sistema automático de correlación de eventos de seguridad, es decir, un SIEM (Security Information and Event Management). Desde la Delegación de Tecnología y Digitalización se ha llevado a cabo un estudio de los SIEM existentes en el mercado. Se ha llegado a la conclusión de que dicha herramienta ha de cumplir lo siguiente:

- Punto único de control securizado y almacenamiento centralizado de logs.
- Securización de los registros o logs para generación de evidencias digitales.
- Detectar y resolver amenazas en tiempo real mediante un motor de correlación.
- Priorizar e investigar incidentes relevantes mediante casos de uso (playbooks) personalizables.
- Analizar el comportamiento del usuario (UEBA).
- Ciberinteligencia de Amenazas mediante la integración con MISP/ REYES.
- Responder de forma automática (Security Orchestration and Automation Response).
- Integración con The Hive/Cortex.
- Tratamiento y almacenamiento ilimitado de eventos diarios (desde 5Gb a más de 1,5 Tb).
- Integración con el resto de ecosistema de herramientas del Centro Criptológico Nacional, de valor para la seguridad: SAT-INET, REYES, LUCIA, microCLAUDIA, MISP RNS, ANA.
- Producto cualificado y de desarrollo nacional, que armonice con las directrices de la Estrategia Nacional de Seguridad y fomente el uso de plataformas europeas y españolas.

Además, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en su Anexo II, indica lo siguiente:
"4.1.5 Componentes certificados [op.pl.5].
Requisitos.

– [op.pl.5.1]. Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.
En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.
Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.
– [op.pl.5.2] Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

Refuerzo R1-Protección de emisiones electromagnéticas.
[op.pl.5.r1.1] La información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor.
Refuerzo R2 - Lista de componentes software.

[op.pl.5.r2.1] Cada producto y servicio incluirá en su descripción una lista de componentes software, acorde a lo especificado en [mp.sw.1.r5].
Aplicación de la medida.
- *Categoría BÁSICA: no aplica.*
- *Categoría MEDIA: op.pl.5.*
- *Categoría ALTA: op.pl.5."*

Por todas estas razones, la Delegación de Tecnología y Digitalización selecciona como SIEM la solución NGSIEM MONICA del Centro Criptológico Nacional, puesta a disposición de las Administraciones Públicas con licenciamiento gratuito, cumpliendo todas las características anteriores.

Además, Diputación de Badajoz está dentro de la Red Nacional de SOCs. Para pertenecer a la misma se ha de contar con un SOC, ya sea propio o externo. En un SOC es imprescindible contar con un SIEM o una herramienta similar de servicio de análisis de logs.

Un Centro de Operaciones de Ciberseguridad (SOC) es un conjunto de tecnologías, procesos y personas que mediante su interrelación, cooperación y coordinación prestan servicios de ciberseguridad a su comunidad.
En la actualidad se cuenta para este SOC con recursos humanos insuficientes para la cobertura temporal que se desea.

En Diputación de Badajoz contamos con la tecnología y los procesos, y de un muy cualificado equipo humano con dedicación específica a estas funciones, pero nos falta reforzar las personas con servicios 7x24. Necesitamos a profesionales especializados que sean capaces de interpretar todas las herramientas con las que contamos y, en especial, el SIEM, para poder ofrecer los servicios de detección y respuesta adecuados a ciberincidentes. De ahí la contratación en marcha de Soporte técnico del SOC de Diputación de Badajoz.

Por último, la mejora continua implica complementar la implementación de medidas de seguridad con un incremento de la vigilancia. De este modo, es posible conseguir estándares de seguridad acreditables de acuerdo a las inspecciones STIC (Sistemas y Tecnologías de Información y Comunicaciones) llevadas a cabo. La Diputación de Badajoz está en fase de implantación de la herramienta EMMA, que es una solución del CCN-CERT desarrollada para agilizar la visualización de activos en una red, su autenticación y segregación, así como la automatización de auditorías de seguridad de la infraestructura. Así, es posible obtener visibilidad, control / respuesta y cumplimiento de todos los activos conectados a la red corporativa.

Con EMMA, el CCN-CERT pretende facilitar a las organizaciones visibilidad y control completo de la capa de acceso a la red (routers, switches, puntos de acceso, controladores, etc.), un punto crucial para verificar quién o qué está conectado en una red. En el contexto actual, los modelos de seguridad requieren de una verificación de identidad estricta para cada persona y dispositivo (estén dentro o fuera del perímetro) y es más difícil controlar el crecimiento exponencial de los activos: distintos lugares físicos, data-centers, proveedores, distintos tipos (dispositivos de usuario, IoT, dispositivos de electrónica, etc)...

EMMA es una solución modular, lo que permite a las organizaciones adoptar solo los módulos necesarios en su situación actual y en una aproximación de menos a más. Esta aproximación permite reducir el riesgo e impacto operacional al acotar el alcance funcional de la implementación a las necesidades actuales.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en su Anexo II, indica lo siguiente:

"4.1.2 Arquitectura de seguridad [op.pl.2]
Requisitos.

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

– [op.pl.2.1] Documentación de las instalaciones, incluyendo áreas y puntos de acceso.

– [op.pl.2.2] Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración).

– [op.pl.2.3] Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

– [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Refuerzo R1-Sistema de gestión.

[op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Refuerzo R2-Sistema de gestión de la seguridad con mejora continua.

[op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

Refuerzo R3-Validación de datos.

[op.pl.2.r3.1] Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.2.

– Categoría MEDIA: op.pl.2 + R1.

– Categoría ALTA: op.pl.2 + R1 + R2 + R3."

Los sistemas de información de Diputación de Badajoz categorizados según el ENS son como máximo de categoría MEDIA, por lo que cómo mínimo se ha de cumplir el Refuerzo R1.

Además, indica lo siguiente:

"*4.3.1 Inventario de activos [op.exp.1].*
Requisitos.

[op.exp.1.1] Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo.

Refuerzo R1-Inventario de etiquetado.

– *[op.exp.1.r1.1] El etiquetado del equipamiento y del cableado formará parte del inventario.*

Refuerzo R2-Identificación periódica de activos.

– *[op.exp.1.r2.1] Se dispondrá de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular, los servidores y los dispositivos de red y de comunicaciones.*

Refuerzo R3-Identificación de activos críticos.

– *[op.exp.1.r3.1] Se dispondrá de herramientas que permitan categorizar los activos críticos por contexto de la organización y riesgos de seguridad.*

Refuerzo R4-Lista de componentes software.

– *[op.exp.1.r4.1] Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5].*

Aplicación de la medida.

– *Categoría BÁSICA: op.exp.1.*

– *Categoría MEDIA: op.exp.1.*

– *Categoría ALTA: op.exp.1*."

La solución EMMA contribuye a 31 medidas de las 73 del ENS. De entre las más importantes se encuentran las anteriormente señaladas:

- *op.pl.2 Arquitectura de seguridad:* Diputación de Badajoz tiene la documentación pero está descentralizada. EMMA sería esencial para cumplir con la medida *[op.pl.2.2]*
- *op.exp.1 Inventario de activos:* Diputación de Badajoz tiene varios inventarios pero descentralizados. EMMA sería esencial para cumplir con esta medida de seguridad.

Por tanto, Diputación de Badajoz ha de cumplir obligatoriamente con el ENS. Para alcanzar un adecuado nivel de madurez que le permita mejorar su nivel de cumplimiento del Esquema Nacional de Seguridad se hace necesaria la adquisición de la herramienta EMMA desarrollada para agilizar la visualización de activos en una red, su autenticación y segregación, así como la automatización de auditorías de seguridad de la infraestructura. Así, es posible obtener visibilidad, control / respuesta y cumplimiento de todos activos conectados a la red corporativa.

2. Repercusión para la ciudadanía y las Administraciones

El ENS, cuyo ámbito de aplicación comprende todas las entidades de las administraciones públicas y aquellas del sector privado cuando presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas, persigue fundamentar la confianza en que los sistemas de información prestan sus servicios adecuadamente y custodian la información sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a personas no autorizadas, estableciendo medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de forma que se facilite a los ciudadanos y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera a la ciberseguridad como un ámbito de especial interés de la Seguridad Nacional tal como señala su artículo 10, y que, por ello, requiere una atención específica por resultar básica para preservar los derechos y libertades y el bienestar de los ciudadanos y para garantizar el suministro de los servicios y recursos esenciales. De acuerdo con las previsiones de su artículo 4.3 se aprobó el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017, y posteriormente, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, identificando en ambas al ciberespacio como un espacio común global, que la Estrategia 2021 describe como espacio de conexión caracterizado por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad, añadiendo que en los espacios comunes globales resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13 incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ordenó en su disposición adicional primera que dichas medidas de seguridad se implanten en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). De otra parte, la disposición adicional primera también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales. Por último, y en el mismo sentido, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ha establecido en su artículo 37 la obligación de aplicar las medidas del ENS a los tratamientos de datos personales por parte de las autoridades públicas competentes.

Por todo esto, la Diputación de Badajoz alcanzando un adecuado nivel de madurez desde el punto de vista de la ciberseguridad y permitiendo mejorar su nivel de cumplimiento del Esquema Nacional de Seguridad, repercutirá tanto en la ciudadanía como en la propia administración y relación con el resto de las administraciones públicas.

3. Equipo de desarrollo y proveedores

Los tres contratos en los que se ha invertido para mejorar en ciberseguridad y protección del dato están en fase de adjudicación y/o implantación. De todos modos, los proveedores de MONICA y EMMA solo pueden ser empresas certificadas en dichas herramientas, para prestar los servicios de operación y soporte.

En concreto, las empresas pendientes de adjudicación de ambos contratos son:

Para MONICA: ICA Sistemas y Seguridad.
Para EMMA: Cipherbit.
Para el SOC: Ariadnex Tecnología Flexible S.L.

4. Valoración económica

- MONICA NG SIEM: 100.000 € más IVA.
- Soporte técnico al SOC de Diputación de Badajoz 24x7: 179.999,91 € más IVA.
- EMMA: 70.000 € más IVA.

5. Plazos de cumplimiento

- MONICA NGSIEM:
  - Instalación, parametrización y formación de la herramienta NGSIEM MONICA: 8 semanas
  - Soporte y Mantenimiento herramienta NGSIEM MONICA 8X5: 12 meses

- Soporte técnico al SOC de Diputación de Badajoz 24x7: 12 meses

- EMMA:
  - Instalación, parametrización y formacción de la herramienta EMMA: 3 meses
  - Soporte y Mantenimiento herramienta EMMA 8x5: 12 meses