Candidatura a «IA para el refuerzo de la Ciberseguridad»

Premios Socinfo Digital: IA en las AAPP

1 | abril | 2024

Centro de Ciberseguridad Ayuntamiento de Madrid

ÍNDICE

1. RESUMEN DE LA CANDIDATURA

Ante el aumento del volumen y complejidad de los ciberataques a las Administraciones Públicas, en diciembre de 2021, el Ayuntamiento de Madrid creó el "Centro de Ciberseguridad del Ayuntamiento de Madrid" (CCMAD) como una unidad orgánica, con rango de subdirección general, adscrita al Organismo Autónomo Informática del Ayuntamiento de Madrid, para prestar servicios de ciberseguridad a las Áreas de Gobierno y Organismos Autónomos del Ayuntamiento, con la misión de reforzar la protección de la gestión digital municipal ante el crecimiento exponencial de amenazas en el ciberespacio y convertirse en el centro de referencia en la ciberseguridad de las ciudades inteligentes.

Los recientes avances en materia de Inteligencia Artificial (IA), especialmente en IA generativa, están siendo aprovechados por los atacantes para mejorar sus técnicas, tácticas y procedimientos (TTPs) haciendo, si cabe, más difícil la detección y contención por parte de los centros de ciberseguridad. Ante este panorama, es crucial competir contra los atacantes usando sus mismas armas, pero orientadas a la detección y respuesta.

El Ayuntamiento de Madrid, a través de CCMAD, en colaboración con sus proveedores tecnológicos, Microsoft, Crowdstrike y Palo Alto, tiene desplegados controles de seguridad para la protección de los activos críticos (identidades corporativas, plataforma de colaboración, puestos de trabajo, servidores y cortafuegos) que incorporan tecnologías de IA y Machine Learning (ML) con capacidades avanzadas de detección, adaptación continua, automatización de tareas y mejora constante, lo que permite una mejor defensa contra los atacantes y sus amenazas en constante evolución.

2. Uso de IA/ML en CCMAD

Las siguientes soluciones desplegadas en el Ayuntamiento utilizan IA/ML para mejorar la detección y respuesta ante las ciberamenazas:

- Microsoft Defender for Identity: Utiliza tecnologías de IA y ML para analizar el comportamiento de los usuarios y las entidades en la red, identificando patrones anómalos que podrían indicar actividad maliciosa, como el robo de credenciales o el movimiento lateral. Esto mejora la detección temprana de amenazas.
- Microsoft Defender for Endpoint: Emplea IA y ML para analizar el comportamiento de los puestos de trabajo corporativos y detectar actividades sospechosas o maliciosas en tiempo real. Esto permite una respuesta más rápida a las amenazas, así como la identificación proactiva de indicadores de compromiso y TTPs.
- Microsoft Defender for Office 365: Utiliza tecnologías de IA y ML para analizar el contenido de los correos electrónicos y los archivos adjuntos en busca de amenazas como phishing, malware y ransomware. Esto mejora la detección de ataques dirigidos y la protección contra amenazas avanzadas en el correo electrónico.
- Crowdstrike Falcon: emplea técnicas avanzadas de IA/ y ML para monitorizar toda la actividad de los servidores identificando comportamientos anómalos y amenazas potenciales en tiempo real. Esto fortalece la seguridad del core IT al detectar y responder proactivamente a ataques dirigidos y amenazas avanzadas que podrían comprometer la integridad y disponibilidad de los servicios críticos.
- Firewalls Palo Alto: emplean tecnologías avanzadas de IA/ML para analizar el tráfico en tiempo real y, en combinación con la sandbox de Wildfire, pueden identificar y bloquear amenazas desconocidas, protegiendo así los activos críticos de la organización.

3. Ventajas del uso de IA/ML en el Ayuntamiento

La integración de todas estas herramientas en las capacidades y servicios de CCMAD, tiene los siguientes beneficios:

Adaptación Continua

Los ciberataques están en constante evolución, con adversarios que emplean tácticas cada vez más sofisticadas para eludir las defensas tradicionales. La IA y el ML tienen la capacidad única de adaptarse continuamente a nuevas formas de amenazas, aprendiendo de los datos en tiempo real y ajustando sus modelos de detección en consecuencia. Esto nos permite mantenernos al día con las últimas amenazas y defendernos de manera efectiva contra ellas.

Detección de Amenazas Avanzadas

Las amenazas ciber avanzadas, como el malware sin archivos y los ataques dirigidos, pueden pasar desapercibidos para las soluciones de seguridad convencionales. La IA y el ML pueden identificar patrones y comportamientos maliciosos en grandes volúmenes de datos, lo que permite detectar incluso las amenazas más sigilosas y sofisticadas. Esto es especialmente importante en entornos donde las amenazas pueden ser difíciles de detectar mediante métodos tradicionales.

Reducción de Falsos Positivos

Los falsos positivos son una preocupación común en la ciberseguridad, ya que pueden abrumar a los analistas con alertas irrelevantes y consumir recursos valiosos. La IA y el ML nos ayudan a reducir significativamente los falsos positivos al mejorar la precisión de la detección de amenazas y al aprender de las decisiones pasadas de los analistas. Esto nos permite centrarnos en investigaciones más críticas y tomar medidas proactivas para mitigar las amenazas reales.

Automatización de Tareas Repetitivas

Tareas como la correlación de eventos, la clasificación de alertas y la respuesta a incidentes, son repetitivas y propensas a errores cuando se realizan manualmente. La IA y el ML nos permiten automatizar estas tareas, aumentando la eficiencia operativa y liberando tiempo para actividades de mayor valor, como la investigación de amenazas avanzadas.

Mejora Continua

El uso de soluciones basadas en IA/ML nos permite establecer un ciclo de retroalimentación continua, donde los modelos de detección se mejoran constantemente en función de la experiencia y los nuevos datos. Esto permite una mejora continua en la eficacia y la precisión de nuestras defensas intentando estar siempre un paso por delante de los adversarios en constante evolución.

4. Repercusión para el ciudadano y las Administraciones

El uso descrito en este documento de la IA/ML mejora las capacidades de detección y respuesta del CCMAD, lo que tiene un impacto positivo en la confidencialidad de la información de los ciudadanos custodiada por el Ayuntamiento y en la disponibilidad de servicios públicos digitales, proporcionando un entorno digital más seguro y confiable para interactuar con la administración municipal.

5. Proveedores

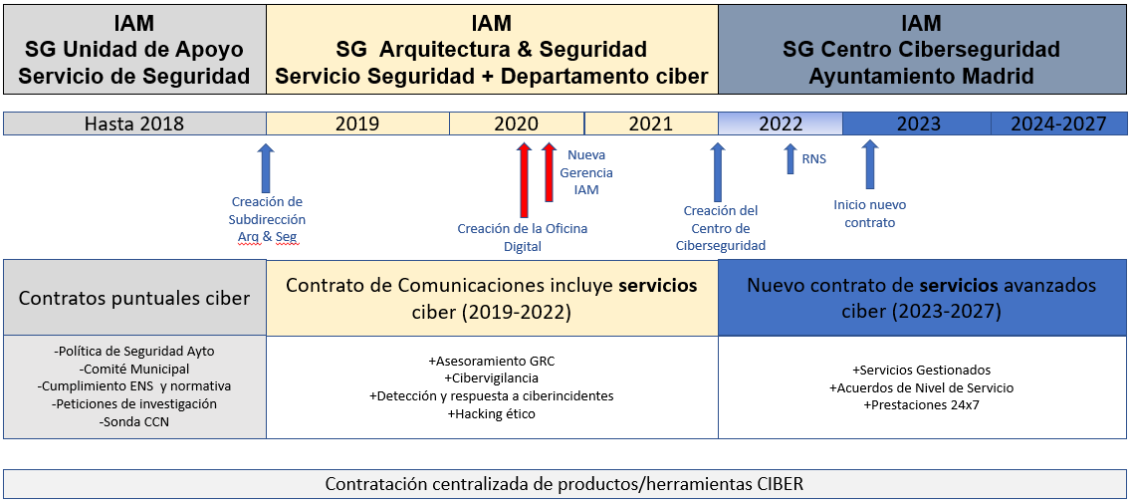
Tal y como se ha comentado, los proveedores que incorporan IA/ML en las herramientas usadas por CCMAD son Microsoft, Crowdstrike y Palo Alto.

6. Información general sobre CCMAD

6.1 SEGURIDAD EN EL AYUNTAMIENTO DE MADRID

A finales del año 2018, se alteró el peso de los servicios de Seguridad de la Información municipales que se prestaban a través del Servicio de Seguridad de la Subdirección General Unidad de Apoyo del Organismo Autónomo Informática Ayuntamiento de Madrid (IAM), con la creación de una Subdirección General específica de Arquitectura y Seguridad.

Ante el aumento del volumen y complejidad de los ciberataques a las Administraciones Públicas y alineado con la lista de compromisos de la alcaldía para la mejora de la ciberseguridad del ayuntamiento, con el objetivo de convertirse en un referente a escala nacional e internacional y ser polo de difusión de la cultura de la ciberseguridad, en diciembre de 2021 el Ayuntamiento de Madrid creó el «Centro de Ciberseguridad del Ayuntamiento de Madrid», en adelante CCMAD, como una unidad orgánica con rango de subdirección general, adscrita al Organismo Autónomo Informática del Ayuntamiento de Madrid, para prestar servicios de ciberseguridad a las Áreas de Gobierno y Organismos Autónomos del Ayuntamiento, con la misión de reforzar la protección de la gestión digital municipal ante el crecimiento exponencial de amenazas en el ciberespacio.



Desde entonces hasta 2022 los servicios de protección se reforzaron gracias a la adjudicación de un voluminoso contrato para la transformación innovadora de las telecomunicaciones del Ayuntamiento, que incorporó a la operativa el apoyo de una oficina de ciberseguridad del adjudicatario en modo servicio, permitiendo mejorar la detección y respuesta a ciberincidentes, obtener asesoramiento en GRC, desplegar monitorización en cibervigilancia y realizar auditorías de hacking ético de forma regular en los Servicios y Sistemas de Información municipales.

En 2023 CCMAD multiplica por cuatro la cantidad y calidad de sus servicios mediante un contrato específico de servicios avanzados de ciberseguridad que suma a todas las responsabilidades anteriores nuevos servicios gestionados, mejoras en los acuerdos de nivel de servicio y prestaciones en formato 24x7.

En el contexto de la Estrategia de Transformación Digital del Ayuntamiento de Madrid, Madrid Capital Digital, la Junta de Gobierno aprobó el 24 de noviembre de 2022 la licitación de un contrato de servicios digitales avanzados para incrementar la ciberseguridad del Consistorio que se adjudicó a SIA en septiembre de 2023.

6.2 HITOS

CCMAD nace como un centro para el desarrollo de la gobernanza y estrategia de ciberseguridad, vigilancia digital en el ciberespacio con servicios de monitorización, detección y respuesta a ciberincidentes, así como promoción de la cultura de ciberseguridad, que contribuye al perfeccionamiento de la resiliencia de los servicios digitales de la ciudad de Madrid.

Presta servicios de cibervigilancia de activos de información municipales, empleando capacidades de inteligencia en amenazas y vulnerabilidades que facilitan una avanzada monitorización, detección y respuesta a ciberincidentes, participando en el diseño y modelado de las arquitecturas y tecnologías de seguridad en la ciudad, vela por el cumplimiento normativo, realiza actividades de formación, concienciación y difusión para el fomento de la cultura de la ciberseguridad, realiza auditorías técnicas y gestiona la identidad electrónica para el personal y los sistemas municipales.

- DE FORMA DIRECTA: Presta servicio a todas las Áreas de Gobierno del Ayuntamiento y sus Organismos Autónomos, incluyendo a más de 30.000 personas que son parte del personal municipal y externo.
- DE FORMA INDIRECTA: Presta servicio a las 3,3 millones de personas empadronadas en la ciudad de Madrid, 5 millones si se incluye a quienes utilizan regularmente sus servicios públicos y 10 millones si se cuentan los turistas.

A diario, se registran alrededor de 1.200 millones de eventos que son analizados automáticamente para verificar si se corresponden con amenazas reales, materializando 70 investigaciones diarias sobre posibles ciberincidentes que requieren de la actuación del personal de CCMAD y sus empresas colaboradoras.

6.2.1 La Sala de Control

El 7 de marzo de 2023, el alcalde de Madrid inauguró la sala de control, que cuenta con un total aproximado de 250 metros cuadrados, incluyendo un espacio para la gestión de cibercrisis, con capacidad para conectarse por videoconferencia con otras ubicaciones remotas, 15 puestos de operador con pantalla curva panorámica de 49 pulgadas, 2 puestos de responsables y un videowall equivalente a 300 pulgadas.

El personal de la sala de control lleva a cabo tres funciones principales:

- Monitorización de los sistemas y servicios municipales para velar por el cumplimiento de los niveles de disponibilidad esperados, de forma conjunta con personal del adjudicatario del contrato de operación de sistemas, NTT Data, que realizo esta función desde su centro de control en Guadalajara.
- Vigilancia Digital, Detección y Respuesta ante ciberincidentes. Todos los días se registran aproximadamente 1200 millones de eventos, que son analizados automáticamente para comprobar si se trata o no de una amenaza y que

generan 70 investigaciones diarias sobre posibles ciberincidentes que requieren la actuación del personal de CCMAD y las empresas colaboradoras.

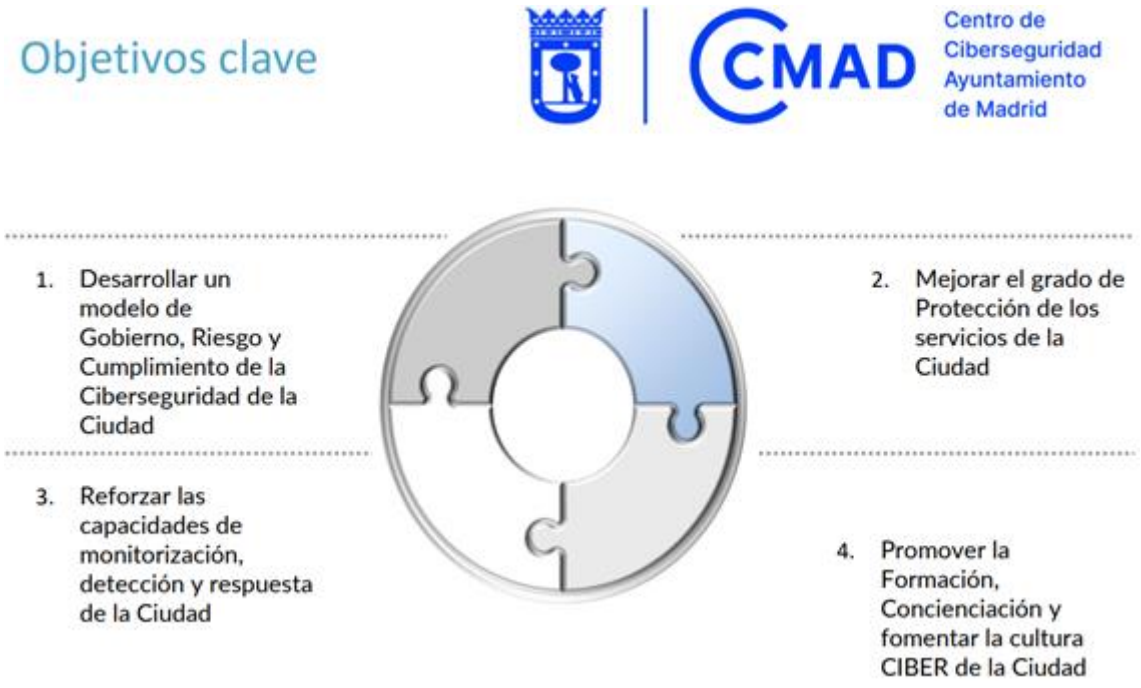
- Otras tareas importantes de ciberseguridad como auditorías de vulnerabilidades, bastionado, seguridad en terceros, cumplimiento normativo, acciones de concienciación para empleados, etc.

La sala de control está preparada para funcionar en 24x7 en situaciones de cibercrisis. En situaciones de normalidad, el servicio 24x7 lo proporcionan los diferentes proveedores de servicio: NTT Data para servicios de infraestructura y sistemas, y SIA para un subconjunto de alertas de ciberseguridad.

6.2.2 Cumplimiento normativo

En mayo de 2017 se estableció la primera Política de Seguridad de la Información del Ayuntamiento de Madrid y sus Organismos Públicos. Desde entonces ha estado sometida a revisión por parte del Comité Municipal de Seguridad de la Información, con actualizaciones regulares y cuya última versión está disponible en el enlace anterior.

«Madrid, Capital Digital», es la estrategia que el Ayuntamiento de Madrid hizo publica en noviembre de 2022, para seguir siendo una ciudad referente en el ámbito digital. En esta iniciativa figura la Estrategia de Ciberseguridad, cuyos objetivos se concentran en el desarrollo de un modelo de gobierno, riesgo y cumplimiento de la ciberseguridad que perfeccione la resiliencia de la ciudad y los servicios municipales, con la colaboración de las diferentes Áreas de Gobierno y Organismos, en el ámbito de sus competencias, la mejora del grado de protección de los servicios de la ciudad mediante la concreción y aplicación de controles en línea con la Política de Seguridad, el refuerzo de las capacidades de monitorización, detección y respuesta ante posibles ciberincidentes que se materialicen en el ámbito de actuación, y la promoción de la formación, concienciación y fomento de la cultura ciber en la ciudad, incluyendo la colaboración con otras Administraciones Públicas y Organismos españoles y europeos.



En la Estrategia de Ciberseguridad, se define una hoja de ruta que contempla 16 líneas de acción enmarcadas dentro de 4 objetivos estratégicos:

- Modelo GRC (Gobierno, Riesgo y Cumplimiento):
  - P01.01 - Cumplimiento de las obligaciones de Esquema Nacional de Seguridad (Real Decreto 311/2022), Ley de Protección de Infraestructuras Críticas (Ley 8/2011) y de seguridad de las redes y sistemas de información (Real Decreto-Ley 12/2018).
  - P01.02 - Extender el gobierno de la seguridad de la información a todas las áreas de gobierno y OOPP.
  - P01.03 - Procesos y procedimiento para un ciclo continuo de identificación y tratamiento de Riesgos.
  - P01.04 - Desarrollo de un inventario de proveedores de servicios para su valoración.
  - P01.05 - Cuadro de mandos integral de ciberseguridad del Ayuntamiento.
  - P01.06 - Plan de continuidad de negocio.
- Protección de la ciudad
  - P02.01 - Definir requisitos de protección en redes/sistemas IT y OT (bastionado).
  - P02.02 - Seguridad en el ciclo de vida de sistemas y desarrollos.
  - P02.03 - Pruebas de seguridad (pentesting y auditorías).
- Monitorización, detección y respuesta
  - P03.01 - Despliegue de capacidades avanzadas de ciberseguridad (monitorización, detección y respuesta) en redes/sistemas IT y OT.
  - P03.02 - Integración en la red nacional de SOCs
  - P03.03 - Plan de gestión de cibercrisis del Ayuntamiento de Madrid.
- Formación, concienciación y cultura CIBER:
  - P04.01 – Formación.
  - P04.02 – Concienciación.
  - P04.03 – Difusión y comunicación de la cultura de ciberseguridad.
  - P04.04 – Creación de un ecosistema público-privado en torno a la temática de “Ciberseguridad en SmartCities”.

Y por último, en materia de cumplimiento se debe reseñar que, en agosto de 2023, CCMAD obtuvo la primera certificación de ciberseguridad en la historia del Ayuntamiento de Madrid.

6.2.3 Cooperación y colaboración

En la naturaleza de CCMAD se encuentra la creencia de que, para gestionar la seguridad de una gran ciudad, es imprescindible compartir conocimientos y experiencias con los responsables de seguridad de ciudades afines dentro y fuera del país, organismos públicos y privados de cooperación y colaboración en la materia e incluso asociaciones, equipos y grupos de trabajo formados por la ciudadanía para la compartición de información o investigación.

Eso hace que la unidad sea muy activa, participando de los siguientes proyectos, entre otros:

- Pertenencia a la Red Nacional de Centros de Operaciones de Ciberseguridad (RNS) desde agosto de 2022.
- Convenio de colaboración con el Centro Criptológico Nacional (CCN-CERT).
- Coordinación del grupo de seguridad de la información y privacidad de la Red Española de Ciudades Inteligentes (RECI), de la Federación Española de Municipios y Provincias (FEMP).
- Pertenencia a la Comunidad de Prácticas (COP) en materia de ciberseguridad en la red de grandes ciudades europeas Eurocities.
- Estrecha cooperación con la asociación de empleados públicos por la mejora de la ciberseguridad en la Administraciones Públicas ProtAAPP.
- Colaboración con el Laboratorio IOT Ciudad de Madrid (iniciativa de colaboración público-privada entre Oficina Digital y UPM) para la realización de pruebas de seguridad sobre dispositivos previa a su despliegue en la ciudad.

Por último y no por ello menos importante, CCMAD es consciente de la necesidad de mantener en su radar a los propios ciudadanos y usuarios de los servicios digitales, ante quienes mantiene la responsabilidad de concienciar en pro de una mejora de la protección individual de las personas, pero también a los investigadores de la comunidad hacker a los que ofrece y agradece la posibilidad de realizar notificaciones responsables sobre vulnerabilidades detectadas en los sistemas del Ayuntamiento de Madrid y para quienes promete guardar alguna sorpresa en un futuro deseablemente cercano.

6.2.4 Participación pública

Durante el año 2023 el Centro de Ciberseguridad del Ayuntamiento de Madrid ha estado presente en los siguientes eventos, publicaciones e iniciativas:

- XVII Jornadas STIC CCN-CERT | V Jornadas de Ciberdefensa ESPDEF-CERT: Ciberseguridad en grandes ciudades
- VI Foro IT User de Administración Pública
- Artículo en CSO Computer World
- Congreso C1B3RW4LL (monográfico con cinco ponencias).
- Jornadas Técnicas Internacionales RECI

- Congreso CNIS
- I CyberSecurity Healthcare & Pharma Congress de CyberMadrid
- Smart City Expo World Congress (SCEWC), Barcelona
- Participación en el Global Mobility Call
- Women4Cyber Spain Panel | Safeguarding the future: Empowering boardrooms to confront and conquer cyber threats
- Seguritecnia - Desayuno de trabajo RECI- Seguridad en SmartCities
- Evento de Eurocities "Cibersecurity Comunity of Practice"
- Premio de la revista ADSLZone a CCMAD
- Eurocities – Visita a la Métropole Euopéenne de Lille, Francia