MÁS CAPACIDAD DE DETECCIÓN Y DE RESPUESTA PARA EL SOC DE LA JUNTA DE CASTILLA Y LEÓN

ENTIDAD:

Administración de la Comunidad de Castilla y León

BREVE RESUMEN

El continuo crecimiento en el uso y la criticidad de las TIC en las Administraciones Públicas viene acompañado de riesgos e incidentes de seguridad, cada vez más numerosos y sofisticados. Para atenderlos adecuadamente la Junta de Castilla y León ha ampliado en los últimos años las capacidades de detección y de respuesta de su SOC, que en este tiempo ha pasado de ceñirse al mundo de las comunicaciones, a convertirse en el SOC integral y maduro que la organización necesita.

ANTECEDENTES/PROBLEMÁTICA

Aunque las Tecnologías de la Información y las Comunicaciones (TIC) eran ya un cimiento esencial de la actividad administrativa y del servicio público, la pandemia COVID-19 disparó la necesidad de digitalización en todos los ámbitos de la vida. Con ello, los riesgos de ciberseguridad crecieron y, posteriormente, se multiplicaron por la conflictiva situación geopolítica. Por todo ello se ha hecho imprescindible prestarles una atención constante y creciente.

En este contexto, la Administración de la Comunidad de Castilla y León (en adelante, ACCyL) ha realizado un conjunto de actuaciones para mejorar la visibilidad de los incidentes de seguridad que se produzcan y para responder ante ellos con más fluidez.

Los fondos del Mecanismo de Recuperación y Resiliencia - Next Generation EU han impulsado este plan financiando algunas de esas actuaciones, en concreto la adquisición de herramientas de correlación de eventos (SIEM) y de automatización de la gestión de la ciberseguridad (SOAR).

RETOS/OBJETIVOS PERSEGUIDOS

Fundamentalmente son tres los objetivos perseguidos. Dos de ellos son operativos: aportar al SOC más **visibilidad** de información de ciberseguridad y más **fluidez** en la comunicación y en la capacidad de respuesta. El tercer objetivo, el que multiplica el valor de los dos anteriores, es **su integración**.

Al comienzo de la pandemia el SOC fue rediseñado para dotarle de herramientas orientadas a atender la creciente complejidad e incertidumbre. Con este objetivo se le asignó la operación de nuevas soluciones tecnológicas de protección perimetral y de red, y se le dotó de capacidad de gestión de registros de actividad (*logs*) y de correlación de eventos de seguridad.

Desde entonces, la creciente actividad del SOC ha sido acompañada por un continuo incremento de la información atendida y por un constante ajuste de sus procedimientos de comunicación y operación, para optimizar el nivel de protección.

Por otra parte, las normas de desarrollo de la política de seguridad de la información y protección de datos de la ACCyL han apuntalado al SOC como pieza esencial en la gestión de los incidentes de seguridad de la organización, incrementando así también el nivel de exigencia en la calidad de sus resultados.

FASES DEL PROYECTO – RECURSOS EMPLEADOS

En cuanto a la **capacidad de detección**, los diversos avances que han proporcionado más **visibilidad** son los siguientes:

a) La adición continua de nuevas fuentes de información de seguridad: servidores, EDR, *sandbox*, directorio, flujos de tráfico de red, Microsoft 365, protección DDoS, vigilancia digital desde Internet, etc.

b) La ampliación de nodos del clúster de la solución *software* para la gestión centralizada de *logs*, que han pasado de 3 a 7, diseñándose su próxima ampliación a 10. Este crecimiento también se ha visto acompañado por el incremento en sus capacidades de proceso y de almacenamiento.

c) La renovación de la herramienta de **correlación** de eventos de ciberseguridad, el SIEM, que ha cambiado de una solución basada en *software* de fuentes abiertas a un producto comercial integral que aporta más capacidades de rendimiento, de normalización, de correlación de eventos y de vinculación con fuentes externas de inteligencia sobre amenazas de ciberseguridad.

d) La adhesión a la Red Nacional de SOCs y la utilización de herramientas proporcionadas por el CCN, como REYES, han enriquecido la información utilizada en la gestión de la ciberseguridad.

e) La implantación del proceso de firmado de *logs* contando con la plataforma de sellado de tiempo TS@, para así dotarles de integridad como evidencias a custodiar.

Por otra parte, en cuanto a la **capacidad de respuesta**, los avances más significativos se centran en la **fluidez** y la capacidad operativa, siempre intentando buscar la forma de **automatizar** cualquier operación manual posible, desde el mero intercambio de información con herramientas de *ticketing,* hasta la realización de sofisticadas operaciones en los equipos de seguridad perimetral. Entre estos avances destacan:

a) La elaboración de procedimientos documentados, que consideran toda la organización de la gestión de los incidentes de seguridad, acompañados de flujos de trabajos muy detallados, que incluyen la comunicación y la notificación a los actores relevantes.

b) La implantación de una herramienta MISP para compartir información de ciberseguridad con diversos elementos de la solución de seguridad como con los IPS, con los cortafuegos y con los filtros de seguridad de correo electrónico y de tráfico de navegación en Internet.

c) La monitorización automática de indicadores de compromiso (IoCs).

d) La implementación de casos de uso para las operaciones y riesgos más importantes, teniendo en cuenta su probabilidad, su impacto y el esfuerzo que suponen las correspondientes respuestas.

e) La implantación de una herramienta de **orquestación y automatización** de operaciones en la gestión de la ciberseguridad, el SOAR, que permite operar directamente diversos de los elementos que forman la solución de seguridad de la ACCyL, evitando así tener que hacerlas de manera manual, forma de hacerlas que, con el incremento constante de la actividad, empieza a volverse imposible.

   Las expectativas de usar esta herramienta SOAR son enormes, tanto para una más ágil gestión de la seguridad, automatizando, por ejemplo, *playbooks* para la obtención de información de contexto relevante para las investigaciones que realizan los técnicos del SOC, o la generación de reportes; como para la automatización de otras operaciones de provisión de servicios y recursos TIC.

Los resultados van más allá de los exclusivamente operativos. La involucración directa e inmediata en la gestión de los incidentes de seguridad de los distintos responsables que la política de seguridad de la organización define, está reforzando la conciencia de que **la seguridad de la información es un trabajo de todos todo el tiempo**.

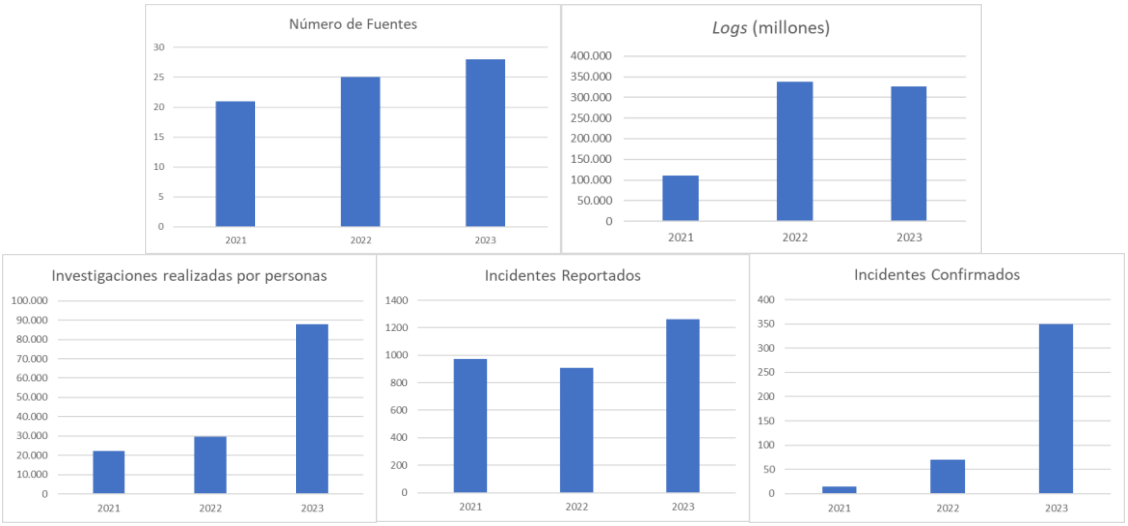
NUEVOS SERVICIOS Y MEJORAS EN EFICIENCIA

La puesta en marcha de los trabajos referidos en el punto anterior ha permitido mejorar:

a) La información que se considera, con más datos y mejores herramientas para obtener información más precisa y útil.

b) La productividad de las personas involucradas, que cuentan con una clara forma de actuar y con la potencia de herramientas que automáticamente les proporcionan datos para enfocar su trabajo o que, directamente, hacen parte de este.

En resumen, se consigue dedicar menos tiempo a operaciones manuales para poder enfocarse en la toma de decisiones con la mejor información. Todo ello, y sobre todo la herramienta SOAR referida previamente, tiene y tendrá un gran impacto en la eficiencia del trabajo de las personas involucradas a la vista de la evolución que en los últimos años ha tenido su actividad, especialmente en cuanto a *logs* considerados, investigaciones realizadas e incidentes confirmados, que se indica a continuación:



CONCLUSIONES DE LA ENTIDAD

El continuo crecimiento en el uso y la criticidad de las TIC en las Administraciones Públicas hace que la protección de las herramientas que soportan la actividad administrativa y el servicio público tenga que ser una fortaleza de la organización.

La protección frente a los riesgos de ciberseguridad supone un reto común para toda la organización y no sólo para las unidades TIC. Disponer de más información y más fiable, y de más fluidez y capacidad operativa, fortalece las defensas y permite responder eficazmente a los riesgos de ciberseguridad. Solo controlando esos riesgos y su impacto se consigue que las TIC sigan siendo una palanca de innovación en el sector público y, en consecuencia, un beneficio para toda la ciudadanía.

Tras un proceso de madurez, el SOC de la ACCyL ha pasado de ceñirse al mundo de las comunicaciones a convertirse en un actor fiable y muy relevante en la gestión de los incidentes de seguridad en toda la organización.

Por último, las expectativas de las nuevas herramientas de correlación de eventos (SIEM) y de automatización de la gestión (SOAR), adquiridas con fondos Next Generation EU, son ilusionantes.