Junta de Castilla y León

EL REFUERZO DEL CENTRO DE OPERACIONES DE SEGURIDAD DE LA ADMINISTRACIÓN DE LA COMUNIDAD DE CASTILLA Y LEÓN

RESUMEN

El continuo crecimiento en el uso y la criticidad de las Tecnologías de la Información y las Comunicaciones (en adelante, TIC) para las Administraciones Públicas viene acompañado de riesgos e incidentes de ciberseguridad, cada vez más numerosos y sofisticados.

La Administración de la Comunidad de Castilla y León (en adelante, ACCYL) cuenta con un Centro de Operaciones de Seguridad (en adelante, SOC) que es el centro que realiza la gestión de los incidentes de seguridad detectados, es decir, analiza su impacto y comportamiento, y toma y promueve medidas de contención y de prevención de los efectos del incidente.

La protección frente a los incidentes de seguridad necesita que la información para su identificación sea visible, que los especialistas que los atienden puedan trabajar y colaborar con fluidez y que se tenga capacidad de respuesta suficiente ante ellos.

La ACCyL ha puesto en marcha diversos trabajos para aumentar y mejorar la información disponible y para reforzar la capacidad operativa del SOC como centro especializado en la gestión de la ciberseguridad, con el objetivo de conseguir unas TIC más seguras y fiables.

ANTECEDENTES

La pandemia consecuencia del COVID-19 ha acelerado el ya creciente uso de los medios electrónicos por los ciudadanos, las empresas y el sector público.

Aunque las TIC eran ya un cimiento esencial de la actividad administrativa y del servicio público, la pandemia ha disparado la necesidad de digitalización en todos los ámbitos de actuación de las Administraciones Públicas.

Ese impulso a la transformación digital del sector público viene acompañado de unos riegos de ciberseguridad mayores. Los incidentes de seguridad son cada vez más numerosos y sofisticados y pueden tener un mayor impacto en el normal funcionamiento de los servicios.

La ACCyL está reforzando el SOC realizando un conjunto de actuaciones en materia de ciberseguridad para prevenir esos riesgos, para detectar los incidentes de seguridad que se produzcan y para reaccionar ante ellos con las mejores capacidades.

OBJETIVOS

Fundamentalmente son tres los objetivos perseguidos: visibilidad, fluidez de la comunicación entre los especialistas y capacidad de respuesta.

En cuanto a visibilidad se abordan diversos retos. Por una parte, obtener datos de muchas más fuentes de información de ciberseguridad, algunas ya existentes en la organización y otras nuevas. Por otra parte, procesar toda esa información con herramientas automáticas para extraer el conocimiento de ciberseguridad útil para los especialistas que la gestionan.

Es esencial que esos especialistas en ciberseguridad se comuniquen habitualmente y con fluidez. En este sentido se han mejorado los canales de comunicación y se han implementado en herramientas integradas.

Por último, la mejora en la capacidad de respuesta se concreta fundamentalmente en la ampliación de las capacidades de monitorización, operación, análisis y atención del

SOC de la ACCyL y con la renovación y ampliación de diversas soluciones técnicas de ciberseguridad desplegadas en la Red Corporativa.

FASES DEL PROYECTO Y PLAZOS

En los años 2021 y 2022 se han realizado diversas actuaciones:

a) Renovación de los equipos y servicios principales de protección de la seguridad perimetral y de red. Se dispone de los siguientes elementos: doble barrera de cortafuegos, sistemas de prevención de intrusos (IPS), sondas para la detección de intrusos (IDS), *sandbox* para la navegación y el almacenamiento y protección de la navegación y del correo electrónico.

b) Puesta en marcha de una solución de antimalware y EDR (*Endpoint Detection & Response*) para proteger los equipos de usuario y los servidores corporativos.

c) Ampliación de las capacidades de la solución para la gestión centralizada de registros de actividad de los productos y los servicios TIC.

d) Protección frente a ataques DDoS desde Internet.

e) Implantación de capacidades de control de acceso a las redes.

f) Más segmentación interna de la red.

g) Conversión de los principales equipos de comunicaciones de la Red Corporativa en sensores que aportan la visibilidad de los flujos de tráfico, tanto internos como con Internet, para la detección de amenazas, evaluación del cumplimiento de las políticas, etc.

a) Reducción de la superficie de exposición de los servicios corporativos en Internet.

b) Monitorización de los accesos desde Internet a recursos de la organización.

c) Refuerzo de los sistemas de autenticación con contraseñas más robustas, de renovación más frecuentemente e incluso acompañadas de doble factor de autenticación.

d) Monitorización de la información en Internet, incluso en la Internet oscura, relativa a la reputación de la organización y a la seguridad de sus servicios.

e) Revisión de configuraciones y procedimientos operativos para agilizar las operaciones rutinarias y así poder dedicar más atención de los especialistas a los incidentes de ciberseguridad.

f) Interconexión de las herramientas de *ticketing* que utilizan los diversos grupos técnicos que participan en la gestión de los incidentes de seguridad y consolidación de la información en la herramienta LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) del Centro Criptológico Nacional (CCN).

g) Integración del SOC en la Red Nacional de SOCs promovida por el CCN-CERT.

Todas estas actuaciones para un tratamiento integral de la ciberseguridad están alineadas para obtener la mejor protección.

El trabajo no termina con las actividades referidas anteriormente, la mejora es continua y ya se han están diseñando otras actividades para ampliar las capacidades de detección, prevención y respuesta que se materializarán en los años 2023 y 2024.

a) Protección de dispositivos móviles y de accesos directos a Internet.

b) Implantación de herramientas de correlación de eventos y de automatización de la gestión de ciberseguridad, proyecto financiado con el apoyo de Fondos *Next Generation (MRR).*

EQUIPO, PROVEEDORES Y COSTES

El proyecto es un cambio integral en la gestión de la ciberseguridad y, por tanto, participan en él mucho personal de la organización de distintas especialidades TIC.

También han participado diversos proveedores externos de soluciones y servicios de ciberseguridad y de telecomunicaciones resultando una inversión agregada que se prevé que llegue a superar los 6 millones de euros entre los años 2021 y 2024.

REPERCUSIÓN PARA LA ADMINISTRACIÓN Y PARA EL CIUDADANO

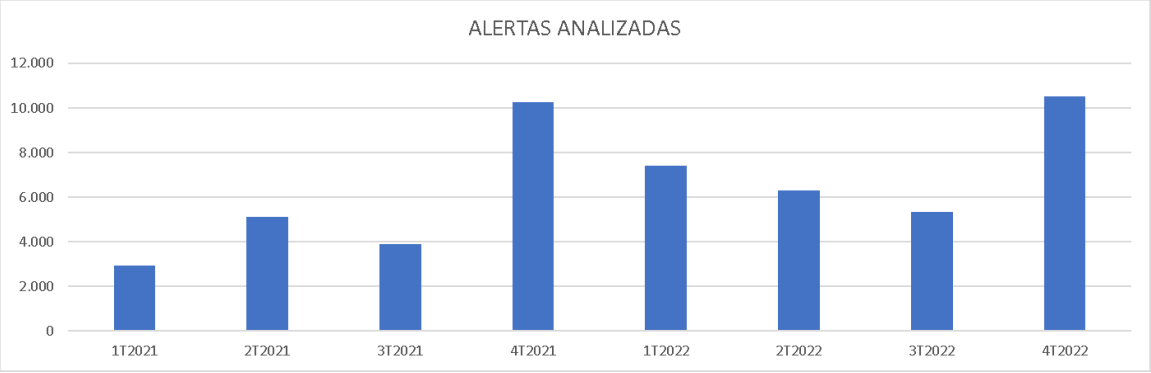
La puesta en marcha de los trabajos referidos anteriormente ha permitido mejorar:

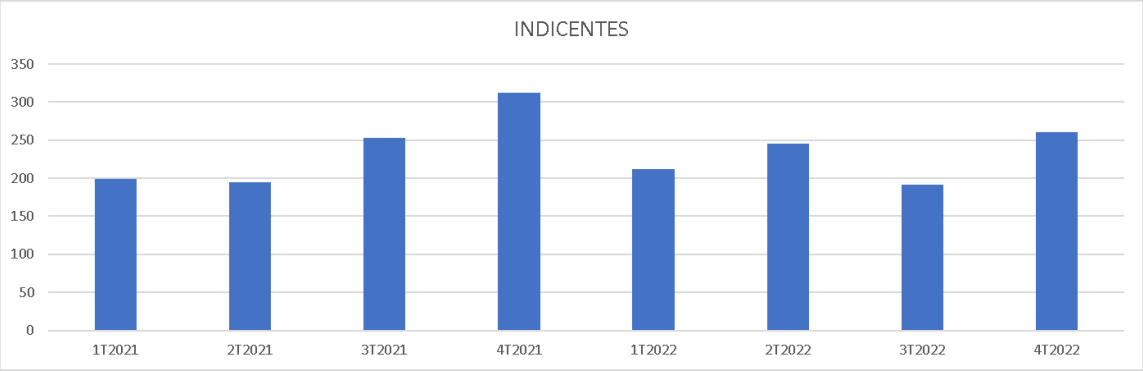
a) El valor de la información. Con más datos, más filtros y más procesados se obtiene información más precisa y útil.

b) El intercambio fluido de información. Al interconectar herramientas y consolidar la información relevante se agiliza la colaboración y la compartición de la información que ayuda a tomar mejores decisiones.

c) La capacidad de respuesta ante incidentes de seguridad. Se dota al SOC de elementos para mejorar la agilidad de sus acciones y más capacidad para una mejor gestión de los incidentes de seguridad.

Con todos estos cambios, además de conseguirse nuevas capacidades de prestación de servicios de ciberseguridad, se automatizan y simplifican muchas comunicaciones y operaciones. Por ello, se dedica menos tiempo a rutinas para poder enfocarse en la toma de decisiones tras el análisis de las alertas recibidas, y en su implementación para la atención de los incidentes.





Todo ello tiene un gran impacto, no sólo en la eficacia, sino también en la eficiencia del trabajo de los actores involucrados en la gestión de los incidentes de seguridad que redunda en una mejora de los resultados obtenidos en relación con los costes dedicados.

Las mejoras en la detección de incidentes de ciberseguridad y en la automatización de la respuesta a los mismos aumenta la protección de los servicios públicos digitales que utilizan los ciudadanos.

CONCLUSIONES

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 tengan que ser una fortaleza de la organización.

La protección frente a los riesgos de ciberseguridad supone un reto común para todas las unidades TIC de la organización. La alineación de todas las actuaciones y operaciones según un plan coordinado es esencial para conseguir esa óptima protección.

Disponer de más información, fiable, integrada y compartida, fortalece las defensas y permite responder eficazmente a los retos de ciberseguridad, cada vez más numerosos y sofisticados.

Solo controlando esos riesgos de ciberseguridad y su impacto se consigue que las TIC sigan siendo una palanca de innovación en el sector público, objetivo con el que la Administración de la Comunidad de Castilla y León está firmemente comprometida.