GESTIÓN INTEGRAL DE LA CIBERSEGURIDAD EN 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 para las Administraciones Públicas viene acompañado de riesgos e incidentes de ciberseguridad, cada vez más numerosos y sofisticados. La protección frente a los mismos necesita que la información para la identificación de los incidentes de ciberseguridad 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 Administración de la Comunidad de Castilla y León ha puesto en marcha diversos trabajos orientados a una gestión integral de la ciberseguridad de las TIC corporativas.

ANTECEDENTES/PROBLEMÁTICA

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 Tecnologías de la Información y las Comunicaciones (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 cada vez 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 Administración de la Comunidad de Castilla y León (ACCyL) está 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.

RETOS/OBJETIVOS PERSEGUIDOS

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

FASES DEL PROYECTO – RECURSOS EMPLEADOS

En 2021, para conseguir los objetivos previstos, se han realizado los siguientes trabajos:

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) 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.

c) Adquisición de una solución de antimalware y EDR (*Endpoint Detection & Response*) para proteger los equipos de usuario y los servidores corporativos.

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

e) Protección frente a ataques DDoS desde Internet.

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

g) 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.

h) 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).

i) 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.

j) Aprobación del Decreto de la Política de Seguridad de la Información y Protección de Datos de la organización y actualización de las normas de control de acceso en el perímetro y en los segmentos de la Red Corporativa.

k) Diseño de un completo Plan de Formación y Concienciación, con actividades de concienciación, formación y evaluación de lo aprendido, y orientado a los diversos colectivos en función de sus responsabilidades (usuarios, responsables de seguridad, directivos, etc.).

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

NUEVOS SERVICIOS Y MEJORAS EN EFICIENCIA

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

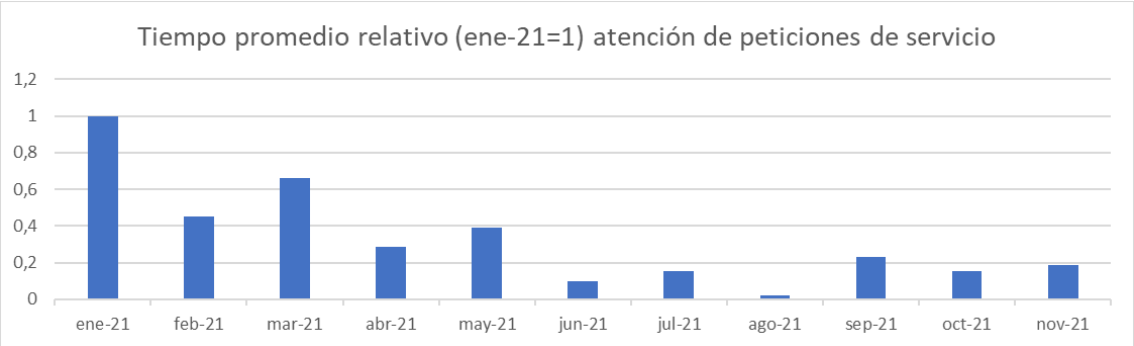
a) El valor de la información. Con más datos, más filtros y más procesados se obtiene información más precisa y útil.

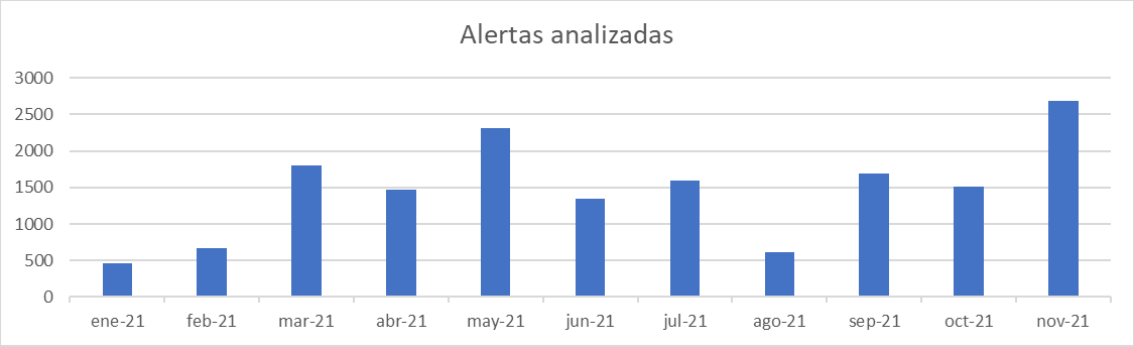
b) El intercambio fluido de información. Al interconectar herramientas y consolidar la información relevante se agiliza la colaboración y la compartición de la información que ayuda a tomar mejores decisiones.

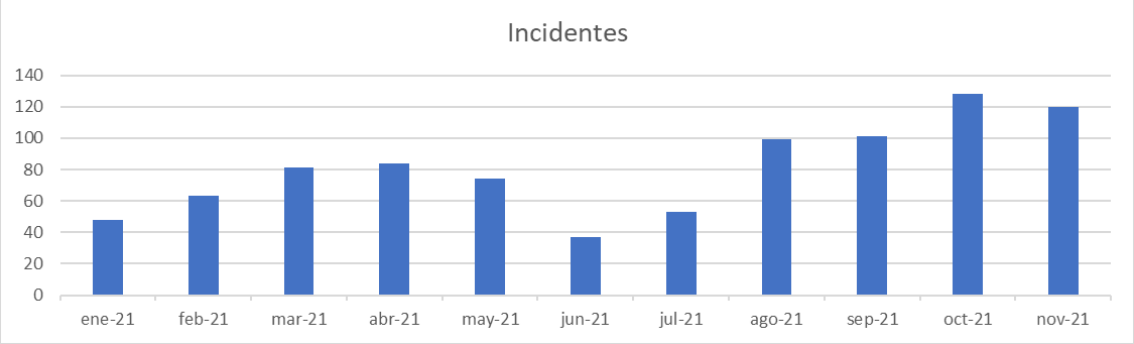
c) La capacidad de respuesta ante incidentes de seguridad. Se ha dotado al SOC de elementos para mejorar la agilidad de sus acciones y más capacidad para una mejor gestión de los incidentes de seguridad.

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 y su implementación.

Todo ello tiene un gran impacto 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.







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 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.