FORO ADMINISTRACIÓN PÚBLICA

it User

MODERNIZACIÓN DEL SECTOR PÚBLICO:

ESTADO DE LAS INICIATIVAS DIGITALES

ORGANIZA

it Digital MEDIA GROUP

SOCIO COLABORADOR

Foro CPP colaboración público-privada TECNOLOGÍA & INNOVACIÓN

PATROCINADOR PLATINO

MicroStrategy

PATROCINADORES GOLD

Flexxible · SONICWALL · Schneider Electric · SOPHOS · WatchGuard

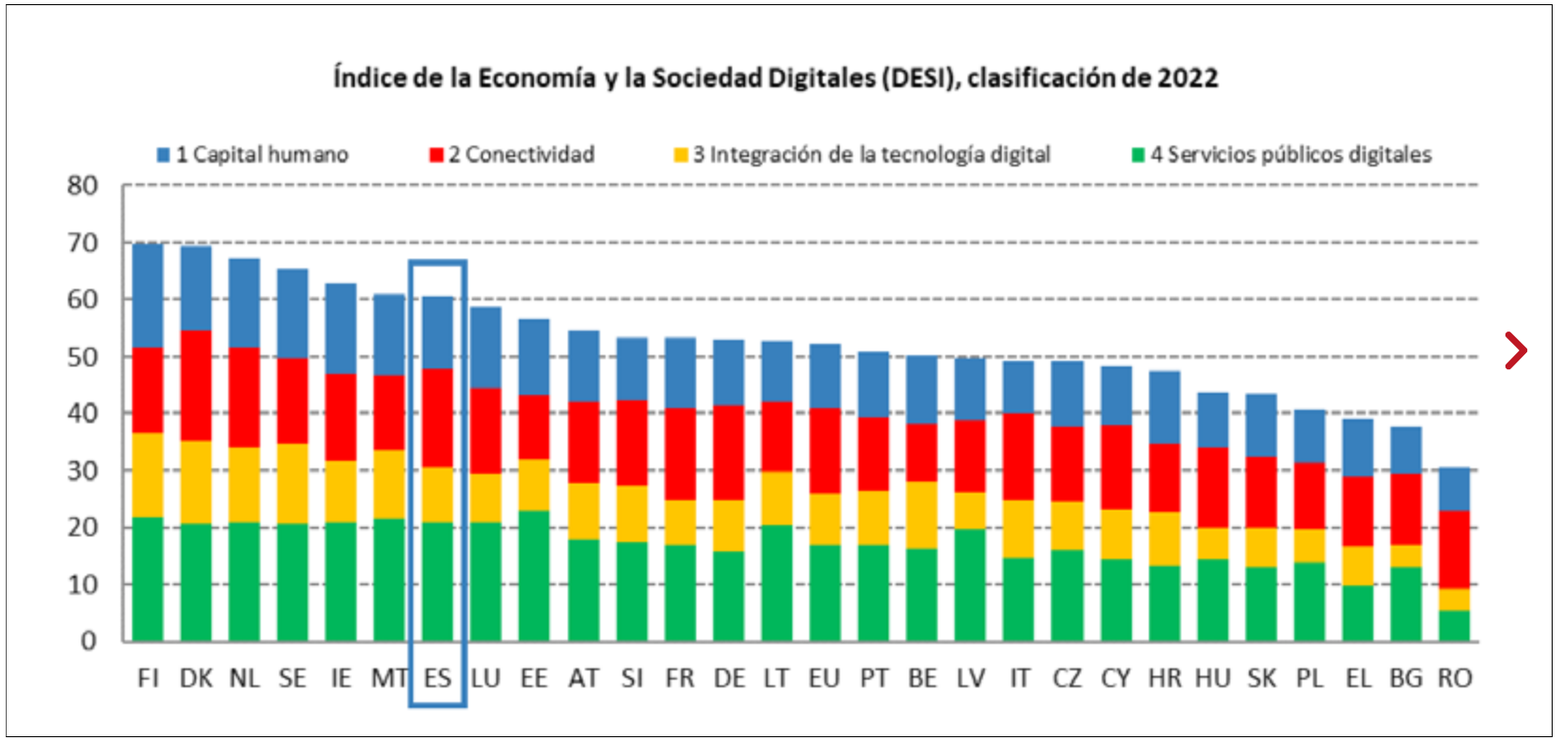
WATCHGUARD FOR SOC

MODERNIZACIÓN DEL SECTOR PÚBLICO

ESTADO DE LA DIGITALIZACIÓN DE LA ADMINISTRACIÓN PÚBLICA ESPAÑOLA

EL SECTOR PÚBLICO ESPAÑOL INICIÓ HACE AÑOS UN CAMINO SIN VUELTA ATRÁS PARA AVANZAR EN LOS NIVELES DE DIGITALIZACIÓN, NO SOLO DE CARA A CONTAR CON UNA INSTITUCIONES MÁS EFICIENTES, PRODUCTIVAS Y SEGURAS, SINO PARA PODER OFRECER UNA GAMA CADA VEZ MÁS AMPLIA DE SERVICIOS DIGITALES A UNOS CIUDADANOS QUE HACE TIEMPO QUE DEJARON DE SER ANALÓGICOS EN SU GRAN MAYORÍA. PERO TRAS MUCHOS ESFUERZOS E INVERSIONES, LLEGA EL MOMENTO DE HACER BALANCE Y LAS CIFRAS DEL ÚLTIMO ÍNDICE DE LA ECONOMÍA Y LA SOCIEDAD DIGITALES, POPULARMENTE CONOCIDO COMO ÍNDICE DESI, NOS COLOCAN EN LA SÉPTIMA POSICIÓN ENTRE LOS 27 PAÍSES DE LA UE. REPASEMOS DÓNDE ESTAMOS Y HACIA DÓNDE VAMOS.

Según los datos que la Comisión Europea ha obtenido en la elaboración del Índice de la Economía y la Sociedad Digitales, España, con los datos de 2022, momento de publicación del informe, ocupaba el séptimo puesto entre los 27 países miembros de la UE, destacando una significativa mejora en varios de los elementos que se tienen en cuenta, como todo lo referido a la integración de la tecnología digital (puesto 11, cinco puestos mejor que en 2021), servicios públicos digitales (puesto 5, dos por encima de 2021) y capital humano (puesto 10 frente al 12 de 2021). Además, España es uno de los líderes de la UE en cuanto a la conectividad, donde ocupa el puesto 3 por segundo año consecutivo.



Fuente:

Índice de la Economía y la Sociedad Digitales (2022)

CLICA EN LA IMAGEN PARA VER LA GALERÍA COMPLETA

UN PUESTO DESTACADO EN SERVICIOS PÚBLICOS DIGITALES

Si ponemos el foco en los servicios públicos digitales, como decíamos, España ocupa el quinto puesto de la UE (séptimo en 2021) con una puntuación de 83,5, muy por encima de la media de la Unión Europea, que se sitúa en 67,3.

Este análisis de los servicios públicos digitales tiene en cuenta cinco indicadores, como son los usuarios de la administración electrónica (el 73% de los ciudadanos participa activamente en la administración electrónica, ocho puntos por encima de la media de la Unión Europea), los formularios precumplimentados (que miden la información que comparten las administraciones, un apartado en el que España obtiene un total de 78 puntos, frente al 64% de la media europea, gracias a la Plataforma de Intermediación de Datos), los servicios públicos digitales para los ciudadanos (87 puntos, 12 por encima de la media europea), los servicios públicos digitales para empresas (un 94 frente a los 82 puntos de la media) y los datos abiertos (España ocupa el tercer peldaño del podio con un 95%, 14 puntos más que la media de los países de la UE).

En cuanto a la conectividad digital, España es uno de los países de la UE que mejores resultados obtiene, con el avance en el despliegue de redes de muy alta capacidad

COMPROMISO CON LA MODERNIZACIÓN DE LA ADMINISTRACIÓN PÚBLICA

Tal y como se destaca en el informe, “España está comprometida con la modernización de la Administración Pública para hacerla más accesible para las empresas y el público en general y está desarrollando de forma proactiva nuevos servicios, sobre todo en los ámbitos de la salud, la identificación digital, la ciberseguridad, las aplicaciones móviles y la integración de la inteligencia artificial en el sector”.

Con todos estos datos, el Índice de la Economía y la Sociedad Digitales concluye que “España está a la vanguardia en administración electrónica y servicios públicos digitales en la UE. Continúa actualizando sus servicios e infraestructura para adap-

tarlos a los rápidos desarrollos tecnológicos y a las necesidades de las personas y las empresas. La interoperabilidad a nivel nacional, regional y local será clave para garantizar una transición digital fluida y eficiente entre los niveles de administración, maximizando los recursos y evitando solapamientos".

LUCES Y SOMBRAS EN EL APARTADO DE CAPITAL HUMANO

Sin embargo, no todo son parabienes, y, si bien España obtiene dentro de capital humano resultados relativamente buenos en habilidades digitales básicas, se sitúa por debajo de la media de los 27 en lo que respecta a la proporción de especialistas y de titulados en TIC.

En cuanto a la integración de las tecnologías digitales, el porcentaje de pymes con un nivel básico de intensidad digital y que utilizan las redes sociales es superior a la media de la UE, si bien las empresas españolas siguen rezagadas en tecnologías nuevas y avanzadas como la nube o los macrodatos.

MÚLTIPLES PROYECTOS DE INTERÉS

Más allá de las cifras, las diferentes Administraciones Públicas españolas siguen poniendo en marcha un gran número de proyectos e iniciativas de las que pueden estar

LA ADMINISTRACIÓN ELECTRÓNICA EN ESPAÑA ES UNA DE LAS MÁS SÓLIDAS DE EUROPA

El Informe Sociedad Digital en España 2023, publicado por Fundación Telefónica, incide en que la relación de la ciudadanía con las Administraciones Públicas a través de medios digitales es cada vez más intensa. El fuerte impulso a la administración electrónica durante la pandemia ha continuado tras la vuelta a la normalidad. El 79,7% de las personas de entre 16 y 74 años utilizaron en 2022 páginas web o aplicaciones móviles de alguna Administración. La actividad más usual es la descarga de formularios oficiales (63,5%), seguida de las interacciones relacionadas con el acceso a la información (56,3%).

La tramitación electrónica de servicios públicos de la Administración General del Estado ha continuado creciendo en 2022. El 91,9% de todos los trámites realizados con la AGE se llevaron a cabo mediante medios electrónicos, 1,5 puntos más que en 2021. El crecimiento del porcentaje de tramitación electrónica ha sido mucho mayor considerando los servicios ofrecidos a ciudadanos (el 87,8% en 2021 frente al 93,3% en 2022) que en el ámbito de las empresas (el 97,2% en 2021 frente al 99,2% en 2022).

El sistema Cl@ve se ha convertido en uno de los principales impulsores de la Administración electrónica en España, ya que proporciona un procedimiento de acceso sencillo y seguro a multitud de trámites. Prueba de su popularidad es el incesante incremento de su utilización. En 2022 se habían realizado más de 965 millones de autenticaciones mediante este sistema, lo que supone un crecimiento del 35,3% respecto a 2021.

SEGÚN EL ÍNDICE DE ECONOMÍA Y SOCIEDAD DIGITALES, ESPAÑA OCUPA EL SÉPTIMO PUESTO ENTRE LOS 27 PAÍSES MIEMBROS DE LA UE, DESTACANDO UNA SIGNIFICATIVA MEJORA EN LOS ÚLTIMOS DOCE MESES

puntualmente informados en nuestra web Administración Pública Digital.

Por destacar algunos de los más significativos, hemos de recordar los Espacios de Datos creados para sectores tan importantes para la economía del país y para los servicios a los ciudadanos como son el Turismo, la Salud, o la Justicia.

En todos los casos, se trata de infraestructuras pensadas como repositorios centrales de datos con los que las diferentes instituciones, así como las empresas y los ciudadanos, pueda interactuar para proporcionar mejores servicios.

Otro de los proyectos importantes puesto en marcha en España en los últimos meses es la Red Nacional de SOC, una entidad que, impulsada por el Centro Criptológico Nacional, coordina la colaboración y el intercambio de información entre los Centros de Operaciones de Ciberseguridad del sector público. El objetivo de esta red es mejorar la seguridad de todos los organismos públicos, gracias también a la ayuda de empresas proveedoras de servicios de seguridad gestionada que trabajen para este tipo de centros. Un claro ejemplo de colaboración público-privada en el ámbito de la ciberseguridad.

¿QUÉ EXPERIENCIA ESPERAN LOS CIUDADANOS DE LOS SERVICIOS PÚBLICOS?

Según el informe de Accenture La experiencia del servicio público a través de una nueva lente, los ciudadanos de hasta nueve países de todo el mundo, entre ellos España, demandan servicios públicos digitales sencillos e intuitivos que sean seguros y garanticen la protección de la privacidad. Además, y de forma complementaria, también quieren acceder a los servicios de manera presencial o telefónica.

El estudio, basado en los resultados de la encuesta realizada en diferentes países de Norteamérica, Europa y Asia-Pacífico, concluye que a medida que los servicios públicos se modernizan, deben centrarse en mantener la sencillez. En este sentido, los datos revelan que más de la mitad (53%) de los españoles desea una mayor interacción digital con las administraciones, 14 puntos por encima de la media global, que se sitúa en 39%.

Los encuestados dan prioridad a la facilidad de uso y a la confianza en la seguridad y privacidad de los datos a la hora de optar por utilizar los servicios digitales. El 57% de los españoles está dispuesto a compartir más datos personales con las administraciones si ello les permite utilizar servicios más personalizados, con mayor comodidad y eficiencia. La encuesta también revela que únicamente el 13% de los españoles indica que su nivel de relación con las Administraciones Públicas sería superior si tuviera más confianza en la seguridad y privacidad de la información.

SI PONEMOS EL FOCO EN LOS SERVICIOS PÚBLICOS DIGITALES, ESPAÑA SUBE AL QUINTO PUESTO EN EL RANKING DE LA UE

En esta misma línea de interoperabilidad este instituciones debemos colocar la Red SARA (Sistemas de Aplicaciones y Redes para las Administraciones, que sus responsables definen como "un conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las Administraciones Públicas Españolas e Instituciones Europeas facilitando el intercambio de información y el acceso a los servicios".

APPS Y SERVICIOS A LOS CIUDADANOS

Más allá de estas infraestructuras, son muchas las aplicaciones y servicios digitales puestos en marcha por el gobierno central, las comunidades autónomas, las diputaciones, los ayuntamientos, los cabildos... como para referenciarlas todas, pero, sin ánimo de ser exhaustivos, podemos recordar algunos de los ejemplos más destacados que se han unido a la lista, como Cartera Digital, una iniciativa para gestionar la identidad digital en el mundo universitario; la Tarjeta Sanitaria Virtual de la Comunidad de Madrid, que, recientemente, ha ampliado su oferta de servicios; Mi Carpeta Ciudadana, que ha alcanzado ya la tercera versión con nuevos servicios incorporados; o la Dirección Electrónica Habilitada Única, donde desde mayo se han empezado también a publicar las notificaciones de la Seguridad Social. ■

CONTENIDO RELACIONADO

Índice de Economía y Sociedad Digitales

Datos de España en el Índice de la Economía y la Sociedad Digitales

HYPERINTELLIGENCE®

Las respuestas le encontrarán

MicroStrategy®
Intelligence Everywhere

DAVID NAVAMUEL, EXPERTO EN SERVICIOS PÚBLICOS DIGITALES DE INECO

"VAMOS HACIA UN MODELO MÁS ORIENTADO A PONER AL CIUDADANO EN EL CENTRO"

Avanzar hacia una Administración moderna es el objetivo principal del Plan de Digitalización de las Administraciones Públicas 2021-2025. Se trata de uno de los elementos principales del componente 11 del Plan de Recuperación, Transformación y Resiliencia, y recoge el desarrollo de las actuaciones concretas que se llevan a cabo dentro del ámbito de la Administración digital.

Para hablar de lo que supone una Administración Pública moderna y de en qué punto del camino nos encontramos, conversamos en el V Foro IT User/Administración Pública Digital, Modernización del Sector Público: estado de las iniciativas digitales, con David Navamuel, Experto en Servicios Públicos Digitales de INECO, que recordaba que esta iniciativa surge "en el contexto provocado por la pandemia, y no es una actuación aislada, porque se han dado pasos a varios niveles, tanto en la prestación de servicios públicos como en el propio trabajo y el día a día de la Administra-

Sobre el avance de la digitalización en la Administración habló David Navamuel durante su entrevista en el Foro.

ción". Para este responsable, "el plan tiene dos partes, una, paliar los efectos de la pandemia, y, otra, preparar nuestras infraestructuras y sistemas para situaciones similares, y que estemos mejor preparados para poder afrontarlas".

UN COMPLEJO SISTEMA ADMINISTRATIVO

Para David Navamuel, "nuestro sistema es particular, porque tenemos una pluralidad de entidades administrativas en diferentes niveles: estado, comunidades autónomas y muchas entidades locales, con algunas entidades intermedias, que pueden ser consorcios, diputaciones e incluso agrupaciones, que exigen tener unos mecanismos de concertación, de colaboración. También hay otro plano, más vertical, entre una administración más pura, que puede ser la administración que viene de los ministerios o de las consejerías de las comunidades autónomas, y una administración que es un poquito más difusa, pero que también ejerce en potestades administrativas y presta en servicios públicos, el sector público empresarial. Y todo eso pasando por modelos de agencias, organismos autónomos, fundaciones públicas... que prestan servicios. Ese plan de digitalización busca mejorar la eficiencia en los procesos de la administración pública y mejorar esto significa también simplificar".

Para David Navamuel , "la simplificación administrativa es una tendencia que viene desde hace muchísimos años, si bien se ha apoyado últimamente la tecnología. Venimos de una administración que es muy garantista, que busca proteger al usuario de los servicios públicos, y eso exige mucho movimiento burocrático. Pero estamos avanzando hacia un modelo más orientado a la calidad, al servicio, a poner al ciudadano en el centro, y lo que le interesa es percibir y recibir ese servicio, finalmente. A partir de la promulgación de la Ley 11 de 2007, se pidió que la digitalización de la administración, la transformación digital, fuera acompañada en las situaciones administrativas, los procedimientos, siempre de una simplificación previa".

AVANZAR EN LA SIMPLIFICACIÓN Y LA INTEROPERATIBILIDAD

Para avanzar en esta simplificación, "lo más básico es la capacidad que tenemos de diagramar los procedimientos, de transformarlos en un sistema lógico, es un punto en común. Esto servía para tener no solamente una simplificación, sino una buena regulación. El siguiente paso era lógico, con no-code o low-code transformar en código esta representación. La simplificación ayuda muchísimo con la interoperabilidad y la consulta de datos. Y ese es uno de los elementos clave".

Y es que otro de los objetivos de esta digitalización era la interoperatibilidad. Para David Navamuel, "esta capacidad se basa, sobre todo, en que el dato sea la herramienta sobre la cual pivotan los servicios públicos. Y no hablamos solo de procedimientos o de prestación de servicios, sino que también la Administración tiene una función importante, la ejecución e implementación de políticas públicas. Estos modelos tienen que estar basados en datos y, además, en diferentes fuentes de datos. El hecho de que los datos sean interoperables y vengan de una fuente homogénea es una de las tendencias que se está persiguiendo".

Por último, también ha habido cambios en la adquisición de tecnología, que "ha tenido su propio proceso de simplificación buscando más agilidad y la homologación de determinados proveedores en sistemas dinámicos, en acuerdos marco". ■

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

ESTRATEGIAS PARA UNA ADMINISTRACIÓN DATA-DRIVEN

Sobre cómo crear una Administración data-driven conversaron los portavoces de Ministerio de Asuntos Económicos y Transformación Digital, Ministerio de Hacienda y Función Pública, Junta de Andalucía, Diputación de Cáceres, Madrid Digital, Ayuntamiento de Alcobendas, Universidad Complutense de Madrid, y MicroStrategy.

POTENCIAR LAS CAPACIDADES DE LAS INSTITUCIONES PÚBLICAS PARA LOGRAR UNA ADMINISTRACIÓN MODERNA PASA POR APROVECHAR EL VALOR DE LOS DATOS. EL SECTOR PÚBLICO ES UN GRAN REPOSITORIO DE INFORMACIÓN DE CIUDADANOS, EMPRESAS E INSTITUCIONES, PERO ES IMPRESCINDIBLE UNA ADECUADA GESTIÓN Y GOBIERNO DE ESTOS PARA OFRECER LA INTEROPERATIBILIDAD Y TRANSPARENCIA NECESARIA A LA HORA DE PROPORCIONAR LOS SERVICIOS A LOS CIUDADANOS.

Para hablar de estas y otras cuestiones, así como de avanzar hacia una Administración data-driven, en la primera mesa redonda del V Foro IT User/Administración Pública Digital, Modernización del Sector Público: estado de las iniciativas digitales, participaron portavoces de **Ministerio de Asuntos Económicos y Transformación Digital, Ministerio de Hacienda y Función Pública, Junta de Andalucía, Diputación de Cáceres, Madrid Digital, Ayuntamiento**

de Alcobendas, Universidad Complutense de Madrid, y MicroStrategy.

OBJETIVOS DE UNA ADMINISTRACIÓN REGIDA POR LOS DATOS

El primero de los temas del debate fue qué objetivos deben definir las actuaciones de una Administración regida por los datos y a qué reto deben enfrentarse. En opinión de Santiago Graña Domínguez, Subdirector General de Planificación y Gobernanza de la Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, "los fines deben ser la simplificación y facilitación de la vida de los ciudadanos, la creación de nuevos servicios activos y la reutilización de la información para el sector privado para realimentar la economía del dato. Tenemos que vigilar la calidad del dato, fomentar la interoperabilidad del dato y protegerlo".

Para Ana María Porras del Río, Jefa de Área de la División de Tecnologías de la Información de la Secretaría de Estado de Función Pública del Ministerio de Hacienda y Función Pública, "lo importante es que la Transformación Digital tiene que venir acompañada de un cambio cultural y organizativo. Tenemos que crear equipos multidisciplinares de expertos para aprovechar los datos. Estos son los principales retos".

En palabras de Jesús Carrillo Castrillo, Subdirector de Calidad, Investigación y Gestión del Conocimiento de la Secretaría General de Salud Pública e I+D+i de la Junta de Andalucía, "el principio básico es, además de la calidad del dato, contar con la información que necesitamos. Además, los datos deben ser útiles, tanto para la Administración como para el ciudadano, y que su uso sea correcto y seguro".

Coincidía con ellos Agustín Aretio, Jefe de Área de Innovación y Provincia Digital de la Diputación de Cáceres, que añadía que "el mayor reto es la transformación cultural de quien usa y recibe los datos. Nuestro papel es conseguir que los ayuntamientos vean en los datos un valor y poder avanzar a con-

"ESTAMOS TRABAJANDO EN LA PLATAFORMA DE INTERMEDIACIÓN DE DATOS, PARA FACILITAR EL INTERCAMBIO DE INFORMACIÓN"

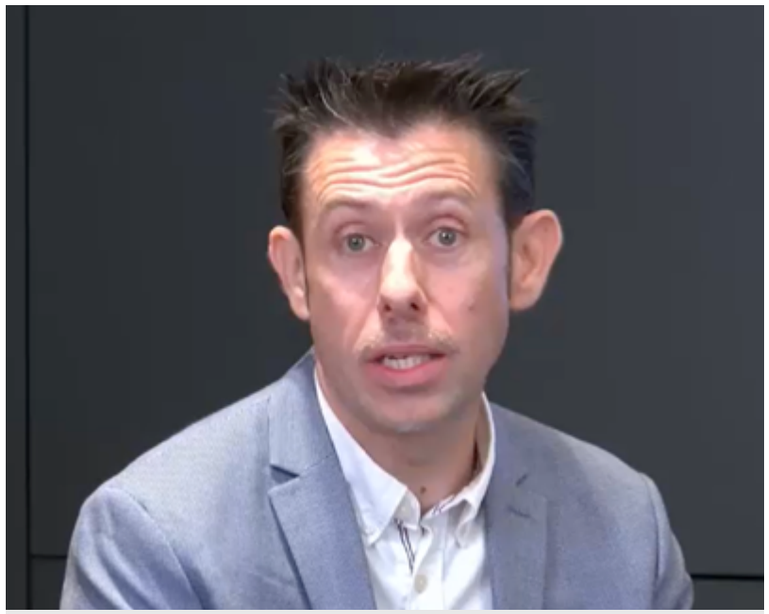
Santiago Graña, SG de Planificación y Gobernanza de la Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital

"ACTUALMENTE EL ARCHIVADO ESTÁ MUY ORIENTADO AL DOCUMENTO, Y TENEMOS QUE APORTAR LA VISIÓN DEL DATO"

Ana María Porras,
Jefa de Área de la División de TI de la Secretaría de Estado de Función Pública

ceptos como los de Territorios Inteligentes o Destinos Turísticos Inteligentes".

Según José Arbués Bedía, Director del Centro de Inteligencia Institucional de la Universidad Complutense de Madrid, "el gobierno apoyado en datos se basa en tres pilares, la gobernanza del dato, el valor público y la confianza. La gobernanza pasa por el liderazgo para implantar el modelo; el valor público con poner al ciudadano en el centro; y la confianza es el punto esencial, la palanca de la transformación en la Administración Pública tiene que ver con la transparencia de los datos".



"DESDE LA ADMINISTRACIÓN LOCAL, DEBEMOS PONER EL FOCO EN LAS PERSONAS PARA OFRECER MEJORES SERVICIOS, EN EL TERRITORIO, Y EN EL ÁMBITO TRIBUTARIO"

Roberto Magro Pedroviejo,
Jefe de Servicios Interactivos del Ayuntamiento de Alcobendas

Desde la perspectiva de Roberto Magro Pedroviejo, Jefe de Servicios Interactivos del Ayuntamiento de Alcobendas, la estrategia de gobierno del dato pasa por tres ejes principales: "el que tiene que ver con procesos y procedimientos; el relativo a las personas y su capacitación, el aprovechamiento de aportaciones externas y la captación de talento; y la tecnología, que es el medio capacitador".

Finalizaba esta primera ronda de opiniones Marta Bilbao Egido, Directora de Innovación, Datos y Transformación Digital de Madrid Digital, que comentaba que los objetivos son "facilitar la interoperabilidad, diseñar servicios personalizados y basados en datos, ofrecer datos en formato analizado o abierto al ciudadano, garantizar la transparencia y optimizar el trabajo de los empleados públicos con datos e inteligencia artificial. Para ello, debemos garantizar la calidad, la soberanía, la seguridad y la confidencialidad de los datos".

TRANSFORMACIÓN DE LA ADMINISTRACIÓN, EN LA PRÁCTICA

A la hora de repasar proyectos ya en marcha, Jesús Carrillo (Junta de Andalucía) exponía dos ejemplos. Primero, "estamos desarrollando un decreto para el uso secundario de los datos, y, segundo, aprovechar los datos para hacer investigación. Además, estamos trabajando en una aplicación para que

"EL MAYOR RETO ES LA TRANSFORMACIÓN CULTURAL DE QUIEN USA Y RECIBE LOS DATOS"

Agustín Aretio,
Jefe de Área de Innovación y Provincia Digital de la Diputación de Cáceres

“DEBEMOS GARANTIZAR LA CALIDAD, LA SOBERANÍA, LA SEGURIDAD Y LA CONFIDENCIALIDAD DE LOS DATOS”

Marta Bilbao,
Directora de Innovación, Datos y Transformación Digital de Madrid Digital

el ciudadano pueda conocer exactamente qué datos tiene sobre él la administración de salud, en aras de apostar por la total transparencia”.

Continuaba Ana María Porras del Río (Ministerio de Hacienda y Función Pública) comentando que “llevamos años publicando los datos estadísticos de empleo en Administraciones Públicas, y el reto ahora es obtener más valor de toda esta información y facilitar una explotación más exhaustiva. Pero es importante saber que los datos no son de la Administración, sino de los ciudadanos”.

En el caso de Santiago Graña (Ministerio de Asuntos Económicos y Transformación Digital) apuntaba que “estamos trabajando en la Plataforma de Intermediación de Datos, para facilitar el intercambio de información, con la que el año pasado conseguimos ahorrar al ciudadano más de 260 millones de consultas de más de 2.000 entidades usándola. Para la reutilización de datos, la iniciativa Porta, para fomentar la economía del dato. Y Carpeta Ciudadana, para el acceso a más de una treintena de servicios por parte del ciudadano”.

En palabras de Marta Bilbao (Madrid Digital), “hemos trabajado en cuadros de mando para consumo interno y externo de los datos, y portales de datos abiertos. Además, estamos trabajando en el despliegue de la IA para personalizar servicios, predecir y facilitar el trabajo del empleado público, y en el proyecto Cuenta Digital, que busca conseguir la personalización de los servicios y la creación de un área privada específica y personal para el ciudadano”.

“EL FUTURO VA A IR MUY DE LA MANO DEL INCREMENTO DEL USO SECUNDARIO DE LOS DATOS PARA LA INVESTIGACIÓN”

Jesús Carrillo, Subdirector de Calidad, Investigación y Gestión del Conocimiento de la SG de Salud Pública e I+D+i de la Junta de Andalucía

En el caso de Roberto Magro (Ayuntamiento de Alcobendas), “el año pasado arrancamos con la creación de un data lake de movilidad. Hemos construido de un centro de control en el ayuntamiento para conocer en tiempo real cómo late la ciudad. Debemos poner el foco en las personas para ofrecer

mejores servicios, en el territorio, y en el ámbito tributario. Por otra parte, estamos liderando proyectos para favorecer la apertura de datos de las diferentes administraciones".

Añadía José Arbués (Universidad Complutense de Madrid) que, en su caso, "tenemos el portal UniversiDATA para publicar datos abiertos de forma común por parte de varias universidades para favorecer no solo el acceso, sino la comparabilidad. Además, somos reutilizadores de datos, publicando informes a partir de esta información".

Por su parte, Agustín Aretio (Diputación de Cáceres) explicaba que "hemos estado trabajando en la integración con sistemas de notificaciones y situación de expedientes de todas las administraciones locales. Una herramienta sencilla y muy potente de servicio al ciudadano. Además, hemos analizado la calidad y el uso de los datos que tenemos para poder implementar posibles mejoras".

"LA PALANCA DE LA TRANSFORMACIÓN EN LA ADMINISTRACIÓN PÚBLICA TIENE QUE VER CON LA TRANSPARENCIA DE LOS DATOS"

José Arbués,
Director del Centro de Inteligencia Institucional de la UCM

PRÓXIMOS PASOS

De cara a futuro, apuntaba Marta Bilbao (Madrid Digital), "tenemos que poner en marcha la Cuenta Digital, incrementando los servicios e integrándonos con otras administraciones. Además, queremos montar y desarrollar la Oficina del Dato y seguir apostando por la IA, garantizando, eso sí, la seguridad de los datos".

En el caso de Roberto Magro (Ayuntamiento de Alcobendas), explicaba que hay que poner el foco "en el gobierno del dato, porque con la información es más fácil gobernar. Pero hay mucho trabajo de back-office y de colaboración con otras administraciones".

En palabras de José Arbués (Universidad Complutense de Madrid), "estamos centrados en controlar el efecto que se provoca al medir a partir de la información que tenemos. No podemos avanzar sin sentar las bases".

Para Agustín Aretio (Diputación de Cáceres), "vamos a insistir mucho en la implantación de la cultura del dato en las administraciones locales. Desarrollar casos de

"VOLUMEN DE DATOS, INTEROPERABILIDAD, SEGURIDAD, CONECTIVIDAD, TRANSFORMACIÓN CULTURAL, GOBERNANZA, CALIDAD... SON LOS PRINCIPALES RETOS DE LA ADMINISTRACIÓN"

Severino Gala, Country Manager para España y Portugal de MicroStrategy

uso concretos para que otras entidades se sumen es esencial para nosotros. Paralelamente, trabajamos en la gobernanza del dato para poder aprovechar toda la información disponible".

En opinión de Jesús Carrillo (Junta de Andalucía), "el futuro va a ir muy de la mano del incremento de la investigación a partir de los datos, de ese uso secundario, muy relacionado con infraestructuras que tendremos que crear. Pensando en la IA, tenemos que definir claramente los criterios de usabilidad, y este será uno de los grandes retos y oportunidades de la inteligencia artificial en la Salud".

Desde la perspectiva de Ana María Porras del Río (Ministerio de Hacienda y Función Pública), "uno de los proyectos en los que estamos interesados es en la conservación de los datos, porque es fundamental para poder desarrollar todo lo demás. El archivado está muy orientado al documento, y tenemos que aportar la visión del dato".

Finalizaba Santiago Graña (Ministerio de Asuntos Económicos y Transformación Digital) indicando que "queremos consolidar una serie de infraestructuras creadas con financiación europea, crear un espacio común de datos para la Sanidad, y movilizar datos de alto valor para ponerlos a disposición del sector industrial".

LA VISIÓN DE LA INDUSTRIA

Al hilo de estos retos, proyectos y oportunidades, Severino Gala, Country Manager para España y Portugal de MicroStrategy, señalaba que "el volumen de datos, la interoperabilidad, la seguridad, la capacidad de conectarse, la transformación cultural, la gobernanza, la calidad, la semántica, la trazabilidad... son los principales retos de la Administración, y nuestro objetivo como compañía es resolver la problemática de una compañía muy intensiva en uso de datos y personal, lo que nos llevó a nuestra apuesta por la escalabilidad, seguridad, gobernabilidad del dato e interoperabilidad, además de la integración de la IA. Por eso somos un claro candidato para ayudar a la Administración Pública con estos retos". ■

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

FlexxClient

by Flexxible®

FERNANDO GUTIÉRREZ-CABELLO, RESPONSABLE DE SECTOR PÚBLICO DE MICROSTRATEGY

"LOS DATOS SON ESENCIALES PARA TOMAR LA MEJOR DECISIÓN POSIBLE"

El elemento central de la transformación de la Administración Pública es el dato. De hecho, las diferentes instituciones del sector público generan y controlan una cantidad ingente de datos, y de su correcto aprovechamiento depende la creación de servicios ágiles, eficientes y modernos para los ciudadanos.

Pero es necesario contar con las políticas y las herramientas necesarias para afrontar los retos que esta modernización plantea, y poder aprovechar las oportunidades que se abren. Y de ello habló Fernando Gutiérrez-Cabello, Responsable de Sector Público de MicroStrategy, en su intervención en el V Foro IT User/Administración Pública Digital, Modernización del Sector Público: estado de las iniciativas digitales, donde recordaba que "los clientes se enfrentan a cuatro retos, principalmente: el gobierno del dato, la interoperatibilidad, el autoservicio y la seguridad".

El dato como elemento esencial para la mejora de los servicios públicos, fue el foco de la intervención de Fernando Gutiérrez-Cabello.

Según nos explicaba Fernando Gutiérrez-Cabello, "trabajamos con nuestros clientes para resolver estos retos a los que se enfrentan. Nuestra estrategia se basa en la inteligencia. Y cuando decimos inteligencia nos referimos al dato en cualquier lugar. Estamos hablando de compañías data driven, y hemos flexibilizado la plataforma para poder llegar a cualquier lugar y permitirles tomar decisiones apoyados en la información".

En opinión de este responsable, “la escalabilidad es un elemento fundamental, porque cuando quieres llevar esta visión a toda la organización, puedes tener problemas, ya sea por la escalabilidad de usuarios o de volúmenes de datos. Algo especialmente importante en la Administración, que tiene tanto muchos usuarios como un altísimo volumen de datos”.

MÚLTIPLES ASPECTOS A TENER EN CUENTA

En MicroStrategy, “tenemos características propias de gobierno del dato, un concepto muy amplio, pero que tiene dos elementos a tener en cuenta: el origen y la calidad del dato, y cómo aplicamos ese gobierno en la exportación del dato; y apuntamos a la interoperabilidad de autoservicio, con la flexibilidad, dado que hemos flexibilizado la herramienta para poder cubrir cualquier caso de uso, apoyándonos en un motor de API para interoperar con cualquier organismo”.

“Y, por último”, añadía, “una seguridad robusta centralizada, porque, cuanto más extiendes el dato en la organización, más control de seguridad hay que poner en ello”.

UNA VISIÓN DIFERENTE

Un aspecto distintivo de la estrategia de MicroStrategy es cómo se explotan los datos. Nos explicaba Fernando Gutiérrez-Cabello que “si no controlamos cómo explotamos la información, podemos echar a perder el trabajo realizado para asegurar la calidad del dato. Los pasos para crear un repositorio de datos, con las especialización necesaria para la Administración, están claros, pero se debe exigir también que las herramientas de visualización tengan características de gobierno, y, en nuestro caso, establecemos una relación uno a uno entre el modelo que se crea y los diferentes tipos de análisis que vamos a realizar. Creamos un elemento único para cada dato que se usa en todos los análisis. Esta reutilización de objetos es la gran diferencia”.

Si apuntamos a la interoperatibilidad con otras entidades y organismos, indicaba Fernando Gutiérrez-Cabello, “hemos flexibilizado el software en base a API, lo que nos permite trabajar con dos elementos importantes: datos federados y analítica en bebida. En el primer caso, nos apoyamos en conectores entre las múltiples fuentes de datos para que puedan ser explotados, y, en el segundo, tenemos la capacidad de embeber esta información en cualquier portal o herramienta de visualización de datos”.

En cuanto al autoservicio, “nuestra plataforma lo permite, pero con unas características y elementos controlados, y sin necesidad de generar código ni conocimiento de lo que hay por debajo, como sucede en otras tecnologías”.

Y, sobre todo esto, “aportamos una tecnología innovadora que se llama HyperIntelligence, que consiste en indexar la información en el navegador, con una tarjeta que consolida la información más relevante de una o de varias fuentes, lo que cambia el paradigma del consumo del dato. No voy a buscar esa información, sino que la información me viene a buscar a mí para facilitar su consumo y la toma de decisiones basadas en datos, enriqueciendo aplicaciones existentes con datos de otras”. ■

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

POTENCIANDO UNA ADMINISTRACIÓN CAPAZ DE PROTEGERSE Y RECUPERARSE ANTE CIBERATAQUES

De la necesidad de avanzar hacia una Administración segura y resiliente debatieron los representantes de Generalitat Valenciana, Agencia Española de Protección de Datos, Universidad de Castilla-La Mancha, Ayuntamiento de Madrid, Ayuntamiento de Fuenlabrada, SonicWall Iberia, Sophos Iberia y WatchGuard.

PHISHING, MALWARE Y RANSOMWARE SON LAS AMENAZAS PRINCIPALES QUE SE CIERNEN SOBRE EL SECTOR PÚBLICO. LAS ADMINISTRACIONES SON UN OBJETIVO CLARO PARA LOS CIBERDELINCUENTES POR LA GRAN CANTIDAD DE INFORMACIÓN CONFIDENCIAL DE CIUDADANOS Y OTROS ORGANISMOS QUE MANEJAN LAS DIFERENTES INSTITUCIONES, PORQUE NO PODEMOS OLVIDAR QUE CUANDO UNA ENTIDAD PÚBLICA ES ATACADA SE ESTÁN COMPROMETIENDO LOS DATOS, PERO TAMBIÉN LOS SERVICIOS QUE OFRECE, Y TIENE UNA GRAN REPERCUSIÓN.

La ciberseguridad fue el foco de la segunda mesa redonda del V Foro IT User/Administración Pública Digital, Modernización del Sector Público: estado de las iniciativas digitales, que contó con la presencia y participación de representantes de **Generalitat Valenciana, Agencia Española de Protección de Datos, Universidad de Castilla-La Mancha, Ayuntamiento de Madrid, Ayuntamiento de Fuenlabrada, SonicWall Iberia, Sophos Iberia y WatchGuard.**

"EL PRINCIPAL OBJETIVO DEL REGLAMENTO DE PROTECCIÓN DE DATOS NO ES LA SEGURIDAD, ES GENERAR CONFIANZA"

Andrés Calvo, Jefe de Área de Innovación Tecnológica de la AEPD

MEJORANDO LA PROTECCIÓN

Con el objetivo de mejorar la protección ante los ataques que puede sufrir la Administración, Carmen Serrano Durbán, Subdirectora General de Ciberseguridad de la Generalitat Valenciana, explicaba que "las administraciones estamos haciendo grandes esfuerzos para adaptarnos al incremento de las amenazas y al nuevo contexto digital. Hemos adaptado nuestras estrategias de defensa y monitorización, porque el perímetro y los accesos han cambiado radicalmente, además de incorporar la nube y los dispositivos IoT. Asimismo, hemos aumentado la vigilancia y la detección temprana, y extendido estas capacidades a las pequeñas entidades de nuestra comunidad"

En palabras de Andrés Calvo Medina, Jefe de Área de Innovación Tecnológica de la Agencia Española de Protección de Datos, "el principal objetivo del Reglamento no es la seguridad, es generar confianza. Desde la Agencia, vamos creando documentos de referencia para entidades, y, en los últimos años, ante la difuminación del perímetro, hemos incrementado nuestros recursos a nivel operativo, porque el incremento de amenazas es parte de nuestro día a día. Y, partiendo de la idea de que la seguridad total no existe, tenemos que estar preparados para reaccionar ante un ataque, y proteger al ciudadano en todas las dimensiones".

Desde el punto de vista de Andrés Prado Domínguez, Responsable de Tecnología de la Universidad de Castilla-La Mancha, "nosotros sufrimos un ataque, y nuestra perspectiva ha cambiado desde entonces. La seguri-

"TRABAJAMOS PARA ELIMINAR LOS SILOS Y COORDINARNOS CON OTROS ORGANISMOS Y ENTIDADES"

David Povedano,
DG de Innovación y Transformación Digital del Ayuntamiento de Fuenlabrada

“ESTAMOS EN UN CAMINO DE TRANSFORMACIÓN DESDE EL ENTENDIMIENTO DE QUE EL PANORAMA DE AMENAZAS HA CRECIDO RÁPIDAMENTE”

José Ángel Álvarez, Head of Cibersecurity Center del Ayuntamiento de Madrid

dad desde el diseño la planteamos desde la perspectiva de que nos van a volver a atacar y que este ataque va a tener éxito. Partíamos de una estrategia de prevención y de cumplimiento normativo, y eso nos ha creado un sentimiento de autosatisfacción. Todo esto es necesario, pero el escenario ha cambiado, y con ello nuestra visión. Ahora apostamos por un perímetro multidimensional, no solo de puertas hacia fuera, en un entorno de confianza cero. Es necesario contar con recursos, pero es importante que estén bien organizados”.

Apuntaba José Ángel Álvarez Pérez, Head of Cibersecurity Center del Ayuntamiento de Madrid, que, en materia de ciberseguridad, “estamos en un camino de transformación desde el entendimiento de que el panorama de amenazas ha crecido rápidamente, desde la necesidad de ocuparse y dedicar recursos. Hemos ido creciendo hasta culminar con la creación del Centro de Ciberseguridad del Ayuntamiento de Madrid, y pasar de ser un departamento de TI del ayuntamiento a ser la clave de la ciberseguridad de la ciudad de Madrid”.

Concluía esta primera ronda de opiniones David Povedano Alonso, Director General de Innovación y Transformación Digital del Ayuntamiento de Fuenlabrada, indicando que “estamos formando una unidad de ciberseguridad dentro del departamento de sistemas con un enfoque multidisciplinar y poniendo a la persona en el centro. Asimismo, trabajamos para eliminar los silos y coordinarnos con otros organismos y entidades. Por último, tenemos que organizarnos desde la premisa de que esto no a va a ir a menos y las amenazas seguirán aumentando”.

“LAS ADMINISTRACIONES ESTAMOS HACIENDO GRANDES ESFUERZOS PARA ADAPTARNOS AL INCREMENTO DE LAS AMENAZAS Y AL NUEVO CONTEXTO DIGITAL”

Carmen Serrano, SG de Ciberseguridad de la Generalitat Valenciana

EL VALOR DE LA COLABORACIÓN PARA LA CIBERPROTECCIÓN

En palabras de Andrés Prado (Universidad de Castilla-La Mancha), “la colaboración es la línea a seguir. Hemos aprendido que solos no vamos a ninguna parte. Iniciativas como la Red de SOC, con colaboración público-priva-

“LA SEGURIDAD DESDE EL DISEÑO LA PLANTEAMOS DESDE LA PERSPECTIVA DE QUE NOS VAN A ATACAR Y QUE ESTE ATAQUE VA A TENER ÉXITO”

Andrés Prado,
Responsable de Tecnología de la UCM

da, y con un entorno de compartición de información y experiencias, es la única forma de tener éxito. Debemos ser capaces de entrar en esa dinámica, y asumir que los recursos no son solo financieros. Tenemos que cambiar los modelos con esta nueva perspectiva”.

Añadía José Ángel Álvarez Pérez (Ayuntamiento de Madrid) que “en la creación de nuestra unidad incrementamos los recursos, pero apostamos por las personas, y por eso multiplicamos por cuatro el número de personas que trabajan en ciberseguridad en el ayuntamiento. Es una apuesta muy definida. Demandamos servicios de ciberseguridad desde el ayuntamiento, y nos apoyamos en la colaboración público-privada para mejorarlos. La colaboración es imprescindible”.

Para David Povedano (Ayuntamiento de Fuenlabrada), “tenemos los primeros análisis desde la creación de nuestro SOC, y estamos avanzando en la organización y ampliación de la colaboración”.

Según Carmen Serrano (Generalitat Valenciana), “siempre hemos venido colaborando entre organizaciones, y hemos trabajado con la confianza que nos da este respaldo. Pero era algo centrado en entidades públicas, y ahora estamos potenciando la compartición de información con el sector privado. Estamos empezando, pero ese es el camino, y tenemos que potenciarlo. Hay que trabajar desde la premisa de optimizar recursos y apoyarnos en otras entidades”.

Desde el punto de vista de Andrés Calvo (Agencia Española de Protección de Datos), “por nuestra naturaleza, trabajamos estrechamente con el Centro Criptológico Nacional y con INCIBE. Pero el Reglamento nos

“PARA REDUCIR LA SUPERFICIE DE EXPOSICIÓN A LOS RIESGOS, HAY QUE IMPLEMENTAR PLANES, POLÍTICAS, SISTEMAS DE GESTIÓN Y LAS MEJORES HERRAMIENTAS POSIBLES A NIVEL DE DETECCIÓN Y PROTECCIÓN”

Eduardo Brenes,
Territory Manager de SonicWall Iberia

habla de coordinación con otras entidades de control, nacionales e internacionales. Además, trabajamos con el sector privado a través de organizaciones de protección de datos y privacidad, y los resultados han sido muy buenos”.

BUENAS PRACTICAS PARA PROTEGERSE Y RECUPERARSE

Tal y como explicaba David Povedano (Ayuntamiento de Fuenlabrada), “la forma-

ción es esencial, pero sigue faltando mucha concienciación todavía, porque los ataques crecen exponencialmente. Pero no podemos ver la seguridad como algo estanco, sin relación con otros departamentos o áreas. Tenemos que subirnos todos al mismo barco y trabajar como equipo. Hay que trasladar una estrategia unificada, soportada a nivel directivo y con todas las garantías normativas".

Para José Ángel Álvarez Pérez (Ayuntamiento de Madrid), "a veces se ve al departamento de ciberseguridad como un enemigo, y esa visión nos lleva a la extinción. Tienen que vernos como aliados e interactuar con otras unidades. Tenemos que ayudarles, que nos vean como un copiloto de confianza. No vamos a dirigir hacia dónde va la organización, pero sí vamos a acompañarla en ese viaje. Es importante también ver dónde están nuestras debilidades para protegernos mejor".

En opinión de Andrés Prado (Universidad de Castilla-La Mancha), "son muy importantes las personas. Hay que poner en valor el perfil del trabajador público, pero también empoderarlo, formarlo... porque la amenaza avanza a un ritmo mayor. De cara a los ciudadanos, los estudiantes en nuestro caso, necesitamos potenciar sus capacidades digitales en seguridad".

"PROPORCIONAMOS LO QUE CADA ENTIDAD NECESITA PARA ALINEAR LOS PROCESOS, LAS HERRAMIENTAS Y PERSONAS"

Álvaro Fernández,
Sales Manager de Sophos Iberia

"TRABAJAMOS CON UNA VISIÓN DE CONFIANZA ZERO, LO QUE NOS OBLIGA A ANALIZAR MUCHO MÁS CADA INTERACCIÓN"

Carlos Castro, Strategic Account Manager de WatchGuard

En el caso de Andrés Calvo (Agencia Española de Protección de Datos), explica que "es muy importante tener recursos humanos, pero también que sean de calidad y que se prolonguen en el tiempo. La formación es clave, tanto en protección de datos como en seguridad. Hay que concienciar al funcionario del valor de su identidad y de su trabajo, y de su papel ante los ataques".

Concluía Carmen Serrano (Generalitat Valenciana) incidiendo en el valor de las personas. "El perímetro está en la persona, el dispositivo y su entorno. Es una labor que hay que hacer a nivel de sociedad, no solo para que tengan el conocimiento de seguridad, sino para que sean aliados nuestros en la protección. Por otra parte, la ciberseguridad debe estar en todos los proyectos desde el principio y de forma transversal".

LA VISIÓN DE LA INDUSTRIA

Para aportar el punto de vista de la industria de ciberseguridad, Eduardo Brenes, Territory Manager de SonicWall Iberia, explicaba que “muchas veces, con pocos recursos, sobre todo en entidades locales, se hace un gran trabajo. Para reducir la superficie de exposición a los riesgos, hay que implementar planes, políticas, sistemas de gestión y las mejores herramientas posibles a nivel de detección y protección. Pero también tenemos que desarrollar capacidades de ciberresiliencia para recuperarnos lo mas rápidamente posible de un ataque. Nuestras soluciones permiten reducir esa exposición de las Administraciones, complementando las diferentes piezas necesarias”.

En palabras de Álvaro Fernández, Sales Manager de Sophos Iberia, “el incremento de los ataques es brutal, así como su sofisticación. Al mismo tiempo, se ha incrementado el coste y la complejidad de las herramientas de protección, porque cada día hay que hacer mas cosas, y eso con unos recursos que no siempre son suficientes. Frente a esto, nosotros aportamos seguridad como servicio, adaptándonos a la realidad de cada cliente. Proporcionamos lo que cada entidad necesita para alinear los procesos, las herramientas y personas”.

Finalizaba Carlos Castro, Strategic Account Manager de WatchGuard, comentando que “hay muchas iniciativas para aglutinar y utilizar los datos. Nosotros trabajamos con una visión de Confianza Zero, lo que nos obliga a analizar mucho más cada interacción, utilizando tecnologías de automatización, como IA o Machine Learning, para poder ofrecer la información necesaria para que las personas puedan obtener valor y proteger a las organizaciones”. ■

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

DESCÁRGUELO AHORA EN:
SONICWALL.COM/THREATREPORT

2023

INFORME DE CIBERAMENAZAS DE SONICWALL

EL CAMBIANTE PANORAMA DEL CIBERCRIMEN

SONICWALL®

sonicwall.com | @SonicwallSpain

VÍCTOR MANUEL MONTORO,

DIPUTADO DELEGADO DE PROGRAMAS EUROPEOS Y ADMINISTRACIÓN ELECTRÓNICA DE DIPUTACIÓN DE CÓRDOBA

"EN SEGURIDAD, LA PREPARACIÓN Y LA ANTICIPACIÓN SON CLAVES"

Las Administraciones Públicas son uno de los claros objetivos de la ciberdelincuencia por la gran cantidad de datos de que disponen sus instituciones. Estar preparados para afrontar cualquier ataque es esencial para poder responder con garantías cuando ocurra, y contar con las herramientas adecuadas es solo una parte de la ecuación para el éxito.

Para poner negro sobre blanco la importancia de la ciberseguridad, en el V Foro IT User/Administración Pública Digital, Modernización del Sector Público: estado de las iniciativas digitales, Víctor Manuel Montoro, Diputado Delegado de Programas Europeos y Administración Electrónica de Diputación de Córdoba, expuso qué necesita la Administración Pública para poder responder ante cualquier amenaza que pueda surgir tanto para los datos como para la continuidad del servicio.

Víctor Manuel Montoro repasó las bases en las que se apoyaron para superar un ciberataque sufrido por la Diputación de Córdoba.

Tal y como explicaba este responsable, “si nos preparamos, tendremos muchas posibilidades de que el ataque que vamos a sufrir no sea catastrófico y podamos superarlo con garantías. En seguridad, la preparación y la anticipación es la clave. Y lo primero para prepararse es tener conciencia de qué va a ocurrir, porque, casi con total seguridad, todos vamos a sufrir un ciberataque a lo largo de la vida”.

ESTAR PREPARADOS PARA MINIMIZAR LOS DAÑOS

En palabras de Víctor Manuel Montoro, “hay que tomar medidas contundentes, incluso algunas que no van a recibir una buena acogida por el personal de la organización a la que cada uno pertenezcamos. Por ejemplo, la restricción del uso de los puertos USB o la necesidad de adoptar e incorporar contraseñas personales complejas”.

La Diputación de Córdoba “cuenta con una empresa de informática, Eprinsa, de la que soy el presidente, que lleva ya trabajando más de treinta años en mejorar las TI, y ha incorporado la ciberseguridad como un componente transversal que impregna todas aquellas aplicaciones o actuaciones que se ponen en marcha. Eso nos ha permitido reducir la superficie de exposición centralizando toda la seguridad en un gran CPD que da servicio a todos los entidades, y hemos segmentado las redes para que la transmisión de aquellos códigos maliciosos que puedan entrar en nuestro sistema no se extienda a toda la red”.

Por otra parte, recuerda Víctor Manuel Montoro que “Eprinsa se ha caracterizado por interactuar e interrelacionarse con todo tipo de entidades, tanto públicas como privadas, lo que ha permitido establecer sinergias y convenios de colaboración que hacen que este viaje sea más llevadero”.

PESE A TODO...

A pesar de todo, la Diputación de Córdoba sufrió un ciberataque “que fue detectado el miércoles 1 de febrero a las 5:40 de la madrugada. Se activaron todos los protocolos y esa maquinaria que habíamos preparado. Desde el primer momento, tanto el Centro Criptológico Nacional como la Agencia Digital de Andalucía no pararon de remitirnos informes y facilitarnos herramientas de ayuda. Con todo, la segmentación de las redes evitó que el intruso llegara hasta la información. Pero hay que tener en cuenta que 90 minutos después 3.500 usuarios iban a empezar a conectarse desde los propios servicios de la Diputación y todos los ayuntamientos. De ahí la necesidad de confeccionar un plan específico de comunicación que permitiera, por un lado, tener informados a todos los usuarios afectados, pero que también internamente se supiera qué estaba pasando y en qué punto exacto de resolución del problema estaba. Con todo, el sistema no dejó de funcionar. Todo el contingente que teníamos previsto funcionó a la perfección. Dimos servicio y localizamos dónde estaba la posible fuga, si bien prácticamente no se llevaron información, la podremos cuantificar en 10 gigas; no cedimos al chantaje y pudimos poner sobre la pista a las autoridades para que se fueran detenidos”.

En definitiva, las claves para sobrevivir a un ataque son, primero, “el personal de la organización, que tiene que estar comprometido y tener las suficiente competencias; una inversión continua y permanente en ciberseguridad; y un plan de comunicación que dé una respuesta contundente y específica”. ■

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

INFRAESTRUCTURAS TECNOLÓGICAS

QUE DAN SOPORTE A UNA NUEVA ADMINISTRACIÓN MÁS DIGITAL

PARA OPERAR EN EL ENTORNO DIGITAL ACTUAL, LAS ADMINISTRACIONES PÚBLICAS NECESITAN ECOSISTEMAS TECNOLÓGICOS FLEXIBLES, SOSTENIBLES Y RENTABLES, EN LÍNEA CON OTRAS REALIDADES DE LA SOCIEDAD. EN ESTA LÍNEA SE DESARROLLAN INICIATIVAS COMO LA CONSOLIDACIÓN DE LOS SERVICIOS DE INFRAESTRUCTURA DE PROCESAMIENTO DE DATOS Y CLOUD O LA IMPLANTACIÓN DE UN PUESTO DE TRABAJO DE NUEVA GENERACIÓN QUE FAVOREZCA LA MOVILIDAD Y LA COLABORACIÓN.

Sobre las infraestructuras modernas que soportan una Administración Pública más digital conversaron los portavoces de Gerencia Informática de la Seguridad Social, Dirección General de la Guardia Civil, ISDEFE, Sociedad Estatal de Infraestructuras para el Transporte Terrestre, Corporación de Radio y Televisión de Galicia, Flexxible y Schneider Electric.

Estos fueron los temas principales de debate de la última de las mesas redondas del V Foro IT User/Administración Pública Digital titulado Modernización del Sector Público: estado de las iniciativas digitales, en la que participaron portavoces de Gerencia Informática de la **Seguridad Social, Dirección General de la Guardia Civil, ISDEFE, Sociedad Estatal de Infraestructuras para el Transporte Terrestre, Corporación de Radio y Televisión de Galicia, Flexxible y Schneider Electric.**

DIFERENTES INICIATIVAS PUESTAS EN MARCHA

Para hablar de algunas de las iniciativas que se han ido poniendo en marcha por parte de la Administración Pública, Fernando Novo Martínez, Jefe de Área de Transformación y Modernización de la Gerencia Informática de la Seguridad Social, explicaba que "estamos evolucionando hacia un modelo de desarrollo mucho más sostenible, escalable, flexible... con tecnologías basadas en la nube, que nos permita poder ofrecer servicios digitales de calidad, pensando en el ciudadano y en la sostenibilidad en el tiempo. Sin olvidar que tenemos uno de los legacy más grande de España".

Para Enrique Ávila, Director del Centro de Análisis y Prospectiva del Gabinete Técnico de la Dirección General de la Guardia Civil, "tratamos de anticipar, a seis meses vista, para proporcionar seguridad interior, un servicio básico de cara a la ciudadanía. Proporcionamos seguridad tanto para nuestras propias infraestructuras como para fuera y, por eso, trabajamos en el desarrollo de un puesto de trabajo orientado al personal desplazado. Antes de la pandemia ya contábamos con 5.000 puestos de teletrabajo. Además, hemos puesto en marcha iniciativas para la detección temprana de talento desde 2019, y, estamos afrontando los problemas de despoblación con la integración de tecnología, como el proyecto de guardias civiles metahumanos hiperrealistas digitales".

En palabras de Ildefonso Vera, Director de Innovación, Procesos y Transformación Digital de ISDEFE, "la Administración Pública tiene que ver su modernización desde dos puntos de vista: los trabajadores y los ciudadanos. Estamos abordando los seis retos que tiene la Administración, esto es, cerrar la brecha de la experiencia de usuario entre el empleado y el ciudadano, transformar los sistemas legados en sistemas integrados, aportar innovación a los procesos internos y externos, aumento de la eficiencia, simplificación de la infraestructura, y la seguridad de la información".

Desde la perspectiva de Isabel Navarro Díez, Directora de Transformación Digital de la Sociedad Estatal de Infraestructuras para el Transporte Terrestre, "en nuestro plan estratégico a diez años, hemos definido seis

"TENEMOS LA INNOVACIÓN COMO ELEMENTO TRANSVERSAL A TODAS LAS ÁREAS, Y PARA ELLO, EL CONTROL DEL DATO ES FUNDAMENTAL"

Esther Medina,
Jefa del Servicio de Innovación
en el Entorno Digital de la CRTVG

líneas de actuación, y una de ellas, que tiene 35 iniciativas, es la referida a la digitalización y la transformación digital. Entre estas, hay iniciativas orientadas a digitalizar la sociedad, y otras a nuestro core de negocio, la explotación de las autopistas de peaje. Estamos estandarizando todas las funciones de peaje, llevando todo lo posible a la nube, tanto pública como privada. Necesitamos infraestructuras de transporte que sean sostenibles, seguras y conectadas. Sin olvidar dos aspectos que deben ser transversales: la gestión del dato y la ciberseguridad".

Finalizaba esta primera ronda de opiniones Esther Medina Ferreiro, Jefa del Servicio de Innovación en el Entorno Digital de la Corporación de Radio y Televisión de Galicia, que apuntaba "la tecnología marca nuestra estrategia y el negocio. En los últimos años hemos invertido en digitalización y en la creación de flujos de trabajo eficientes, y quizá es el cambio de cultura lo que más está costando. Ahora estamos trabajando en la digitalización de los sistemas de gestión interna, con proyectos de big data/data hub y de OTT, que afecta directamente en la creación, comercialización y distribución del contenido. Y para todo esto, necesitamos buscar talento digital y crear grupos interdisciplinares que puedan gestionar toda esta evolución".

ROL DE LA NUBE EN LAS ESTRATEGIAS TECNOLÓGICAS DE LA ADMINISTRACIÓN

Según explicaba Ildefonso Vera (ISDEFE), "empezamos nuestro viaje a la nube migrando el correo electrónico. Luego fuimos analizando qué cargas mover a la nube, porque no hay que llevar todo, sino solo que lo apoya al negocio y al trabajador. El principal reto son las personas, en la resistencia al cambio y en cómo les ayudamos en esta evolución. Lo que hemos hecho en este sentido es crear una línea de gestión del cambio y de cultura digital para aplicar a todos los proyectos, estableciendo objetivos e indicadores".

En palabras de Enrique Ávila (Dirección General de la Guardia Civil), "la nube supone un reto cultural y regulatorio. Este último afecta a nuestra regulación operativa, sobre todo cuando no tienes todo el control sobre esa nube. Por otra parte, están los servicios horizontales, donde hemos empezado un proceso de migración parcial. Ahí nos encontramos con la dificultad de renovar el talento para aprovechar al máximo las nuevas posibilidades que la tecnología te ofrecen. Y en esto nos está ayudando una estrategia de gamificación y recompensas".

Tal y como indica Fernando Novo Martínez (Gerencia Informática de la Seguridad Social), "hemos ido desarrollando servicios nativos en la nube para poder dar una respuesta rápida a las necesidades del ciudadano. Y un ejemplo es el Ingreso Mínimo Vi-

"NUESTRA LABOR ASISTENCIAL ES MÁS IMPORTANTE QUE LA SEGURIDAD, Y ESO REQUIERE RECOGER LA INFORMACIÓN DE TODAS LAS ACTUACIONES PARA PODER AYUDAR EN LA TOMA DE DECISIONES"

Enrique Ávila, Director del Centro de Análisis y Prospectiva del Gabinete Técnico de la DG de la Guardia Civil

tal. Pero la clave es cuál es el coste de migrar todo a la nube, sobre todo si tenemos en cuenta la cantidad de datos que poseemos. Hay que valorar las ventajas que nos puede aportar la nube y aprovecharlas. En nuestro caso, tenemos dos tipos de clientes, los tramitadores y funcionarios, cuyo número es tendente a bajar, y los ciudadanos de servicios digitales, que no paran de crecer y nos pueden generar picos de demanda muy altos que no podemos atender en nuestro CPD. Ahí es donde la nube nos da una oportunidad muy grande para diseñar servicios que puedan estar en la nube con los datos mínimos para proporcionar el servicio, de forma ágil. Por eso, estamos pensando en cambiar nuestro modelo de desarrollo a metodologías ágiles y la mentalidad de los trabajadores para que se oriente a producto, al servicio que tienes que ofrecer, y aquí entra en juego la apificación".

Añadía Esther Medina Ferreiro (Corporación de Radio y Televisión de Galicia) que, en su caso, "usamos la nube en dos líneas, para el proyecto de data hub, integrando todas las fuentes de datos para poder tomar decisiones, sobre todo porque son datos menos sensibles; por otro lado, para OTT, muy ligado a la producción, lo que nos permite flujos de trabajo más rápidos".

Para Isabel Navarro Díez (Sociedad Estatal de Infraestructuras para el Transporte Terrestre), "lo más importante es ayudar a las personas con el cambio, pero hay otro elemento fundamental: los procesos. Muchas veces nos enfocamos a la tecnología, y un proceso analógico deficiente, si no lo analizas, se convierte en un proceso digital deficiente. Nosotros nos hemos movido a la nube con el puesto de trabajo, con el análisis de datos y con el primer contacto con el cliente. Pero tenemos que mantener pequeños sistemas aislados on-premise para poder dar el ser-

"LA CLAVE ES CUÁL ES EL COSTE DE MIGRAR TODO A LA NUBE, SOBRE TODO SI TENEMOS EN CUENTA LA CANTIDAD DE DATOS QUE POSEEMOS"

Fernando Novo,
Jefe de Área de Transformación y Modernización de la GISS

"HEMOS ANALIZADO QUÉ CARGAS MOVER A LA NUBE, PORQUE NO HAY QUE LLEVAR TODO, SINO SOLO QUE LO APOYA AL NEGOCIO Y AL TRABAJADOR"

Ildefonso Vera,
Director de Innovación, Procesos y Transformación Digital de ISDEFE

vicio necesario en todo momento, así como servicios en nubes privadas".

ANALIZAR LOS RESULTADOS ANTES DE SEGUIR ADELANTE

Indicaba Esther Medina Ferreiro (Corporación de Radio y Televisión de Galicia) que

"MUCHAS VECES NOS ENFOCAMOS A LA TECNOLOGÍA, PERO UN PROCESO ANALÓGICO DEFICIENTE, SI NO LO ANALIZAS, SE CONVIERTE EN UN PROCESO DIGITAL DEFICIENTE"

Isabel Navarro Díez, Directora de Transformación Digital de la SEITT

"el ecosistema audiovisual está cambiando, así que o analizas los datos o estar perdido. Sobre todo, porque lo que no mides no puedes saber si funciona. Un ejemplo es el consumo de OTT, que nos están quitando una parte significativa de las audiencias; o el ajuste de la programación en función de los comportamientos de los usuarios. Tenemos la innovación como elemento transversal a todas las áreas, y para ello, el control del dato es fundamental".

Se mostraba de acuerdo Isabel Navarro Díez (Sociedad Estatal de Infraestructuras para el Transporte Terrestre), que añadía "que, a partir de los datos, hemos transformado alguno de los servicios que ofrecemos. Un ejemplo de ello es el pago on-line en algunos peajes y la introducción de los sistemas contact-less, algo que iremos ampliando al resto de las autopistas paulatinamente. Asimismo, los análisis de tendencias nos ayudan a dimensionar los servicios para optimizar la infraestructura".

En el caso de Ildefonso Vera (ISDEFE), "vamos dando pequeños pasos, pero firmes. Hemos estado documentando los procesos para poder realizar una reingeniería de estos desde un punto de vista funcional. Asimismo, hemos implementado herramientas de trabajo colaborativo, lo que ha supuesto un decrecimiento del uso de correo electrónico. Con todo, vamos avanzando y está repercutiendo muy positivamente en nuestro negocio".

Apuntaba Enrique Ávila (Dirección General de la Guardia Civil) que, "sobre todo en la España despoblada, nuestra labor asistencial es más importante que la seguridad, y eso requiere un despliegue tecnológico que nos permita recoger todas las actuaciones

"NOSOTROS PONEMOS EL FOCO EN ELIMINAR LA FRICCIÓN ENTRE EL EMPLEADO Y LA TECNOLOGÍA"

Manuel de Dios,
FlexxClient Director de Flexxible

para poder ayudar en la toma de decisiones. Tenemos integrada toda esa información para aprovecharla en beneficio de la ciudadanía. Ahora nos enfrentamos al reto de gestionar los datos provenientes de vehículos conectados, barcos, helicópteros... es lo que estamos desarrollando y esperamos a levar a buen puerto en los próximos años".

Finalizaba Fernando Novo Martínez (Gerencia Informática de la Seguridad Social) comentando que "hace un año implantamos la analítica web para ver cómo los ciudadanos se relacionaban con nosotros, y estamos usando estos datos para diseñar mejores servicios. Y lo mismo para las interacciones internas, que también repercutirán en un mejor servicio al ciudadano. Hay que tener en cuenta las cuestiones técnicas, pero también la experiencia de usuario".

LA VISIÓN DE LOS PROVEEDORES

Frente a estos retos y necesidades, Manuel de Dios, FlexxClient Director de Flexxible, explicaba que "nosotros ponemos el foco en eliminar la fricción entre el empleado y la tecnología, dando la información al responsable del posible problema para poder medir tanto las cuestiones objetivas como subjetivas, ayudando a implementar la mejores herramientas para incrementar los niveles de productividad".

Concluía Ramón Rodríguez, Data Center Solution Architect de Schneider Electric, indicando que "cuando hablamos de acercar los servicios al ciudadano y de aprovechar el dato, hay veces que perdemos la visión de que estos se mueven a través de los centros de datos, y ahí es donde aportamos nuestro granito de arena. En estos años, los datos se han multiplicado por 20, la capacidades necesarias por 6 y, sin embargo, el consumo de estos CDP apenas ha crecido. Así es donde aportamos soluciones de infraestructura y de mejora a partir de la monitorización, permitiendo contar con infraestructuras más eficientes y sostenibles". ■

"EN ESTOS AÑOS, LOS DATOS SE HAN MULTIPLICADO POR 20, LA CAPACIDADES NECESARIAS POR 6 Y, SIN EMBARGO, EL CONSUMO DE LOS CENTROS DE DATOS APENAS HA CRECIDO"

Ramón Rodríguez, Data Center Solution Architect de Schneider Electric

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

JOAQUÍN GRANDE BAOS,
JEFE DE SERVICIO DE LA UNIDAD DE APOYO A LA DIRECCIÓN DEL SERVICIO CANARIO DE SALUD

“LOS ASISTENTES COGNITIVOS PARA LA SALUD VAN A CAMBIAR EL PARADIGMA DE LOS RECURSOS ASISTENCIALES”

Joaquín Grande explicó los detalles del proyecto MedP Big Data.

La prestación de mejores servicios es uno de los objetivos de la modernización de las Administraciones Públicas, tanto de cara al ciudadano como en el incremento de la eficiencia de los procesos internos. Aplicar nuevas tecnologías, como los asistentes cognitivos, permiten dar una respuesta más rápida y personalizada para los usuarios.

Y, precisamente, de esta integración y de la mejora ofrecida en el servicio al ciudadano, hablamos con Joaquín Grande Baos, Jefe de Servicio de la Unidad de Apoyo a la Dirección del Servicio Canario de Salud, como cierre del V Foro IT User/Administración Pública Digital, Modernización del Sector Público: estado de las iniciativas digitales. Tal y como explicaba este responsable, “los asistentes cognitivos para la salud van a cambiar el paradigma de los recursos asistenciales incorporando un nuevo actor, que no solo no va a competir con los actuales, sino que va a

aumentar la calidad y a garantizar la sostenibilidad del sistema".

El proyecto del que nos hablaba Joaquín Grande se denomina Medicina Personalizada Big Data (MedP Big Data), implementado de forma coordinada por la Generalitat Valenciana y el Servicio Canario de Salud, con un presupuesto de casi 6 millones de euros. Según nos explicaba, "tiene un formato de compra pública precomercial y pretende desarrollar soluciones basadas en la inteligencia artificial de doble naturaleza. Por una parte, la que habilite una interfaz entre los pacientes y el sistema de registro de datos de su servicio sanitario, y, por otro, la que provea herramientas analíticas a los profesionales sanitarios dedicados a la atención, la gestión y la investigación. Además de aprovechar las sinergias entre ambas líneas".

DOS FASES Y 18 CASOS DE USO

El proyecto está organizado en dos fases y lo componen 18 casos de uso. "La primera fase tuvo lugar entre abril y septiembre de 2022, con la participación de tres adjudicatarios: Virtual Doctors & Medicine, Laberit Qwerty y GMV. Incluyó cinco casos de uso de una interfaz usuario-servicio sanitario de promoción de la salud y otros tres de herramientas de analítica productiva. El Comité Ético para la Investigación con Medicamentos de Tenerife aprobó su modelo de implementación y sus correspondientes consentimientos informados, y la usabilidad de la interfaz se priorizó en el baremo para seleccionar la ganadora, contando la satisfacción y el número de interacciones de los participantes".

Esta primera fase "se concretó en la app denominada Cuídat-e, sobre cinco casos de uso dirigidos a población general: la promoción de alimentación saludable, la actividad física, el bienestar emocional, el manejo de las adicciones, y la superación de la soledad no deseada. Las herramientas analíticas se concretaron en tres casos de uso sobre etiquetado automático, análisis de imagen médica, y la predicción de ingresos por urgencia respiratoria vinculados a niveles de contaminación ambiental".

La segunda fase ha sido desarrollada por GMV. Comenzó en diciembre de 2022, debe concluir el próximo 30 de junio, y ha incluido 4 casos y medio de uso de interfaz paciente-servicio sanitario, y otros cinco y medio de herramientas de analítica predictiva. También se prolongaron de la fase anterior los cinco casos de interfaz unificados en uno solo, el de imagen médica lumbar, al que se añadió el supuesto de rayos X de radiología simple de tórax y el de predicción ajustada a perfiles personalizados de urgencia respiratoria por niveles de contaminación ambiental".

APLICACIÓN DE LA IA PARA MEJORAR LOS SISTEMAS DE SALUD

En palabras de Joaquín Grande Baos, "todos estamos de acuerdo en aplicar la inteligencia artificial a la mejora de los sistemas de salud. En MedP Big Data planteamos casos de uso concretados en determinados supuestos que deberían servir para validar la factibilidad de conseguir resultados y la idoneidad de la metodología empleada. Es decir, una factoría demostrativa de 18 pilotos generadores de algoritmos aplicables en circunstancias estrechamente delimitadas. Contamos con tres aliados, los espacios de datos sanitarios interoperables que a nivel estatal está impulsado por el Ministerio de Sanidad y los propios de cada servicio regional de salud, los proyectos PERTE y los Fondos Next Generation EU, y sugerimos la creación de un clúster tecnológico, dada la alta complejidad y coste de estas herramientas y su potencial aprovechamiento por muchos actores". ■

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

El 93% de las organizaciones admiten que les resulta difícil llevar a cabo tareas esenciales de seguridad

Actúe contra las amenazas con un servicio gestionado de expertos

Sophos Managed Detection and Response

Sophos MDR es un servicio de seguridad gestionada que se adapta a sus necesidades y le permite alcanzar sus objetivos de seguridad y empresariales, compatible con las herramientas de ciberseguridad que ya tiene.
Más información en: es.sophos.com/mdr

SOPHOS

230606 ES [PC]

EXPERIENCIA DEL EMPLEADO... "LOST IN TRANSLATION"

MANUEL DE DIOS

FLEXCLIENT DIRECTOR
DE FLEXXIBLE

El sector TI es un gran generador de conceptos, recogiendo situaciones complejas, identificando puntos relevantes, sintetizando y posteriormente categorizando. Al común de los profesionales nos acaba llegando una miríada de siglas que manejamos con cierta alegría y muchas veces perdiendo el contacto con las realidades que fueron la base de la génesis de esas siglas.

La maquinaria TI está compuesta por elementos puramente tecnológicos: hardware, software, comunicaciones. Y, por otra parte, un componente humano. La evolución de ambas partes no es pareja. La tecnología evoluciona día a día a gran velocidad y es exigente. Pide a sus usuarios una actualización constante de conocimientos referentes a su entorno de trabajo que no es posible de mantener por la mayor parte de ellos, mientras que a los equipos de soporte TI tampoco les es fácil implementar, mantener y formar tanto a personal técnico como usuarios.

Esas diferentes velocidades son fuente de una fricción permanente que afecta de forma directa a la productividad, por una parte, y, por otra, al bienestar laboral de la plantilla, de forma general, y de los equipos de TI, en particular.

Un pantallazo azul del sistema operativo, una respuesta lenta de la aplicación, una pérdida y olvido de contraseña, de las múltiples usadas diariamente, un "crash de aplicación" que se repite y obliga al usuario a comenzar tarea desde el principio... son situaciones que se repiten a diario.

Adicionalmente, en los últimos años hemos incrementado la deslocalización y mejorado el trabajo en movilidad, pudiendo usar las herramientas corporativas desde cualquier lugar y con multitud de dispositivos. Esto es una gran ventaja en productividad, pero pone distancia entre los usuarios y los recursos técnicos que facultan el buen funcionamiento de las plataformas, lo que es un reto para ambos jugadores.

Se han creado herramientas y diseñado procedimientos para poder abordar ese reto y reducir el impacto. Sobre el papel son diseños técnicos y procedimentalmente buenos, pero se asume un conocimiento implícito por parte de los usuarios sobre el funcionamiento de sus herramientas y del entorno de uso y condiciones por parte de los técnicos.

Por otra parte, añadimos a la ecuación la ciberseguridad, por si la complejidad del escenario no era suficiente. Parece demostrado que uno de los puntos más débiles, lo que lo convierte en un vector de ataque recurrente, es el usuario y sus dispositivos. Estar al día, como usuario, de las prácticas sofisticadas de los cibercriminales es tarea imposible, por más formación, avisos, e información que se facilite. Por tanto, se requiere un respaldo por parte de los equipos de soporte delegado en expertos que proporcionen unos umbrales de seguridad aceptables y se tengan planes de contingencia preparados para cuando esos umbrales se vean rebasados.

Este es a muy grandes rasgos el entorno sobre el que conceptualizamos rápidamente y concretamos unas cómodas siglas como DEX (Digital Employee Experience).

Como usuarios, nos enfrentamos a no poder realizar nuestras tareas de forma eficiente, no tener acceso a una solución ágil de todas esas contingen-

cias, o el desconocimiento de los factores que nos afectan y que nos hacen imposible en muchas ocasiones informar de forma adecuada a los equipos técnicos.

Como técnicos, a tareas de identificación, cualificación y diagnosis, donde solo el recabar la información necesaria puede ser el mayor de los problemas y empleo de tiempo; al proceso de escalado a los diferentes responsables y la gestión de la intervención que pueden suponer tanto más tiempo cuantos más "saltos" va dando el incidente por el flujo de soporte y aprobación; o avalanchas de petición de servicio en cambios de versión, aplicación o migración...

En suma, es una pérdida de productividad y eficiencia inherente al propio modelo, además de un impacto en el bienestar laboral de los empleados, tanto usuarios como profesionales TI.

Esto ha puesto al DEX como uno de los factores claves a medir y como indicador de mejora productiva. Y la industria tecnológica ha comenzado a desarrollar herramientas que ayuden en ese sentido.

Hay factores que son fundamentales a la hora de considerar estos desarrollos. La medición, obviamente es clave. Medir todos los aspectos objetivos que impactan en esa experiencia, dispositivos, rendimiento, aplicaciones, comunicaciones, seguridad... y los subjetivos, que es básicamente la percepción del usuario.

De esa medición se obtienen una cantidad ingente de datos, que hay que convertir en conocimiento. Además debe ser un conocimiento basado en unos datos vivos, dinámicos y cambiantes, no son fotos estáticas. Debo tener herramientas que me permitan ver lo que es relevante en cada momento y poder tomar decisiones en tiempo y forma.

Actuación. Ya tenemos la diagnosis y las decisiones, necesitamos implementar, de forma rápida y eficiente. Y automatizar la gran mayor parte de las actuaciones que podemos prever tras la experiencia que nos da el conocimiento.

Monitorización y observación. Sería el otro gran factor a considerar. Tengamos en cuenta que hablamos de la maquinaria de información de las organizaciones. El acercarnos a los datos que nos proporciona desde los diferentes puntos de vista, nos ofrece información vital, no solo a los equipos técnicos de soporte, sistemas, aplicaciones, seguridad... sino también a negocio, finanzas, legal, RRHH, dirección... Podemos llegar a medir con fiabilidad el impacto en consumo eléctrico y huella de carbono. Es decir, el alcance va más allá de lo que en principio podíamos esperar.

Por tanto, cuando traducimos las siglas DEX en román paladino de nuestro día a día, vemos que tiene una capilaridad asombrosa en nuestras organizaciones y un impacto en la viabilidad de estas. Resulta paradójico que mirando desde un punto superior la maquinaria de la tecnología de la información, y considerando que el elemento humano es esencial e imprescindible para el procesamiento adecuado y eficiente de la misma, no hayamos considerado poner el foco en este concepto mucho antes. ■

PARECE DEMOSTRADO QUE UNO DE LOS PUNTOS MÁS DÉBILES, LO QUE LO CONVIERTE EN UN VECTOR DE ATAQUE RECURRENTE, ES EL USUARIO Y SUS DISPOSITIVOS

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

Flexxible

LA DIGITALIZACIÓN DE LA ADMINISTRACIÓN PÚBLICA, RETOS EN CIBERSEGURIDAD

SERGIO MARTÍNEZ

COUNTRY MANAGER
DE SONICWALL

La proliferación de Internet, con más de 4.000 millones de usuarios a nivel mundial, ha impulsado la transformación en las estructuras empresariales de todos los sectores, desde el sector privado, la educación, la sanidad, la industria, sin dejar de lado a la Administración Pública.

Los entornos de trabajo híbrido están siendo la palanca de cambio en esta transformación, ya que se ha convertido en la forma más favorecedora de trabajar y una de las más valoradas por empleados, también del Sector Público y la Administración.

A esto hay que añadir que los ciudadanos, en este entorno de digitalización, cada vez son más exigentes y han tendido a normalizar el acceso de manera eficiente a cualquier servicio gubernamental en cualquier momento y desde cualquier lugar. Los gobernantes, para adaptarse a estas nuevas exigencias, han ido adecuando la necesidad de desarrollar la Sociedad de la Información y la administración electrónica, con todas las ventajas que esto supone, pero también los nuevos desafíos que conlleva, sobre todo en términos de seguridad.

La Administración Pública tiene por tanto el compromiso de dar servicio y promover el beneficio de los ciudadanos con el uso de las nuevas tecnologías y las comunicaciones, transformando la Administración Pública en e-administración, generando, al mismo tiempo, la confianza y la seguridad en el uso de las tecnologías.

La Administración Pública necesita que el uso de información se realice de forma segura para garantizar el servicio al ciudadano. Al manejar un gran volumen de datos, es primordial salvaguardar la confidencialidad de los mismo, garantizando su autenticidad, su integridad y la disponibilidad de los mismos. Es primordial garantizar la protección de la información pública, sus sistemas y servicios, así como las redes que lo soportan es imperativo.

Y es que el sector público se ha convertido en uno de los blancos preferidos de los ciberdelincuentes, sufriendo cada vez un mayor número de ataques de ransomware. Pero no sólo esto, sino que, según diferentes estudios, el 72% de las Administraciones Públicas que han sido atacadas por ransomware han visto cifrados sus datos, y tan solo el 20% de las administraciones han logrado detener un ataque ransomware antes de que sus datos fueran cifrados.

Como consecuencia, los gobiernos deben adoptar los medios y tecnologías adecuadas para la protección y control del acceso a la información, y ha de regular unos procedimientos eficaces para su almacenamiento, procesamiento y transmisión seguros. Estamos, pues, ante un escenario complejo, en el que la digitalización del sector público está sujeto a nuevos desafíos, ya que se combinan, por un lado, el hecho de que la transformación digital es fundamental en los servicios prestados por las administraciones y por otro, los crecientes los riesgos y ciberamenazas.

Este escenario complejo, hay que simplificarlo con herramientas que ayuden a mantener a los empleados

en sus tareas, facilitando los procesos y garantizando la seguridad de estos. Las tecnologías han de permitir una comunicación fluida y han de ser una herramienta de colaboración entre los empleados gubernamentales y los ciudadanos, apoyando formas nuevas, más participativas, innovadoras y ágiles en la prestación de servicios.

Desde SonicWall ayudamos a las administraciones a construir una defensa por capas, con sistemas preparados para detectar amenazas de todo tipo, incluidas las de corte desconocido, y a reaccionar de forma inmediata, con entornos de gestión que facilitan la visibilidad y el control de lo que sucede en las infraestructuras.

Esta situación en la que estamos sumergidos, recuerda a aquello que ya decía un representante el IRA a Margaret Thatcher, “nosotros sólo necesitamos suerte una vez, vosotros todo el tiempo”. ■

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

Sonicwall

EL COMPLEJO ESCENARIO ACTUAL HAY QUE SIMPLIFICARLO CON HERRAMIENTAS QUE AYUDEN A MANTENER A LOS EMPLEADOS EN SUS TAREAS, FACILITANDO LOS PROCESOS Y GARANTIZANDO LA SEGURIDAD DE ESTOS

WATCHGUARD FOR SOC – EFICIENCIA Y PROACTIVIDAD

Empowering the SOC

Threat Hunting

Detección, investigación y respuesta

Ciber Resiliencia

Anticípate a las ciberamenazas en constante evolución

WatchGuard for SOC se basa en la combinación de soluciones de seguridad avanzada y plataforma de threat hunting para buscar, detectar y responder de manera eficiente a amenazas que hayan logrado evadir otras protecciones en endpoints, servidores, entornos virtuales y dispositivos móviles.

Contacto: **900 840 407** **strategic.accounts@watchguard.com** **www.watchguard.com**

SEGURIDAD ENDPOINT AVANZADA

AUTENTIFICACIÓN MULTIFACTOR

SEGURIDAD DE RED

NUBE SEGURA WI-FI

EL CIBERCRIMEN AVANZA EN LA ADMINISTRACIÓN PÚBLICA PONIENDO EN JAQUE SUS DEFENSAS DURANTE EL ÚLTIMO AÑO

JOHN SHIER

CTO DE SOPHOS

El ransomware creció un 70% en la Administración Pública a lo largo de este año. Con las capacidades de detección y respuesta ante amenazas, Sophos MDR ayuda a los organismos a estar preparados.

Más de la mitad (58%) de las instituciones gubernamentales se vieron afectadas por el ransomware en 2021, frente al 34% en 2020. Este aumento del 70% en un año demuestra la rápida aceleración del desafío en materia de ciber-amenazas al que se enfrenta el sector público. En términos más generales, la mayoría de los responsables de TI que trabajan en el sector observaron un aumento en el volumen (59%), la complejidad (59%) y el impacto (56%) de los ciberataques durante el último año. A medida que los ciberdelincuentes sigan sirviéndose de la automatización y el modelo de "malware como servicio" en sus ataques, estas cifras no harán más que aumentar.

El impacto de las ciber-amenazas avanzadas en el sector público es grave. Un ciber-incidente importante tiene unas repercusiones financieras y operativas muy considerables dentro de la Administración Pública. En 2021, el coste medio de remediar un ataque de ransomware fue de 660.000 dólares, y casi la mitad (42%) de los datos cifrados no se recuperó después del incidente. Los costes de recuperación son solo una parte de la historia. La gran mayoría (82%) de los organismos afectados por el ransomware afirmaron que el ataque afectó a su capacidad de operar. Si los sistemas informáticos dejan de funcionar, la capacidad de una agencia gubernamental para prestar servicios críticos suele verse gravemente mermada, lo que en última instancia podría afectar a la seguridad nacional, las infraestructuras y la economía. La recuperación también puede llevar mucho tiempo, ya que más de una quinta parte (21%) de las víctimas de ransomware en estas organizaciones tardan entre una y seis semanas en volver a la normalidad después del ataque.

Las amenazas actuales requieren de una respuesta coordinada y oportuna. Desgraciadamente, demasiadas organizaciones están atrapadas en el modo reactivo. Y esto no solo tiene un impacto sobre las prioridades del negocio, sino que también conlleva un coste humano considerable, ya que más de la mitad de los encuestados confiesa que los ciber-ataques les quitan el sueño. Eliminar las conjeturas y aplicar controles defensivos basados en inteligencia aplicable permitirá a los equipos de TI centrarse en habilitar el negocio, en lugar de intentar apagar los continuos incendios de los ataques activos.

Podemos afirmar que la realidad es que las soluciones tecnológicas por sí solas no pueden evitar todos los ciber-ataques. Para no ser detectados por las soluciones de ciberseguridad, los ciberdelincuentes se sirven cada vez más de herramientas de TI legítimas, utilizan credenciales y permisos de acceso robados, y aprovechan vulnerabilidades sin parchear en sus ataques. Al hacerse pasar por usuarios autorizados y explotar los puntos débiles en

las defensas de una organización, los ciberdelincuentes pueden evitar la activación de las tecnologías de detección automatizadas. La única manera de detectar y neutralizar de forma fiable a los ciber-atacantes es prestando una especial atención 24/7 con operadores expertos que se sirvan de diversas alertas de seguridad e información sobre amenazas en tiempo real para identificar y detener las amenazas antes de que provoquen daños. Sin embargo, la complejidad de los entornos operativos modernos y la velocidad de las ciber-amenazas hacen que sea cada vez más difícil para la mayoría de las organizaciones gestionar con éxito la detección y la respuesta a las amenazas por su cuenta. Organizaciones de todos los sectores, incluido el sector público, luchan por seguir el ritmo de adversarios bien financiados que innovan e industrializan continuamente su capacidad para evadir las tecnologías defensivas.

Uno de los mayores riesgos para las organizaciones hoy en día son los adversarios activos, actores de amenazas que adaptan sus técnicas, tácticas y procedimientos (TTP) sobre la marcha, utilizando acciones prácticas en tiempo real en respuesta a las acciones de las tecnologías de seguridad y los defensores, y como táctica para eludir la detección. Estos ataques, que a menudo dan lugar a devastadores incidentes de ransomware y violación de datos, se encuentran entre los más difíciles de detener.

Permitir que los defensores superen a los atacantes en la carrera de la ciberseguridad de 2023 requiere un enfoque integral, pero sencillo. Los servicios gestionados de ciberseguridad de detección y respuesta ante amenazas, por tanto, son clave a la hora de hacer frente a la nueva industrialización del cibercrimen, tanto para la protección de organismos públicos como privados, ya que reducen el riesgo y los costes asociados a los incidentes en ciberseguridad.

A lo largo de este artículo hemos resaltado la importancia de avanzar y eliminar el modelo reactivo ante incidentes y en cómo el tiempo de respuesta es determinante a la hora de protegernos frente al nuevo modelo de ciberataques. Sophos Managed Detection and Response ofrece el respaldo de un equipo de expertos que detectan y responden a ciberataques dirigidos con un tiempo medio de respuesta de 38 minutos, que es considerablemente más rápido que la media de los equipos internos.

Sophos MDR protege a cientos de organismos gubernamentales, lo que nos aporta una experiencia con una profundidad y amplitud sin precedentes sobre las amenazas a las que se enfrenta el sector público. Nos servimos de esta extensa telemetría para generar inmunidad comunitaria, aplicando lo aprendido al proteger a un proveedor a todos los demás clientes del sector, reforzando así las defensas de todos. ■

PERMITIR QUE LOS DEFENSORES SUPEREN A LOS ATACANTES EN LA CARRERA DE LA CIBERSEGURIDAD DE 2023 REQUIERE UN ENFOQUE INTEGRAL

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

Sophos MDR

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

COMPARTIR MÁS LA INTELIGENCIA DE SEGURIDAD EN LOS SOC, CLAVE PARA AVANZAR EN LA PROTECCIÓN DE LA ADMINISTRACIÓN PÚBLICA

GLORIA TAMAYO

ENTERPRISE ACCOUNT MANAGER ADMINISTRACIÓN PÚBLICA DE WATCHGUARD TECHNOLOGIES

La Administración Pública desempeña un papel crucial en la ciberseguridad, ya que maneja una gran cantidad de datos sensibles y realiza funciones y servicios esenciales para la sociedad. La protección de los sistemas y la información en manos de los gobiernos es fundamental para garantizar la confidencialidad, integridad y disponibilidad de los datos, así como para prevenir y mitigar posibles ciberataques.

En general, los gobiernos de todo el mundo son cada vez más conscientes de la importancia de la ciberseguridad y han tomado medidas para fortalecerla. Entre algunas de las acciones están el establecimiento de organismos y agencias especializadas, la elaboración de marcos normativos, el impulso de formación y la concienciación, la evaluación y establecimiento de auditorías de seguridad o la coordinación con el sector privado y otros actores relevantes en materia de colaboración.

Es cierto que la ciberseguridad es un desafío en constante evolución, y los gobiernos, como las empresas, deben adaptarse y mejorar continuamente sus enfoques y estrategias para hacer frente a las nuevas amenazas. No hay duda, la situación del cibercrimen actual es extremadamente grave. Los datos revelan un aumento en número (+27% anual) y sofisticación de ataques y costes empresariales ocasionados. Aunque el incremento de la inversión en ciberseguridad, se ha traducido en un mayor nivel de prevención, la seguridad absoluta no existe: ya no es suficiente con “sentarse y esperar” al atacante.

Esta realidad impulsa a entidades y organismos a adoptar un modelo de búsqueda activa y de caza de amenazas, y a evolucionar sus programas de seguridad avanzada combinando, por un lado, estrictas medidas preventivas con una exhaustiva reducción de la superficie de ataque, y un estricto gobierno de ejecución de aplicaciones; y por otro, robustas capacidades proactivas de detección y respuesta ante incidentes ocasionados por atacantes que han conseguido superar los controles existentes.

En el afán por combatir las ciberamenazas con mayor eficiencia y efectividad ante el panorama actual y futuro de seguridad, los centros de operaciones de seguridad (SOC) han evolucionado para dar paso a los SOC modernos que, además de las funciones más tradicionales del SOC, tienen la capacidad de reducir el riesgo al limitar el daño de atacantes avanzados que obtienen acceso a los recursos de la organización estando preparados para supervisar la actividad de la red, los endpoints, las aplicaciones y los usuarios con el fin de detectar de manera proactiva comportamientos anormales, investigar los indicadores de incidentes o ataques de seguridad y responder de manera inmediata a las amenazas.

En este avance hacia los SOC modernos existen tecnologías que ya permiten combinar la visibilidad ampliada en tiempo real con analítica y herramientas de seguridad a gran escala, lo que fortalece a buscadores, analistas, y responsables de respuestas de SOC para afrontar de manera eficiente las amenazas sofisticadas no detectadas. Su arquitectura de múltiples usuarios y nativa de la nube permite pasar menos tiempo gestio-

nando la infraestructura y más tiempo anticipando amenazas.

De este modo, los SOC están listos para mejorar su postura de seguridad e incrementar la eficiencia de su SecOps gracias a:

➤ La adopción de una estrategia de defensa proactiva: la analítica de comportamiento innovadora de tecnologías como Orion ayuda a detectar, priorizar y contextualizar automáticamente la actividad anómala a gran escala. Respaldada por expertos en ciberseguridad y por inteligencia actualizada, permite a los equipos de operaciones de seguridad anticipar a los adversarios más sigilosos, lo que aumenta la precisión y eficacia del SOC.

➤ Búsqueda de ataques desconocidos y sofisticados: las reglas de búsqueda analizan los 365 días del año la telemetría endpoints para descubrir, priorizar y contextualizar indicadores como señales de ataque asignadas a MITRE.

➤ Investigación y respuesta más rápida: los analistas de SOC pueden crear y ampliar las investigaciones listas para usar a través de cuadernos de plataforma para que se adapten a sus prácticas.

➤ Mayor nivel de madurez a través de la colaboración: la plataforma WatchGuard Orion agiliza el tiempo de creación de valor de los analistas a través de la colaboración en casos de incidentes y el uso compartido de conocimiento. Los analistas novatos aprenden de los profesionales con experiencia a crear sus habilidades con reglas de búsqueda, cuadernos y cuadernos de estrategias, lo que acelera la madurez de todo el SOC.

➤ Montar una batería completa de seguridad capaz de integrarse sin problemas a su ecosistema de operaciones para ampliar la investigación y preparar el flujo de trabajo de respuestas de funcionalidad cruzada.

REFORZAR LA COLABORACIÓN PÚBLICO-PRIVADA Y ENRIQUECER LA RNS

Para garantizar un nivel de seguridad adecuado en los sistemas, es necesario actuar antes de que se produzca un incidente o, por lo menos, ser capaz de detectarlo en un primer momento para reducir su impacto y alcance. La implantación del SOC no es una tarea fácil, y requiere de un proceso de mejora continua.

Hay varias formas para que una entidad adopte capacidades de SOC modernos. Los modelos de implementación más comunes incluyen: SOC interno, SOCaaS (Security Operations Center as a Service), SOCaaS híbrido. Elegir uno u otro dependerá de las necesidades y recursos de la entidad.

El CCN-CERT tradicionalmente ha colaborado y colabora en varios SOC de diferente magnitud, ya sea a nivel de ministerios, diputaciones/cabildos, o entidades locales, a los que se han venido a añadir últimamente Operadores de Servicios Esenciales. Para ello, ha creado Red Nacional de SOC (RNS), como instrumento para coordinar la colaboración y el intercambio de información entre los Centros de Operaciones de Ciberseguridad del sector público español.

Si entre todos los SOC que dan protección al sector público, se comparte e inteligencia sobre las tácticas, técnicas y procedimientos de nuevas amenazas, se podrán mejorar las capacidades de detección y respuesta a posibles ciberincidentes.

En este sentido, y ante la evolución de los SOC, creemos que el próximo paso está en enriquecer la red de SOC federados con avances como la tecnología Orion, pues es clave contar con herramientas que permitan la explotación de la información tanto la detección como la contención de amenazas, facilitando una gestión jerárquica de la información para que pueda ser conocida por todos los organismos de forma rápida y sencilla. Además de permitir aplicar diferentes niveles de madurez en la explotación de los SOCs y automatizar la actividad. ■

CONTENIDO RELACIONADO

Modernización del Sector Público: estado de las iniciativas digitales

WatchGuard Technologies

FORO ADMINISTRACIÓN PÚBLICA

it User

Modernización del Sector Público:

estado de las iniciativas digitales

Ver ahora las ponencias