



AURRERA!

Nº 80

junio 2022

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico

Dirección de Tecnologías de la Información y la Comunicación

ÍNDICE

▲ Jornadas
TEKgunea 2.0
Pág. 2

▲ Plan Director de
Seguridad del
Gobierno Vasco
Pág. 6

Alboan

▲ El Gobierno del
Dato en el
Gobierno Vasco
Pág. 10

Contraportada

▲ 40 aniversario de
EJIE
▲ Kateryna
Yushchenko y los
lenguajes de
programación
Pág. 12

Si siguiendo la estela de la primera edición de las **Jornadas TEKgunea** celebradas en 2021, el Gobierno Vasco acaba de celebrar una nueva edición. Su objetivo sigue siendo el mismo: compartir experiencias e información sobre proyectos innovadores que se están llevando a cabo en la Administración Pública vasca o navarra, bien directamente o bien a través de sus entidades públicas. A lo largo del primer artículo os hacemos un resumen de los proyectos expuestos.

En el segundo artículo nos centraremos una vez más en un aspecto que cada vez tiene más importancia para las empresas y las administraciones públicas: la seguridad de sus sistemas de información. En esta ocasión, en concreto, haremos un repaso al contenido del **Plan Director de Seguridad del Gobierno Vasco**, detallando las distintas iniciativas que ya se han llevado a cabo o se están desarrollando, así como de los proyectos que se tienen previsto implantar en los próximos meses.

El **Gobierno del Dato** es un tema del que ya hemos hablado en un boletín anterior, sin embargo, en este boletín Aurrera queremos fijarnos en este tema desde un punto de vista mucho más cercano, ya que el pasado mes de febrero el Gobierno Vasco puso en marcha un Equipo de Trabajo cuyo objeto es definir precisamente las líneas estratégicas que el Gobierno Vasco deberá seguir a lo largo de los próximos años. En el artículo haremos una breve introducción de cuáles son sus objetivos y las Direcciones que integran dicho Equipo de Trabajo.

Este año, la Sociedad Informática del Gobierno Vasco, **EJIE**, está de celebración, ya que acaba de cumplir **40 años**. Para recordar dicha efeméride, en el apartado «*Contraportada*», hemos incluido una breve reseña con la que queremos felicitar a todas las personas que de una u otra manera han formado parte de dicha entidad y han aportado su granito de arena para mejorar los servicios que EJIE presta a la Administración Pública vasca y, por ende, a la sociedad vasca.

Por otro lado, en la sección «*Protagonistas*», repasamos la vida profesional de **Kateryna Yushchenko**, una científica de origen ucraniano pionera de los lenguajes de programación.

Jornadas TEKgunea 2.0



Con objeto de seguir promoviendo y facilitando el intercambio de experiencias y la colaboración interadministrativa, el Gobierno Vasco ha organizado la segunda edición de su encuentro tecnológico «TEKgunea 2.0».



¹ **Arantzazu:** la jornada se celebró en el Espacio «ArantzazuLab», ubicado junto al Santuario de Arantzazu. <https://arantzazulab.eus>



² **TEKgunea release I.0:** para saber cómo se desarrolló la primera edición (celebrada en marzo de 2021), podéis consultar el artículo titulado «Jornadas TEKgunea I.0», publicado en el boletín Aurrera Nº 76 (junio 2021).

El miércoles 25 de mayo de 2022 tuvo lugar la segunda edición de las jornadas TEKgunea o, como las define nuestro equipo, «TEKgunea working days-egunak. Release 2.0». Por fin el encuentro se pudo realizar en formato presencial, pero manteniendo el canal on-line para las personas que no pudieron desplazarse.

El lugar elegido fue un sitio muy especial, el entorno del Santuario de Arantzazu¹ en Oñati (Gipuzkoa), donde nuestra visión tecnológica competía con la **naturaleza, el arte y la arquitectura** del entorno. Así lo vivimos en palabras de nuestra Consejera de Gobernanza Pública y Autogobierno, Olatz Garamendi Landa:

«Difícil lo va a tener el Metaverso para competir con los espacios naturales y mágicos que tenemos en nuestra tierra»

Y siguiendo sus indicaciones, apagamos por



Entorno del Santuario de Arantzazu [arriba] y edificio de ArantzazuLab [abajo]. [Foto: ArantzazuLab]



una mañana el móvil, escuchamos, disertamos y participamos para compartir conocimiento y visualizar proyectos «en colaboración» que nos ayuden a tener esta visión común para seguir por este camino de éxito, compartiendo equipos, recursos tecnológicos, presupuestos y resultados.

LA JORNADA

La jornada comenzó con un repaso a los servicios y objetivos que se propusieron el año pasado en la edición «TEKgunea release I.0»² para poder conocer si se han podido cumplir los retos planteados. Desde luego que ha sido un año intenso y así nos lo demostraron los distintos proyectos presentados:

- ▲ la pasarela de pago ya permite el pago a través de Bizum y también el pago «en movilidad» para las tramitaciones de sanciones en el propio lugar, facilitando la labor de la Ertzaintza y la policía municipal y para la comodidad de la persona sancionada
- ▲ el servicio de bibliotecas sigue creciendo en sus fondos culturales
- ▲ NISAE sigue avanzando por toda la Administración Pública Vasca para eliminar las fotocopias en trámites administrativos
- ▲ el repositorio de software sigue publicando poco a poco aplicaciones de las Administraciones Públicas
- ▲ Itzuli, nuestro traductor neuronal, sigue dando pasos profesionales aportando en el mismo TEKgunea, para las personas que estaban conectadas on-line, un modelo de traducción automática

Y tras esa visión de pasado-presente llegó el

turno de conocer proyectos que en el presente nos ubican ya en el futuro. Este fue el caso del proyecto que nos propuso Nasertic³ con Gonzalo R. Ordoñez hablando de medicina personalizada alrededor de la supercomputación y la tecnología cuántica. Sorprendente conocer los pasos que están dando en Navarra en la secuenciación genómica. Un proyecto que trabaja con tecnología emergente con vocación de compartir conocimiento, resultados y recursos.

«200 personas aproximadamente siguieron el desarrollo del evento en representación de distintas Administraciones Públicas y entidades públicas»

Igor Goirizelaia Ziardegi del Departamento de Salud del Gobierno Vasco, por su parte, nos presentó los avances en la Tarjeta Sanitaria Digital que está poniendo en marcha Osakidetza en su versión *Wallet* con una demo en real que mostró el potencial de esta nueva tecnología.

Toni Sáez González desde Izenpe nos aportó una visión para simplificar y evitar desplazamientos innecesarios para la obtención de un certificado digital BakQ. Gracias a la tecnología de «*identificación biométrica*» en breve vamos a poder obtener el certificado desde nuestra casa o nuestro trabajo, sin tener que acudir a una oficina de atención ciudadana. Pudimos conocer todo el proceso, tan complejo como sorprendente. Y como cierre de esta sección de proyectos

excelentes pudimos vivir casi en directo los problemas de un ciberataque que ha padecido Animsa⁴. De esta forma, Ana Burgui Aldunate, que tuvo que conectarse on-line a través de videoconferencia, nos presentó su proyecto de ciberseguridad para pequeños municipios mostrando la vulnerabilidad que en muchas ocasiones tenemos a pesar del gran trabajo realizado en prevención y en reacción, tomando como base el ataque que habían sufrido pocos días antes de celebrarse nuestra jornada.

Tras una pausa para el café y el «*networking*», la jornada puso rumbo a su recta final con varias mesas redondas en las que seguimos hablando de **colaboración**.

Abrió la sección Gaia⁵ aportando su visión sobre la Colaboración Público-Privada, que según nos indicaba Tomás Iriondo es una práctica con gran potencial y así nos lo demostraron las empresas y los ejemplos que aportaron Joana Epalza, de la empresa Ludus Global, y Aitor Alzola, del grupo Betean.

El proyecto TicketBAI, del que ya hablábamos el año pasado en TEKgunea I.0, se pone en marcha y lo hace, como no podía ser de otra forma, colaborando entre las distintas Diputaciones Forales que nos propusieron distintas visiones sobre un mismo proyecto: la colaboración con empresas de software con Iñaki Arantzabal desde Gipuzkoa, la colaboración con sectores de actividad con la visión de Ainara Etxeandia desde Bizkaia, la colaboración con empresas y contribuyentes que nos aportó Alvaro Pérez desde Araba y la visión transversal de colaboración de Izenpe que nos aportó Raquel Garay. Un proyecto que está ya obteniendo grandes resultados y que está favoreciendo a



³ **Nasertic**: son las siglas de Navarra de Servicios y Tecnologías S.A.
www.nasertic.es



⁴ **Animsa**: es la Asociación Navarra de Informática Municipal.
www.animsa.es



⁵ **Gaia**: es la Asociación de Industrias de Conocimiento y Tecnologías Aplicadas.
<https://gaia.es>





⁶ **UX:** son las siglas en inglés de «*User eXperience*» (en castellano, experiencia de usuario). Se centra en analizar la experiencia general que tiene un usuario final cuando visita una web o usa una aplicación móvil (app), por ejemplo. Para ello, se estudia la interacción de la persona, sus percepciones, emociones y respuestas ante el producto, sistema o servicio que ofrece la empresa. Se tienen en cuenta aspectos como la facilidad de uso, la accesibilidad y la conveniencia.

⁷ **CCASA:** son las siglas de Centro de Cálculo de Álava, S.A.
<https://ccasa.eus>



pequeños comercios en su proceso de digitalización, rompiendo una brecha digital que parecía no estar en su agenda a corto plazo.

Una sorpresa muy didáctica en la que casi todos y todas nos vimos reflejados fue la visión de Experiencia de Usuario (UX)⁶ que nos aportó Andoni Martín de CCASA⁷. Una visión para facilitar la relación con la ciudadanía a través del lenguaje y los mensajes con los que interactuamos, un modelo de trabajo que también ha realizado en este campo Izenpe. Visto lo visto, tendríamos que poner en nuestra agenda una oficina de experiencia de usuario para mejorar nuestros modelos de relación ciudadana.

Y como cierre tocaba hablar de «*Gobierno del Dato*». Gracias a ello, conocimos la asociación DAMA presentada por el responsable del modelo regional de Euskadi en la península, Joserra Santos acompañado de Lucía Engo

«El objetivo de TEKgunea es promover y facilitar el intercambio de experiencias y la colaboración interadministrativa»

responsable del área de Calidad de Datos y Contenido y de Nerea Sevilla de Lanbide que fue presentada como la primera persona certificada por DAMA en Euskadi. A destacar su propuesta para acompañar a cualquier Administración Pública a la hora de validar su hoja de ruta del Gobierno del Dato, sus objetivos y metas en este complejo, pero necesario viaje, para dotar de valor al dato que se dispone y que no se explota en la

actualidad. Un proyecto (con principio, pero sin fin) que debe iterar y mejorar de forma continua para que la Oficina del Dato de cada Administración Pública pueda alcanzar resultados.



Olatz Garamendi Landa, Consejera de Gobernanza Pública y Autogobierno del Gobierno Vasco [Foto: Irekia]

EL CIERRE

El cierre de la jornada la puso nuestro Viceconsejero de Administración y Servicios Generales, Polentzi Urquijo, quien agradeció a todas las personas ponentes su participación y colaboración, así como la asistencia de todas aquellas personas que nos acompañaron *in-situ* o a través de internet, y, por último, nos invitó a la próxima edición de TEKgunea 3.0.

El final del día tuvo también su momento cultural respirando vanguardia e innovación, ya que Aitor Orobengoa de ISEA nos propuso un viaje a través de los distintos proyectos de arquitectura, arte y diseño que culminaron con la creación del Santuario de Arantzazu.





TEKgunea 2.0

Podéis ver el vídeo de las distintas ponencias en la siguiente página web:

<https://www.euskadi.eus/gobierno-vasco/tekgunea/inicio/>

Asistencia

200 personas aproximadamente siguieron el desarrollo del evento, en representación del Gobierno Vasco, EJJIE, Diputaciones Forales de Araba, Bizkaia y Gipuzkoa, Gobierno y otras entidades públicas de Navarra, Ayuntamientos, UPV-EHU (Universidad del País Vasco) y Parlamento Vasco.

Plan Director de seguridad del Gobierno Vasco



El contexto de las amenazas que cada día nos acechan en Internet se ha diversificado, y cada vez es más difícil hacerles frente, por lo que es necesario actualizar y revisar continuamente las medidas de protección de nuestra infraestructura y nuestros equipos tecnológicos.



⁸ Plan de Evolución de Servicios de Seguridad:

para más información, podéis consultar el artículo «Evolución del modelo de ciberseguridad del Gobierno Vasco y su sector público», publicado en el boletín Aurrera nº 72 (junio 2020).

⁹ Plan Director de Seguridad: un Plan de estas características consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos **niveles aceptables**, a partir de un análisis de la situación inicial.

El desarrollo de las tecnologías de la información y de la comunicación (TIC) ha supuesto una transformación radical en pocos años en cualquier tipo de actividad social o económica, y también a la hora de prestar los servicios públicos. La dependencia de las redes y sistemas de información hace que su fiabilidad y seguridad resulte crucial para garantizar la continuidad y desarrollo normal de las actividades de cualquier Administración; razón por la que su protección ha sido abordada siempre desde diferentes perspectivas:

- ▲ la seguridad pública
- ▲ la protección de las infraestructuras críticas (la de las propias redes, sistemas y telecomunicaciones)
- ▲ y la privacidad de los datos personales

La **ciberseguridad** tiene como objetivo garantizar la seguridad de los servicios digitales y su información, así como de las infraestructuras, comunicaciones y sistemas que los soportan, tanto si son prestados por una entidad privada como pública, mejorando para ello sus capacidades de prevención, detección y respuesta ante incidentes.

NECESIDAD DEL PLAN

En un contexto en el que la movilidad, los servicios en la nube («cloud») y el nivel de exposición hacia el exterior de los servicios internos es cada vez mayor, el **nivel de riesgo** aumenta exponencialmente.

Por su parte, las redes criminales están cada vez más especializadas y tienden a dirigir sus ataques

a entidades o sectores concretos.

Como consecuencia de todo ello, EJJIE (la Sociedad Informática del Gobierno Vasco), dentro del proyecto de Convergencia BATERA, se encuentra en una fase de evolución y mejora de los Servicios de Seguridad que ofrece a los Departamentos, Organismos Autónomos y demás entidades del Sector Público Vasco, todo ello con objeto de mejorar las capacidades ya disponibles e incorporar nuevas funcionalidades



que permitan hacer frente a la **situación de riesgo** en la que nos encontramos.

En el año 2020 se realizó un **Plan de Evolución de Servicios de Seguridad**⁸ que pretendía marcar el camino de BATERA en materia de Ciberseguridad para los siguientes 4 años. Este plan llamado «Plan Director de Seguridad»⁹ tenía dos grandes objetivos:

- ▲ internamente que se incorporase la Seguridad como algo implícito y necesario en todos los ámbitos y entornos
- ▲ y externamente (clientes/usuarios), poder ofrecer la Seguridad como Servicio

Este Plan no se centra únicamente en los **riesgos**, sino que intenta buscar también de la **excelencia** en los servicios ofrecidos, y su implantación

sigue el modelo propuesto por INCIBE¹⁰.

Tras varias fases, se ha ido desarrollando el Plan Director y se han definido una serie de proyectos, su criticidad y su prioridad.

INICIATIVAS Y PROYECTOS

Dentro del plan se identificaron **42 iniciativas** clasificadas por ámbitos y prioridades. A continuación, se muestra el estado de ellas.

NUEVOS PROYECTOS

- ▲ **Gestión de Identidad:** durante el año 2020 se puso en marcha la plataforma OKTA¹¹ para ofrecer un servicio de identidad en la nube (IDaaS). La plataforma está ya en producción para varias aplicaciones (VDI Horizon, Zoom, Office365, ServiceNow, VPN, etc.). En estos momentos, se está en fase de extender esta solución a otros clientes y se quiere implantar para otros servicios «on-premise» internos.
- ▲ **SOC, SIEM, EDR, Vigilancia Digital:** en 2020 EJJIE publicó un pliego para contratar estos servicios y poder ofrecerlos a las entidades que están adheridas al Proyecto de

Convergencia «BATERA». El pliego fue adjudicado en octubre de 2021 y durante 2022 el objetivo es consolidar el servicio, definiendo el modelo de relación con el SOC e integrándolo en las herramientas corporativas. Asimismo, se pondrá en marcha el servicio de Vigilancia Digital y CSIRT (Grupo de Respuesta a Incidentes de Seguridad).

- ▲ **NAC:** en 2020 EJJIE realizó una consultoría para desarrollar un servicio que permita a las entidades que lo implementen conectar equipamiento de forma segura a la red. Durante 2021 se tenía previsto avanzar en la ejecución de lo propuesto por la consultoría, sin embargo, no se ha avanzado en esa línea ya que no se ha considerado prioritario.
- ▲ **WAF** [«*Web Application Firewall*»]: este proyecto se implementó durante 2021 y está ya protegiendo algunas aplicaciones piloto del Gobierno Vasco.
- ▲ **Oficina Técnica Seguridad/Cumplimiento:** aprovechando el proceso de definición de servicios de seguridad convergentes, se quiere fijar varios aspectos durante 2022-23:



¹⁰ **INCIBE:** es el Instituto Nacional de Ciberseguridad de España. Es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y, especialmente, para sectores estratégicos.

¹¹ **OKTA:** para más información, podéis consultar el artículo titulado «*Gestión de Identidades seguras (okta)*», publicado en el boletín Aurrera nº 79 (marzo 2022).

Normativa

La Unión Europea ha abordado la **seguridad de las redes y sistemas de información** a través de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, —Directiva NIS— y la **protección de la información personal** por medio del Reglamento General de Protección de Datos aprobado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 —RGPD—. Posteriormente, se aprobó el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 («*Reglamento sobre la Ciberseguridad*»).

En el ámbito del estado español, la ciberseguridad se ha incorporado como un

elemento más a la Estrategia de Seguridad Nacional, tanto es así que el Consejo de Seguridad Nacional ha elaborado una «Estrategia Nacional de Ciberseguridad». La citada Directiva NIS se ha traspuesto por el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.



En cuanto a la **administración electrónica**, se ha regulado el Esquema Nacional de Seguridad —ENS— contemplado en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y desarrollado por el nuevo Real Decreto 311/2022, de 3 de mayo. Hay que tener en cuenta, asimismo, el impacto de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y la trasposición del RGPD por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales —LOPD-GDD—.



¹² **BCSC:** es el acrónimo de «*Basque CyberSecurity Centre*» (Centro Vasco de Ciberseguridad) y es la organización designada por el Gobierno Vasco para promover la ciberseguridad en Euskadi. Su misión es desarrollar una cultura de ciberseguridad entre la sociedad vasca y fortalecer el sector profesional.

¹³ **Planteamiento 3/2/1:** la regla 3/2/1 es una técnica para hacer copias de seguridad y consiste en hacer 3 copias de tus datos en 2 soportes diferentes, y 1 en un lugar físico distinto.

¹⁴ **LTS:** son las siglas en inglés de «*Long Term Support*» (soporte a largo plazo). Es un término informático usado para hablar de un software que tendrá un soporte que será actualizado durante más tiempo que una versión normal.

- Relación Servicios Convergentes – Cumplimiento Normativo (ISO27001, ENS, etc.)
- Estándares de Seguridad: definición de estándares de obligado cumplimiento
- Procedimientos de Respuesta a Incidentes de Seguridad

- ▲ **Backup de SharePoint O365:** durante 2021 se probó una solución para proteger y archivar la información con una retención más allá del servicio base que incluye la papelera de reciclaje. A lo largo de 2022 se espera disponer de un suministro de licencias para ofrecer este nuevo servicio.
- ▲ **Señuelo:** durante 2022, en colaboración con el BCSC¹², se pretende hacer algún ejercicio en este ámbito.

PROYECTOS EN EVOLUCIÓN

- ▲ **Backup y Recuperación:** el nuevo servicio de copias de seguridad «*Zaintza*» usa un planteamiento 3/2/1¹³, en el que además se siguen varias prácticas para evitar los ataques *ransomware*: los repositorios que almacenan las «*copias offsite*» están aislados de la red y sólo permiten el tráfico entrante de réplica. Asimismo, todos los elementos relacionados con el entorno de *backup* están en versiones LTS¹⁴ en vigor para evitar la exposición a vulnerabilidades, etc. A lo largo de 2022 se tiene previsto incluir las siguientes mejoras:
 - Las bibliotecas del repositorio se van a marcar como «*WORM*» («*Write Once, Read Many*»; «*escribe una vez, lee muchas veces*») para que no puedan ser borradas accidentalmente o expresamente hasta que expiren, según la política de retención.
 - Se va a poner autenticación de doble factor para proteger los inicios de sesión del personal técnico en los repositorios de *backup*.
- ▲ **Reglas, Segmentación y Firewall:** durante 2020 se estableció un grupo de trabajo para realizar la «*higienización*» de los *firewall* existentes en BATERA. En 2022 se pretende migrar varios entornos *firewall*.
- ▲ **Servicio Rapid7 y HDIV:** a finales de 2020 se empezó a trabajar en un proyecto para mejorar

la gestión de vulnerabilidades completa. Durante 2021 se definió el servicio de gestión de vulnerabilidades, que se pretende consolidar durante 2022. En 2023 se quiere ampliar el servicio con nuevas herramientas. Por otra parte, durante 2021 se implantó el uso de la herramienta HDIV en todos los grupos de Asistencia Técnica de EJIE en formato IAST (análisis de vulnerabilidades de código fuente), quedando pendiente para 2022 la incorporación de las funcionalidades RASP (protección frente a la explotación de vulnerabilidades).

«Dentro del Plan Director de Seguridad se identificaron 42 iniciativas clasificadas por ámbitos y prioridades»

- ▲ **Cuadro de Mando:** en 2020 se definieron los servicios de seguridad que se ofrecen en BATERA. Durante 2021 se redefinieron estos servicios, pasando a integrar los Servicios Convergentes de Seguridad. El objetivo es tener todos los indicadores definidos y modelados durante 2022-23.
- ▲ **Bastionado y Cifrado:** durante 2021 se definieron parte del bastionado o «*hardening*» en el ámbito del Puesto de Trabajo y en 2022 se ha comenzado a trabajar en el ámbito de las Plataformas. En el Puesto de Trabajo se está avanzando en el cifrado de los Puestos de Trabajo. En el caso del Gobierno Vasco, por ejemplo, los equipos renovados ya van cifrados. En otras entidades se ha empezado por los portátiles, siendo la siguiente fase la extensión del cifrado a los equipos de sobremesa.
- ▲ **CMDB:** el objetivo es consolidar ServiceNow como la nueva CMDB.
- ▲ **Revisión VPN:** durante 2022 se va a montar el servicio de «*VPN Convergente*» que permitirá actualizar los entornos «*legacy*» actuales. Asimismo, este año también se pretende definir el modelo de Acceso Remoto en todos los ámbitos.

▲ **Securización Correo:** durante 2021 se realizó una revisión y configuración de los mecanismos SPF, DKIM y DMARC para todos los dominios albergados en O365 Elkarlan. Durante 2022 se pretende ir implementando DMARC en modo «reject». Asimismo, se harán avances en otros ámbitos fuera de O365 y en 2023 se pretende proporcionar niveles de seguridad adicionales en el correo electrónico.

«La movilidad, los servicios en la nube y el nivel de exposición hacia el exterior de los servicios internos, hace que el nivel de riesgo aumente exponencialmente»

▲ **DRP** [«Disaster Recovery Plan» o «Plan de Recuperación de Desastres»]: se han realizado los simulacros previstos en el Plan de Continuidad de 2020, se preparó el Plan de Continuidad de 2021 y se está trabajando en adecuar el escenario de continuidad «legacy» a BATERA. En 2021 se empezó a trabajar en el desarrollo del sistema de gestión de la Continuidad de Negocio sobre el servicio IaaS para su futura certificación bajo ISO 22301.

▲ **BIA** [«Business Impact Analysis» o «Análisis de Impacto del Negocio»]: en 2021 se realizó el BIA tanto de EJJIE como del Gobierno Vasco y está planificada su revisión periódica.

▲ **Concienciación:** en EJJIE se ejecutó en 2021 el Plan anual de formación, se realizaron varios simulacros de «phishing»¹⁵ y se cumplió el Plan de publicación de «píldoras» de concienciación sobre seguridad. En el caso del Gobierno Vasco se ha ido publicando información relacionada con la seguridad en

distintos boletines Aurrera, se ha impartido una formación en ciberseguridad a todo el personal y también se ha hecho una campaña de «phishing».

▲ **Revisión de productos certificados:** se ha analizado el grado de cumplimiento de los productos de seguridad implantados en EJJIE según el catálogo de productos certificados, y se ha concluido que, si bien el grado de cumplimiento es muy bajo (basándose en el catálogo del CCN [Centro Criptológico Nacional]) no se identifica ningún riesgo ya que el catálogo del CCN todavía es muy limitado y los productos de EJJIE son de reconocido prestigio.

▲ **Revisión de algoritmos certificados:** durante 2022 se quiere definir el alcance de esta revisión y los ámbitos donde se aplicará.

▲ **Etiquetado y Clasificación de soportes:** en 2021 se desarrolló un procedimiento en el Gobierno Vasco (dentro del ámbito «GureSeK») para gestionar el etiquetado y la clasificación de los soportes. Se tiene previsto implantar durante 2022.

▲ **Gestión de obsolescencia:** se está avanzando en el ciclo de vida de sistemas operativos en el ámbito del Puesto de Trabajo para agilizar las actualizaciones. En el ámbito de las aplicaciones, se dispone de un análisis de 2021 sobre obsolescencia tecnológica que periódicamente se revisa con los departamentos para establecer las acciones necesarias para la migración, un proceso que se llevará a cabo durante 2022 y 2023.

Tal y como hemos comentado, la idea es revisar periódicamente el estado en el que se encuentran los proyectos e incluir aquellas iniciativas que sean necesarias, incorporando los últimos avances tecnológicos en materia de Seguridad.



¹⁵ **Phishing:** para más información, podéis consultar el artículo titulado «Los viejos peligros de Internet: el phishing o la suplantación de identidades», publicado en el boletín Aurrera número 66 (diciembre 2018).





ALBOAN

El Gobierno del Dato en el Gobierno Vasco

El mayor activo que tiene hoy en día cualquier organización, aparte de las personas, son los DATOS que alberga en sus sistemas de información.

Actualmente estamos inmersos en una transformación digital que hace que la cantidad de datos que tiene que gestionar cada año cualquier entidad (incluidas las Administraciones Públicas) aumente de forma exponencial.

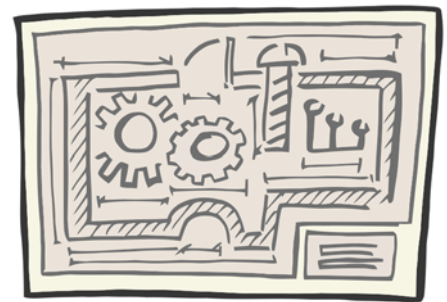


De hecho, el recurso «dato» es considerado hoy en día como el «oro» de la era digital, por lo que cualquier entidad debería disponer de una **estrategia global** para conseguir gestionar esos datos de una forma eficiente y eficaz, y al mismo tiempo, hacer que esos mismos datos se conviertan en un valor estratégico para la entidad. Y es ahí donde surge el concepto de «*gobernanza*» o «*gobierno del dato*».

GOBERNANZA DEL DATO

Si pensamos en el futuro, la «*gobernanza del dato*» constituye hoy en día un instrumento esencial para cualquier Administración, ya que permite generar valor público y responder a las necesidades y demandas de la ciudadanía de una manera mucho más efectiva.

Con objeto de preparar el camino a seguir, el pasado mes de febrero el Gobierno Vasco



puso en marcha un Equipo de Trabajo o **Comité Técnico** cuyo objeto es definir precisamente las líneas estratégicas a seguir por parte del Gobierno Vasco en este ámbito.

EQUIPO DE TRABAJO

Los órganos responsables de impulsar los trabajos de este Comité Técnico son la Dirección de Atención a la Ciudadanía y Servicios Digitales (DACSD) y la Dirección de Tecnologías de la Información y la Comunicación (DTIC).

Con respecto a las personas u órganos encargados del liderazgo y supervisión del proyecto (**nivel estratégico**) son las siguientes:

- ▲ Consejera de Gobernanza Pública y Autogobierno
- ▲ Viceconsejera de Relaciones Institucionales
- ▲ Viceconsejero de Administración y Servicios Generales
- ▲ Comisión Interdepartamental (Directores/as de Servicios y equivalentes)

En cuanto a la dirección y control del proyecto (**nivel operativo**) recaen en:

- ▲ Director de Atención a la Ciudadanía y

Servicios Digitales

▲ Director de Tecnologías de la Información y la Comunicación

▲ Responsables técnicos del Proyecto

Mientras que los responsables de la ejecución de las acciones para lograr los objetivos (**nivel ejecutivo**) son:

▲ Comité Técnico (personas responsables de los objetivos e iniciativas concretas y órganos administrativos implicados)



En este caso, el Comité Técnico lo constituyen un grupo de personas que actúan en representación del Eustat, de los Órganos estadísticos de los Departamentos, de OpenData Euskadi, de GeoEuskadi, de EJIE, técnicos de la Dirección de Tecnologías de la Información y la Comunicación (DTIC), de la Dirección de Atención a la Ciudadanía y Servicios Digitales (DACSD), de la Dirección de Economía y Planificación y de la Delegada de Protección de Datos de la Comunidad Autónoma de Euskadi.

CONTEXTO

Según la planificación inicial, el proyecto tendrá una duración aproximada de dos años, y se han establecido una serie de hitos o entregables que irá elaborando el propio Equipo de Trabajo, el cual, tal y como hemos detallado, está compuesto por responsables de distintas áreas, conformando un equipo multidisciplinar.

A día de hoy, se ha entregado y validado ya el documento titulado «Contexto y marco

estratégico», y se está trabajando en el «Diagnostico», en el que se concluirán los principales retos a los que deberemos enfrentarnos en los diferentes aspectos de la gobernanza del dato y los riesgos de la estrategia.

En el primer documento («Contexto y marco estratégico») se recoge el contexto normativo en el que se encuentra actualmente la Administración Pública y su relación con la gestión de datos, presentando para ello la normativa existente a nivel internacional y europeo, así como las iniciativas y medidas que se han llevado a cabo por parte de la Administración General del Estado para impulsar la gobernanza de datos, se presenta también un resumen de las distintas iniciativas que se están llevando a cabo en otras Comunidades Autónomas y, finalmente, se hace un repaso a las iniciativas que se han realizado o se están realizando en Euskadi (incluido el Gobierno Vasco).

El documento incluye, además, un apartado sobre los aspectos que implica este tipo de proyectos y que hay que tener en cuenta (marco legislativo), incidiendo también en las áreas de actuación y responsabilidades que deberá asumir cada área.

CONCLUSIONES

Como hemos comentado, se trata de un proyecto de largo recorrido que poco a poco irá perfilando su alcance, elaborando otros documentos o entregables, por lo que os iremos informando. □



Más información en el artículo titulado «Gobierno del Dato», publicado en el boletín Aurrera número 77 (septiembre de 2021)

AL CIERRE

40 aniversario de EJIE

El 23 de marzo de 1982 se publicaba en el Boletín Oficial del País Vasco el «Decreto 60/1982, de 1 de febrero, a propuesta del Departamento de Economía y Hacienda, sobre la constitución de la Entidad Mercantil Anónima Eusko Jaurlaritzaren Informatika Elkarte - Sociedad Informática del Gobierno Vasco, S.A», a través del cual se creaba oficialmente EJIE.

Por lo tanto, este año EJIE ha cumplido 40 años.

EJIE es el órgano gestor tecnológico del Gobierno Vasco que facilita la digitalización de los servicios públicos, y garantiza la calidad, seguridad y continuidad de las tecnologías de la información y la comunicación que los soportan.

La relación entre la Administración de la Comunidad Autónoma del País Vasco y EJIE está hoy en día definida mediante el Decreto 36/2020, de 10 de marzo, y como Órgano Tecnológico que es, EJIE se encarga del mantenimiento de los servicios y la infraestructura corporativa del Gobierno Vasco, así como de gestionar los proyectos tecnológicos estratégicos de la Administración vasca, entre los que podemos destacar el proceso de Convergencia («proyecto BATERA») que está llevando a cabo la Administración Vasca, y cuyo objetivo es optimizar el uso de los recursos disponibles y permitir a las Administraciones ser más eficientes a la hora de prestar sus servicios a la sociedad vasca.

Actualmente, son más de 200 personas las que forman parte de la plantilla de EJIE, a quienes desde aquí les enviamos nuestra felicitación por este 40 aniversario.

Más información en:
<https://www.ejie.eus>



PROTAGONISTAS

Kateryna Yushchenko y los lenguajes de programación

Kateryna L. Yushchenko (Chigirin, 8 de diciembre de 1919 - 15 de agosto de 2001) fue una científica de la computación ucraniana, miembro de la Academia de Ciencias de la URSS (1976) y de la Academia Internacional de Ciencias de la Computación.

Fue la encargada de desarrollar uno de los primeros lenguajes de programación de direcciones indirectas de alto nivel del mundo llamado **Lenguaje de Programación basado en Direcciones** («Address Programming Language»).

Kateryna recibió dos premios estatales de la URSS: el premio del Consejo de Ministros de la URSS y el premio del académico Glushkov. Fue nombrada también miembro de la Orden de la Princesa Olga.

Durante su carrera académica Yushchenko supervisó a 45 estudiantes de doctorado.

Yushchenko fue la primera mujer en la URSS en convertirse en **doctora en física y matemáticas** para programación.



En 1955 Korolyuk y Yushchenko desarrollaron el «address language», un lenguaje basado en dos principios generales para trabajar con computadoras: direccionamiento de memoria y gestión de software. Este lenguaje estaba muy adelantado con respecto a otros lenguajes de la época como Fortran (1958) y Cobol (1959). Sus formas y construcciones fueron incluidas posteriormente en lenguajes modernos. Kateryna, Gnedenko y Korolyuk escribieron en 1961 el **primer libro de programación** soviético, titulado «The Elements of Programming».

Más información en:
Wikipedia y <https://mujeresconciencia.com>