



# URRERA!

Nº 68

junio 2019

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico

Dirección de Informática y Telecomunicaciones

## ÍNDICE

- La Administración Electrónica sigue avanzando en Euskadi  
Pág. 2
- El Análisis de Riesgos en el ámbito del ENS  
Pág. 6

### Alboan:

- Consejos sobre Windows10 y Office365: Introducción  
Pág. 10

### Contraportada:

- La desinformación en el ciberespacio
- Alicia Monje Micharet gana el premio Ada Byron  
Pág. 12

**L**levamos mucho tiempo hablando de la Administración Electrónica y de las grandes ventajas que puede suponer tanto para la propia Administración como para la ciudadanía. Pero, después de tanto trabajo y esfuerzo, ¿sabemos en qué situación estamos? En el primer artículo, titulado «*La Administración Electrónica sigue avanzando en Euskadi*», tomando como base un reciente estudio comparativo llevado a cabo por la empresa de consultoría Ernst & Young, tendremos la oportunidad de ver cuál es el resultado de todo ese esfuerzo.

En el segundo tema, titulado «*El Análisis de Riesgos en el ámbito del ENS*», nos hemos centrado en esta ocasión en un asunto aparentemente poco atractivo pero que, sin embargo, es fundamental precisamente para que la Administración Electrónica ofrezca un buen servicio, se trata del trabajo que supone analizar los peligros y riesgos que nos rodean y, sobre todo, cómo gestionarlo correctamente para que no afecte al servicio que se presta a la ciudadanía a través de sus Sistemas de Información.

En el apartado Alboan, por su parte, comenzamos una serie de artículos (o píldoras formativas) todos ellos relacionados con el Windows10 y el Office365 que se están instalando en nuestros puestos de trabajo. Son muchas las novedades que nos trae esta nueva plataforma y es por ello que hemos considerado que sería interesante explicar algunas de sus funcionalidades, así como la forma en que tendremos que trabajar a partir de ahora. Esperando que sea de utilidad para todo el personal del Gobierno Vasco, en esta ocasión hablaremos de conceptos como: la «nube», las ventajas de «compartir ficheros», el «versionado» de los documentos, etc.

En la última sección, repasamos brevemente el peligro que puede suponer para un país algo tan simple como es «*la desinformación en el ciberespacio*», y el informe que al respecto ha publicado recientemente el Centro Criptológico Nacional (CCN).

Para acabar, queremos destacar también el premio Ada Byron 2019 que hace unas semanas entregó la Universidad de Deusto a la Doctora por la Universidad de Extremadura Concepción Alicia Monje Micharet, cuya investigación gira en torno a los robots.

## La Administración Electrónica sigue avanzando en Euskadi



Durante muchos años, las Administraciones Públicas han realizado grandes esfuerzos para implantar la llamada «Administración Electrónica» o «eAdministración». Ahora, gracias a un estudio publicado recientemente, podemos ver cuál es la situación de las distintas administraciones.



### <sup>1</sup> Normativa:

**Ley 39/2015**, de Procedimiento Administrativo Común, publicada en el BOE número 236, del 2 de octubre de 2015  
<https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565>

**Ley 40/2015**, de Régimen Jurídico del Sector Público, publicada en el BOE número 236, del 2 de octubre de 2015.  
<https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566>

<sup>2</sup> **Ernst & Young:** el origen de la empresa se remonta al Siglo XIX y sus fundadores fueron Arthur Young y Alwin C. Ernst.

El nombre EY de la empresa surge de la fusión global entre Ernst & Whinney y Arthur Young en 1989.

Página web de la empresa:  
<https://www.ey.com/es>

**E**n octubre de 2015 se aprobaron dos importantes normas que están suponiendo un gran cambio en el funcionamiento de las Administraciones Públicas, sobre todo a la hora de prestar los servicios públicos a la ciudadanía. Como no podía ser de otra forma, nos estamos refiriendo a la **Ley 39/2015** de Procedimiento Administrativo Común (LPAC), y a la **Ley 40/2015** de Régimen Jurídico del Sector Público (LRJSP)<sup>1</sup>.

Los cambios que introducen estas dos leyes suponen un gran impulso para la digitalización de la administración, y en el fondo también supone un importante beneficio tanto para la ciudadanía/empresas como para la propia administración.

### EL INFORME

La empresa Ernst & Young (EY<sup>2</sup>), especializada en proyectos de consultoría y auditoría, ha analizado en total 90

administraciones públicas para conocer el grado de cumplimiento de esas dos normativas en su ámbito, tomando de referencia la percepción de una persona que necesita realizar un trámite online con su administración.



Portada del informe de Ernst & Young titulado: «La Administración Digital en España. Desde la perspectiva del ciudadano y de la empresa»



El resultado de ese trabajo ha quedado recogido en un informe titulado «*La Administración Digital en España. Desde la perspectiva del ciudadano y de la empresa*», publicado el pasado mes de marzo.

El informe, que consta de 48 páginas, tiene como objetivo analizar el **grado de madurez digital** de las administraciones públicas en España. Para ello, se han analizado el cumplimiento de todos los requerimientos básicos recogidos en la Ley 39/2015 y en la

Ley 40/2015.

Para llevar a cabo el trabajo, la consultora EY ha analizado todas las comunidades autónomas (17), las diputaciones y cabildos (52), así como los principales ayuntamientos de España (21).

«El informe, que consta de 48 páginas, tiene como objetivo analizar el grado de madurez digital de las administraciones públicas en España»

Veamos ahora cuáles son las principales conclusiones de este informe...

## LOS DATOS

Para la elaboración de este informe se han identificado 132 requerimientos contenidos en las Leyes 39 y 40/2015 que han sido agrupados en diferentes temáticas.

Para conocer el grado de cumplimiento sobre los indicadores seleccionados, se han utilizado múltiples fuentes de información y canales de comunicación abiertos por las propias administraciones públicas para que las personas usuarias (así como las empresas) puedan realizar sus trámites:

1. Portal web
2. Sede electrónica
3. Identidad digital y firma electrónica
4. Registro electrónico y representación
5. Asistencia al Ciudadano y empresa
6. Comunicaciones y notificaciones a la ciudadanía
7. Expediente, documento y archivo electrónico

Pues bien, según los datos recogidos en el informe de Ernst & Young, **Euskadi** es la comunidad autónoma más avanzada en funcionamiento digital, al cumplir el 94,7%

de esas exigencias, seguido de Galicia (94,2%), Cataluña (93,5%), Asturias (90,2%) y Madrid (89,5%).

De todas formas, tras el resultado del análisis realizado, se constata que ninguna de las administraciones públicas analizadas cumple con la totalidad de los requerimientos extraídos de las Leyes 39/2015 y 40/2015. A este respecto, es importante recordar que la moratoria aprobada en septiembre de 2018 afecta a los siguientes requerimientos, que entrarán en vigor en 2020: registro electrónico de apoderamientos, registro electrónico, registro de empleados públicos habilitados, punto de acceso general electrónico de la administración y archivo único electrónico.



Por otra parte, según se indica en el informe, las temáticas en las cuales las Administraciones Públicas analizadas deben realizar un mayor esfuerzo son: comunicaciones y notificaciones a la ciudadanía, registro electrónico y representación.

La empresa EY señala, además, que la Administración Digital supone un cambio de funcionamiento muy importante para cualquier administración pública, y supone, además, un gran reto para muchas de ellas.



Plan Estratégico de **Gobernanza e Innovación Pública 2020**

Por ello, la EY recomienda que para conseguir implantar una Administración Digital con garantías y seguir mejorando los servicios que se ofrecen, las administraciones deben desarrollar previamente un plan de transformación digital con vista a varios años. A este respecto, el Gobierno Vasco dispone en estos momentos del PEGIP2020<sup>3</sup> («Plan Estratégico de Gobernanza e Innovación



<sup>3</sup> **PEGIP2020**: son las siglas del «Plan Estratégico de Gobernanza e Innovación Pública» y podéis consultar toda su información en la siguiente web:

[www.euskadi.eus/blog/pegip2020/](http://www.euskadi.eus/blog/pegip2020/)



Una pieza importante de la Administración Electrónica del Gobierno Vasco es **PLATEA**. Es la palabra con la que identificamos la «Plataforma Tecnológica para la eAdministración» del Gobierno Vasco, la cual está compuesta por diferentes módulos que pueden usar los Departamentos y Organismos Autónomos a la hora de desarrollar sus aplicaciones, sin preocuparse de las tareas relativas al desarrollo y mantenimiento de los elementos comunes.

*Pública*»), que tiene entre sus objetivos estratégicos la implantación y despliegue de la administración electrónica en nuestro ámbito, así como completar la oferta de servicios electrónicos y promover su uso entre la ciudadanía.



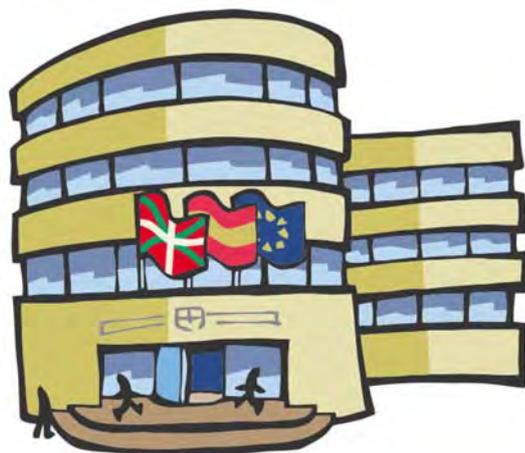
**4 Sede electrónica:** es el lugar en Internet (web) donde cualquier persona puede acceder a la información y hacer trámites de una forma segura. Esta web garantiza que la información y los servicios que en ella aparecen son completos, reales y están actualizados.

La sede electrónica de la Administración Pública de la Comunidad Autónoma de Euskadi es la siguiente:

<https://www.euskadi.eus>

**5 Carpeta Ciudadana:**

es una herramienta online que permite a una persona comunicarse con su Administración sin necesidad de desplazarse físicamente a sus oficinas. La «Carpeta Ciudadana» ofrece servicios de administración digital a la ciudadanía, como pueden ser, entre otros: acceder a información pública, descargar formularios, consultar datos personales, etc. dando la posibilidad de operar y establecer relaciones telemáticas seguras que actualmente sólo podrían realizarse de forma presencial por la persona interesada.



## EUSKADI

Si nos centramos en Euskadi, la consultora EY destaca como **puntos fuertes** los siguientes aspectos:

- ✓ Disponer de un portal web que incluye una sección para peticiones de la ciudadanía, propuestas y respuestas del Gobierno y preguntas parlamentarias.
- ✓ Ser líder en los requerimientos relacionados con la sede electrónica<sup>4</sup>, ofreciendo un servicio eficaz y ágil a la ciudadanía y empresas, así como una navegación y una cartera de servicios amplia.



- ✓ En el apartado de las comunicaciones y notificaciones a la ciudadanía, emplear medios electrónicos para notificar a las partes interesadas que hayan seleccionado esta forma de notificación, y dar un paso más en este aspecto realizando las comunicaciones por medio de la «Carpeta Ciudadana»<sup>5</sup> o un

buzón de notificaciones, siendo referente en esta práctica junto a Galicia.

- ✓ Ser una de las mejores prácticas del Estado respecto a la atención a la ciudadanía y empresas por medios electrónicos.
- ✓ En cuanto al Registro Electrónico y Representación, Euskadi es (también junto a Galicia) la comunidad autónoma con mejor puntuación, a pesar de no superar el 83% del cumplimiento. [La consultora EY considera este apartado uno de los aspectos en los que más margen de mejora tienen todas las Comunidades Autónomas]

## OTROS DATOS

Asimismo, si nos fijamos en los servicios ofrecidos por las **Diputaciones Forales** (o equivalentes) y los **ayuntamientos**, estos son los datos más significativos:

- La media del índice de cumplimiento de todas las diputaciones se sitúa en un 64%. Se observa que ninguna diputación cumple la totalidad de los requerimientos extraídos de las leyes analizadas. La Diputación Foral de Guipúzcoa es el organismo que más se aproxima al modelo de cumplimiento básico, con un 96,5%, seguido por la Diputación de Sevilla, con un 84,7% del índice establecido.
- Los resultados del estudio elaborado revelan la dificultad de las diputaciones en el desempeño de los requisitos recogidos en las temáticas de Representación y registro electrónico y Comunicaciones y notificaciones a la ciudadanía.



- Asimismo, se destacan también los servicios ofrecidos en otros ámbitos por parte de la Diputación Foral de Vizcaya y la Diputación Foral de Álava.

**«Según los datos recogidos en el informe de Ernst & Young, Euskadi es la comunidad autónoma más avanzada en funcionamiento digital»**

- En referencia a los ayuntamientos analizados, se indica que la media del índice de cumplimiento se sitúa en un 64,5%. Se observa, además, que ningún Ayuntamiento cumple la totalidad de requerimientos extraídos de las leyes analizadas.
- De los ayuntamientos analizados, Sólo el 33% cumple con los requisitos de firma electrónica estipulados por Ley. Entre ellos resaltan, entre otros, los de Málaga, Bilbao y Palma de Mallorca.
- Los ayuntamientos de Vitoria-Gasteiz, Málaga y Valencia ofrecen la asistencia necesaria en materia de identificación y representación para los sujetos obligados a relacionarse con la

administración telemáticamente.

### CONCLUSIÓN

Una vez analizado el trabajo realizado por la empresa Ernst & Young, el informe sitúa a Euskadi a la cabeza del Estado en Administración Digital en cuanto al importante esfuerzo demostrado en el ámbito de la Administración Digital. No obstante, también hay que ser conscientes que aún queda camino por recorrer, y por ello el Gobierno Vasco seguirá realizando esfuerzos tanto a nivel de inversiones como de organización con el fin de cumplir lo antes posible los requerimientos legales que la administración electrónica nos impone y satisfacer así las necesidades de las personas a las que prestamos servicio. □



#### EL INFORME

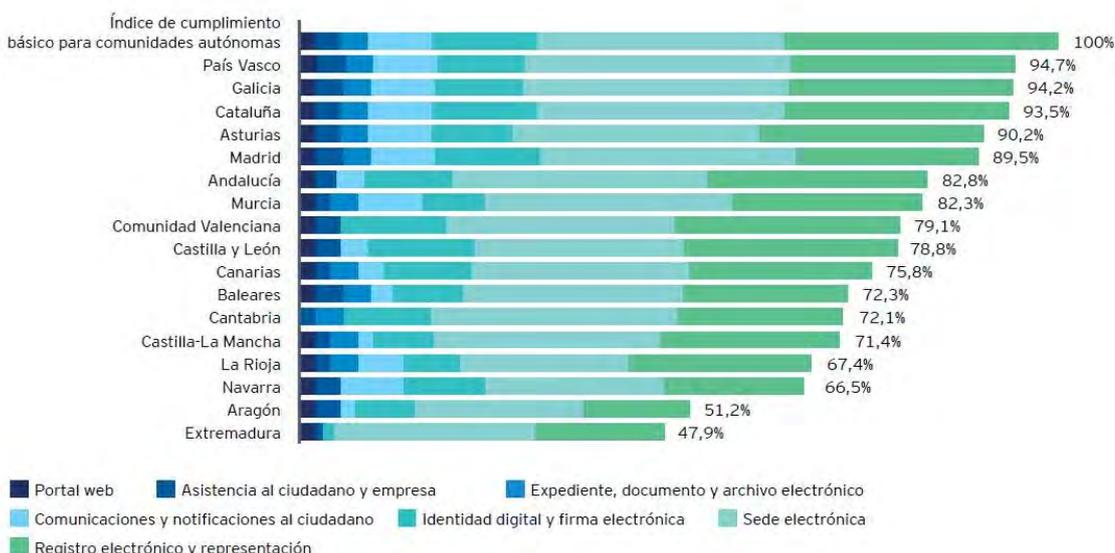
El informe elaborado por la consultora Ernst & Young, titulado «La Administración Digital en España. Desde la perspectiva del ciudadano y de la empresa», está disponible en la siguiente dirección:

[https://www.ey.com/Publication/vwLUAssets/ey-la-administracion-digital-en-espana/\\$FILE/ey-la-administracion-digital-en-espana.pdf](https://www.ey.com/Publication/vwLUAssets/ey-la-administracion-digital-en-espana/$FILE/ey-la-administracion-digital-en-espana.pdf)



Foto de la portada del informe de Ernst & Young

## Análisis del índice de madurez de las comunidades autónomas



## El Análisis de Riesgos en el ámbito del ENS



Se trata de la metodología para prevenir las amenazas y combatir los riesgos que los distintos tipos de ataques pueden provocar en la información en poder de la Administración. Veamos cómo lo gestiona el Gobierno Vasco.



<sup>6</sup> ENS: Son las iniciales del Esquema Nacional de Seguridad que viene regulado por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

(publicado en el BOE, núm. 25, de 29 de enero de 2010)

<https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330>

El ENS tiene como finalidad la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos en la Administración Electrónica, para lo cual se establecen los principios básicos y requisitos mínimos a cumplir en materia de seguridad.

En cumplimiento del ENS, el Consejo de Gobierno de la Comunidad Autónoma de Euskadi, en sesión celebrada el día 30 de junio de 2015, acordó la aprobación de la estructura organizativa y asignación de roles de seguridad para la Administración Electrónica del Gobierno Vasco.

Dentro del proceso de «Seguridad de la Información» en el Gobierno Vasco, liderado desde la Dirección de Informática y Telecomunicaciones en el ámbito del ENS<sup>6</sup>, existe una tarea obligatoria a realizar de manera periódica: el **Análisis de Riesgos**.

Antes de nada, cabe indicar que el ENS se regula en el Real Decreto 3/2010, de 8 de enero, y es establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y fue modificado por el Real Decreto 951/2015. En ellos se indica que:

*«El ENS persigue fundamentar la confianza de que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas, desarrollándose y perfeccionándose en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan»*

Se podría resumir diciendo que el ENS busca afianzar la confianza de las personas en su interacción electrónica con las administraciones públicas.

### EL OBJETIVO

El objetivo del Análisis de Riesgos en el ámbito del ENS es el siguiente:

✓ Saber qué información y sistemas se usan

en el Gobierno Vasco

- ✓ Saber quién es el responsable real
- ✓ Saber qué impacto tendría su indisponibilidad
- ✓ Saber qué amenazas sobrevuelan
- ✓ Saber qué probabilidad hay de que ocurran
- ✓ Saber qué medidas hay de cobertura

El Gobierno Vasco ha decidido realizar un análisis de riesgos corporativo con los siguientes objetivos:

- ✓ Conseguir que la organización tome conciencia de sus principales riesgos
- ✓ Identificar las principales vulnerabilidades de la organización
- ✓ Fijar las prioridades de actuación en base a una metodología global
- ✓ Ejecutar acciones que consigan minimizar los riesgos, dando así mayor seguridad a la organización
- ✓ Proteger la imagen de la organización.

Para llevarlo a cabo, es necesario contar con la colaboración de los responsables de los Departamentos y Organismos Autónomos con servicios electrónicos dentro del alcance del análisis. La manera de colaborar es **rellenando una encuesta** que se les envía para que valoren el impacto de las cinco dimensiones de la seguridad (se explican más adelante) sobre los servicios que quedan bajo su responsabilidad.



La «encuesta» se realiza con una herramienta

llamada **GlobalSuite**<sup>7</sup> y, a continuación, se explican los pasos que se han realizado para su cumplimentación.

Aquellas personas que son responsables de los servicios electrónicos del Gobierno Vasco



Software de implementación integral de ISO 27001 - ISO 20000 - ISO 22301  
Notificaciones GlobalSUITE

Estimado cliente,

Su contraseña de acceso a GlobalSUITE (R) ha sido restablecida.

Para registrarse utilice los nuevos datos de acceso:

- Introduzca en su navegador la dirección web <https://s.g.globalsuite.es/> o haga click sobre la misma.
- Introduzca su nombre de usuario: patrobaz.
- Introduzca la nueva contraseña.

Nota: No conteste a este correo, pues se envía desde una dirección no habilitada para la recepción de mensajes.

reciben un correo electrónico (Alertas GlobalSUITE) en el que se les informa de que tiene pendiente una serie de valoraciones.

Cuando la persona encargada accede a la encuesta, visualiza su listado de servicios electrónicos asignados. Por cada uno de los servicios, hay que realizar una valoración de



su criticidad desde los cinco puntos de vista que el ENS establece para la seguridad, a saber:

➤ **Disponibilidad [D]:** esta dimensión recoge el impacto que tendría no disponer del servicio o no poder acceder a él. Cabe indicar que la disponibilidad de un servicio no siempre tiene que ser 24x7, ya que hay algunos que sólo requieren estar disponibles en horario de oficina y de lunes a viernes.

➤ **Integridad [I]:** se valora el impacto que tendría la alteración de una información o dato vinculada al servicio que resulte ser incorrecta, bien sea por un error de un usuario, por una acción deliberada contra la información o por una modificación de una persona sin autorización para dicho cambio.

➤ **Confidencialidad [C]:** esta dimensión debe reflejar el impacto que tendría el hecho de que un usuario sin permisos accediese a información de un servicio determinado o que dicha información fuese publicada.

➤ **Autenticidad [A]:** el impacto que tendría que el usuario identificado no sea quien dice ser. A la hora de valorar esta dimensión, la situación más fácilmente valorable es una suplantación de identidad en aquellos servicios que requieran de unas capacidades o especialización determinada en las personas encargadas de su tratamiento o gestión.

➤ **Trazabilidad [T]:** el impacto que tendría no disponer de información de actividad (qué se ha hecho, quién lo ha hecho y cuándo ha sido). Como ejemplo del impacto de la trazabilidad de un servicio electrónico, sirva la necesidad de demostrar si un trámite ha sido hecho en plazo o no. En caso de que se pierdan o no existan trazas de actividad, sería difícilmente demostrable una situación de incumplimiento de plazos.

El análisis de las dimensiones presenta una independencia entre sus valoraciones, ya que un nivel alto en alguna de ellas no debería afectar, en absoluto, en la valoración del resto de ellas. Sirva como ejemplo la criticidad en materia de confidencialidad relacionada con la información asociada a la solicitud de

Nombre	Flujo	Responsables	Plazo	Planificado inicio	Planificado fin
1. Generación de fichas de comunicación				Integración + 5 segundos	Integración + 5.5 horas
2. Control de actividad de acceso controlado del usuario				Integración + 5 segundos	Integración + 2 horas
3. Gestión de alertas				Integración + 2 horas	Integración + 3.5 horas
4. Gestión de usuarios				Integración + 3.5 horas	Integración + 3.5 horas
5. Gestión de usuarios				Integración + 3.5 horas	Integración + 3.5 horas
6. Gestión de usuarios				Integración + 3.5 horas	Integración + 3.5 horas
7. Gestión de usuarios				Integración + 3.5 horas	Integración + 3.5 horas
8. Gestión de usuarios				Integración + 3.5 horas	Integración + 3.5 horas
9. Gestión de usuarios				Integración + 3.5 horas	Integración + 3.5 horas
10. Gestión de usuarios				Integración + 3.5 horas	Integración + 3.5 horas



<sup>7</sup> **Global Suite:** Es el software seleccionado por el Gobierno Vasco para gestionar el ciclo completo de los riesgos (Identificación, Análisis y Evaluación de riesgos) en base a la norma ISO 31000 para la Gestión del Riesgo.

Página web: [www.globalsuite.es](http://www.globalsuite.es)





## DEFINICIONES

### Activo

Componente, funcionalidad o recurso que tenga valor para la organización: información, datos, servicios, aplicaciones, equipos, comunicaciones, recursos administrativos, físicos y humanos...

### Amenaza

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Las amenazas siempre están presentes, pero se puede intentar evitarlas o paliar los efectos de su materialización.

### Análisis de Riesgos

Proceso para el análisis de las amenazas, vulnerabilidades, riesgos e impactos a los que está expuesto un sistema de información, teniendo en cuenta las medidas de seguridad ya presentes. Sirve como punto de partida para identificar las mejoras en las medidas de seguridad, tanto en lo que se refiere a su efectividad como a sus costes.

ciertos programas de ayuda, siendo su disponibilidad, al mismo tiempo, de una menor criticidad por el amplio espacio temporal que se ofrece para realizar la solicitud.

Gestión de Encuestas: Valoración Servicios ENS - Cultura y Política Lingüística 30/07/2010 17:00:31

Guardar Finalizar Encuesta Export

Información de la Encuesta

Datos Generales Encuesta

Encuesta

Tabla de Elementos

Añadir Eliminar

Elemento	Categoría	Disponibilidad	Integridad
WT - Escuela Nueva: Tecnología - Renovar sílabos verb	Servicios		
SAREA - Subvenciones a las compañías de danza	Servicios	Despreciable	
Escuela En Entidades Locales - Diseño	Servicios	Bajo	
Producción Material - Campañas de nueva creación	Servicios	Medio	
Artes plásticas - Difusión Artes plásticas - Producción	Servicios	Alto	
Subvenciones para el inventariado de materiales arqueológicos	Servicios		

Cada **servicio** se evalúa por cada una de estas dimensiones, seleccionando uno de los cuatro niveles posibles de impacto:

- **Despreciable:** no se aprecian consecuencias que provoquen ningún tipo de perjuicio sobre las funciones de la organización
- **Bajo:** las consecuencias supondrían un perjuicio limitado sobre las funciones de la organización o sobre sus servicios (reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque éstas sigan desempeñándose)
- **Medio:** las consecuencias supondrían un perjuicio grave sobre las funciones de la organización o sobre sus servicios (reducción significativa de la capacidad de la organización para atender eficazmente con sus obligaciones fundamentales, aunque éstas sigan desempeñándose)
- **Alto:** las consecuencias supondrían un perjuicio muy grave sobre las funciones de la organización o sobre sus servicios (anulación de la capacidad de la organización para atender alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose)

Cuando se valora el perjuicio, hay que pensar en aspectos como el económico que pudiera resultar para una persona, grupo de personas u organizaciones; otro ámbito de perjuicio es el que se puede producir sobre la imagen pública del departamento u organismo autónomo responsable del servicio electrónico; y, por otro lado, podría existir un perjuicio sobre el cumplimiento normativo del Gobierno Vasco, como el que podría provocar una pérdida de información frente a los requisitos establecidos en el ámbito de la protección de datos, siendo este ejemplo una concatenación de impactos negativos por suponer sanciones económicas y publicidad negativa ante un incumplimiento de los deberes de la organización.

El análisis de riesgos se realiza mediante la consolidación de las valoraciones indicadas en las encuestas completadas por los responsables de los Departamentos y Organismos Autónomos de los servicios electrónicos dentro del alcance del ENS.

Con los resultados del análisis de riesgos realizado en el último ciclo, el Gobierno Vasco dispone que la existencia de una serie de servicios valorados con nivel ALTO se traduce en la necesidad de categorizar como ALTOS todos los sistemas informáticos que dan

Encuesta

Tabla de Elementos

Añadir Eliminar

Elemento	Categoría	Disponibilidad	Integridad	Confidencialidad
Bonos Elkarekin participación ciudadana	Servicios	Alto	Alto	Alto
Bonos Elkarekin ámbito educativo	Servicios	Alto	Alto	Alto
Ayuda para Víctimas del Terrorismo: Organizaciones y Asociac	Servicios			
Becas Irelia de Gobierno Abierto, Transparencia y Participació	Servicios	Alto	Alto	Medio
Becas de especialización en Acción Exterior	Servicios	Alto	Alto	Medio
Ayudas de Derechos Humanos: Municipios	Servicios	Alto	Alto	Alto
IREKIA Gestión de Propuestas Ciudadanas	Servicios	Alto	Medio	Alto
Ayudas de Derechos Humanos: Organizaciones Sociales	Servicios	Alto	Alto	Alto
Vulneración derechos humanos	Servicios			
IREKIA Gestión de actividades con la Prensa	Servicios	Alto	Alto	Alto
Premio «Realidad Social Vasca»	Servicios	Alto	Alto	Alto

soporte a dichos servicios. El Gobierno Vasco debe asegurar que dichos sistemas cumplen las medidas establecidas en el ENS para niveles altos, o establecer un plan de adecuación para aquellos que no lo cumplan, para que se mantenga la calidad de los servicios prestados por el propio Gobierno Vasco a la hora de utilizar la información de los ciudadanos y de las empresas que interactúan con ellos.

## CONCLUSIÓN

Como conclusión, es necesario recordar a todas las personas del Gobierno Vasco que la Seguridad de la Información, dentro de la que se enmarca el ENS, es un **proceso integral**, que requiere medios técnicos, humanos, materiales y organizativos, con capacidad de identificar, evaluar, analizar, gestionar y mantener el nivel de riesgo dentro de los valores definidos.

Dentro del Gobierno Vasco existe un proceso de gestión de la seguridad denominado **GureSeK**<sup>9</sup> que es el encargado de gestionar la



seguridad de los servicios electrónicos prestados a la ciudadanía por los Departamentos y sus Organismos Autónomos y que es quien lidera las tareas requeridas, como es la del análisis de riesgos.

Recordamos que en la política de seguridad

se establecen una serie de obligaciones a cumplir por todo el personal, tanto perteneciente como subcontratado por la Administración Pública de la Comunidad Autónoma de Euskadi, a la hora de participar

**Todo el personal que trabaja en la Administración Pública de la CAE está sujeto a cumplir las normas de seguridad**

en la prestación de dichos servicios electrónicos, bien de forma directa o bien de manera indirecta, tal y como se indica en el apartado «9.4 - Obligaciones generales de las personas usuarias».

Así mismo, se establecen unas directrices a cumplir desde el punto de vista de la seguridad de la información a la hora de llevar a cabo la adquisición de productos o la contratación de servicios relacionados con la prestación de servicios electrónicos por parte de la Administración General de la Comunidad Autónoma de Euskadi y sus Organismos Autónomos. □

### DATOS DE LA ÚLTIMA ENCUESTA

En febrero de 2017, el Gobierno Vasco llevó a cabo una primera auditoría para conocer el grado de cumplimiento de las medidas de seguridad dentro de su ámbito.

El resultado de la auditoría, en general, se consideró suficiente, ya que al haberse llevado a cabo un proceso específico de adecuación a las exigencias del ENS, la mayor parte de los requisitos específicos del ENS se cumplieron.

La DIT presenta un grado global de adecuación al ENS del 80% de conformidad de los controles y medidas de seguridad



aplicables de acuerdo al nivel de protección declarado, teniendo en cuenta que el nivel de protección declarado ha sido un nivel ALTO de protección.

La evaluación del cumplimiento de las medidas de seguridad se ha dividido por cada una de las categorías, dimensiones de las medidas de seguridad establecidas en el anexo II del RD 3/2010 y el RD 951/2015.

A lo largo de los últimos meses, el Gobierno Vasco ha realizado una nueva auditoría cuyos resultados se darán a conocer a los Departamentos y Organismos Autónomos en breve.



<sup>9</sup> **GureSeK**: es la palabra que define el Sistema de Gestión de la seguridad de la información (SGSI) [en inglés, *Information Security Management System*, ISMS], el cual ha sido bautizado con el nombre en euskera de «*Gure Segurtasun Kudeaketa*».

GureSeK es el proceso encargado de gestionar la seguridad de los servicios electrónicos prestados por el Gobierno Vasco a la ciudadanía, garantizando que las medidas de seguridad aplicadas en torno a ellos satisfacen los requisitos legales vigentes y permiten asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de la información asociada.



ALBOAN:



## Consejos sobre Windows10 y Office365: Introducción

«Gracias a la nueva plataforma de Windows10 y Office365 el adjuntar ficheros se va a acabar»

**E**l Office365 y el Windows10 ya han llegado a nuestros puestos de trabajo. Con idea de que todos/as podamos sacar el mayor provecho posible de esta nueva herramienta de trabajo, os presentamos a continuación las características más significativas que nos ofrece, así como una serie de consejos y/o buenas prácticas a tener en cuenta.

Comencemos....

### EN LA NUBE

Una de las primeras ideas que debemos tener clara es que, a partir de ahora, todos nuestros documentos, en lugar de estar ubicados físicamente en nuestro ordenador, van a estar almacenados «en la nube», es decir, en los servidores, y nuestro ordenador lo usaremos únicamente para acceder y trabajar con ellos.



Como consecuencia de ello, las famosas unidades de red M, N... que todos/as hemos usado hasta ahora en alguna ocasión, serán sustituidas por carpetas que estarán soportadas por SharePoint y OneDrive. Esto nos aporta una gran ventaja: nos permite acceder a todos esos documentos desde cualquier otro ordenador (no tiene que ser el nuestro) y desde cualquier lugar (por



ejemplo, desde nuestro ordenador de casa, desde un KZgunea, etc.) sin tener que instalar ningún programa especial o tener que pedir permisos especiales (VPN, OWA, etc.).

El acceso a esta nueva plataforma será a través del siguiente portal web:

<https://portal.office.com>

### LA COMODIDAD DE COMPARTIR

Hasta ahora, en nuestro trabajo del día a día, estamos acostumbrados/as a escribir un documento y enviárselo a alguien (como fichero anexo a través del correo electrónico) para que pueda leerlo y, si es necesario, lo modifique. Posteriormente, esa persona nos lo vuelve a enviar para poder seguir trabajando con la última versión de ese documento. Pues bien, gracias a la nueva plataforma de Windows10 y Office365 el adjuntar ficheros se va a acabar, y en su lugar se va a potenciar el **COMPARTIR** documentos y se impulsará la **COLABORACIÓN** entre distintas personas.

Para ello, sólo tendremos que seleccionar el documento que estamos editando, pulsar la opción de compartir y elegir la persona destinataria para que tenga acceso a nuestro documento. Así de fácil. En lugar de seguir el procedimiento que hacíamos hasta ahora: copiar el documento que queremos enviar, abrir el correo electrónico, anexar el fichero dentro del email, escribir el mensaje y enviárselo.



Además, el nuevo Office365 ofrece otras importantes funcionalidades, como pueden ser la **seguridad** y **control** que nosotros/as, como creadores y propietarios de ese documento, tenemos sobre ese documento. A

la hora de compartir un documento, por ejemplo, podremos elegir cómo lo queremos compartir, es decir, qué permisos vamos a conceder a la otra persona sobre ese documento. Aquí os dejamos algunos ejemplos sobre cómo podemos compartir un documento:

- ✓ Con cualquier persona que tenga su enlace de acceso
- ✓ Con varias personas a la vez (incluso si son trabajadores/as externos al Gobierno Vasco)
- ✓ Sólo con una persona determinada (sin que ninguna otra pueda acceder a su contenido)
- ✓ Con una persona, pero sólo hasta una fecha determinada (fijando una fecha de caducidad)
- ✓ Compartir un documento con una persona para que lo pueda editar con nosotros/as (el nuevo Office365 nos permite coeditar un documento, es decir, que dos o más personas simultáneamente modifiquen el contenido de un documento)

Otra característica importante que nos ofrece el nuevo Office365 es la gestión del **versionado** que hace de un documento. La nueva plataforma es capaz de guardar hasta 500

versiones de un mismo documento y todo ello lo hace de forma automática y sin que el usuario/a tenga que hacer nada. Esta opción nos permite recuperar una versión anterior determinada de un documento de una forma



muy sencilla (sin tener que recurrir a EJE para que nos recupere una copia de seguridad o *backup* de un día concreto).

## FORMACIÓN

Dado que esta nueva plataforma ofrece muchas novedades, la Dirección de Informática y Telecomunicaciones, junto con EJE, ha programado una serie de cursos o sesiones formativas que nos facilite este cambio y conocer todas sus posibilidades.

Asimismo, se ha incluido en la intranet Jakina un apartado específico dedicado a este proyecto. [ver cuadro «Si necesitas ayuda...»]



### SI NECESITAS AYUDA...

En caso de que necesitéis más información, indicarnos que se ha habilitado en la intranet Jakina (dentro del apartado «Formación») una sección titulada «Windows 10 y Office 365», en la cual se irán publicando distintos **documentos** de ayuda, como pueden ser:

- Vídeos (a día de hoy se han publicado más de 50 vídeos de aproximadamente 2 minutos de duración cada uno sobre diferentes utilidades de Windows, Word, Excel, Power-Point y Outlook)
- Manuales u otros documentos de interés (p.ej.: información sobre la migración de los Puestos Informáticos, etc.)



Para resolver cualquier **incidencia** que pudiese surgir, tenéis dos canales que se han habilitado específicamente para este proyecto:

el correo electrónico [o365era@eje.eus](mailto:o365era@eje.eus) (buzón «Eje, Gestion Office365») y el teléfono: 72940.

Para más **información**, podéis consultar los siguientes artículos:

- ✓ Artículo «Llega el Office365» del boletín Aurrera nº 62 (diciembre 2017)
- ✓ Artículo «Windows10 y Office365» del boletín Aurrera nº 63 (marzo 2018)



«El nuevo Office365 ofrece importantes funcionalidades, como pueden ser la seguridad y control que tenemos sobre un documento»



Web de acceso al portal del nuevo Office365:  
<https://portal.office.com>



## AL CIERRE

### La desinformación en el ciberespacio

Saber cómo actuar frente a las campañas de desinformación en el ciberespacio es uno de los mayores retos de seguridad a los que se enfrenta un país.

Diferentes estudios sobre el uso de Internet y los hábitos de consumo de información digital indican que cerca del 90% de la población de entre 16 y 65 años puede ser potencialmente víctima de un **ataque de desinformación**.

El Centro Criptológico Nacional (CCN) ha hecho público recientemente un estudio, titulado «Informe de Buenas Prácticas, Desinformación en el ciberespacio», con el que pretende explicar las características y metodología de las actuales acciones de desinformación, con el objetivo de que la ciudadanía disponga de las herramientas que le permita consumir y compartir información de manera crítica y evitar ser cómplices involuntarios de acciones contra los intereses de un país, facilitando para ello recursos para identificar productos y plataformas de comunicación propias de este tipo de acciones.

Evitar ser víctimas de una campaña de desinformación no es responsabilidad de un único agente. Las **instituciones públicas**, por ejemplo, tienen la obligación de desarrollar las capacidades necesarias para prevenir, detectar y neutralizar este tipo de ataques que se generan contra los

sistemas públicos; las **empresas privadas**, por su parte, deben evitar que sus plataformas digitales se conviertan en herramientas empleadas en campañas maliciosas; y finalmente, **la ciudadanía**, usuaria de medios digitales, deberá concienciarse, tal y como se describe en el **decálogo** incluido en el informe antes citado, para detectar las campañas de desinformación y manipulación. Podemos consultar el decálogo completo, así como ampliar la información, en la siguiente dirección:

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3552-ccn-cert-bp-13-desinformacion-en-el-ciberespacio-1/file.html>

## PROTAGONISTAS

### Alicia Monje Micharet gana el premio Ada Byron

El pasado 16 de mayo, la Universidad de Deusto entregó el Premio Ada Byron 2019 a Concepción Alicia Monje Micharet.

Doctora por la Universidad de Extremadura en 2006, con Premio Extraordinario de Doctorado y Mención de Doctorado Europeo, Concepción Alicia desarrolla actualmente su trabajo en el grupo RoboticsLab de la Universidad Carlos III de Madrid.

Su investigación gira en torno al robot humanoide TEO, concebido como un robot asistencial que permita mejorar la calidad de vida de las personas. Gracias a esta labor ha recibido varios galardones,

como el premio de Excelencia a la Investigación de la Universidad Carlos III de Madrid (2018) y Premio Mujer y Tecnología de la Fundación Orange (2018).

Actualmente codirige también el proyecto europeo RoboCom++, cuyo objetivo es desarrollar el robot compañero asistencial del futuro.

#### Premio Ada Byron Joven

Por otra parte, Ana Freire ha sido galardonada con el premio Ada Byron joven. La ganadora es Ingeniera y Doctora en Informática, Investigadora y docente en la Escuela de Ingeniería de la Universitat Pompeu Fabra (Barcelona), Directora del Centro sobre Sostenibilidad de la misma Universidad. A sus 36 años ha contribuido ya con más de 40 publicaciones científicas, tres patentes y su trabajo tiene varios reconocimientos internacionales: *Google Anita Borg Scholarship*, *Big Data Talent Award*, entre otros. Fue incluida por la revista *Business Insider* entre los 67 jóvenes españoles llamados a liderar la revolución tecnológica.

Su investigación se centra en el estudio de datos con fines sociales, como puede ser el análisis de las redes sociales para detectar enfermedades mentales.

Más información en: <https://www.deusto.es>



Concepción Alicia Monje



Ana Freire

