EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

59

marzo 2017

Boletín divulgativo de Innovación y Nuevas Tecnologías
Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

Seguro que en casa tenéis varios teléfonos móviles, *smartphones* y dispositivos electrónicos. Pero, ¿sabéis con qué minerales están hechos?, ¿y de dónde se extraen? o ¿cuáles son las condiciones laborales de los hombres y mujeres que trabajan en las minas en las cuales se extraen? Y, lo más importante, ¿podemos hacer algo desde aquí por mejorar sus condiciones de vida? Mediante este artículo os presentamos la campaña que ha puesto en marcha la ONG Alboan, titulada «***Lo que tu móvil esconde***», que tiene como principal objetivo mejorar las condiciones laborales de las personas que extraen esos minerales. No os perdáis el artículo y sabréis cómo colaborar con la campaña.

Sin duda alguna, el **correo electrónico** ha sido, es y (posiblemente) será durante mucho tiempo la herramienta más utilizadas en el mundo para la comunicación e intercambio de documentos tanto por las personas como por las empresas. Es por ello que en el segundo artículo repasamos algunos aspectos técnicos sobre su funcionamiento en nuestro ámbito (Gobierno Vasco) y, lo más importante, incluimos un decálogo sobre las obligaciones generales que todo el personal del Gobierno debe tener en cuenta y cumplir a la hora de usar el correo corporativo.

Como es sabido, la **interoperabilidad** es una de las piezas sobre las que pivota la llamada Administración Electrónica. Por ello, y con objeto de potenciar y facilitar dicho servicio entre las distintas administraciones de Euskadi y con el resto de entidades nacionales y europeas, se ha puesto en marcha el denominado Nodo de Interoperabilidad y Seguridad de las Administraciones de Euskadi, también conocido por sus siglas **NISAE**. A lo largo del artículo, os comentamos sus principales características y el papel que va a desempeñar Izenpe, entre otros aspectos.

Por último, en el apartado «*Breves*», os informamos, por un lado, de las ventajas que ofrecerá el nuevo protocolo **WiFi 802.11ax**; y, por otro lado, de la reciente publicación de la nueva versión de ***LibreOffice on line*** y sus características más significativas.

«Lo que tu móvil esconde»

Seguro que muchas de las personas que nos leen tienen en casa algún dispositivo obsoleto (teléfono móvil, *smartphone* o *Tablet*) que ya no usan, y no saben qué hacer con él. Si es así, no os perdáis este artículo, ya que en él os damos a conocer una interesante iniciativa que ha puesto en marcha la ONG Alboan[1], y en la que, dentro de poco, podréis colaborar.

En el mercado hay muchos tipos de dispositivos móviles (teléfonos, tabletas...), pero todos ellos tienen algo en común, los materiales que se han utilizado para su fabricación, entre los cuales podemos destacar los siguientes minerales: tantalio (también llamado tántalo), wolframio (o tungsteno), niobio, coltán, estaño y oro.

Aunque no lo sepamos, estos minerales se hallan «*escondidos*» dentro de nuestros móviles, *tablets* y ordenadores.

El tántalo, por ejemplo, gracias a su gran eficiencia, su alta fiabilidad, estabilidad y su capacidad para almacenar una alta carga electrónica en un volumen muy pequeño, se utiliza principalmente para crear condensadores.

En el caso del niobio, por su parte, se usa, sobre todo, en aeronáutica gracias, a la superconductividad que ofrece, la cual permite a los fabricantes crear electroimanes muy potentes, que son usados en aparatos de resonancia magnética, y en aceleradores de partículas, por ejemplo.

Gracias a todas estas características, las compañías de telefonía han podido crear baterías cada vez más pequeñas y ligeras, y, por lo tanto, dispositivos más pequeños, lo cual es fácil de comprobar si comparamos cualquier teléfono antiguo con los actuales.

MATERIAS PRIMAS

Todos esos minerales son, por tanto, muy valiosos para las grandes empresas, y para los países que disponen de ellos, ya que sin estos minerales no habría sido posible la revolución de las nuevas tecnologías, y en especial la de la tecnología móvil que hemos vivido y disfrutado en los últimos años. Pero hay un problema, y es que muchos de estos minerales son escasos y se concentran en unos lugares muy concretos del mundo.

Según distintos estudios, actualmente los mayores yacimientos o reservas de muchos de estos minerales se encuentran en África, y en concreto en la República Democrática del Congo[2], donde se estima que se encuentran el 80% de las reservas mundiales de coltán, por ejemplo.

Además, debido a los millones de dólares que mueve el sector de las compañías tecnológicas, y la escasez de esa materia prima, la extracción y explotación de este tipo de recursos es motivo de conflictos geopolíticos en esa zona de África, donde se mezclan los intereses de varios países, los de las guerrillas que operan en la región, los de las multinacionales, los de las bandas de contrabando, etc. Tal es así que, según varios informes de Naciones Unidas, su extracción, procesado y venta están controladas por varios grupos armados. Gran parte del dinero que obtienen de la explotación y el tráfico ilegal de estos minerales lo utilizan para comprar más armas con las que perpetuar el conflicto más sangriento desde la Segunda Guerra Mundial.

Es por ello que a todos esos minerales se les conoce también con el nombre de «*minerales*

[1] **ONG Alboan:** es la ONG de cooperación al desarrollo de los Jesuitas en Euskadi y Navarra.

www.alboan.org

[2] **República Democrática del Congo:** es un país de África central, denominado Zaire entre los años 1971 y 1997.

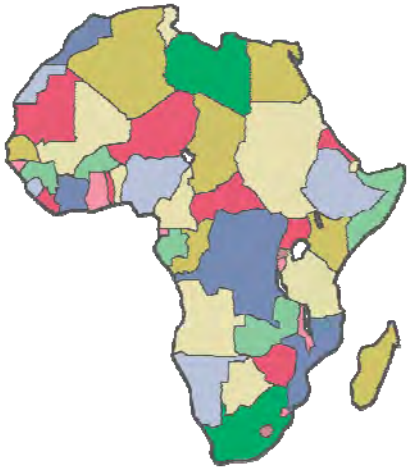
Actualmente es el segundo país más extenso del continente africano.

Tiene una población de 74.618.000 habitantes y su capital es Kinsasa.

[fuente: wikipedia.org]

en conflicto» o «*minerales de sangre*».

La exportación de coltán, en concreto, ha ayudado a financiar a varios grupos armados enfrentados en la guerra del Congo, un conflicto que ha provocado algo más de cinco millones de personas muertas desde 1998, así como un millón de personas desplazadas (sólo en 2013).



Si bien el conflicto en la República Democrática del Congo, que dura ya casi 20 años, tiene raíces muy complejas y profundas, se ha visto agravado por las disputas por el acceso y control de los recursos minerales de la zona, que como ya hemos comentado, se extraen, principalmente, para fabricar teléfonos móviles, tabletas, ordenadores, maquinaria industrial y hasta coches y joyas.

Pero la peor parte se la llevan sin duda las mujeres. Cada año, por ejemplo, más de cien mil mujeres son violadas. La violencia sexual contra las mujeres es un arma de guerra que se utiliza para sembrar el terror y expulsar a la población de sus pueblos. De esta forma, los grupos armados se quedan con el control del territorio donde están las minas.

Las mujeres arrastran de por vida los traumas psicológicos de la violación y del desplazamiento. Muchas veces las dejan embarazadas o les contagian enfermedades de transmisión sexual, como el SIDA. Además, las mujeres violadas normalmente son rechazadas por sus maridos, familias y por su entorno. A menudo tienen que huir de su comunidad y vivir su dolor en silencio y soledad para no ser estigmatizadas.

Además, en los campos de personas desplazadas escasea la comida, y la necesidad de alimentar a sus hijos e hijas las convierten en víctimas de todo tipo de abusos.

CONCIENCIAR

Tanto Naciones Unidas como diversas ONG indican que existe una vinculación directa entre la extracción y la compra-venta de esos minerales, y la financiación de los grupos armados que operan en esa zona. Y eso es precisamente lo que la ONG Alboan quiere evitar a través de una iniciativa que ha puesto en marcha, bajo el nombre de «*Tecnología Libre de Conflicto*»[3]. El objetivo de la misma es dar a conocer la conexión que existe entre los móviles, *tablets* y ordenadores que usamos diariamente, con la guerra y la vulneración de derechos de las personas que se sufre en el Congo, y **concienciar a la sociedad de la situación que viven muchas personas en esa zona de África**.

Ya que, si bien no somos muy conscientes de ello (y aunque sea de manera indirecta), estamos contribuyendo al mantenimiento de los grupos armados involucrados, y a que continúe la explotación de tanta gente en las minas de donde se extraen esos minerales.

Esa es la razón por la que la ONG Alboan quiere impulsar a la **movilización ciudadana**, y pedir que se regule el comercio internacional precisamente de esos minerales.

[3] **Campaña «*Tecnología Libre de Conflicto*»**: podéis encontrar más información sobre la campaña en los siguientes enlaces:

www.tecnologialibredeconflicto.org

www.tecnologialibredeconflicto.org/moviles-por-el-congo/

www.youtube.com/watch?v=qbuZ5FYI9E4

TECNOLOGÍA LIBRE DE CONFLICTO

OBJETIVOS

El **objetivo general** de la campaña es dar a conocer a la ciudadanía de Euskadi el drama humanitario que se vive en el Este de la República Democrática del Congo, evidenciando la vinculación que existe entre la guerra en la región, la extracción de esos minerales y nuestro consumo de tecnología.

El objetivo es ambicioso y se antoja difícil. Sin embargo, desde la ONG Alboan creen que se puede lograr si contamos con una ciudadanía consciente de las repercusiones de nuestras decisiones de consumo, con representantes políticos comprometidos con el respeto de los Derechos Humanos más allá de nuestras fronteras, y con empresas responsables que tengan valores y estén comprometidas con un desarrollo sostenible.

Asimismo, se han establecido otros **objetivos específicos**, como son:

- ✓ Incidir en la normativa europea[4], que regula la importación de minerales, para que ésta garantice que los minerales que entran en la Unión Europea no están contribuyendo a financiar a grupos armados en conflicto. Se trata de poner fin al negocio del contrabando ilegal de minerales y de impedir que nos lleguen productos tecnológicos «*manchados de sangre*».
- ✓ Implicar a la ciudadanía vasca mediante propuestas de acción y movilización concretas para romper los vínculos que existen entre tecnología y violencia en el Este del Congo, especialmente el vínculo de la violencia que sufren las mujeres. Para ello, se están llevando a cabo varias acciones, como son:
  - Exposición fotográfica sobre las minas del Congo y las condiciones de vida de las personas que trabajan en ellas.
  - Formación en un uso responsable de la tecnología
  - Reciclaje de móviles
  - Recogida de firmas para la modificación de la normativa europea
  - Colaboración económica con proyectos de acción humanitaria en la región

«El objetivo de la campaña *"Tecnología Libre de Conflicto"* es dar a conocer la conexión que existe entre los dispositivos móviles y la vulneración de derechos humanos en el centro de África.»

[4] **Normativa europea**: tras dos años de duras negociaciones, el pasado día 22 de noviembre de 2016 se llegó a un acuerdo sobre la ley europea de «*minerales en conflicto*».

Por vez primera, las empresas que importen cuatro minerales concretos asociados a la financiación de conflictos (como el tantalio, el wolframio, el estaño y el oro) deberán declarar su origen y tomar las medidas necesarias para evitar las violaciones de derechos humanos en su cadena de suministro.

Sin embargo, la ley presenta lagunas importantes. Deja libres de obligación a las empresas importadoras de productos manufacturados con dichos minerales (como móviles, ordenadores, joyas o baterías), confiando en que se autorregulen; y establece unos umbrales de volumen altos para eximir a buena parte de quienes importan estos minerales en bruto o procesados.

LibreCon2016

En la última edición del Congreso LibreCon2016 (evento centrado en el Software Libre y que tuvo lugar en Bilbao los días 22 y 23 de noviembre), la Coordinadora de *Synergie des Femmes*, Justine Masika, tuvo la oportunidad de ofrecer a todos los asistentes una ponencia, a través de la cual dio a conocer la grave situación que se vive actualmente en el Congo, como consecuencia de los llamados «*minerales en conflicto*» o «*minerales de sangre*».

Durante su presentación, Justine Masika, activista congoleña por los derechos humanos, expuso en primera persona el rol que ocupan las mujeres en las comunidades mineras de Rubaya y su lucha diaria.

Esta ponencia se enmarcaba dentro de la Campaña «*Tecnología Libre de Conflicto*» que viene desarrollando la ONG Alboan.

[foto: twitter de @librecon]

COLABORACIÓN

Para que esta iniciativa tenga éxito, es necesaria la colaboración tanto de las personas como de las instituciones.

Es por ello que el Gobierno Vasco, a través de la Dirección de Informática y Telecomunicaciones, y la Dirección de Recursos Generales, van a poner todos sus medios para facilitar la colaboración de todas aquellas personas que deseen aportar su granito de arena, y que detallamos a continuación:

- **Comunicar la campaña**. El Gobierno Vasco difundirá a través de distintos medios (Intranet *Jakina*, paneles informativos, etc.) los objetivos de la campaña.
- **Reciclar móviles en desuso**. El Gobierno Vasco va a habilitar distintos puntos de recogida (cajas en forma de **buzón**) donde podremos depositar aquellos móviles viejos que tengamos en casa y no usemos. Como hemos indicado, se cree que el reciclaje y reutilización de los dispositivos móviles viejos es una opción que contribuirá a reducir la necesidad de extraer más mineral.

La ONG Alboan, por su parte, se encargará de recoger los móviles depositados en los buzones, y destinará todos los fondos que se recauden gracias a esta colaboración a los proyectos gestionados directamente por ella en la República Democrática del Congo.

En la medida que somos personas consumidoras de productos tecnológicos, formamos parte de la cadena que «*alimenta*» la violencia contra las mujeres, y por eso también podemos jugar un papel muy importante para romperla.

Es por ello que, desde aquí, os invitamos a que pongáis vuestro granito de arena y colaboréis con vuestro viejo teléfono móvil[5]. ❑

[5] **Teléfono móvil**: se calcula que en Europa se renueva cada año el 40% del parque de móviles existentes (alrededor de 18 millones de móviles sólo en España).

Mientras la vida útil de un aparato es de unos 10 años, batería aparte, el tiempo medio de utilización se sitúa entre el año y medio y los dos años y medio.

KZgunea y EJIE colaboran con la campaña

KZgunea (la Red de telecentros de Euskadi) y la ONG Alboan colaboran conjuntamente desde hace varios meses para denunciar la situación de la extracción de minerales en el Congo y sus consecuencias.

El pasado 18 de noviembre, EJIE y la ONG Alboan firmaron un convenio de colaboración para la recogida de *smartphones* en los centros KZgunea, para su posterior reciclaje. Alex Etxeberria, Director General de EJIE, Marimar Marañón, Directora de Alboan, y Luis Mari Guinea, Responsable del Proyecto KZgunea, fueron los protagonistas del acto que tuvo lugar en el KZgunea de Uribarri (Bilbao, Bizkaia).

Foto: buzones ubicados en EJIE

La Directora de Alboan recalcaba durante la presentación la importancia de colaborar con la red de KZgunea, ya que es una oportunidad muy grande para extender la sensibilización de la campaña «*Tecnología Libre de Conflicto*» por todo Euskadi.

Gracias a esta colaboración, desde hace varias semanas, ya están disponibles buzones en los 100 centros KZgunea más visitados.

Por su parte, **EJIE**, la sociedad informática del Gobierno Vasco, también ha instalado en su sede central de Vitoria-Gasteiz (Araba) dos buzones para la recogida de móviles.

Nuestro correo electrónico corporativo

Parecía que con la llegada de nuevas herramientas colaborativas y de comunicación el correo electrónico tenía los días contados, pero, contra todo pronóstico, este servicio sigue siendo hoy en día uno de los más utilizados, tanto por personas particulares como por empresas. Por ello, es una vía perfecta para poner en peligro nuestros sistemas y datos. Vamos a indicar cómo debe ser el uso correcto de nuestro correo corporativo.

El correo electrónico o *email* es una herramienta que utilizamos de una forma habitual para intercambiarnos información, tanto en el ámbito profesional como en el personal.

El proceso de envío y recepción de un correo electrónico, en la mayoría de los casos, es el siguiente: la persona usuaria completa el mensaje incluyendo la información requerida en los campos Destinatario, Asunto y Cuerpo del mensaje, su cliente de correo[6] se encarga de enviarlo al servidor de correo corporativo (si estamos dentro de una organización, como puede ser el Gobierno Vasco), este último realiza una serie de comprobaciones (entre ellas que la dirección de destino sea una dirección válida), y lo envía al servidor

de destino, el mensaje viaja por una serie de servidores hasta llegar al servidor de destino, el cual comunica a la persona destinataria que tiene un correo pendiente de leer, realizando todas las acciones pertinentes para que el correo pueda ser leído.

Además de nuestra cuenta corporativa (con dominio **@euskadi.eus**, en nuestro caso), cada una de nosotras y nosotros casi seguro que tenemos al menos una cuenta de correo particular (Gmail, Yahoo…). Para la persona usuaria del servicio de correo, el envío y recepción de correos es un proceso transparente, cuando en realidad, desde el punto de vista de la **seguridad**, lleva aparejados unos protocolos y elementos que requieren una atención particular.

El servicio de correo electrónico tiene dos entornos bien diferenciados: por una parte está el **entorno del servidor de correo**, y, por otra, nuestro **cliente de correo electrónico**.

SERVIDOR DE CORREO CORPORATIVO

En nuestro ámbito, el servidor de correo lo componen una aplicación informática y unos servidores que permiten el envío y recepción de correos en nuestra organización. Esta aplicación se instala en servidores con capacidad para actuar en Internet (denominados igual que el servicio: servidores de correo electrónico corporativo), que por seguridad deben ser alojados en una zona denominada «*desmilitarizada*» (DMZ[7]). Estos servidores físicos, además de estar en la DMZ, están conectados a un *firewall* (cortafuegos), cuya misión básicamente es filtrar los paquetes de datos que viajan entre la red interna y la red externa, esto es, están ubicados en un segmento de red aislado por cortafuegos, además, existen dos niveles de cortafuegos de diferentes tecnologías, limitando todo el tráfico saliente de modo que dicho tráfico sólo sea enviado por nuestros servidores de correo (evita que otras aplicaciones puedan enviar correo al exterior). Ubicar los sistemas de correo en una zona interna es un riesgo que no se debe asumir, ya que los problemas de seguridad afectarían directamente a nuestros servidores internos.

Los servidores de correo corporativo, además de cumplir con todo lo que se ha dicho

[6] **Cliente de correo:** es un programa de ordenador usado para leer y enviar mensajes de correo electrónico.

Algunos ejemplos son:

- Microsoft Outlook/ Exchange
- Mozilla Thunderbird
- Zimbra
- Evolution
- Opera Mail

[7] **DMZ:** *demilitarized zone,* es una zona que se encuentra entre la red **interna** de la organización, donde están nuestras máquinas, y la red **externa**, generalmente Internet, esto es, donde se ubican servidores que deben ser accedidos desde fuera y dan servicio a Internet, como es el caso del servicio de correo electrónico.

anteriormente, disponen de alta capacidad, es decir, son replicados en tiempo real en unos servidores secundarios que entrarán en funcionamiento en caso de fallo grave, estando ubicados los servidores de correo en un Centro de Proceso de Datos (CPD) y los servidores replicados en otro CPD diferente; las comunicaciones de entrada y salida hacia Internet se realizan a través de dos sistemas de comunicación distintos en cada uno de los CPD, asimismo, la comunicación con los puestos de trabajo también es redundante. En los dos CPD que hemos citado existe alimentación ininterrumpida y grupos electrógenos, es decir, la infraestructura se ha diseñado para proporcionar altos niveles de disponibilidad y continuidad. Respecto a las comunicaciones de este servicio, sólo se permiten las comunicaciones necesarias para proveer el mismo.

Por otro lado, las comunicaciones entre los puestos cliente de las personas usuarias y los servidores de correo electrónico están cifradas, tanto si se utiliza un cliente de correo pesado (el que se instala en el puesto cliente –PC– de la persona usuaria, Microsoft Outlook en nuestro caso) como si se utiliza un acceso a través de un cliente de correo basado en un navegador (como pueden ser Internet Explorer, Google Chrome, Firefox, Opera…), lo que se conoce como acceso a través de OWA (*Outlook Web Access*). No se puede garantizar que el correo con terceros se cifre, ya que eso depende de la capacidad de cifrado de los servidores de correo ajenos.

A su vez, las personas que trabajan en sistemas se encargan de que el servicio de correo electrónico, en el entorno del servidor, esté en todo momento asegurado, a través de las actualizaciones de seguridad y parches que se publican por parte de los fabricantes de los equipos y del software, de la eliminación de los servicios que no son estrictamente necesarios en los servidores de correo (limitar a los servicios SMTP, POP e IMAP), que debe ser un servicio dedicado, aplicando las restricciones de acceso que corresponden, aplicando las políticas de gestión contraseñas corporativas, monitorizando y controlando los accesos, etc.

Cabe destacar que todos los correos electrónicos que entran en nuestra organización, previamente han pasado un filtro que elimina un porcentaje muy alto de correo basura[8] (*spam*) en el lado de nuestro proveedor de servicios de Internet (ISP), también los equipos corporativos analizan el correo (tanto entrante como saliente) con herramientas comerciales (como *McAfee Email Gateway)*, que protegen nuestra red de virus, contenido no deseado, *spam* y otras amenazas, por lo que los correos que nos llegan están casi libres de «correo no deseado».

ENTORNO DEL CLIENTE DE CORREO

Es la parte que está en el lado del equipo de la persona usuaria, generalmente el software que se instala en su PC (equipo cliente) para gestionar el correo electrónico; como medida general se utiliza un antivirus corporativo, que complementa las herramientas que hemos descrito en el apartado anterior, también se bloquean las sesiones abiertas, de forma automática, tras un período de inactividad en el puesto. Hay que tener en cuenta que el equipo cliente es el punto más débil y son la puerta de entrada de la mayoría de las amenazas.

ALGUNOS ATAQUES A TRAVÉS DEL CORREO ELECTRÓNICO

Últimamente han tomado mucha fuerza los ataques de *spear-phishing*, que es una estafa que utiliza el envío de correos electrónicos, para obtener acceso no autorizado a datos confidenciales, a grupos u organizaciones reducidos (a diferencia de otro tipo de ataques cuyo público objetivo no está definido, y que se denominan ataques masivos), incluyen ficheros adjuntos ofimáticos dañinos, por ejemplo de Microsoft Word o Excel, con macros[9] (serie de

[8] **Correo basura (*spam*):** para más información, podéis consultar el boletín Aurrera nº 16, publicado en diciembre de 2004.

[9] **Macros en documentos Word o Excel:** permiten automatizar y ejecutar tareas, utilizan un lenguaje de programación orientado a eventos denominado *Visual Basic for Applications*.

instrucciones que automatizan procesos) asociadas y JavaScript maliciosos, o enlaces a sitios web que infectan al equipo de la persona usuaria.

El ataque conocido como *ransomware* suele utilizar el envío masivo de mensajes de correo electrónico para intentar «*secuestrar*» los datos de las personas usuarias que abran esos correos electrónicos.

La ocultación de la extensión de un fichero (por ejemplo, hacer creer que un fichero tiene extensión .docx cuando realmente es un fichero ejecutable con extensión .exe) es una técnica comúnmente utilizada por las personas atacantes (un ejemplo, hacer pasar el fichero README_*xcod.exe* por el fichero README_*exe.docx*, mediante la inversión del orden de visualización de los últimos caracteres).

[10] **Ingeniería social**: técnica que se basa en la manipulación de las personas usuarias para obtener de ellas información confidencial y datos sensibles.
Para más información podéis consultar el boletín Aurrera nº 13 (marzo de 2004)

[11] **ICANN**: *Internet Corporation for Assigned Names and Numbers,* Corporación de Internet para Nombres y Números Asignados, organización sin ánimo de lucro que, entre otros temas, gestiona los DNS (nombres de dominio de Internet).

BUENAS PRÁCTICAS

Por todo ello la **concienciación**, la utilización de **buenas prácticas** de uso (ver el cuadro «*Uso correcto del correo corporativo*») y el **sentido común**, son las mejores armas para defenderse de los ataques, ya que en muchas ocasiones las personas delincuentes cibernéticas utilizan técnicas de ingeniería social[10] para perpetrar sus ataques.

Cuando se utilice la cuenta de correo corporativa fuera de las instalaciones de trabajo, en equipos no corporativos, utilizando el correo vía web, habrá que tener presente las siguientes recomendaciones:

- ✓ NO utilizar la opción de guardar la contraseña.
- ✓ SI utilizar la opción de borrar el historial y cerrar la sesión.

Al utilizar el correo corporativo en dispositivos móviles se deberá habilitar la opción de bloqueo del dispositivo si éste no está en uso. Asimismo, es recomendable utilizar mecanismos de cifrado de su contenido.

Cuando recibimos un correo electrónico de un remitente que nos es desconocido, es importante fijarse en el dominio del nombre del remitente, la parte derecha después de la arroba (@), ya que nos puede dar información relevante de la empresa o compañía a la que pertenece; existe una herramienta en línea: https://whois.icann.org/es, que pertenece a ICANN[11]

y que nos devuelve información asociada a un nombre de dominio o una dirección IP, como, por ejemplo, la persona responsable de dicho dominio.

Cuando se envía información sensible a través del correo electrónico es recomendable **cifrar** esa información; en nuestro ámbito, Gobierno Vasco, se pueden cifrar correos electrónicos utilizando la tarjeta digital de **IZENPE**.
El que se reciba un correo electrónico con reglas gramaticales incorrectas, por ejemplo, con faltas ortográficas, es un síntoma para sospechar de ese correo. Y ponernos en alerta.

En la tabla «*Uso correcto del correo corporativo*» de la página siguiente os indicamos los 10 principios de uso correcto de nuestro correo electrónico corporativo. ❑

CCN-CERT BP-02/16

El Centro Criptológico Nacional (CCN) ha publicado un documento de **Buenas Prácticas** para el **Correo electrónico** (**CCN-CERT BP-02/16, de julio de 2016**) en el que se distinguen dos bloques, el primero habla sobre el correo electrónico como vía de infección, y el segundo sobre las buenas prácticas en el uso del correo electrónico.

+info: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-16-correo-electronico

Uso correcto del correo corporativo

El documento «**Obligaciones Generales de las personas usuarias del Gobierno Vasco**»[12], respecto al uso del correo electrónico, establece los siguientes 10 principios:

1. Se considerará al correo electrónico como **una herramienta más de trabajo** provista a la persona usuaria con el fin de ser utilizada conforme al uso para el cual está destinada
2. El sistema de correo electrónico de Gobierno Vasco no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares
3. Las persona usuarias no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples personas usuarias)
4. En relación al intercambio de información a través del correo electrónico, se considerarán no autorizadas las siguientes actividades:
   - Transmisión o recepción de material protegido por *copyright* infringiendo la Ley de Protección Intelectual
   - Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal
   - Transferencia a terceras partes no autorizadas de material de la Organización o material que es de alguna u otra manera confidencial
   - Transmisión o recepción de ficheros que infrinjan la Ley de Protección de Datos de Carácter Personal o las directrices del Gobierno Vasco
   - Transmisión o recepción de cualquier tipo de dato e información no relacionadas con la actividad del Gobierno Vasco
5. Se atenderá expresamente a las disposiciones legales vigentes en materia de envío de información, limitando en la medida de lo posible el uso del correo electrónico a aquellos casos en los que no se determinan especiales exigencias en materia de protección de datos, trazabilidad, autenticidad, confidencialidad o no repudio. En caso contrario se utilizarán de manera preferente las vías oficiales establecidas por el Gobierno Vasco para el envío de comunicaciones y notificaciones electrónicas
6. Se deberán utilizar todas aquellas utilidades de seguridad dispuestas para la protección del correo electrónico:
   - Uso de firma electrónica con aquellos correos electrónicos destinados al exterior cuya autenticidad e integridad se quiera garantizar
   - Uso de cifrado con aquellos correos electrónicos cuya confidencialidad se quiera garantizar
   - Uso de las utilidades del antivirus para verificar que los correos electrónicos no tienen virus
7. No se permitirá la transmisión vía correo electrónico de información cuya CONFIDENCIALIDAD esté clasificada como ALTA ni que contenga datos de carácter personal de nivel alto, salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido
8. Se verificarán expresamente las direcciones de correo incluidas como destinatarias, con el fin de evitar, en la medida de lo posible, el envío de correos electrónicos a direcciones incorrectas o erróneas
9. Se prestará especial atención al uso de los campos CCO (con copia oculta) para definir las personas u organizaciones destinatarias de todos aquellos correos que se dirijan a grandes cantidades de persona usuarias u organizaciones, listas de distribución o destinatarias de diferentes organizaciones externas al Gobierno Vasco
10. Para la interacción con la ciudadanía y otras organizaciones se deberán utilizar cuentas de correo genéricas, limitando en estos casos el uso de las cuentas de correo personalizadas exclusivamente a aquellos casos en los que sea imprescindible.

[12] **Documento «*Obligaciones Generales de las personas usuarias del Gobierno Vasco*»**: aprobado en el Comité Técnico de Seguridad (**Comité GureSeK**) celebrado el 21 de octubre de 2016, contempla las **obligaciones generales de las personas usuarias** que deberán ser cumplidas por todo el personal de la Administración General de la Comunidad Autónoma del País Vasco (Departamentos) y de sus Organismos Autónomos en el ámbito de la Administración Electrónica, así como por todo el personal perteneciente a empresas externas subcontratadas que tenga acceso a la documentación o información asociada a alguno de los servicios del Gobierno Vasco.

ALBOAN:

NISAE, Nodo de Interoperabilidad y Seguridad de las Administraciones de Euskadi

«NISAE es la nueva plataforma común para el intercambio de datos entre las administraciones y entidades del sector público vasco»

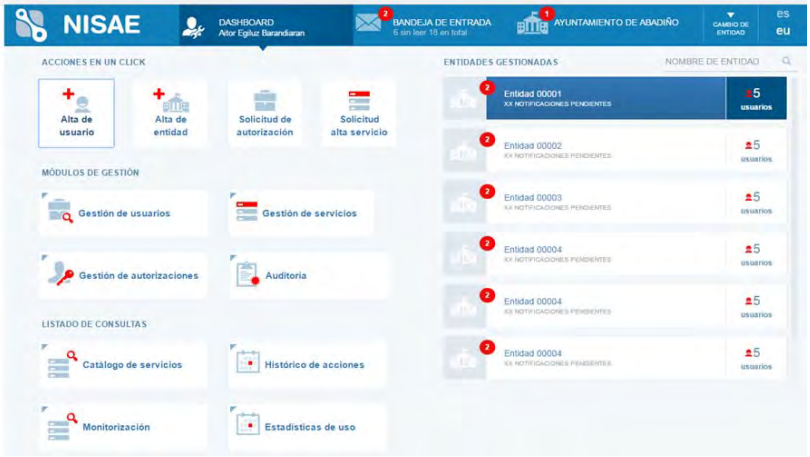
NISAE es la nueva plataforma común para el intercambio de datos entre las administraciones y entidades del sector público vasco, y de éstas con el resto de administraciones (AGE y otras CC.AA).

Se trata de una **solución común** que se articula en torno a un modelo de **gestión distribuido** en el intercambio de datos entre entidades. Más allá de su funcionalidad natural, su diseño está basado en un esquema que articula la **interoperabilidad** adecuándose a la realidad organizativa de las diferentes administraciones de Euskadi, ya que la solución que os presentamos en este artículo ha sido **consensuada** con los diferentes agentes institucionales que participan en la misma.

NISAE es también una herramienta necesaria para la **eficiencia** y la **racionalidad** a la hora de realizar la intermediación (intercambio y comunicación) de datos en las organizaciones del sector público. Asimismo, es la solución que da respuesta a los requerimientos, cada vez más exigentes en relación al cumplimiento normativo que establecen las regulaciones actuales (Leyes 39 y 40 de 2015) y que ya venían siendo reguladas en disposiciones anteriores (Ley 11/2007). Todo ello sin olvidarnos de que ya desde el año 2010 el Real Decreto 4/2010 que reguló el Esquema Nacional de Interoperabilidad fuera la norma que marcó el paso firme para la implementación de estas soluciones.

En 2014, **Izenpe**, como primer acercamiento al concepto NISAE ya desarrolló un proyecto piloto de «*Nodo de Interoperabilidad*», con la funcionalidad suficiente para soportar la exposición de los servicios del Padrón individual por parte de las Administraciones Locales y el consumo de los servicios de verificación de la identidad de la AGE, cumpliendo en todo momento la normativa del ENI.

Todas las entidades del sector público vasco están llamadas a utilizar NISAE desde sus respectivos ámbitos de gestión; esto supone más de **300 potenciales administraciones y entidades del sector público** interoperando sobre el mismo nodo en un volumen estimado superior a 5.000.000 de intermediaciones anuales.



Cada entidad final actuará como responsable de la exposición y consumo de datos. En el modelo de gestión colaborativo que implementa esta plataforma existe, también, un nivel intermedio (formado por sectores institucionales y ayuntamientos de capitales) que actuarán como administradores de sus propias entidades. Mientras que **Izenpe** será la entidad responsable de coordinar y administrar la evolución general de la plataforma que da soporte al nodo, así como

de la delegación de tareas de gestión que pudieran considerarse.

DEL PROYECTO A LA REALIDAD

NISAE ya es una realidad que permite la intermediación de datos. Su finalidad es actuar como nodo autonómico de interoperabilidad para gestionar el intercambio de información, y que incluye 3 fases:

- Fase previa: gestión de autorizaciones de solicitudes de intermediación de datos
- Fase de intermediación de datos
- Fase posterior: auditoría de trazas y gestión estadística de la actividad realizada

Es importante destacar que la plataforma NISAE cumple con los estándares establecidos en la Norma Técnica correspondiente a los protocolos de intermediación de datos previstos en el Esquema Nacional de Interoperabilidad (Real Decreto 4/2010, de 8 de enero). Gracias a ello, cumple las siguientes funciones:

a) Gestionar Cesionarios y Requirentes de datos según las condiciones establecidas por cada Proveedor (Cedente).
b) Asegurar la confidencialidad e integridad de la información intercambiada.
c) Mantener un portal web (https://www.nisae.izenpe.eus) con toda la documentación e información sobre la plataforma, donde se expondrá entre otros contenidos:
   - ✓ El Catálogo de Servicios de intercambio de datos disponibles por parte de las diferentes organizaciones participantes (protocolos de acceso a los servicios, métodos de consulta, información técnica, etc.).
   - ✓ Formularios de solicitud de acceso a los servicios.
   - ✓ Acuerdos de prestación de cada servicio disponible y de la plataforma en general.
d) Mantener el sistema en funcionamiento 24x7.
e) Dar soporte a las organizaciones y gestionar todas las comunicaciones e incidencias producidas colaborando para ello con Requirentes y Emisores.
f) Mantener un centro de atención a usuarios e integradores que canalice todas las incidencias relativas al sistema y que informará sobre los datos de contacto del mismo.
g) Elaborar informes de actividad y uso de la plataforma.
h) Evolucionar y mantener sus sistemas garantizando la seguridad y privacidad de los datos acorde a la normativa aplicable.
i) Colaborar en las labores de auditoría siempre que el Emisor o el Cedente así lo requiera y defina, conservando los datos de trazabilidad y estadísticos acordados.

El nodo se ha diseñado de forma que ponga en funcionamiento un modelo de roles según la función que cada agente juegue en cada caso. Las combinaciones son múltiples, las más frecuentes serán aquellas en las que las entidades requirentes sean distintas a las cesionarias, pero también habrá casos en los que una entidad podrá ser requirente de un servicio e incluso emisora del mismo.

NISAE realizará todas las consultas de datos, bien mediante intermediación manual bien de forma automática, sobre los servicios publicados en el propio nodo y será accesible a través de **EuskalSarea**, asegurando la conectividad de las diferentes entidades públicas de la CAE a los servicios expuestos en un entorno **seguro**, en línea con la filosofía de reutilizar los sistemas y plataformas existentes. ❑

«Izenpe será la entidad responsable de coordinar y administrar la evolución general de la plataforma»

[+info]:

Web de Izenpe

http://www.izenpe.eus

Web del portal NISAE

https://www.nisae.izenpe.eus

¡¡BREVES!!

WiFi 802.11ax

Actualmente, en lo que respecta a las conexiones WiFi, el estándar **802.11ac** es el que se está utilizando, siendo una evolución del viejo estándar 802.11n; sin embargo, ya se están produciendo circuitos integrados que soportan el nuevo protocolo **802.11ax** (aún no es un estándar, lo será a finales de año).

¿Cuáles son las **ventajas del 802.11ax**? La capacidad de una red WiFi se mide por los parámetros siguientes: velocidad de conexión, alcance de la red inalámbrica, y número de dispositivos que se pueden conectar de un modo simultáneo. El estándar 802.11ac Wave 2 ya utiliza MU-MIMO (*Multi-User Multiple Input Multiple Output*), que permite conectarse con dispositivos de una forma simultánea; pues bien, 802.11ax permitirá hasta cuatro veces más dispositivos conectados que la versión anterior, utilizando 12 canales simultáneos, 8 en la frecuencia de 5 GHz y otros 4 en la de 2.4 GHz. También permitirá conectar equipos simultáneamente sin que el descenso de la velocidad sea tan drástico como lo es ahora. Este nuevo protocolo, que es compatible con los protocolos anteriores, a su vez aporta más eficiencia y un comportamiento mejorado.

La empresa estadounidense *Qualcomm* ha creado dos circuitos integrados (*chips*) que soportan el nuevo estándar: el **IPQ8074**, que mira hacia el campo de los *routers* y puntos de acceso (AP); y el **QCA6290**, diseñado para integrarse en la electrónica de los dispositivos móviles (teléfonos inteligentes, tabletas, ordenadores portátiles…). Si los dispositivos que utilicemos y los *routers* inalámbricos y AP a los que nos conectemos son compatibles con este nuevo protocolo, podremos disfrutar de sus ventajas, por ejemplo, el chip QCA6290 permite doble banda simultánea, es decir, podremos conectarnos a un punto de acceso o *router* inalámbrico utilizando las dos bandas de frecuencias (2.4 GHz. y 5 GHz.) y obtener mayor velocidad; además, incorpora tecnología para reducir el consumo de batería de una forma importante.

Ya está disponible LibreOffice 5.3 on line

Desde hace unas semanas, ya está disponible la nueva versión del paquete ofimático LibreOffice.

Según la entidad que se encarga de su gestión, The Document Foundation, esta nueva versión incorpora un gran número de novedades y características muy interesantes para toda aquella persona que necesite utilizar un paquete ofimático.

En esta ocasión a parte de desarrollar aspectos de mejoras generales, así como conseguir un programa más fiable, también se han introducido nuevas funciones y cambios en la interfaz de usuario.

A este respecto, una de las novedades más significativas de la nueva versión es que LibreOffice 5.3 incorpora la edición de documentos en línea de forma colaborativa dentro de la nube privada: *LibreOffice Online*, una *suite* de ofimática en la nube que ofrece funciones básicas de colaboración entre personas que permite editar documentos dentro del navegador.

En cuanto a la interfaz, la cual recibe el nombre oficial de «*MUFFIN*» (acrónimo de «*My User Friendly & Flexible Interface*», «Mi interfaz amigable y flexible» en inglés), también ha sido actualizada.

Asimismo, se ha mejorado la compatibilidad con otros programas de ofimática, el procesador de texto soporta ahora estilos para las tablas, las hojas de cálculo tienen un nuevo estilo de celdas por defecto, etc.

LibreOffice es un proyecto de código abierto en el que trabajan más de 300 personas.

Página web: http://www.libreoffice.org