EUSKO JAURLARITZA
GOBIERNO VASCO

nº 57
Septiembre de 2016

Aurrera!

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

A través del primer artículo de este nuevo boletín Aurrera queremos dar a conocer varios proyectos que durante los últimos meses (e incluso años) han sido desarrollados por el personal técnico de EJIE, y que están a disposición de todos los Departamentos y Organismos Autónomos, como un servicio horizontal más que pueden complementar algunos proyectos departamentales. Se trata de iniciativas conocidas como PIF, PID, BigData, y notificaciones PUSH.

Para poder hacer frente a un incidente (y no sufrir sus posibles consecuencias) nuestra organización debe estar preparada. Y, para ello, primero hay que saber cuáles son nuestros activos, que riesgos tienen, clasificarlos, estimar la probabilidad de que una incidencia se materialice, y disponer de las medidas que vamos a poner en marcha para contrarrestarlas. De todo ello os informamos en esta ocasión en el segundo tema que hemos incluido en este boletín.

En esta ocasión aprovecharemos la sección «*Alboan*» para explicaros brevemente una nueva iniciativa que hemos puesto en marcha recientemente, denominada «*Seminarios Alboan*», y que va dirigida especialmente al personal informático del Gobierno Vasco. Iniciativa que tiene como objetivo crear un foro o plataforma donde exponer e intercambiar ideas, problemáticas y experiencias que puedan resultar de interés para todo el personal.

Dentro del apartado titulado «*Breves*», queremos daros a conocer a «*Electronic Frontier Foundation*» (EFF), una entidad poco conocida que, sin embargo, se encarga de proteger la privacidad de todas las personas (internautas) que navegamos por Internet.

Por último, os presentamos «*Basque Global Network*», una red social puesta en marcha por el Gobierno Vasco que posibilitará a personas vascas así como a sus descendientes, amistades y simpatizantes, colaborar en proyectos tanto culturales, empresariales, como institucionales.

Servicios horizontales para los Departamentos y Organismos Autónomos

Son muchos los proyectos que EJIE desarrolla y gestiona para atender y dar respuesta a las necesidades que requieren los Departamentos y Organismos Autónomos del Gobierno Vasco, algunos de los cuales son utilidades horizontales que pueden complementar los proyectos departamentales. Veamos algunos de ellos.

DICCIONARIO

[1] **Big data:** es un concepto que hace referencia al almacenamiento de una gran cantidad de datos y los procedimientos que se usan para gestionarlos y encontrar en ellos una serie de patrones repetitivos, y que normalmente superan la capacidad del software convencional para ser capturados, administrados y procesados en un tiempo razonable.

Más información en el boletín Aurrera nº 44 (junio de 2013), artículo «*Datos masivos (Big Data)*».

[2] **PLATEA:** es la Infraestructura tecnológica base que da soporte a toda la Administración Electrónica del Gobierno Vasco.
Para más información podéis consultar el Documento de Estándares Tecnológicos que define todos sus componentes y módulos que lo componen. Dicho documento está disponible en la web http://www.euskadi/informatica (apartado «*Estándares Tecnológicos*»)

Dentro del área de Integración de Sistemas de EJIE son varias las iniciativas que se han desarrollado durante los últimos meses (e incluso años) que pueden ser de gran utilidad para muchos Departamentos/Organismos Autónomos y, por lo tanto, merecen ser conocidos.

A lo largo de este artículo nos centraremos en los proyectos conocidos como PIF, PID, BigData[1], y notificaciones PUSH.

PLATEA INTEGRACIÓN FICHEROS

PLATEA[2] Integración Ficheros, también conocido por sus siglas PIF, es una solución técnica que facilita el **intercambio de ficheros entre aplicaciones**. Se trata de una solución horizontal que posibilita el intercambio ágil y escalable y, sobre todo, suple las carencias de las soluciones NFS utilizadas en los *back-end*.

Desde un punto de vista técnico, el PIF consta de los siguientes componentes:

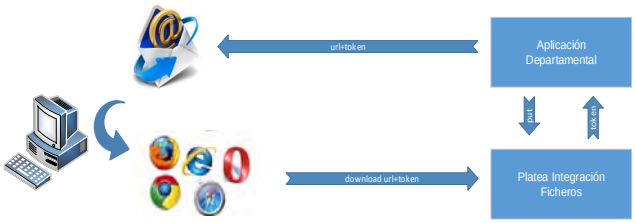
- ✓ Un **repositorio** de ficheros temporal donde tanto personas como aplicaciones dejarán documentos para ser recogidos por otras aplicaciones/personas
- ✓ Un conjunto de **canales técnicos** como pueden ser: JavaScript (componentes AJAX que puedan ser utilizados en el navegador); REST (funciones que podrán ser invocadas por aplicaciones en plataformas técnicas distintas a Java); Nativo (funciones que podrán ser usas en aplicaciones Java sin tener que montar la pila de ejecución de Web Service); Batch (comandos que podrán ser utilizados desde cadenas *batch* de cualquier aplicación)

Indicar que existe la posibilidad de usar Componentes que facilitan la construcción de aplicaciones más allá de funciones básicas. Un ejemplo ello es la opción de subida de ficheros (*upload*) o el *servlet* que puede ser usado para las descargas (*download*). Asimismo, destacar el componente «Edición Online» que posibilita disponer de URLs a documentos «editables» (en base a una dirección web de tipo spif://host/path/doc), tal y como se realiza en las plataformas de gestión documental (*SharePoint*, *Documentum*, *Alfresco*…).

Gracias a las distintas opciones que ofrece PIF, y a los Eventos que se pueden implementar, su uso es muy práctico en situaciones en las que se quieren trasladar eventos que nacen en el mundo *online* y el destinatario es más del mundo *batch*. Un caso de uso real podría ser, por ejemplo, notificaciones que llegan a un ayuntamiento pequeño, que prefiere recogerlas diariamente en un proceso nocturno, mediante ficheros, en vez de implementar una serie de *web services* [sistema para intercambiar datos entre aplicaciones], que requieren una mayor atención ante incidencias, por ser una solución *on-line*.

Desde el punto de vista de la seguridad, indicar que la solución gira entorno a XLNets, y que los datos que se transmiten navegan siempre encriptados vía SSL.

En cuanto al funcionamiento, cualquier aplicación puede dejar ficheros en la zona de otras aplicaciones; pero sólo la aplicación dueña de su zona podrá recoger esos ficheros. En definitiva, funciona como un apartado de correos.



Algunas de las funciones que ofrece la API[3] desarrollada son las siguientes: *copy* (permite copiar ficheros), *get* (descargar ficheros), *move* (mover ficheros), *delete* (eliminar ficheros).

Si bien en la versión 1.0 el proyecto se orientó exclusivamente al uso interno dentro de nuestra organización, en la versión 1.1, por el contrario, el objetivo fue cubrir escenarios de intercambio de ficheros con aplicativos alojados fuera del CPD (Centro de Procesamiento de Datos) de EJIE. Para ello, se implementaron canales técnicos basados en **estándares independientes**, lo que ha permitido implantar el **intercambio de ficheros con terceros**: Ayuntamientos, Diputaciones, redes sectoriales (Osakidetza, Justicia, Interior) y otro tipo de entidades.

Es importante destacar que PIF nos ofrece, además, una **consola para el seguimiento de las trazas** (*logs*) de las distintas operaciones realizadas (movimientos, copias, borrados, etc.). En ella se nos mostrará una serie de filas. Al seleccionar alguna de esas filas (registros) aparecerá una ventana con toda la información necesaria (si la operación se ha realizado correctamente, si ha habido alguna incidencia —entonces, aparecerá el código del error correspondiente—, etc.). Por lo tanto, la aplicación es totalmente auditable y, además, cumple con la LOPD (Ley Orgánica de Protección de Datos).

«PLATEA Integración Ficheros es una solución horizontal que posibilita el intercambio ágil y escalable de ficheros.»

Una de las grandes ventajas que ofrece PIF es que ofrece un rendimiento excepcional en cuanto a tiempos de transferencia: dentro del CPD de EJIE, por ejemplo, se alcanzan los 10 MB en 300 ms y los 200 MB en 4,6 segundos. En los puestos clientes de la Red Corporativa se consiguen 10 MB en 1,5 seg. y en el caso de usar la red JASO[4], utilizada, por ejemplo, por Osakidetza, 500 KB en 200 ms.

Todo ello está posibilitando que ya no sea necesario en muchos casos entregar CDs o discos duros con información al Servicio de Explotación de EJIE, tal y como se hacía hasta hace poco.

A día de hoy, son varios los servicios y áreas del Gobierno Vasco las cuales están usando PIF para sus operaciones diarias, por ejemplo:

- ✓ Educación
- ✓ SIPCA (Sistema Integral de Pagos y Cobros de la Administración)
- ✓ Asuntos Sociales con el Ayuntamiento de Bilbao
- ✓ Industria con las notificaciones del servicio de correos
- ✓ Datos de laboratorios de Osakidetza
- ✓ Dokusi y PLATEA-Tramitación ofrecen interfaces tipo PIF
- ✓ Otro servicio que utiliza PIF es EJIEbox

PLATAFORMA DE INTEGRACIÓN—DOCUMENTOS

La Plataforma de Integración - Documentos (PID) nace para cubrir algunas necesidades básicas de gestión documental en el ámbito departamental. Estas necesidades son siempre relativas a documentación electrónica no ligada a procedimientos administrativos y con nivel de LOPD bajo. Ofrece 3 **modelos de integración:**

- Básica (almacenamiento de contenidos): este modelo de integración se corresponde a departamentos o aplicaciones cuyo único objetivo es disponer de un repositorio en el cual depositar contenidos electrónicos que, de no existir PID, deberían almacenar en otras plataformas no especializadas en este propósito (bases de datos o *file system*).
- Media (gestión de contenidos): este modelo contempla la utilización de funcionalidades avanzadas de la plataforma que no ofrece la opción básica, como pueden ser: asociación de firmas a los documentos, transformaciones entre formatos, búsquedas por metadatos, refuerzo de la seguridad inter-departamental.
- Avanzada (gestión y búsquedas *fulltext*): se optará por esta opción cuando sea necesario hacer uso de las funcionalidades avanzadas que ofrece la plataforma, como por ejemplo las búsquedas *fulltext*.

Cada iniciativa que se integre en PID, tendrá su propia «área de almacenamiento» o *filestore* dedicado (uno o varias áreas), lo cual facilita saber en todo momento el espacio en disco utilizado por cada iniciativa, así como realizar ampliaciones de dicho disco si fuera necesario.

Desde el punto de vista de la seguridad, debe tenerse en cuenta que los usuarios de PID son siempre **aplicaciones**, y no usuarios nominales.

Se trata de una solución técnica donde se ha primado la sencillez y el rendimiento. Tanto es así que se ha calificado como «Gestión Documental ligera», la cual ofrece los servicios básicos de almacenamiento, recuperación, modificación,

DICCIONARIO

[3] **API**: son las siglas en inglés de *Application Programming Interface*, es decir, la Interfaz de Programación de Aplicaciones, y hacen referencia al conjunto de subrutinas, funciones y procedimientos que ofrece una «biblioteca» para ser utilizado por otro software como una capa de abstracción.

[4] **JASO**: son las siglas en euskera de Jaurlaritzaren Sare Orokorra (Red General del Gobierno). Es un modelo de interconexión de redes que permite el intercambio eficiente de información entre distintas redes, como son la Red Corporativa Administrativa del Gobierno Vasco, las redes sectoriales y sus entes dependientes.

eliminación, búsqueda y transformación de contenidos. Los principales objetivos han sido:

- Facilitar a los Departamentos/Organismos Autónomos la generación de un «compartimento estanco» en el cual poder gestionar su documentación.
- Posibilitar a los Departamentos/Organismos Autónomos una configuración flexible de su «compartimento», permitiendo que cada uno defina sus grupos, usuarios y ACLs[5] según sus necesidades, y de forma aislada al resto de Departamentos.
- Dejar la puerta abierta a un posible acceso inter-departamental de la documentación, aunque conlleva una mayor complejidad en la configuración de la seguridad.

Como ya sabemos, toda documentación almacenada en un repositorio de Documentum (sistema sobre el que se basa PID) debe asociarse a un tipo documental concreto. Indicar que cada iniciativa departamental podrá definir sus propios tipos documentales, siendo esa tipología asociable exclusivamente a los documentos del departamento al cual pertenece esa tipología.

El *framework* de PID hace uso de diferentes infraestructuras horizontales del Gobierno, como pueden ser, entre otras:

- XLNets: herramienta corporativa de seguridad del Gobierno Vasco que permite al *framework* autenticar a las aplicaciones y obtener la información de conexión al repositorio.
- PLATEA Integración-Servicios: los servicios del *framework* se harán accesibles a las aplicaciones a través del Bus de Servicios, con los beneficios que esto conlleva (trazabilidad, monitorización, etc.).
- PLATEA Integración-Eventos: se utilizará esta plataforma para la comunicación de eventos asíncronos, como la realización de transformaciones entre formatos.
- PLATEA Integración-Ficheros (PIF): se utilizará esta plataforma como almacén temporal para el intercambio de documentos entre las aplicaciones y la PID.

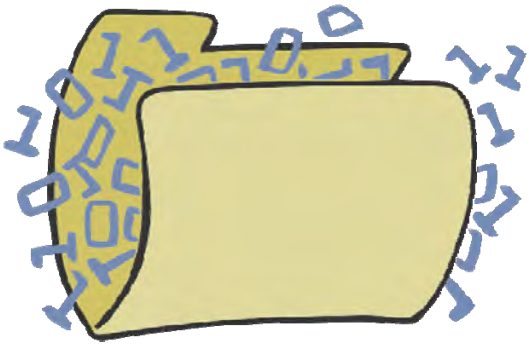
La plataforma PID está accesible desde cualquier red (Intranet, Extranet e Internet), tanto interno de EJIE (del propio CPD) como de terceros (redes sectoriales, albergues o terceros que acceden vía Internet).

Gracias al PID se evitan los problemas típicos del uso de los sistemas NAS (almacenamiento conectado en red), como pueden ser la gestión de permisos de las personas usuarias y grupos en Weblogic, degradación ocasional del rendimiento, acceso entre distintos entornos, llenado del *file-system* o sistema de ficheros...). Por ejemplo, mediante el uso de PIF, una aplicación puede dejar un fichero en la zona de intercambio correspondiente, y llamar al servicio de PID (desplegado en Intranet) solicitando el almacenamiento de dicho fichero. Este escenario es a día de hoy inabordable usando una NAS como zona de almacenamiento temporal, ya que una aplicación Intranet no tiene acceso (por comunicaciones) a la NAS de Internet.

PLATEA INTEGRACIÓN BIG DATA

Las aplicaciones escriben trazas (*logs*) para poder confirmar el correcto funcionamiento de los programas. En el mundo de la web es complicado gestionar grandes volúmenes de datos relativos a invocaciones ya que generan con facilidad gigas y gigas de información que es necesario almacenar y, sobre todo, gestionar.

El proyecto Platea Integración BigData (PIB) tiene como objeto suministrar una solución que



posibilite la recogida de trazas (*logs*) sin que ello interfiera en el funcionamiento normal de las aplicaciones y la explotación de las mismas.

Básicamente existen 3 tipos de trazas:

- ✓ Ejecución: info, error, *warning*...
- ✓ Tiempo: una operación concreta ha tardado x segundos
- ✓ Propias: una persona usuaria X ha modificado una tabla T aportando un valor Z

El proyecto BigData ha tenido dos enfoques: por un lado, tiene el espíritu de *toolkit* para ser utilizado por los aplicativos en la fase de construcción que se ciñen principalmente a la recogida de datos; por otro lado, existe también un

DICCIONARIO

[5] **ACLs**: son las siglas en inglés de Access Control List, es decir, Lista de Control de Acceso. Se trata de un concepto utilizado en el ámbito de la seguridad informática y que se utiliza para fomentar la separación de privilegios o permisos. Gracias a ella se establecen los permisos de acceso a un sitio o recurso determinado.

Básicamente es una lista de reglas que detallan, por ejemplo, los puertos de servicio o nombres de dominios (de una red) que están disponibles, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar ese servicio.

enfoque de consumo que posibilitará que los datos almacenados puedan ser consumidos tanto por el personal de Asistencia Técnica como por el personal de Explotación.

Esta utilidad se puede utilizar en distintos entornos: aplicaciones Web sobre Java (Weblogic11), aplicaciones .Net y para procesos de *backend*. También se puede utilizar como un componente javascript que se incluye en el código html de una página web para que envíe información sobre la navegación que ha realizado una persona para, posteriormente, poder ser analizada con las herramientas de gestión.

Para poder explotar toda la información que se recaba, el personal técnico de EJIE ha desarrollado una web que incluye un Cuadro de Mando o *Dashboard* (ofrece una visión gráfica de los indicadores de las últimas x horas); una opción de Búsqueda (visión textual que permite buscar diferentes datos almacenados); un *tail* (permite capturar directamente los datos según son generados por el servicio o aplicación).

Todos los datos se encuentran almacenados en una solución específica para *bigdata*, en nuestro caso **hbase**[6].

Desde el punto de vista de la seguridad, el acceso y consulta de datos por parte de las personas usuarias será previa autenticación en XLNets y en función del Servicio. P.ej. el grupo de Asistencia Técnica del área de Educación podrá ver las trazas de todas las aplicaciones del Departamento.

A día de hoy son varios los Servicios y Áreas que están haciendo uso de esta solución de BigData:

- ✓ Soluciones horizontales funcionales: Tramitación, etc.
- ✓ Departamentales: IVAP, etc.
- ✓ Soluciones horizontales técnicas: Integración Servicios, Integración Documentos (PID), Sistema de mensajería Latinia, Integración Ficheros (PIF), etc.

NOTIFICACIONES PUSH

Los Departamentos y Organismos Autónomos del Gobierno Vasco han venido utilizando a lo largo del tiempo distintos canales para comunicarse con la ciudadanía (tablón de anuncios, teléfono, email…) y facilitar toda la información necesaria.

Sin embargo, todo el mundo sabe que los nuevos dispositivos móviles (*smartphones*) posibilitan ya una relación más proactiva y cercana, por lo que se hace necesario aprovechar la potencialidad de dichos dispositivos para conseguir una administración más cercana y eficaz.

Tal es así que, basándose en la plataforma de mensajería ya existente en el Gobierno Vasco (denominada Latinia) y, sobre todo, en la potencialidad de los *smartphones*, se propone incorporar un nuevo canal de comunicación (basado en mensajes de notificación) que facilite la interacción entre los Departamentos y la ciudadanía.

Mezu, por ejemplo, es un aplicativo que permite establecer un canal de comunicación directo con la ciudadanía mediante este servicio de mensajería que ha desarrollado el personal técnico de EJIE. La idea es facilitar un canal de comunicación con los terminales móviles como alternativo a los SMS.

Su funcionamiento se basa en la tecnología o método *push*. Ello significa que la notificación es iniciada desde un Servidor hacia la persona destinataria (usuario/a final). Lo cual requiere establecer un acuerdo previo entre el Servidor y la persona usuaria mediante el cual esa persona autoriza recibir notificaciones. Es decir, el funcionamiento es muy similar al que usan aplicaciones como whatsapp, telegram, etc., se debe descargar una app y registrarse en el servicio.

Recordar que Mezu se basa en la aplicación Latinia, por lo que si estáis pensando incluir este servicio dentro de alguna aplicación Departamental y ésta no utiliza Latinia, habrá que desarrollar un *webservice* para conectar ambas.

Si bien en 2008, año en que se puso en producción, el número de mensajes enviados apenas superaba los 11.000, en 2015 se superaron ampliamente los 2.000.000 de mensajes enviados por año. Lo que da idea de su potencial. ❑

DICCIONARIO

[6] **hbase**: es una base de datos distribuida no relacional de código abierto modelada a partir de Google BigTable y escrita en Java. Su desarrollo forma parte del proyecto Hadoop de la Fundación de Software Apache y se ejecuta sobre HDFS (el sistema de archivos distribuidos de Hadoop) y es multiplataforma.

[fuente: wikipedia.org]

http://hbase.apache.org

Incidentes de seguridad (de la información)

Mientras se desarrolla la actividad de cualquier organización suelen ocurrir incidentes de seguridad, por ello hay que estar preparados para responder adecuadamente a los mismos, minimizando su impacto y aprendiendo de cara al futuro.

DICCIONARIO

[7] **ISO/IEC 27035:2011:** es una norma sobre Tecnologías de la información, técnicas de seguridad, gestión de incidentes de seguridad de la información; estándar publicado por ISO para ayudar a las organizaciones a mejorar la gestión de los incidentes relativos a la seguridad de la información.

Un «**incidente de seguridad de la información**» *es un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.* [ISO/IEC 27035:2011][7]

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

La Política de Clasificación de la Información determina los criterios de clasificación de la información de una organización, en nuestro caso el Gobierno Vasco, desde el punto de vista de su seguridad, identificando los niveles de criticidad aplicables a cada una de las **dimensiones de la seguridad (o garantías de la seguridad)** afectadas.

De acuerdo a la regulación aplicable, **toda información existente debe ser clasificada en función de la valoración del impacto que tendría sobre la organización un incidente**. Dicha valoración debe ser realizada en torno a las diferentes **dimensiones** de la seguridad contempladas:

1. **Disponibilidad [D] y Conservación**: Propiedad o característica de la información consistente en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran, preservando dicha propiedad del deterioro temporal a lo largo de todo su ciclo de vida.
2. **Integridad [I]**: Propiedad o característica consistente en que la información no ha sido alterada de manera no autorizada.
3. **Confidencialidad [C]**: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a personas, entidades o procesos no autorizados.
4. **Autenticidad [A]**: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
5. **Trazabilidad [T]**: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Los **criterios de valoración** de la información dependen, de manera general, de los siguientes aspectos:

1. Repercusiones negativas en la capacidad operativa de la organización para atender eficazmente sus obligaciones.
2. Efectos dañinos sobre los activos de la organización.
3. Repercusiones en el cumplimiento de la legalidad vigente por parte de la organización.
4. Causa de perjuicios a personas físicas.
5. Repercusiones sobre los derechos de las personas.

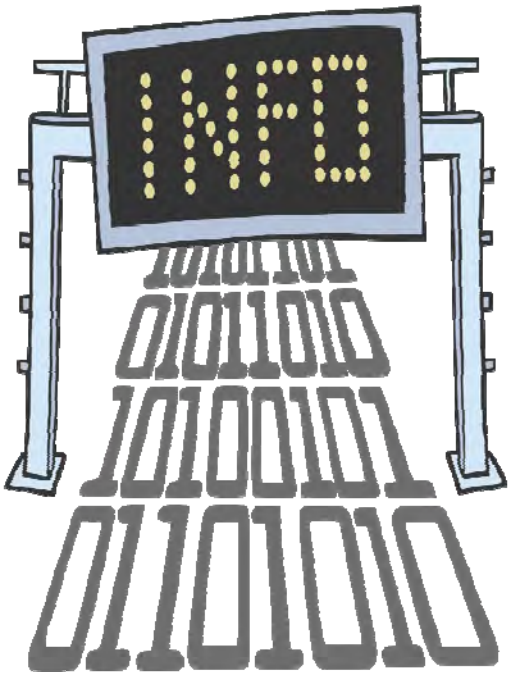
6. Daños a la imagen de la organización.
7. Otros de naturaleza análoga.

VALORACIÓN DEL IMPACTO DE UNA INCIDENCIA

La valoración del impacto, que se llevará a cabo de manera independiente para cada dimensión de la seguridad, se realizará en base a los niveles de seguridad específicos que se definen a continuación:

1. **BAJO**: Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones antes comentadas supongan un **perjuicio limitado** sobre las funciones de la organización, sobre sus activos o sobre las personas afectadas.
2. **MEDIO**: Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones supongan un **perjuicio grave** sobre las funciones de la organización, sobre sus activos o sobre las personas afectadas.
3. **ALTO**: Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de la seguridad supongan un **perjuicio muy grave** sobre las funciones de la organización, sobre sus activos o sobre las personas afectadas.

Puede ser que en alguna dimensión de la seguridad la valoración del impacto dé como resultado «**sin valorar**», por ejemplo, la autenticidad de una determinada información podrá ser catalogada como de esa forma cuando el origen es irrelevante o ampliamente conocido por otros medios, o cuando el destinatario es irrelevante, por tratarse de información de difusión anónima o generalista.



IDENTIFICACIÓN DE INCIDENTES DE SEGURIDAD

Todo persona, tanto interna como externa, que trabaja para una organización, tiene la obligación de notificar cualquier situación que suponga, o considere que puede suponer, un funcionamiento anómalo, incorrecto o inapropiado de algún componente de cualquier sistema de información (equipo, servicio, red, archivo, etc.), que será considerada como incidencia.

En particular, cualquier incidencia detectada que indique una posible **violación de la política de seguridad de la información**[8] de la organización, un fallo de las medidas de seguridad establecidas, o cualquier situación desconocida hasta el momento y que pueda ser relevante para la seguridad será considerada incidente de seguridad.

Una categorización inicial para aquellas incidencias susceptibles de ser catalogadas como incidentes de seguridad puede ser la siguiente (categorías y subcategorías):

- **Confidencialidad**: La incidencia ha supuesto (o ha podido suponer) la violación de la confidencialidad de la información asociada, puesto que esa información ha sido conocida (o ha podido serlo) por personas que no deberían haber tenido acceso a dicha información:
  - ✓ **Pérdida de Soporte** (papel, USB, CD, DVD, disco duro, etc.) que contenía dicha información, de modo que no se puede garantizar que la información no haya sido conocida por personas no autorizadas a conocerla.
  - ✓ **Difusión de información**: La pérdida de confidencialidad se ha producido porque la información se ha comunicado (de forma verbal o escrita), de forma accidental o intencionada, a personas que no deberían haber conocido dicha información.

DICCIONARIO

[8] **Política de seguridad de la información:** para más información podéis consultar el boletín Aurrera nº 56 (y, en concreto, el artículo titulado «*Política de seguridad de la información (PSI)*»).

- ✓ **Acceso no autorizado**: La pérdida de confidencialidad se ha producido porque alguien, a priori no autorizado, ha accedido (intencionadamente o por error) a la información.

- **Integridad**: La incidencia ha supuesto (o ha podido suponer) la violación de la integridad de la información asociada, de modo que esa información es incorrecta (por haberse modificado de forma no controlada) o se ha corrompido por completo:
  - ✓ **Difusión de información incorrecta**: La pérdida de integridad se ha producido porque se ha difundido formalmente en un medio abierto una información errónea.
  - ✓ **Incumplimiento de Política de Seguridad**: La pérdida de integridad se ha producido porque se ha violado, de manera intencionada o accidental, alguna norma de seguridad que ha puesto en riesgo la validez de la información.

- **Trazabilidad**: La incidencia ha supuesto (o ha podido suponer) un fallo en la trazabilidad del servicio, de forma que no se pueda verificar de forma completa lo que ha sucedido en torno al mismo:
  - ✓ **Auditoría de datos de nivel alto**: La pérdida de trazabilidad se ha producido en torno a la funcionalidad de auditoría de datos del servicio.
  - ✓ **Acceso**: La incidencia está relacionada con el sistema de control de acceso lógico a los sistemas de información.
  - ✓ **Olvido de contraseña**: La persona usuaria no puede acceder a un sistema de información porque ha olvidado la contraseña de acceso.
  - ✓ **Uso indebido de contraseña**: La persona usuaria no ha respetado las normas de uso de la contraseña[9], lo que ha provocado (o ha podido provocar) que otras personas puedan haberla conocido.
  - ✓ **Acceso no autorizado**: Una persona usuaria ha accedido, mediante el uso de los identificadores de persona usuaria bajo su control, a dependencias que contienen sistemas de información con datos de carácter personal o información clasificada como restringida o confidencial.

Además de encuadrarse en alguna de las categorías y subcategorías que se acaban de indicar, la incidencia podrá tener una categorización adicional, denominada **LOPD**[10], en función de si hay o puede haber datos de carácter personal en el ámbito de ocurrencia de la misma. Esta categorización adicional es aplicable a todas las categorías anteriores excepto a las categoría de "*Auditoría de datos de nivel alto*", a la que siempre aplica, y a la categoría de "*Incumplimiento de política de seguridad*", donde nunca lo hace.

Así mismo, existe un tipo de peticiones específicas a las que también aplica la categorización adicional **LOPD**, que son las peticiones del tipo **Recuperación de datos personales**, en las que se requiere la restauración, a partir del *backup*, de información catalogada como datos de carácter personal.

REGISTRO DE INCIDENCIAS SEGÚN LA LOPD Y EL ENS

La información mínima (según el Reglamento que desarrolla la LOPD, art. 90) que se debe incluir en

el registro de incidencias desde el punto de vista LOPD es la siguiente:

1. El tipo de incidencia.
2. El momento en que se ha producido, o en su caso, detectado.
3. La persona que realiza la notificación.

DICCIONARIO

[9] **Normas de uso de la contraseña**: debe existir una **política de contraseñas** en cuanto a su longitud, su composición, su caducidad, sus restricciones y su bloqueo, cuyo objetivo sea garantizar la calidad y seguridad de las mismas.

[10] **LOPD**: Ley Orgánica de Protección de Datos de carácter personal (LO 15/1999).

4. A quién se le comunica.
5. Los efectos que se hubieran derivado de la misma.
6. Las medidas correctoras aplicadas.

Además, tal y como se ha apuntado anteriormente, para los procedimientos de recuperación de datos (que incluyan datos de carácter personal de nivel medio o alto) deberán consignarse (art. 100 del Reglamento):

1. Los procedimientos realizados de recuperación de los datos.
2. La persona que ejecutó el proceso.
3. Los datos restaurados.
4. Y, si ha lugar, qué datos han sido necesarios grabar manualmente en el proceso de recuperación.

En cuanto al Esquema Nacional de Seguridad (ENS), que en nuestro ámbito, Gobierno Vasco, tiene como alcance a la Plataforma Tecnológica para la eAdministración (PLATEA[11]), respecto al registro de incidencias (para todas las dimensiones de la seguridad y categorías media y alta), dice lo siguiente:

«*Se registrarán todas las actuaciones relacionadas con la gestión de incidencias, de forma que:*

1. *Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.*
2. *Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.*
3. *Como consecuencia del análisis de las incidencias, se revisará la determinación de los eventos auditables.*» ❑

DICCIONARIO

[11] **PLATEA:** se constituye como la infraestructura tecnológica base para la e-Administración del Gobierno Vasco, de obligado uso en los desarrollos de aplicaciones relacionadas con la mecanización de procedimientos de tramitación de expedientes.

Gestión de incidencias de seguridad de la información

Es un proceso continuo, que debe controlar las actividades antes, durante y después de que un incidente ocurra.

Su objetivo principal es solucionar las incidencias de seguridad que se produzcan.

Esta gestión debe de tener claros los siguientes aspectos:

- ✓ Definición de responsabilidades y procedimientos.
- ✓ Establecer canales para que las personas (tanto internas como externas) puedan comunicar los incidentes.
- ✓ Permitir notificar también los puntos débiles.
- ✓ Establecer mecanismos para registrar, clasificar, evaluar y priorizar incidentes de seguridad, para, de este modo, evaluar el impacto.
- ✓ Indicar cómo se responden y solucionan los incidentes registrados, cómo se recogen las evidencias, y como se registran las acciones desarrolladas y su posterior análisis.
- ✓ Aprender de los incidentes ocurridos de cara al futuro.
- ✓ Especificar los procedimientos necesarios para recuperar evidencias desde un punto de vista legal.

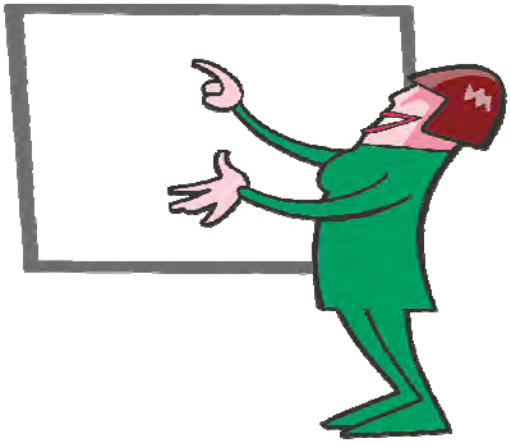
ALBOAN:

Seminarios «Alboan»

Dirección de Informática y Telecomunicaciones

«El objetivo principal de estos Seminarios es conocer las especificidades y funcionamiento interno de los Departamentos y Organismos Autónomos»

Durante los últimos años, la Dirección de Informática y Telecomunicaciones (DIT) del Gobierno Vasco, a través de su Gabinete Tecnológico, ha venido impulsando distintas iniciativas con el objetivo de poner a disposición del personal informático los medios para comunicar e intercambiar información que pudiese ser de interés para todos ellos. Con ese fin, se pusieron en marcha, entre otras iniciativas, el propio boletín Aurrera que estás leyendo, así como una serie de encuentros (denominados «seminarios»), que tenían (y tienen) como objetivo dar a conocer proyectos o nuevas tecnologías/tendencias que existen en el mercado.



SEMINARIOS

Sin nos centramos en los seminarios que se organizan a lo largo de todo el año, y cuya información está disponible en la intranet del Gobierno Vasco (Jakina), su principal objetivo es informar de los proyectos o iniciativas (tanto internas como externas) y servir de plataforma para dar a conocer esas nuevas tecnologías que puedan ser de interés.

Los seminarios que organizamos desde la DIT están dirigidos inicialmente al personal técnico informático del Gobierno Vasco, a las jefaturas de proyecto de EJIE y al personal relacionado con cada uno de los temas que se tratan en cada momento.

La DIT este año ha querido dar un nuevo enfoque a los contenidos de los Seminarios y, para ello, ha puesto en marcha una nueva iniciativa denominada «*Seminarios Alboan*».

El objetivo de estos «*nuevos*» Seminarios es básicamente conocer las especificidades y funcionamiento interno de los Departamentos y Organismos Autónomos que componen el Gobierno Vasco, es decir, a nuestro «vecindario», con el que en muchas ocasiones (y debido al trabajo del día a día) no tenemos ocasión de tratar asuntos o problemáticas comunes que nos surgen en nuestro trabajo departamental.

El objetivo principal de esta iniciativa, por tanto, es dar a conocer la labor que desempeñan nuestros compañeros/as («vecinos/as») del área informática de otros Departamentos u Organismos Autónomos.

EMAKUNDE
EMAKUMEAREN EUSKAL ERAKUNDEA
INSTITUTO VASCO DE LA MUJER

Para ello, mediante esta iniciativa, la Dirección de Informática y Telecomunicaciones pretende:

- ✓ Impulsar la relación y comunicación entre el personal informático del Gobierno Vasco, es decir, aquellas personas que desarrollan su trabajo en cualquier área informática de los Departamentos u Organismos Autónomos del Gobierno.
- ✓ Facilitar el intercambio de experiencias, problemáticas y/o conocimientos sobre asuntos del trabajo que pueden surgir en el día a día.

Para ello, se quería contar con la participación directa de la persona responsable/s del área informática de cada Departamento, para que fuese ella, en primera persona, quién desarrollase cada tema.

Además, se quería aprovechar el evento para conocer cuáles han sido los proyectos más

relevantes que se han llevado a cabo en esta legislatura, cuáles son los proyectos que se tienen previsto abordar durante los próximos meses, cómo se gestionan los proyectos, cuáles son las funciones del equipo informático, cómo está organizado el Departamento u Organismo Autónomo correspondiente, personal asignado al mismo, presupuesto que maneja el área informática, Asistencia Técnica de EJIE con la que cuenta para poder abordar los distintos proyectos, etc.

PRIMERAS SESIONES

La primera sesión de este tipo tuvo lugar el pasado mes de junio y tuvo como protagonistas a **Lehendakaritza y Emakunde** (Instituto Vasco de la Mujer). A lo largo de este encuentro, el Responsable Informático de Lehendakaritza nos comentó cuál ha sido su trayectoria en el Gobierno, cuáles son sus principales tareas y su relación con las Delegaciones que el Gobierno Vasco tiene en el extranjero, así como las diferentes problemáticas que surgen en el día a día y cómo las afronta.

El Responsable informático de Emakunde, por su parte, nos explicó los inicios del organismo autónomo y cuáles son, a día de hoy, los principales proyectos o iniciativas que se están llevando a cabo o se tiene previsto poner en marcha en breve (convocatorias de ayuda, webs, nuevas *apps* o aplicaciones para móviles...).

Poco después, en el mes de julio, tuvimos la oportunidad de organizar con el **Departamento de Salud** otro seminario-alboan. En este caso, el Responsable del área informática realizó una amplia descripción de cómo está organizado el Servicio de Atención Sanitaria en Euskadi, diferenciando cuáles son las competencias y tareas de cada uno de sus actores: el Departamento de Salud, por una parte; y, el ente público Osakidetza, por otra parte. Asimismo, el Jefe de Proyecto de EJIE aprovechó la última parte del encuentro para explicarnos brevemente los aspectos más relevantes del proyecto con más repercusión en la sociedad que lleva a cabo el Departamento: la Receta Electrónica o eRezeta.

Teniendo en cuenta la valoración y buena acogida que han tenido entre los asistentes estos primeros seminarios, la idea de la Dirección de Informática y Telecomunicaciones es dar continuidad a este tipo de eventos (seminarios-alboan), por lo que en fechas próximas tendremos la oportunidad de conocer los entresijos de más Departamentos/ Organismos Autónomos.

Para acabar, desde la DIT, os animamos a que asistáis y participéis en estos encuentros, ya que creemos pueden ser de gran utilidad para todo el personal informático del Gobierno Vasco. ❑

«La primera sesión tuvo como protagonistas a Lehendakaritza y Emakunde»

[+info]:

Web de la Dirección de Informática y Telecomunicaciones

http://www.euskadi.eus/informatica

¡¡BREVES!!

nº 57

Septiembre de 2016

Electronic Frontier Foundation (EFF)

La EFF es una organización sin ánimo de lucro con sede en San Francisco (Estados Unidos), poco conocida por el público en general, y cuyos objetivos son concienciar sobre las libertades civiles relacionadas con las tecnologías, defender estas libertades (defensa legal en los tribunales) y realizar acciones educativas y formativas.

La EFF, que fue fundada en julio de 1990 por Mitch Kapor, John Gilmore y John Perry, se financia a través de donaciones (muchas de las cuales provienen de empresas, ya que hay tecnologías que dependen de los resultados de la EFF), siendo su misión principal **proteger la privacidad de los internautas**.

La creación de la organización estuvo motivada por el registro y embargo que sufrió un editor de Texas a principios de 1990 por parte del servicio secreto de Estados Unidos. En aquel momento, las autoridades registraron varios domicilios y empresas en busca de pistas sobre la filtración de un documento que describía el funcionamiento del servicio de emergencias 911. Si bien el editor no tenía nada que ver con la filtración, como resultado del embargo de todos sus equipos y material informático, su negocio quedó al borde de la ruina. Posteriormente, cuando fue a buscar ayuda para reclamar por los perjuicios que le habían acarreado, no obtuvo ningún tipo de respaldo, lo cuál motivó que se crease la EFF.

Una de las luchas abiertas que mantiene EFF es respecto al DRM (gestión de los derechos digitales), la tecnología de control de acceso utilizada por las empresas editoriales. El World Wide Web Consortium (W3C), que regula los estándares de Internet, quiere establecer como estándar de Internet el DRM, lo cual supondría que al personal investigador de seguridad en navegadores Web, por ejemplo, se les podría aplicar las leyes de *copyright* y podrían ser demandados si denuncian los agujeros de seguridad que pudieran encontrar.

Página web: http://www.eff.org

Nace la red social «*Basque Global Network*»

Recientemente, el Gobierno Vasco ha presentado la iniciativa «*Basque Global Network*» (BGN), que consiste en una red social en internet cuyo objetivo es integrar en ella a las personas que forman parte de la comunidad vasca en el exterior, así como a vascos y vascas que tengan una proyección internacional, o personas con afinidad hacia lo vasco.

Esta red pretende convertirse en un punto de encuentro entre dichas personas y las instituciones vascas con un tema central: Euskadi-Basque Country.

La red, que está funcionando desde hace unas semanas, cuenta ya con usuarios/as que residen en al menos 20 países.

Esta red vasca global está dirigida a las personas de origen vasco que viven fuera de Euskadi (de forma permanente o temporal); vascos y vascas con proyección internacional; personas asociadas a las Euskal Etxeak y personas con afinidad hacia lo vasco.

Los idiomas iniciales de la nueva plataforma serán el euskera, castellano, inglés y francés.

La BGN incluirá 5 áreas temáticas: institucional, empresarial, cultural, educativa y de cooperación al desarrollo.

A diferencia de otras redes sociales, las personas integrantes de ésta podrán, además de tejer redes de contactos o crear grupos en función de intereses comunes, gestionar y compartir eventos, calendarios y documentos.

Desde el punto de vista tecnológico es una solución a medida desarrollada en **Joomla** y **MySQL**, la cual está soportada en un servidor con Linux/Apache, infraestructura que esta albergada en EJIE.

Página web: http://www.basqueglobalnetwork.eus