EUSKO JAURLARITZA
GOBIERNO VASCO

Aurrera!

Nº 33

marzo de 2009

Boletín Divulgativo de Nuevas Tecnologías en Informática y Telecomunicaciones

Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

- Seguridad en dispositivos móviles externos (robos y pérdidas) — Pág. 2
- Gestión de Identidades — Pág. 6
- Alboan: El nuevo BOPV electrónico — Pág. 10
- Breves: Dominio .eus; El Gobierno Vasco adquiere un superordenador — Pág. 12

Seguridad. Esa es la palabra que puede resumir los dos primeros temas de este nuevo Boletín Aurrera!

El primero de ellos, titulado "**Seguridad en dispositivos móviles externos**", trata de exponer los problemas a los que se enfrentan las organizaciones que no contemplan los nuevos dispositivos móviles como otros elementos más dentro de su ámbito de seguridad.

El segundo de ellos, titulado "**Gestión de Identidades**", por su parte, se centra en la problemática que existe hoy en día en las grandes organizaciones a la hora de gestionar todos los códigos y passwords de acceso a las aplicaciones de sus usuarios. A lo largo del artículo se definirán, entre otros, conceptos como "*ciclo de vida*" del perfil de usuario, metadirectorio o *«single sign-on»*.

Dentro del apartado Alboan, os damos a conocer la última novedad relacionada con el **Boletín Oficial del País Vasco** (BOPV): desde el pasado 1 de enero éste ha dejado de publicarse en soporte papel y, por lo tanto, únicamente se encuentra disponible en formato electrónico. Con motivo de este nuevo hito en la historia del Boletín Oficial, os detallamos el por qué de esta decisión, qué soluciones tecnológicas se han adoptado (firma electrónica) y otros datos de interés sobre el mismo.

El apartado Breves incluye, como primera noticia, la iniciativa impulsada por la asociación PuntuEus, cuyo objetivo es solicitar que se habilite el **dominio .eus** dentro de Internet. Y como segunda noticia hemos incluido la última compra que ha realizado EJIE, la cual ha consistido en la adquisición de un "***superordenador***". Este nuevo equipo pretende dar servicio, entre otros, al servicio de meteorología y a la Universidad del País Vasco para facilitar el desarrollo de investigaciones climatológicas de alto nivel.

Por último, tal y como ya habréis comprobado, con motivo de este nuevo número, y después de 3 años mostrando la misma cara, nuestro Boletín Aurrera ha decidido actualizar su diseño. El objetivo es, en primer lugar, hacer que sea aún más atractivo y, en segundo lugar, facilitar al usuario la lectura de los artículos. En este sentido, informaros que el Gabinete Tecnológico, responsable tanto del diseño como del contenido del mismo, queda a la espera de vuestras opiniones y/o nuevas sugerencias.

Seguridad en dispositivos móviles externos (robos y pérdidas)

Hoy en día las tecnologías de movilidad aportan un evidente beneficio para cualquier persona, empresa o corporación; sin embargo, existe un claro riesgo ligado a la utilización de este tipo de dispositivos: muchas entidades se olvidan de aplicar políticas de seguridad en referencia a su utilización y manejo.

DICCIONARIO

[1] **PDA:** contracción que proviene del inglés, y que significa ***P****ersonal* ***D****igital* ***A****ssistant* (Asistente Digital Personal), es un dispositivo de mano, que en su origen fue una agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura. Hoy día se puede usar como un ordenador doméstico y empresarial, y desde el cual se pueden realizar tareas tales como ver el correo electrónico, navegar por Internet, leer ficheros, reproducir contenidos multimedia, sincronizar con un ordenador personal, navegar a través de GPS...

(Para más información, ver boletín AURRERA nº 18, artículo titulado "*Soluciones de movilidad*")

Las tecnologías de movilidad están creciendo de una manera importante, tanto en el ámbito personal como en el empresarial. Un caso de éxito es el de la telefonía móvil, con un crecimiento exponencial en un breve período de tiempo. Estas tecnologías permiten, y de ahí parte de su éxito, conciliar la vida profesional y personal.

Para poder utilizarlas manejamos diferentes dispositivos, conocidos como dispositivos portátiles, tales como teléfonos móviles inteligentes (*smartphones*), ordenadores portátiles, memorias USB (también conocidas como *USB flash drives, pen-drive´s o memory sticks*), discos externos portátiles, PDAs[1], etc.

Las organizaciones deben estar preparadas para, por un lado, poder dar estos servicios móviles, y, por otro lado, controlar los riesgos asociados a su uso, sorteando el problema de la velocidad del cambio en el mundo de los terminales móviles y la heterogeneidad de los mismos.

PÉRDIDAS DE INFORMACIÓN

Dentro de cualquier organización, las pérdidas de información son las principales causas que generan los incidentes de seguridad más graves, además, pueden suponer una fuerte pérdida de prestigio, así como el inicio de acciones legales contra la compañía, junto con una repercusión económica negativa para la misma.

Las fugas de datos pueden deberse a un sinfín de causas, pero se pueden encuadrar en estas dos:

- Las que son intencionadas
- Las que tienen su origen en descuidos, robos o pérdidas

> **"Según Gartner Group para este año 2009 más de un 25% de los dispositivos móviles serán PDAs y teléfonos móviles inteligentes."**

Estas últimas, descuidos, robos o pérdidas, ocurren con una frecuencia más habitual de lo que se piensa, además, no se llevan a cabo utilizando complejos ataques técnicos.

Muchas compañías reconocen que no cuentan con una estrategia de seguridad para este tipo de problemas, aun a sabiendas de que la propiedad intelectual y la seguridad de los datos confidenciales son un pilar básico para el éxito del negocio, y todo esto muchas veces ocurre pese a contar con algún tipo de estrategia para evitar incidencias relacionadas con la pérdida de datos, por lo que se deduce que se descuida la protección de los dispositivos móviles.

Generalmente, las **políticas y procedimientos de seguridad** están orientadas a defender a la organización contra ataques externos, pero no se suelen tener en cuenta las amenazas que provienen desde dentro, las amenazas internas (se puede entender, por ejemplo, que la pérdida de una memoria USB con datos sensibles para la organización es una amenaza clasificada como interna). La mayor amenaza de seguridad para las empresas han dejado de ser los ataques externos que pueden recibir, y han pasado a ser

las fugas de información internas.

En los medios de comunicación hemos escuchado con harta frecuencia la noticia de fugas de datos sensibles de importantes compañías, debido a la pérdida de dispositivos móviles por parte de una persona perteneciente a esa compañía o subcontratada por la misma.

"Los dispositivos portátiles son un «agujero» en lo que llamamos seguridad empresarial."

Como ejemplo, cabe destacar la pérdida, por parte del Gobierno del Reino Unido, de información del orden de cuatro millones de datos de ciudadanos, en tan solo un año, motivada tanto por el extravío de CDs como por el robo de equipos portátiles.

Está claro que para evitar estas fugas (puede que no se evite la pérdida o sustracción, pero si se debe evitar el posterior acceso a esos datos) se deben establecer políticas y procedimientos de seguridad que permitan, por un lado, las comunicaciones seguras (por ejemplo a través de VPN[2]), y por otro, que el uso del dispositivo móvil se limite a las personas autorizadas, además de garantizar la protección de los datos contenidos en el dispositivo, tanto de usos no autorizados como de intentos de lectura, en caso de pérdida o robo. Esto implica el uso de herramientas especializadas.

La seguridad hasta el día de hoy se basaba en proteger un perímetro conocido, pero, desde el punto de vista de la movilidad, este perímetro se ha "ampliado" de una forma importante.

La implantación de un "Sistema de Gestión de Seguridad de la Información" (SGSI), como el modelo ISO 27002:2005, pretende, tal y como se explica en la tabla inferior, mitigar el riesgo al que están sujetos los activos de información, a través de la realización previa de un análisis y evaluación del riesgo, y una posterior actuación sobre ese riesgo (mediante el uso de "dominios",

ISO 27002:2005

El estándar para implantar un "*Sistema de Gestión de Seguridad de la Información (SGSI)*" es el modelo ISO 27002:2005, **estándar internacional certificable**, centrado en "reducir" el riesgo al que están sujetos los activos de información, para lo cual se realiza previamente un **análisis y evaluación del riesgo**. Este modelo (al implementarse) asegura la continuidad en las operaciones de la organización y minimiza las posibilidades de que una amenaza haga daño a los activos de información de la organización.

Este estándar gira entorno a la gestión del riesgo, dentro del alcance previamente definido, teniendo claro que las excepciones dentro de ese alcance deben ser compatibles con lo que la propia norma marca.

Los pasos a dar para evaluar la exposición al riesgo son los siguientes (análisis de riesgos):

- ✓ Identificar los activos de información
- ✓ Tasar los activos identificados
- ✓ Identificar las amenazas para cada activo y estimar la probabilidad de que esta amenaza se materialice
- ✓ Identificar las vulnerabilidades y la posibilidad de que sean explotadas por las amenazas
- ✓ Estimación de la exposición al riesgo de los activos
- ✓ Priorizar las amenazas según su exposición al riesgo

Una vez realizada esta tarea se debe realizar la evaluación del riesgo, usando los siguientes criterios:

- ✦ Impacto económico del riesgo
- ✦ Tiempo de recuperación de la organización
- ✦ Posibilidad de ocurrencia del riesgo
- ✦ Posibilidad de interrumpir actividades de la empresa

Una vez el riesgo ha sido evaluado y contabilizados los activos importantes asociados al riesgo, se debe elegir la estrategia adecuada para, de este modo, tratar de minimizar dicho riesgo.

Existen cuatro posibles acciones para tratar el riesgo:

- Reducirlo
- Aceptarlo
- Transferirlo (por ejemplo, a través de una aseguradora)
- Evitarlo

DICCIONARIO

[2] **VPN**: *Virtual Private Network* o Red Privada Virtual, es una red construida usando canales públicos. Por ejemplo, hay sistemas que posibilitan la creación de redes usando Internet como medio de transporte de información. Estos sistemas usan la encriptación y otros medios de seguridad para asegurarse de que sólo los usuarios autorizados pueden acceder a la red y que la información no puede ser interceptada.

(Ver boletines AURRERA nº 1 y nº 2, con los artículos "*E-business*" y "*La migración de Windows 2000*" respectivamente)

"objetivos de control" y "controles").

TECNOLOGÍAS ENFOCADAS A LA PROTECCIÓN DE LA INFORMACIÓN

Estamos de acuerdo en que dotar a los distintos sistemas portátiles de medidas de seguridad es un factor fundamental.

El objetivo es, como hemos subrayado anteriormente, evitar que, debido a un robo o extravío, cualquier persona pueda acceder libremente a los contenidos de ese dispositivo móvil.

DICCIONARIO

[3] **CryptoAPI:** son las siglas en inglés de *Cryptographic Application Programming Interface*, es una interfaz de programación de aplicaciones (API) que se suministra como parte de Microsoft Windows, y que proporciona un conjunto de funciones que permiten a las aplicaciones cifrar o firmar datos de forma flexible, al tiempo que protegen los datos claves privados y confidenciales pertenecientes al usuario.

> **"La evolución e implantación de los sistemas de contraseña, cifrado y encriptado —en lo que se refiere al mundo de los dispositivos móviles— no hace otra cosa que seguir las pautas marcadas por los ordenadores de sobremesa."**

Actualmente, en el mercado existen tantas tecnologías como fabricantes, y cada una de ellas está orientada a una parcela concreta.

Autenticación de usuarios

El primer nivel de seguridad, el nivel básico, es el que tienen las aplicaciones, que se encargan de la autenticación de los usuarios. A partir de aquí los departamentos de TI (Tecnologías de la Información) tienen la posibilidad de asegurar los dispositivos con nuevas políticas y opciones de certificados, encriptación de tarjetas de memoria y discos, así como las posibilidades de borrado remoto o local de la información de un dispositivo concreto.

Uso de contraseñas

Las contraseñas son otro nivel de seguridad, y aseguran que el usuario que tiene permisos para acceder a ese equipo es realmente quien lo está utilizando, tal y como ocurre con los equipos de sobremesa corporativos o personales, a través de la clásica interfaz basada en introducir "nombre" y "contraseña".

Cifrado de la información

Como es lógico, la mayoría de los sistemas operativos asociados a dispositivos móviles ofrecen herramientas de cifrado, por ejemplo, Windows Mobile incluye servicios de cifrado basados en las herramientas CryptoAPI[3].

Muchos discos duros portátiles y memorias USB incorporan programas propietarios cuyo objetivo es encriptar los datos contenidos en su interior.

Sistemas biométricos

Los sistemas biométricos (evaluación de características únicas del cuerpo humano) son la última moda en cuanto a la seguridad de estos dispositivos móviles, en un primer momento se integraron en sistemas de seguridad y control de presencia, en la actualidad ya están perfectamente adaptados a estos dispositivos. Todo sistema biométrico requiere de un "repositorio" para almacenar los patrones asociados a cada individuo, y tiene las siguientes ventajas respecto a los sistemas clásicos:

- Es necesaria la presencia física del usuario
- No es necesario recordar una contraseña o llevar una tarjeta

TAXONOMÍA DE LOS SISTEMAS BIOMÉTRICOS

Principalmente existen tres tipos de sistemas biométricos diferenciados:

- ✓ Identificación de huella dactilar
- ✓ Lectura del iris
- ✓ Escaneado del rostro

El sistema más popular es el primero, la **identificación a través de la huella dactilar**, que se puede realizar mediante dos formas: por presión o por arrastre del dedo, debiéndose registrar primero la huella dactilar del usuario, bien situando el dedo sobre el sensor o arrastrándolo; entonces el sensor digitaliza el dedo y elabora una imagen de la huella dactilar, extrayéndose puntos específicos de la imagen, y mediante un algoritmo se convierten en datos numéricos, que son encriptados y almacenados, por lo que no se almacena ningún tipo de imagen. Cuando se accede al sistema, se realiza idéntica operación y se compara el dato matemático obtenido con el que previamente hemos almacenado en el repositorio.

Otro sistema, poco extendido, es el que elabora un mapa del entramado de las venas de la palma de la mano (por ejemplo, el equipo Palm Secure de Fujitsu utiliza esta tecnología de reconocimiento sin contacto).

Los otros dos sistemas, **reconocimiento del iris** y

escaneado del rostro, son más complejos y menos populares, aun así, existen equipos, como el Asus U6, que incorporando una webcam integrada, y utilizando el programa SmartLogon,

reconoce el rostro del propietario, proporcionando un acceso seguro a través del escaneado facial.

TECNOLOGÍA DLP: CÓMO EVITAR LA FUGA DE INFORMACIÓN SENSIBLE

El sector de tecnologías de la seguridad de la información dispone de una nueva tecnología (bastante reciente e innovadora), denominada DLP (*Data Loss Prevention* o *Data Leak Protection*), que no es sino una conjunción de diferentes mecanismos y procedimientos de seguridad cuyo **objetivo** es **evitar las temidas fugas de información sensible o confidencial**; básicamente intenta evitar que esa información salga de la organización a través de usuarios internos.

Cómo funciona

Controla la forma por la que se accede, transmite o copia la información; previamente se clasifica la información y los datos según su contenido, siendo el sistema el que aplica la acción oportuna (monitorización, cifrado, bloqueo, cuarentena…) una vez analizado el contenido y el contexto de los archivos de salida. Esta política sólo es válida en el interior de la organización. El perímetro de protección ya no sólo se basa en los recursos que se deben de proteger, sino que, gracias a tecnologías como DLP, también definimos los contenidos a proteger.

RECOMENDACIONES EN EL ÁREA DE PROTECCIÓN DE DISPOSITIVOS MÓVILES

La tecnología tiende a combinar los diferentes métodos de protección, dando lugar a infinitas posibilidades de seguridad, como por ejemplo, soluciones de seguridad basadas en hardware y software pensadas para gestionar contraseñas y claves de cifrado junto a la utilización de técnicas biométricas.

Respecto a los problemas derivados del *malware*[4] cabe destacar que dependen en gran medida del tipo de dispositivo utilizado, del software de protección instalado y de las políticas de seguridad definidas, junto con la gestión responsable de los usuarios finales.

Las recomendaciones básicas son las siguientes:

- ✓Dentro de las políticas y procedimientos de seguridad tener en cuenta la existencia del entorno móvil (si implantamos un SGSI ya tenemos avanzado una parte importante)
- ✓Elaborar lo que se llama una guía de buenas prácticas para usuarios, e incidir en la formación y concienciación
- ✓Plan para realizar copias de seguridad desde el punto de vista de estos dispositivos portátiles (almacenadas físicamente de un modo independiente al portátil)
- ✓Se podrían utilizar procedimientos y mecanismos que permitan reinicializar y borrar de forma remota, además es conveniente y necesario tener claro el procedimiento para poder aplicar esta política
- ✓Aplicar de forma obligatoria el control de acceso al dispositivo, esto es, que no se pueda desactivar por el usuario, y que sea resultado de una política de seguridad clara (lectores de huellas digitales, lectores de tarjetas… junto con contraseña de arranque y de BIOS)
- ✓Mantener una gestión centralizada de este tipo de dispositivos en lo referente a inventario, carga de aplicativos, comunicaciones, VPN…
- ✓Utilizar el cifrado de datos sensible para la organización (si se saca el disco duro del dispositivo que éste no sea legible)
- ✓Protección ante software malicioso (*malware*)
- ✓Control de políticas en los puntos de acceso
- ✓Prevenir las fugas de información, por ejemplo, a través de la utilización de la tecnología DLPs. ❑

DICCIONARIO

[4] **Malware:** Cualquier software, macro, activex, javascript… cuyo objetivo sea causar daños a uno o varios de los siguientes elementos: equipos, sistemas informáticos, redes de comunicación y usuarios —sin el conocimiento de estos últimos— (ralentización del sistema, usos fraudulentos, robos de información…); como por ejemplo, virus, gusanos, troyanos, *jokes* (programas broma), *hoaxes* (bulos), bombas lógicas, *spyware*, *adware*, *keyloggers* (programas o dispositivos que registran las pulsaciones sobre el teclado), etc.

(Ver boletín AURRERA nº 3, artículo titulado "*Seguridad: virus*")

Gestión de Identidades

Actualmente, el número de claves que tiene un usuario para acceder a todas sus aplicaciones es cada vez más mayor. Ello está provocando que las organizaciones tengan problemas a la hora de gestionarlas: dar de alta, de baja o modificarlas. Asimismo, los usuarios tienen dificultades para recordarlas, lo cual, puede provocar graves problemas de seguridad tanto para la entidad como para el propio usuario.

DICCIONARIO

[5] **Ciclo de vida**: El perfil de un usuario tendrá las siguientes tres fases:

- **Creación**: Cuando el usuario llega a la organización hay que crearle un perfil con los datos precisos.
- **Mantenimiento**: Una vez creadas, hay que gestionar esa cuenta de usuario. Por ejemplo, cambiar la contraseña, el nombre, los permisos, etc.
- **Supresión**: Cuando un usuario deja la organización se borran todos sus permisos para impedir el acceso a los sistemas que usaba.

[6] **Gestión de Identidad:** (*Identity Management o IdM*) es el término usado para referirnos al conjunto de sistemas y procesos que gestionan y controlan de forma centralizada la identidad de la persona que ha accedido a unos recursos (aplicaciones), estableciendo qué es lo que puede hacer cada usuario con esos recursos, desde dónde se puede conectar, cómo y cuándo. Actualmente, toda esta información suele estar dispersa en diferentes sistemas y, en consecuencia, es difícil de gestionar.

Muchas organizaciones, tanto públicas como privadas, se enfrentan todos los días al problema que supone la gestión de un usuario, lo que incluye la creación del código del usuario, la asignación o modificación de sus privilegios, y la suspensión o eliminación del perfil. Todo este proceso recibe el nombre de "*ciclo de vida* [5]" del perfil del usuario.

Veámoslo con un ejemplo: cada vez que una persona se incorpora a nuestra organización debemos responder a preguntas como: ¿a qué aplicaciones debe acceder?, ¿con qué permisos debe ser configurado ese acceso? o ¿qué información necesitamos de esa persona para esa aplicación?; asimismo, si el usuario cambia

de puesto ¿cuáles son sus nuevos requisitos?, ¿qué aplicaciones se ven afectadas por el cambio?... Como es fácil de imaginar, y desde el punto de vista de los Responsables Informáticos de las distintas áreas, esta situación es cada día más difícil de controlar, ya que tenemos que dar de alta ese usuario en varios sistemas distintos.

En la mayoría de los casos, las gestiones del ciclo de vida del usuario se van atendiendo sobre la marcha, cuando la persona afectada va solicitando el alta para cada una de sus necesidades al departamento correspondiente. Pero tan importante es dar de alta un usuario en el plazo más corto posible como anular a tiempo todos los permisos de acceso.

Según los expertos, las soluciones tecnológicas más adecuadas que podemos encontrar en el mercado para hacer frente a toda esta problemática reciben el nombre de "*Gestión de Identidades*[6]" (GdI).

GESTIÓN DE IDENTIDADES

En una situación ideal, una organización debería contar con un **proceso automatizado** para dar acceso a los usuarios a todas sus aplicaciones, así como para anular los permisos de acceso cuando un empleado abandona la entidad. Sin embargo, la mayoría de las entidades se encuentran lejos de esta situación ideal.

Dada la gran complejidad existente hoy en día para mantener los datos de todos los usuarios, sus permisos, etc. las grandes corporaciones han empezado a interesarse ahora por herramientas que faciliten, en la medida de lo posible, la gestión de identidad y permisos de sus usuarios.

De todas formas, señalar que, si bien, estas soluciones no son nuevas, es ahora cuando tratan de abordar toda esa problemática de una forma global. Para ello añaden el control y la automatización de muchas tareas del llamado "*ciclo de vida*" del usuario, todas las cuales, hasta ahora, era necesario realizar con técnicas específicas para ello (*ad hoc*), propias de cada organización.

Se trata, en definitiva, de contar con un sistema que facilite la tarea y aumente la productividad, además de eliminar errores y permita detectar incoherencias entre los datos de un sistema y otro.

¿POR QUÉ AHORA?

La Gestión de Identidades ha existido siempre, incluso en los tiempos de los sistemas *mainframe* y del *midframe*, pero fue en los años 90 cuando

se empezó a abordar más en detalle con la adopción de numerosos sistemas de información que incluían gestión de usuarios.

Lo que ocurría era que, en el pasado, la "creación" de un usuario (dar de alta) y habilitar sus permisos era fácil de gestionar, ya que el número de autorizaciones a manejar al día era pequeño. Además, únicamente existían usuarios internos y el acceso a los sistemas de Tecnologías de la Información (TI) era solo a través de redes internas.

> "El *Single Sign-On* (SSO) permite a los usuarios registrarse una única vez y, posteriormente, acceder a distintas aplicaciones, sin necesidad de identificarse de nuevo."

Hoy en día, por el contrario, hay un mayor número de usuarios (internos, externos, colaboradores, clientes o proveedores) que acceden a los recursos por nuevos canales, hay múltiples aplicaciones y sistemas con sus propios módulos de autenticación y autorización, los usuarios tienen múltiples autorizaciones basadas en diferentes mecanismos de autorización, existen aspectos relacionados con la LOPD que debemos cumplir (trazas o logs de auditoría...), etc.

SOLUCIONES

A la hora de abordar este problema, el principal obstáculo al que se tienen que enfrentar las organizaciones está relacionado, directamente, con la heterogeneidad de las infraestructuras ya instaladas en la propia organización, en las que abundan los sistemas obsoletos.

Asimismo, en muchos casos, las organizaciones se dan cuenta que muchas de sus aplicaciones no soportan el acceso basado en "**roles**"; lo cual implica el tener que añadir esa capacidad a cada aplicación, siendo ello complejo y muy costoso[7].

Tanto es así que la definición, creación y el modelado de roles es, generalmente, un proceso largo que exige gran dedicación y esfuerzo. Demanda una estrecha colaboración de los responsables informáticos con todas las áreas de la organización para acordar los distintos perfiles de usuarios y los derechos de acceso que deberán otorgarse a cada uno de ellos.

Sin embargo, antes de empezar a analizar nuestras aplicaciones, la existencia o no de roles bien definidos, etc. conviene que conozcamos algunos **conceptos** que manejan los consultores de estas soluciones informáticas:

- **Gestión de contraseñas**: Los usuarios se suelen conectar a los sistemas mediante un identificador y una contraseña. Las passwords (claves) tienen el peligro de ser reveladas (los usuarios las anotan en papeles, los hackers pueden adivinarlas, etc.). Además, y en este mismo sentido, recordar que el Reglamento que desarrolla la LOPD obliga al cambio de contraseña. Por todo ello, es conveniente cambiar periódicamente las claves de acceso. Muchos sistemas modernos, en especial los usados internamente, obligan a los usuarios a cambiar sus contraseñas, por ejemplo, cada 30 días. Cuando los usuarios tienen muchas contraseñas en distintos sistemas, y expiran en diferentes fechas, suelen acabar escribiéndolas u olvidándolas. Para evitar estos problemas, los sistemas de gestión de identidades proporcionan a los usuarios un sistema que gestiona de modo consistente, por un lado, el olvido de una clave, situación en la que se envía a su correo electrónico la clave que tenía el propio usuario; y, por otro lado, el cambio de clave en todas las aplicaciones, en este caso el sistema previamente pregunta al usuario sobre algún aspecto que sólo él debe conocer, y posteriormente acepta la nueva clave introducida, replicándola a todas sus aplicaciones de forma automática y transparente para él.

- **Aprovisionamiento de usuarios** (*user provisioning*): Este concepto encierra el ciclo de vida de la gestión de la identidad digital, aportando ventajas sobre la información del usuario en la infraestructura de los directorios de las organizaciones. Acelera la concesión y revocación de cuentas de usuario, y los derechos de acceso para los recursos de información. Esto incluye correo electrónico, servicio telefónico, aplicaciones, acceso intranet y extranet, y servicios de CAU o *help-desk*. Todos estos sistemas gestionan perfiles de usuario internos y no tienen la posibilidad de acceder a un directorio externo para comprobar la identificación, autenticación y permisos de ese usuario. Estos sistemas intentan coordinar la administración de la identidad de los usuarios a través de múltiples sistemas de forma centralizada. La identidad se gestiona en una única aplicación y,

DICCIONARIO

[7] **Costes**: Si bien, las ventajas de un sistema de Gestión de Identidades aporta ventajas significativas, no hay que olvidar que, según distintos estudios, el despliegue de estas soluciones puede resultar muy costoso, y la complejidad aumenta con el tamaño de la organización. En este sentido, las consultoras estiman que las organizaciones deberán pagar entre 20 y 30 dólares por usuario en concepto de software, y entre dos y seis veces esa cantidad por la integración.

posteriormente, se trasmite al resto de aplicaciones. El principal inconveniente de los sistemas de aprovisionamiento de usuarios suele ser su elevado coste y plazo de implantación, en algunos casos, varios años.

- **Metadirectorio**[8]**:** Representa el corazón de una arquitectura de administración de identidades y acceso a la información. Un directorio corporativo está diseñado para centralizar en un único punto la gestión de los datos de todos los usuarios (dirección, teléfono, nombre, etc.), así como de otros objetos de la organización, por ejemplo, grupos de usuarios, servidores, impresoras, etc. Las aplicaciones clientes acceden a esos datos, para leerlos y escribirlos, mediante un protocolo estándar, por ejemplo el llamado **LDAP** *(light-weight directory access protocol)* o el X.500. Los directorios permiten configurar las aplicaciones para que tomen los datos de los usuarios de una fuente centralizada, en vez de que cada sistema gestione su propia lista de usuarios, datos de autenticación, etc. La limitación más importante de los directorios es su integración con los sistemas existentes: *mainframes*, aplicaciones antiguas y otros sistemas, ya que no soportan su uso o requieren costosas adaptaciones.

- **Single Sign-On (SSO)**: Es el mecanismo de autenticación que permite a los usuarios registrarse una única vez y, posteriormente, acceder a distintas aplicaciones para las que dispone de autorización, sin necesidad de identificarse de nuevo en cada aplicación. Muchos sistemas antiguos no soportan medios externos de identificación y autenticación de sus usuarios. Sin embargo, es posible almacenar las credenciales de los usuarios fuera de las aplicaciones y, posteriormente, introducirlas automáticamente en esas aplicaciones cuando sea necesario. Los sistemas de *single sign-on* en aplicaciones antiguas hacen justamente esto. Puesto que se requiere la instalación de software en los puestos de trabajo, estos sistemas sólo son apropiados para uso interno. Su éxito en grandes organizaciones está limitado por diversos factores: costes de integración, inquietudes sobre su seguridad —pues los sistemas SSO almacenan todas las contraseñas de los usuarios de todas sus aplicaciones—, preocupación sobre la disponibilidad, ya que si el sistema SSO falla, muchos usuarios no podrían conectarse a sus aplicaciones y, eventualmente, tendrían que parar de trabajar.

Para evitar esto se suelen habilitar

BENEFICIOS

Las ventajas que aporta el tener un sistema de Gestión de Identidades son:

- ✓ **Ahorro de costes de gestión**: Se asegura la consistencia de los datos, ya que éstos se actualizan en un único directorio y desde ahí son propagados automáticamente a los distintos sistemas. De esta forma, se reduce el esfuerzo a la hora de dar acceso a un usuario, los errores se minimizan y las incidencias disminuyen.
- ✓ **Incremento de la seguridad**: Cualquier cambio en el estatus de un empleado puede ser "propagado" y actualizado a través de los sistemas informáticos de una manera rápida y eficiente (cuando un empleado deja de pertenecer a la entidad, el sistema suspende automáticamente sus cuentas, reduciendo con ello el riesgo de accesos no autorizados o cuentas fantasma de las que se desconoce el propietario, etc.). En general, se mejora la seguridad ya que al no tener que recordar varias contraseñas, el usuario ya no ve necesario anotar sus claves en post-its que, posteriormente, deja encima de su teclado.
- ✓ **Ventaja competitiva**: Se incrementa la productividad de la entidad. El nuevo sistemas reduce los costes del CAU[9] (*help-desk*), gracias a la disminución de la carga de tareas manuales de reajuste de contraseñas.
- ✓ **Mejora la experiencia del usuario**: El usuario solo tendrá que recordar una única contraseña para todos los sistemas.
- ✓ **Cumplir las regulaciones legales**: La organización estará mejor preparada para garantizar el cumplimiento de la regulación vigente (LOPD, etc.) y para demostrar a los auditores, mediante informes y pruebas auditables, su cumplimiento.

DICCIONARIO

[8] **Metadirectorio**: La primera vez que se utilizó el término metadirectorio fue por parte de un analista de la consultora Burton Group, que lo definió como "*la unión de todos los directorios en la empresa*". Sin embargo, la frase es original de Kim Cameron, uno de los fundadores de la empresa Zoomit. Cameron vendió su cita al Burton Group por un dólar en 1997.

[9] **Incidencias del CAU**: Os indicamos a continuación las incidencias de seguridad (XLNet, dominio...) gestionadas por el CAU del Gobierno Vasco durante 2008:

- Total: 7.482 casos

(9,21% sobre el total de incidencias atendidas, es decir, 81.227 casos)

- Duración total: 2.257 h.
- Duración media por incidencia: 18 minutos

Por último, y siguiendo dentro del ámbito de la administración vasca, cabe mencionar el proyecto de gestión de identidades y Single Sign-On (SSO) llevado a cabo por Osakidetza, el cual recibe el nombre de **Norbide**.

medios alternativos de acceso.

En general, los productos de SSO abarcan la fase de autenticación, dejando a la aplicación la autorización. Son productos especialmente útiles en aplicaciones web.

- **Identidad Federada:** Permite a los usuarios usar la misma identificación personal (usuario, contraseña) para registrarse en redes de diferentes empresas, lo que facilita a las organizaciones poder compartir información sin compartir tecnologías de directorio, seguridad y autenticación. Se basa en el

> "Una organización debería contar con un proceso automatizado para dar acceso a los usuarios a todas sus aplicaciones."

"círculo de confianza", un concepto que garantiza que un usuario es conocido en una red determinada (un dominio) y tiene acceso a unos servicios específicos. Su mayor dificultad radica en que se requiere confianza entre redes diferentes. La industria ha establecido una alianza, denominada *Liberty Alliance Project* para desarrollar estándares abiertos y neutrales para potenciar la Identidad Federada y *WebServices*.

Si analizamos las soluciones de Gestión de Identidades existentes en el mercado[10], nos daremos cuenta que algunos de esos productos se centran en el almacén (estrategia de Directorio); otros en los procesos de gestión: circuitos de validación, delegación, etc.

(estrategia de aprovisionamiento); y un tercer grupo en el puesto del usuario y en facilitar un acceso controlado a las aplicaciones y servicios (estrategia del *logon* o código de usuario único).

De todas formas, todas ellas tienen una serie de componentes comunes que comentamos a continuación:

- ✓ **Sistema de integración:** este componente obtiene, de diversas fuentes ya existentes y de naturaleza heterogénea (directorios, sistemas operativos, bases de datos, etc.), información de acceso usada de forma independiente por sistemas ya existentes, para incorporarla al nuevo sistema de gestión de identidades.
- ✓ **Sistema de provisión:** este se encargará de dar de alta nuevos usuarios y asignarles su rol, propagando a los diferentes puntos de autenticación, y de forma transparente para el usuario, la información de los mismos.
- ✓ **Sistema de autogestión:** la gestión de claves representa el mayor porcentaje de tareas del servicio o Centro de Atención a Usuarios (CAU) de una organización. Por eso, y con la idea de agilizar el proceso, se suele permitir al usuario dar los datos necesarios para su alta o modificación y, posteriormente, son validados por el responsable correspondiente.
- ✓ **Motor de sincronización:** permite gestionar, de forma centralizada, las diversas identidades del usuario, los sistemas a los que tiene acceso y los cambios de rol, propagando a cada uno de los servicios corporativos todos los cambios.
- ✓ **Sistema de auditoría:** permite guardar todos los cambios realizados para un posible análisis o auditoría (interna o externa) posterior.

CONCLUSIONES Y FUTURO

La gestión de la identidad es una tecnología que, si bien no es nueva, es ahora cuando se hace más necesaria dentro de las organizaciones. El grado de madurez de las diferentes tecnologías del mercado es variable. Los directorios, gestores de contraseñas o *single sign-on* en web son tecnologías ampliamente implantadas y que demuestran un beneficio real y cuantificable. El aprovisionamiento de usuarios, por su parte, es una tecnología que promete beneficios significativos, pero todavía hay pocas implantaciones.

De todas formas, seguro que seguiremos hablando de estas soluciones en próximos números. ❑

DICCIONARIO

[10] **Soluciones de Gestión de Identidades**: Relación de algunos de los fabricantes existentes en el mercado y sus productos:

- **Sun Microsystems**: *Sun Java Identity Manager* (SJIM)
- **Computer Associates**: *eTrust Identity and Access Management Suite*
- **Novell**: *Nsure*
- **IBM**: *Tivoli Identity Manager* (TIM)
- **BMC**: *BMC*
- **Oracle**: *Oracle Identity Management* (OIM)
- **Microsoft**: *Identity Integration Server* (MIIS)

ALBOAN:
El nuevo BOPV electrónico

EUSKAL HERRIKO AGINTARITZAREN ALDIZKARIA

BOLETÍN OFICIAL DEL PAÍS VASCO

"La edición digital ha pasado a ser el único formato valido ante la ley."

"Las suscripciones a la Difusión Selectiva de Información se incrementaron, en 2008, un 15,61% con respecto a 2007."

El Boletín Oficial del País Vasco (BOPV) es el diario oficial de la Comunidad Autónoma de Euskadi, a través del cual se da publicidad a los documentos que deben ser objeto de publicación oficial, de acuerdo con el ordenamiento jurídico vigente.

Con el paso del tiempo, y gracias a la evolución de las Nuevas Tecnologías, el Boletín ha ido optimizando durante los últimos años: por un lado, su funcionamiento interno, y por otro lado, el servicio que presta hacia el exterior, es decir, hacia la ciudadanía.

El avance continuo de las herramientas informáticas, la generalización del uso de las mismas y la implantación de nuevos medios electrónicos, informáticos y telemáticos han hecho que el Boletín Oficial se haya tenido que ir adaptando una y otra vez a los nuevos tiempos.

El BOPV se configura como un servicio público de acceso universal y gratuito, el cual abarca todos los Boletines publicados hasta la fecha, incluyendo los editados durante la II República (años 1936-1937) y los correspondientes al periodo del ente preautonómico del Consejo General del País Vasco (1978-1980).

Actualmente, la página web del BOPV permite visualizar cualquier Sumario y/o Disposición de un Boletín, marcando en la propia página web el año/mes/día/nº de boletín. Las búsquedas ofrecen el texto de las Disposiciones encontradas a través de su Base de Datos Documental BRS, así como un enlace directo a su versión en formato PDF (*Portable Document Format*).

Gracias a la homogenización de los contenidos de las Disposiciones publicadas en categorías temáticas, se posibilita la búsqueda de cualquier tipo de información.

El BOPV ofrece, mediante suscripción, un servicio diario de alarmas por e-mail (servicio de *"Difusión Selectiva de Información" —DSI—* del BOPV) que, previa inscripción por cualquier persona o entidad con una cuenta de correo electrónico, envía diariamente, y de forma gratuita, aquellas disposiciones, si las hubiera, que cumplen los requisitos del perfil temático señalado en la suscripción.

¿POR QUÉ LA DIGITALIZACIÓN?

El pasado dos de enero de 2009 se puso en marcha el nuevo BOPV electrónico. Gracias a ello, a través de la web de euskadi.net, se ofrece al ciudadano un documento oficial consultable, autentico y no manipulado, firmado electrónicamente, como sustituto del anterior documento en papel.

Los motivos que han llevado a los responsables de la publicación del BOPV (Dirección de la Secretaría del Gobierno y de Relaciones con el Parlamento) a adoptar el Boletín electrónico son, entre otros, los siguientes: en primer lugar, la disminución progresiva en el número de suscriptores a la edición en papel. Concretamente entre 2007 y 2008 se produjo una disminución de 300 suscriptores, siendo la previsión para 2009 de un descenso aún mayor. Y, en segundo lugar, el aumento de las consultas a la web (366.870 visitantes en 2008), así como las suscripciones a la Difusión Selectiva de Información (15.050 suscriptores a 31 de diciembre de 2008, incremento del 15,61% con respecto a 2007).

BENEFICIOS

Las principales consecuencias que implica la desaparición del papel en este proceso son:

- Ahorro en papel, con el consiguiente beneficio económico, además de las ventajas que reporta para el medio ambiente y la ecología, mejorando el desarrollo durable o sostenible.
- La propia edición, al ser digital, sin ningún fascículo en papel, ha supuesto la revisión de

los servicios prestados por la imprenta.

- No existen segundas copias del original, para el trabajo de traducción, corrección, revisión, etc.
- Disminución de la dependencia de servicios externos. Ahora se reducen a la maqueta y diseño de los textos.
- Mayor agilidad en el proceso, ya que no se está sujeto a las exigencias técnicas de la impresión. Con la versión electrónica no hay límites, el tiempo de edición es independiente del número de páginas.
- Se adelanta en un día la recepción de los textos del servicio de diseño. Ya no es necesario esperar al día siguiente, al desaparecer los tiempos de impresión y de distribución.
- Se reduce el espacio necesario para archivo, y también el mobiliario.
- Disminución de las tareas al eliminarse el proceso de archivo, tanto de originales, como de copias, boletines editados, libros encuadernados, etc.

ASPECTOS TÉCNICOS

El nuevo formato digital incorpora, entre otros aspectos, la firma electrónica reconocida (proporcionada por **Izenpe**), lo cual asegura la autenticidad, integridad e inalterabilidad de los textos.


29 ZK. BOPV - viernes 28 de noviembre de 2008 28887

Disposiciones Generales

DEPARTAMENTO DE HACIENDA Y ADMINISTRACIÓN PÚBLICA
DEPARTAMENTO DE VIVIENDA Y ASUNTOS SOCIALES

6622

El proceso que se sigue es el siguiente: una vez que el servicio del BOPV da el visto bueno a los textos enviados por el servicio de diseño (archivos separados de Sumario, Disposición y Anexos), procede a la confirmación de la publicación para el día siguiente del boletín correspondiente. Este proceso se realiza a través de la aplicación de gestión, mediante firma electrónica (Servicio Horizontal de Firma), cuya política de certificado es la de Órgano Administrativo de la Secretaría del Gobierno y de Relaciones con el Parlamento.

La consulta vía Internet permite a los ciudadanos ver los datos de firma y verificar la firma electrónica asociada a cada una de las disposiciones, demostrándole que el documento electrónico original que se halla en poder de la Administración es auténtico y no ha sido manipulado, ni alterado. Asimismo, se ofrece al ciudadano la posibilidad de consultar de una manera accesible el documento electrónico original.

PROPUESTAS DE CARA AL FUTURO

Dado que se pretende eliminar el papel en todos los flujos de trabajo actuales, tanto en la relación con los peticionarios internos del Gobierno Vasco como con los peticionarios externos, distinguiéndose los grandes Organismos Públicos: UPV, UTAP, Diputaciones... de otros organismos locales: ayuntamientos..., a la hora de gestionar las peticiones de asuntos a publicar es imprescindible que todo el mundo entienda que se trata de textos definitivos. Desaparece, por tanto, el concepto de "adelanto" y de las consiguientes modificaciones "sobre la marcha".

El motivo es que, por una parte, al reducirse los plazos no se dispone de tiempo intermedio entre el envío y la publicación para poder incluir correcciones. Y por otra parte, la práctica de "adelantos" entraña una gran indefinición sobre la seguridad del texto, y al mismo tiempo, una repetición de tareas en cuanto al formato, la corrección, la revisión y la traducción.

Al mismo tiempo, la digitalización del BOPV ha supuesto la desaparición del hasta ahora único formato con validez legal, el soporte en papel. Sólo en el caso de incidencias técnicas de carácter grave que afecten al funcionamiento del sistema informático que impidan el acceso telemático a la edición electrónica del Boletín, la Vicepresidenta del Gobierno podrá autorizar la edición de copias del mismo en soporte papel, con carácter oficial.

Desde enero, el canal web es el único medio de comunicación a utilizar por el ciudadano para obtener la edición digital, que ha pasado a ser el único formato valido ante la ley.

De cara al futuro, los responsables de su publicación, estiman que es necesario llevar a cabo la revisión de la web del BOPV, es decir, mejorar el Interfaz de Acceso: renovar su imagen respecto al diseño y sus funcionalidades (libro de estilo, usabilidad, accesibilidad, búsquedas, contenidos...). ❑

"El nuevo formato electrónico incorpora la firma electrónica reconocida, lo cual asegura la autenticidad, integridad e inalterabilidad de los textos."

BOPV

Página web:
www.lehendakariordetza.ejgv.euskadi.net
Para más información ver:
Decreto 217/2008, 23 de diciembre, del Boletín Oficial del País Vasco

¡¡BREVES!!

Nº 33

marzo de 2009

Dominio .eus

El pasado mes de enero se presentó la asociación **PuntuEus**. Ésta, compuesta por once entidades de campos como el euskera, la educación y la comunicación, tiene como objetivo el obtener el visto bueno para crear y gestionar el dominio .eus en Internet. La intención es agrupar y convertirse en el signo identificativo que englobe a todas las páginas web de la comunidad de la lengua y la cultura vasca.

Las once entidades que forman la asociación PuntuEus son: Euskaltzaindia, el Consejo de Organizaciones Sociales del Euskara, la Confederación Vasca, la Asociación de Escritores Vascos, la Universidad del País Vasco, la Confederación de Ikastolas del País Vasco, Ikastolas Concertadas, EiTB, la Asociación para la Promoción del Euskara en Internet, la Asociación de Ingenieros de Telecomunicaciones del País Vasco y el Colegio oficial de Ingenieros Informáticos de Euskadi.

A diferencia de los códigos de Estados (.fr, .uk, .es), los dominios históricos (.com, .net, .org) y los no esponsorizados (.biz para negocios, .name para personas), los dominios esponsorizados representan comunidades y, por lo tanto, deben ser fomentados por ellas.

Los trámites que se deben completar antes de obtener el visto bueno de la organización internacional **ICANN** (*Internet Corporation for Assigned Names and Numbers*), responsable de la gestión del sistema de dominios en Internet, es bastante largo (2 años). De todas formas, los responsables de la iniciativa pretenden seguir el mismo camino seguido por el dominio .cat, el de la comunidad de la lengua y cultura catalana, el cual obtuvo el visto bueno en 2005.

Tras ese éxito, otros pueblos europeos tratan que su cultura y su lengua sean también visibles en internet. Es el caso, por ejemplo, de las comunidades gallegas, bretona y galesa, que están trabajando bajo el nombre de puntogal, pointbzh y dotcym, respectivamente, para que sean reconocidas.

Web de la asociación: www.puntueus.org

El Gobierno Vasco adquiere un superordenador

El Gobierno Vasco, a través de la empresa pública Sociedad Informática del Gobierno Vasco, S.A. (EJIE), acaba de adjudicar a la empresa IBM, por un montante cercano al millón de euros, el concurso para el suministro, instalación, puesta en marcha y mantenimiento de un nuevo superordenador que dará servicio al **Centro Meteorológico del País Vasco**, así como a universidades y diversos centros tecnológicos para el desarrollo de investigaciones climatológicas, lo que permitirá realizar investigaciones de alto nivel en este ámbito.

Esta es la primera instalación en el Estado de un superordenador IBM iDataPlex, con altos niveles de capacidad de proceso y eficiencia energética. Para encuadrar la potencia de este superordenador reflejar el dato de que el centro de supercomputación del Gobierno Vasco alcanzará una potencia de cálculo superior a 11 TeraFLOPS (11 billones de operaciones por segundo), es decir, podrá realizar en un período de tiempo de 48 horas cálculos que un PC convencional tardaría en realizar 114 años.

El servidor iDataPlex ejecuta un sistema operativo Linux, y está basado en procesadores Xenon de cuatro núcleos.

En cuanto a la eficiencia energética cabe destacar su innovadora tecnología de refrigeración, permitiendo ahorros de energía de hasta un 40%, al tiempo que multiplica por 5 la capacidad de procesamiento.