

Sistema de Gestion de Locutorios SIGELOC Para acceso a Internet. Ministerio de Defensa

DATOS GENERALES

Antecedentes del servicio

En el MINISDEF se han recibido solicitudes de diferentes Organismos solicitando una solución para que en los diferentes puntos de acceso libre a Internet se disponga de tecnología WIFI para facilitar el acceso, pero requiriendo que este acceso sea controlado para poder responder ante requerimientos gubernativos de identidades que pudiesen realizar actividades delictivas. Con esa Intención la Inspección General CIS confeccionó una serie de requisitos y contrato a una empresa especializada en Software Libre para proporcionar una solución única para todo el departamento, cualquiera que fuese la ubicación y minimizando los trabajos de administración para los centros de acogida de la solución

Objetivos específicos

Funcionales

- Emisión de localizadores de varios tipos (limitados en tiempo, con fecha de caducidad, gratuitos o de pago) que autoricen la conexión
- Registro individual del uso hecho de internet en vista de poder proporcionarlo en caso de requerimiento judicial.

De respeto de la privacidad:

- Limitación, vía técnica, del acceso a los datos sensibles y, en particular, a la relación "Identidad/Uso hecho de internet" en vista asegurar la confidencialidad en las comunicaciones.
- Posibilidad, para el propio usuario, de proteger su perfil de conexión.

Recursos empleados

Delegaciones

- Un servidor (equiparable a un ordenador de escritorio) para la emisión de los tickets y el control del acceso a Internet.
- Una impresora (específica) para la impresión de los tickets
- Un router para la conexión a ADSL.

Servicios centrales

- Un Servidor central que almacena los datos de los servidores locales en BBDD

Implementación

Arquitectura Cliente Servidor

Servidor Central

Hospedado en Servicios Centrales, almacena, en bases de datos separadas y relativas a cada centro, los datos que generan los servidores locales.

Sirve los datos necesarios a los centros, poniendo en común los datos de los usuarios finales registrados en todos los centros.

Servidor Local

Proceden al registro de los usuarios finales, emiten los localizadores (tickets), sirven servicios DHCP

Captan y cifran el uso hecho de Internet.

Los datos que registrar son enviados al servidor central, sea inmediatamente sea cuando la conexión lo permita en caso de desconexión del servidor central. Los datos son eliminados en cuanto es confirmado su almacenamiento en el servidor central.

Seguridad

- Todas las comunicaciones, sea entre servidores sea entre las capas software, utilizan el protocolo SSL. Los accesos a las interfaces de producción y de administración también utilizan un protocolo seguro (https).
- La clave de acceso a la relación DNI/Uso hecho de internet queda compilada en la aplicación.

Resultados

El piloto fue implementado en un centro real, ha garantizado el registro de usuarios, el acceso identificado y registrando el uso hecho de internet.

Tras los resultados Obtenidos está en marcha la operación de despliegue para dotar a doscientos emplazamientos a lo largo de 2010 de esta solución.

Lecciones aprendidas y conclusiones

Las mayores dificultades, para la implementación del proyecto, fueron:

- La implementación de un satélite que pueda cumplir con sus objetivos en situación desconectada e incluso que consiga mantener su función en caso de desconexiones erráticas
- Proteger la privacidad de los usuarios cifrando la información desde su generación así como controlando la forma de acceder a la información.

Referencias y enlaces

Aún no hay enlaces disponibles pero, quizás, se pueda adelantar www.sigeloc.org (o .net, o .info) como futuro sitio web del proyecto.

El sitio que centralizaría e informará del proyecto además de la Propia Inspección General CIS del MINISDEF C/Joaquín Costa 6 es::

- Web principal de presentación
- Demostración en línea (reinicializada cada noche por ejemplo)
- Un espacio para "Comunidad SIGELOC (Forja de descarga y espacio de colaboración [controlado por supuesto]).

Un ejemplo, que creamos nosotros, puede ser consultado en :

- <http://comunidad.molinux.info/index.php/Portada>
- <https://forja.molinux.info/>

DATOS ESPECÍFICOS

Características que contribuyen a la confianza en el servicio

- Los módulos principales de software que permiten captar y registrar los datos son iptables/netfilter, bajo licenciamiento libre (usados por gran cantidad de fabricantes como son CISCO y Red Hat) y squid, también bajo licencia libre, que es un servidor proxy caché de referencia. Estos productos son estándar en SIGELOC por lo que su funcionamiento, su código, pueden ser controlados.
- Encriptación de los datos sensibles
Los datos que permiten poner en relación la identidad del usuario y el uso hecho de Internet son cifrados. Resulta imposible acceder a ellos directamente (a partir de una búsqueda SQL por ejemplo) sin disponer de la clave de encriptación.
- Control aplicativo
Sólo un perfil, el super administrador de SIGELOC, puede acceder al informe que permite extraer la relación "identidad/uso hecho de Internet". La aplicación pedirá una clave, almacenada en una caja fuerte, específica para ello.
- Procedimiento
El acceso a los datos sensibles, que supone disponer de la clave de acceso (y de encriptación) sólo será autorizado por orden judicial.
- Auditoría
Un proceso aplicativo registra todas las acciones de los administradores, incluyendo el acceso a los informes, la auditoría. Quedarán registradas por lo tanto todas las acciones de los administradores (creación y modificación de usuarios, de roles, de consultas de informes etc ...)
- Siendo prevista la liberación del proyecto, y por lo tanto de sus fuentes, a otras estructuras de Administración Pública es posible controlar qué hace y como lo hace.

Características que contribuyen a la seguridad del servicio

Desde el punto de vista del administrador de la solución, desde el origen de la información hasta su almacenamiento, las comunicaciones se hacen de forma cifrada. OpenSSL es la respuesta.

Las conexiones entre las bases de datos y la aplicación local, inclusive, están cifradas. Al mismo tiempo, la lógica del modelo de base de datos y de los tratamientos hace que sólo se deje en local la información mínima para trabajar (todo acaba "subiendo" a Servicios Centrales).

De esta forma, en caso de intrusiones físicas, o incluso de robo de las máquinas satélites, la información que se obtendría, aparte de cifrada, sería mínima (datos de navegación, datos de red, etc) pero en ningún caso, información personal que permita cruzar y responder a la pregunta ¿quién a hecho qué? dado que esta lógica sólo se puede aplicar en Servicios Centrales y a través de un perfil protegido y cuya única funcionalidad será esa.

Aspectos de accesibilidad del servicio

Cualquier navegador que soporte medidas de accesibilidad, podrá soportar el módulo de usuario de SIGELOC.

La aplicación, desarrollada de forma nativa para Firefox, es compatible, también, con Internet Explorer (versiones 7 y 8) así como con Safari.

Aspectos de usabilidad del servicio

La lógica de la aplicación es en todo momento bastante sencilla. Es organizada en pestañas de menú y submenús., el usuario siempre sabe dónde está y existen múltiples asistencias para comprender que es lo que está viendo. Cuenta con una ayuda contextual.

Características de participación ciudadana del servicio

La solución resulta de particular interés para cualquier organización que ponga a disposición un locutorio de Internet via WIFI. Siendo esta Solución del MINISTERIO de DEFENSA, es totalmente trasportable a otros entornos de la administración (Colegios y Consejerías de Educación, Ayuntamientos, centros oficiales, etc...). Al ser un proyecto 100% software libre, cualquiera de estas entidades podría ser usuaria del proyecto sin coste de licencias, aplicando pocos recursos en la operación y, si necesario, adaptando el código a sus necesidades propias

Datos de utilización del servicio

No constan por ahora datos significativos de utilización (fase de piloto). El alcance de la solución es de unos 600 Centros en el Minisdef, iniciándose en 2010 con unos 200 centros, incluidas las Zonas de operaciones exteriores.

Datos del grado de satisfacción del servicio

Los usuarios han quedado satisfechos en el uso del sistema se han realizado algunas mejoras antes del despliegue definitivo y se está a la espera en los próximos meses del resultado.

Características de multiplataforma del servicio

Por motivos de rendimiento y de independencia tecnológica a la hora de tener que recurrir a configuraciones y desarrollos específicos de nivel sistema la plataforma de ejecución elegida es GNU/Linux (Debian). El Gestor Relacional de Bases de Datos, MySQL, también está disponible en la mayoría de los sistemas operativos del mercado y permitiría, con sólo la necesidad de una adaptación, portar la solución a otro entorno. La aplicación, realizada en Java/J2EE, podría también ser ejecutada en otras plataformas y el entorno de usuario por fin sólo supone la utilización de un navegador web teniendo activada la interpretación de Javascript.

Características de multicanalidad del servicio

Podemos adelantar, sin lugar a duda, que en caso de ser liberado, más aún por parte de un organismo público, del Ministerio de Defensa, SIGELOC se beneficiará de un a priori muy favorable por parte del Mundo del Software Libre (o Comunidad del Software Libre) y los organismos satélites (empresas, prensa ...) que contribuyen en la comunicación de todo lo que pasa en este Mundo. El coste global de SIGELOC para Administración Pública, muy reducido en comparación con

una solución propietaria, la posibilidad de acceder a las fuentes para su control y adaptación o la de poder contribuir al proyecto original para su evolución facilitarán, motivarán incluso, la comunicación a su respecto.

Características de multilingüismo del servicio

La aplicación ha sido diseñada para soportar la internacionalización en cada una de las etiquetas.
Actualmente solo incluye un idioma, el español.

Aspectos de reingeniería del servicio

El carácter FLOSS de la solución, que supone la disponibilidad de las fuentes, y de su estructura, permite un máximo nivel de reingeniería.

Aspectos de simplificación del servicio

La solución facilita, asegurándola, la gestión de la puesta a disposición de las instalaciones WIFI en las instalaciones del Ministerio. SIGELOC memoriza los datos de los usuarios y de los tickets en vista de facilitar el servicio de cara al usuario final.
También se puede simplificar parte de la administración autorizando la emisión de informes (no sensibles -historiales o estadísticas de uso por ejemplo-) desde los servidores locales.
Supone esto implementar un acceso transparente desde las delegaciones a los servicios de generación de informes hospedados en Servicios Centrales.

Aspectos de integración del servicio

SIGELOC, en su versión 1.0, no tenía previsto ser integrarse con otros entornos u aplicaciones. Podría esto haber sido considerado contrario con la confidencialidad de los datos con la que la aplicación debe cumplir.

Características de eficacia del servicio

Aún no disponemos de datos al respecto. Esperamos, una vez la entrega hecha y entrados en la fase de despliegue, poder proporcionar, este tipo de datos.

Características de eficiencia (rendimiento, consumo) del servicio

Aún no disponemos de datos al respecto aunque, una vez entrados en la fase de despliegue, pensamos poder proporcionar, aunque sea a partir de muestras, extrapolando, proporcionar este tipo de datos que sean algo más que una simulación.

Aspectos de interoperabilidad del servicio

Para funcionar la aplicación sólo necesita un navegador web teniendo activado Javascript. Por otra parte, en su parte de administración, los informes puede ser exportados a los siguientes formatos: HTML, PDF, XML, CSV, RTF, TEXT y XLS, La interoperabilidad es por lo tanto total.

Características de neutralidad tecnológica del servicio

SIGELOC ha sido diseñada para ser independiente del material en el que funciona, independiente de un editor o empresa que pueda, en un futuro, impedir sus correcciones, mejoras o adaptación.

Los componentes y lenguaje de programación, todos bajo licenciamiento libre, y por lo tanto de de fuentes abiertas, de libre uso y de libre transmisión sin ninguna restricción garantizan la posibilidad de portar la solución a cualquier entorno.

En caso necesario (exigencias de rendimiento, seguridad, estabilidad etc ...) cualquiera de los componentes de SIGELOC, incluyendo su lenguaje de programación, podrá ser remplazado sin que esto suponga ninguna autorización o acuerdo previo con cualquier empresa.

Del punto de vista económico SIGELOC sólo supone el coste de los servicios de implantación, de mantenimiento y de administración pudiendo estos servicios hacerse libremente de forma interna o externalizada.

Creemos por lo tanto que SIGELOC asegura la máxima garantía independencia tecnológica.

Características de arquitecturas abiertas del servicio

Las tecnología utilizadas en la solución se basan en componentes independientes del material y portados todos en prácticamente la totalidad de las plataformas hardware y/o software del mercado.

El sistema operativo, "Unix Like", Debian (GNU/Linux), disponible prácticamente todas las plataformas hardware del mercado.

Los componentes aplicativos (JAVA fundamentalmente) disponen igualmente de una disponibilidad universal tanto del punto de vista hardware como software.

Los protocolos de comunicación (TCP/IP, SSL) son estándares para la comunicación multiplataforma entre equipos y aplicaciones

Las tecnologías de visualización (HTML y Javascript) son estándares integrados por todos los navegadores de internet. La aplicación ha sido validada en MS IE 7, 8 así como en Firefox en sus versiones 3.0 y superiores.

Características de reutilización del servicio

Siendo de fuente abierta la solución puede ser adaptada a entornos y necesidades específicas

Otros aspectos o características del servicio cualitativos o cuantitativos.

No sé si, del punto de vista cualitativo, convendría aquí hablar de que con este tipo de sistema se participa, contribuyendo a que disminuyan las zonas de conexión anónima, a la lucha contra desvíos del uso de Internet, al Cibercrimen y abuso de las tecnologías.