REF:	2008-1-INF-321 v1	Creado:	CERT3
Difusión:	Público	Revisado:	TECNICO
Fecha:	23.12.2008	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2008-1. BITACORA 4.0.2

Datos del solicitante: A-20686150 Grupo S21sec Gestion S.A.

Referencias:

- EXT-449. Solicitud de Certificación de BITACORA v4.0.2.
- EXT-676. Informe Técnico de Evaluación de BITACORA v4.0.2.
- CCRA. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

Informe de Certificación del producto BITACORA, versión 4.0.2, según la solicitud de referencia EXT-449, de fecha 24.01.2008, y evaluado por el laboratorio EPOCHE & ESPRI, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en EXT-676, de acuerdo a CCRA, recibido el pasado 07.11.2008.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

ÍNDICE

RESUMEN **3**
RESUMEN DEL TOE 4
REQUISITOS DE GARANTÍA DE SEGURIDAD 5
REQUISITOS FUNCIONALES DE SEGURIDAD 5
IDENTIFICACIÓN **6**
POLÍTICA DE SEGURIDAD **6**
HIPÓTESIS Y ENTORNO DE USO **6**
ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS 7
FUNCIONALIDAD DEL ENTORNO. 7
ARQUITECTURA **8**
DOCUMENTOS **9**
PRUEBAS DEL PRODUCTO **9**
CONFIGURACIÓN EVALUADA **10**
RESULTADOS DE LA EVALUACIÓN **10**
RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES **11**
RECOMENDACIONES DEL CERTIFICADOR **11**
GLOSARIO DE TÉRMINOS **12**
BIBLIOGRAFÍA **13**
DECLARACIÓN DE SEGURIDAD **13**

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto BITACORA, versión 4.0.2.

Fabricante: S21Sec.

Patrocinador: S21Sec.

Organismo de Certificación: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

Laboratorio de Evaluación: EPOCHE & ESPRI.

Perfil de Protección: Ninguno.

Nivel de Evaluación: EAL2.

Fortaleza de las Funciones: no aplica en CC v3.1

Fecha de término de la evaluación: 06.11.2008.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2 presentan el veredicto de “PASA”. Por consiguiente, el laboratorio EPOCHE & ESPRI asigna el VEREDICTO de “PASA” a toda la evaluación, por satisfacer todas las acciones del evaluador correspondientes al nivel EAL2, definidas por los Criterios Comunes v3.1 [CC-P3] y por la Metodología de Evaluación v3.1 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto BITACORA v4.0.2, se propone la resolución ESTIMATORIA de la misma.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Resumen del TOE

BITACORA es una solución de centralización, gestión y correlación de logs que permite a una organización recolectar y consolidar los logs provenientes de los diferentes sistemas operativos, los dispositivos de red, las bases de datos y las aplicaciones.

BITACORA posibilita el cumplimiento legal y de auditoría para la retención y análisis de logs, permitiendo así alcanzar, e incluso superar, los requerimientos regulativos al poder archivar históricamente toda la información recogida en un formato consolidado y consultable.

BITACORA facilita una interfaz singular de consulta llamada “Consola de consultas” que permite recuperar datos concretos de ficheros de una semana, de un día o, incluso, de una hora concreta, filtrándolos, por ejemplo, según un identificador de usuario, una máquina, una fecha, etc. El acceso a BITACORA se realiza con un navegador web.

En una red corporativa se genera un volumen inmenso de datos en los ficheros de logs. Estos logs pueden corresponder a la actividad en un sistema operativo, en una aplicación, en una red, etc., y se almacenan en el host o servidor donde se produjeron, de forma dispersa y desvinculada.

El Recolector de BITACORA se encarga de recopilar estos logs e integrarlos en el sistema de manera diferida (por medio de ftp, http, SSH, consultas a BBDD, etc.) y en tiempo real mediante un software del propio sistema BITACORA.

Por debajo de este proceso existe un sistema de planificación de tareas. El planificador se encarga de asignar tareas a los recolectores de eventos y proporcionarles el código necesario para ejecutarlas.

Los eventos recibidos en diferido llegan desordenados, pero están sujetos al mecanismo de ordenación de BITACORA que los organiza por día.

Los eventos ordenados se almacenan dentro del sistema de ficheros, organizados como ficheros y directorios, en una estructura de datos en disco. Dentro de un día se guardan todos los eventos que se han producido en dicho día, totalmente ordenados. En un día, sólo existen eventos desde las 00:00:00 hasta las 23:59:59.

A partir de la ordenación y almacenamiento, los eventos son accesibles para usuarios autorizados mediante una aplicación. Utilizando la interfaz amigable de la consola de consultas, los usuarios pueden formular consultas SQL (SELECTs)

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

utilizando, además, criterios de consulta complejos para recuperar los datos almacenados.

Sin embargo, el almacén de eventos tiene una estructura de directorios y ficheros, y no una estructura de una base de datos relacional. Además, no existe integridad referencial entre los datos. Por tanto, es el motor de consultas Aleph quién se encarga de transformar las entradas de los ficheros de logs en tablas, posibilitando su consulta mediante SQL, simulando así la estructura de una base de datos.

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL2, según [CC-P3].

Se enumeran, a continuación, los componentes de garantía satisfechos en esta evaluación:

- ASE_CCL.1
- ASE_ECD.1
- ASE_INT.1
- ASE_OBJ.2
- ASE_REQ.2
- ASE_SPD.1
- ASE_TSS.1
- ALC_CMC.2
- ALC_CMS.2
- ALC_DEL.1
- ADV_ARC.1
- ADV_FSP.2
- ADV_TDS.1
- AGD_OPE.1
- AGD_PRE.1
- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2
- AVA_VAN.2

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto satisface los requisitos funcionales, según [CC-P2], siguientes:

- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FMT_MSA.1.FUENTES Management of security attributes
- FMT_MSA.1.USUARIOS Management of security attributes
- FMT_MSA.3 Static attribute initialization
- FIA_UID.2 User identification before any action
- FIA_UAU.2 User authentication before any action
- FDP_ACF.1.FUENTES Security attribute based access control
- FDP_ACF.1.USUARIOS Security attribute based access control

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- FDP_ACC.1.FUENTES Subset access control
- FDP_ACC.1.USUARIOS Subset access control
- FDP_ITC.1 Import of user data without security attributes
- FDP_SDI.2 Stored data integrity monitoring and action

IDENTIFICACIÓN

Se relacionan, a continuación, los principales datos que permiten identificar claramente el alcance de la evaluación y certificación correspondientes a BITACORA.

Producto: BITACORA v4.0.2.

Declaración de Seguridad: "Declaración de Seguridad de BITACORA" v3.0 de 3 de noviembre de 2008.

Perfil de Protección: ninguno.

Nivel de Evaluación: CC v3.1 r2 EAL2.

Fortaleza de las Funciones: no aplica en CC v3.1.

POLÍTICA DE SEGURIDAD

El uso del producto BITACORA, NO obliga a implementar ninguna política organizativa.

HIPÓTESIS Y ENTORNO DE USO

Las siguientes hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la Declaración de Seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas.

Para garantizar el uso seguro del TOE, se parte de las siguientes hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

Hipótesis 01: A.ENV. Configuración Segura

La plataforma de uso de BITACORA, está configurada de manera que no presenta caminos o modos de acceso directo a los activos de BITACORA. Las vulnerabilidades propias de los elementos de terceros no son competencia de

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

BITACORA por lo que deberán ser solucionadas por los fabricantes de los elementos de terceros.

La única forma de acceso a BITACORA es a través del interfaz web que expone BITACORA. La máquina servidora en la que se ha instalado BITACORA deberá estar correctamente aislada y securizada para que nadie pueda acceder a través de otros interfaces a la misma. Una vez instalado BITACORA, el único acceso físico permitido a la máquina servidora de BITACORA será a los usuarios autorizados, para reiniciar BITACORA a través del botón de arranque y/o parada de la máquina física.

Los administradores y usuarios autorizados a acceder a BITACORA se consideran confiables y competentes en el uso de la aplicación.

Aclaraciones sobre amenazas no cubiertas

Las siguientes amenazas no suponen un riesgo explotable para el producto BITACORA v4.02, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a “BASIC” de EAL2, y siempre bajo el cumplimiento de las hipótesis de uso.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Amenaza 01: T.ALOGS

Un atacante genera logs falsos y consigue remitirlos a BITACORA como si se tratara de una fuente fiable. Igualmente, un atacante consigue evitar la recepción de logs auténticos, mediante ataque directo a BITACORA.

Amenaza 02: T.ACCESS

Un atacante consigue acceder a datos de logs para los que no tiene concedido permiso de lectura.

Amenaza 03: T.INT

Un atacante consigue, a través de los interfaces de BITACORA, modificar o suprimir los datos de logs almacenados en un repositorio.

Funcionalidad del entorno

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Los objetivos que se deben cubrir por el entorno de uso del producto son los que se relacionan a continuación.

Objetivo entorno 01: O.ENV

La plataforma de uso de BITACORA, incluyendo todos los elementos de terceros requeridos para su funcionamiento, se configurará de manera que no presentan caminos o modos de acceso directo a los activos de BITACORA. Los manuales de instalación y uso del producto incluirán los detalles de dicha instalación segura. Las vulnerabilidades propias de los elementos de terceros no son competencia de BITACORA por lo que deberán ser solucionadas por los fabricantes de los elementos de terceros.

La única forma de acceso a BITACORA es a través del interfaz web que expone BITACORA. La máquina servidora en la que está instalado BITACORA deberá estar correctamente aislada y securizada para que nadie pueda acceder a través de otros interfaces a la misma. Una vez instalado BITACORA, el único acceso físico permitido a la máquina servidora de BITACORA será, a los usuarios autorizados, para reiniciar BITACORA a través del botón de arranque y/o parada de la máquina física.

Los administradores y usuarios autorizados a acceder a BITACORA se consideran confiables y competentes en el uso de la aplicación.

Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad), o de los requisitos de seguridad del TOE se encuentran en la correspondiente Declaración de Seguridad.

ARQUITECTURA

BITACORA tiene una arquitectura modular y funcionalidad altamente configurable, lo que la hace apropiada para resolver las necesidades de un amplio abanico de usuarios con necesidades de gestión de la seguridad de redes y sistemas complejos. Está basada en desarrollos propios pero requiere de componentes de terceros, tales como un sistema operativo, una base de datos, un servidor de aplicaciones o un servidor web, todos ellos de libre distribución.

El TOE se estructura en los siguientes subsistemas:

1. Motor de consultas (ALEPH ENGINE)
2. Planificador
3. Agente de tareas
4. Consola de consultas

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

5. Administración del planificador de tareas (UATU PORTEL)

También se considera parte del TOE el siguiente software de terceros:

- Tomcat 5.5.26
- Apache 2.2.8
- PostgreSQL 8.2.3
- Liferay 4.3.3

DOCUMENTOS

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada:

- BITACORA. Administración v3.0
- BITACORA. SQL v3.0
- BITACORA. XML v3.0
- BITACORA. Usuario v3.0
- BITACORA. Instalación v3.0

PRUEBAS DEL PRODUCTO

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todas las pruebas han sido realizadas por el fabricante en sus instalaciones con resultado satisfactorio.

El proceso ha verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea cubrir.

Todas las pruebas se han realizado sobre un mismo escenario de pruebas acorde a la arquitectura identificada en la Declaración de Seguridad y descrita en el manual de instalación del producto.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

Para verificar los resultados obtenidos por el fabricante, el laboratorio ha repetido las pruebas funcionales definidas por aquel, en la plataforma de pruebas montada en el laboratorio de evaluación.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Adicionalmente, el laboratorio ha desarrollado una prueba independiente por cada una de las funciones de seguridad del producto, verificando que los resultados así obtenidos son consistentes con los resultados obtenidos por el fabricante.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no representaba un problema para la seguridad, ni suponía una merma en la capacidad funcional del producto.

CONFIGURACIÓN EVALUADA

Además de los componentes software enumerados en el apartado ARQUITECTURA, los requisitos software y hardware son los que se indican a continuación. Así, para el funcionamiento del producto BITACORA es necesario disponer de los siguientes componentes software, que NO se consideran parte del TOE:

- UBUNTU Server 6.06 LTS
- Java version "1.5.0_13"
- Paquete SSL (openssl y libssl-dev)
- Compilador gcc
- Paquete make
- Paquete ‘expect’
- Navegador web: Internet explorer 6.X, 7.X o Firefox 2.X

En cuanto a los componentes hardware, BITACORA requiere de un ordenador de propósito general, conectado a la red de donde se reciben los logs, sin más requisitos que el de soportar los elementos software detallados previamente y, especialmente, los establecidos por el sistema operativo, UBUNTU Server 6.06 LTS, para su funcionamiento.

RESULTADOS DE LA EVALUACIÓN

El producto BITACORA 4.0.2 ha sido evaluado frente a la Declaración de Seguridad “Declaración de Seguridad de BITACORA” v3.0 de 3 de noviembre de 2008.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL2** presentan el veredicto de “PASA”. Por consiguiente, el laboratorio EPOCHE & ESPRI asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador correspondientes al nivel EAL2, definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 revisión 2.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

A continuación se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto, teniendo en cuenta el alcance de los problemas encontrados durante la evaluación.

Aunque el fabricante ha incluido en la Declaración de Seguridad una hipótesis de uso seguro respecto a la protección física del TOE y a los interfaces de accesibilidad declarados (A.ENV), se destacan los siguientes aspectos:

1) El producto no implementa protecciones contra un atacante que posea acceso físico al equipo que aloja el TOE. Un atacante podría modificar el contenido del disco duro mediante un LiveCD o directamente mediante la extracción del mismo. Como medida de protección se podría usar un sistema de encriptación del disco a bajo nivel. Por otra parte, para minimizar los riesgos sería recomendable deshabilitar los dispositivos de arranque distintos al disco duro.

2) Interfaz consola UNIX: la sola presencia de este interfaz supone una clara vía de ataque para un usuario malintencionado del TOE. Aunque no se declara como interfaz del TOE, a la vista de la hipótesis de uso realizada, cualquier usuario con acceso a la consola UNIX podría realizar una escalada de privilegios hasta tomar un control total del TOE.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto BITACORA 4.0.2, se propone la resolución ESTIMATORIA de la misma.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

GLOSARIO DE TÉRMINOS

CC	Criterios Comunes
CCN	Centro Criptológico Nacional
CEM	Common Methodology for Information Technology Security Evaluation
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
TOE	Target Of Evaluation

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

BIBLIOGRAFÍA

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CC_P1] "Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, revision 1, September 2006".

[CC_P2] "Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, revision 2, September 2007".

[CC_P3] "Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, revision 2, September 2007".

[CEM] "Common Methodology for Information Technology Security Evaluation, Version 3.1, revision 2, September 2007".

DECLARACIÓN DE SEGURIDAD

Conjuntamente con este informe de certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación: **"Declaración de Seguridad de BITACORA" v3.0 de 3 de noviembre de 2008**.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es