No.22 / agosto-septiembre 2014 ISSN: 1251478, 1251477

# .Seguridad

Cultura de prevención para TI

22

# Protección de datos

## Quehacer de usuarios y profesionales

Gestionar seguridad | Autorregulación y privacidad | Cifrado en base de datos | Detección de intrusos | Ciberseguridad en educación | Derechos de autor

# Contenido

.Seguridad
Cultura de prevención para TI


04 Lo que no debes pasar por alto para gestionar la seguridad de la información

07 Modelo de autorregulación como como parte del sistema de protección de datos personales - II

11 Consideraciones para el uso del cifrado en las bases de datos

15 Instalando un Sistema de Detección de Intrusos Inalámbrico (WIDS) en Raspbian - I

23 Ciberseguridad para la educación online

27 Técnicas de protección de derechos de autor en imágenes digitales capturadas con dispositivos Android: fortalezas y debilidades



Universidad Nacional Autónoma de México. Dirección General de Cómputo y Tecnologías de Información y Comunicación. Coordinación de Seguridad de la Información/UNAM-CERT. Revista .Seguridad Cultura de prevención para TI M.R., revista especializada en temas de seguridad del UNAM-CERT.

# Editorial

## Protección de datos

### Quehacer de usuarios y profesionales

Un dato tiene la extensión que requiere, la simpleza o complejidad que amerite y todos los calificativos que deseemos adjudicarle, incluso si es tan pequeño como el cero en una cadena binaria o infinito, como la historia del universo almacenada en los ecos del lejano big bang.

En nuestra era, la humanidad genera 3 exabytes más de información cada día, esto es $4 \times 10^{19}$ ceros o unos llamados bits, el mismo latido de la humanidad acontece al ritmo de piezas de información que viajan y regresan, que se duplican, que se transforman, se pierden, se obtienen, se generan, se conocen o se asimilan, pero pocas se protegen.

Es aquí donde pensamos en cuánto, realmente, hemos dedicado tanto usuarios como profesionales a proteger esta cadena infinita de información de la que dependemos todos los días. Para algunos serán fotografías, correos o documentos, algunos más nos preocupamos por contraseñas, por la agenda de nuestros clientes, por los registros de criminales o por el archivo histórico de una nación, pero cuando nos sumamos todos a la generación de datos, nos es difícil dilucidar siquiera cuán importante es para nuestra forma de vida cuidar de esta información.

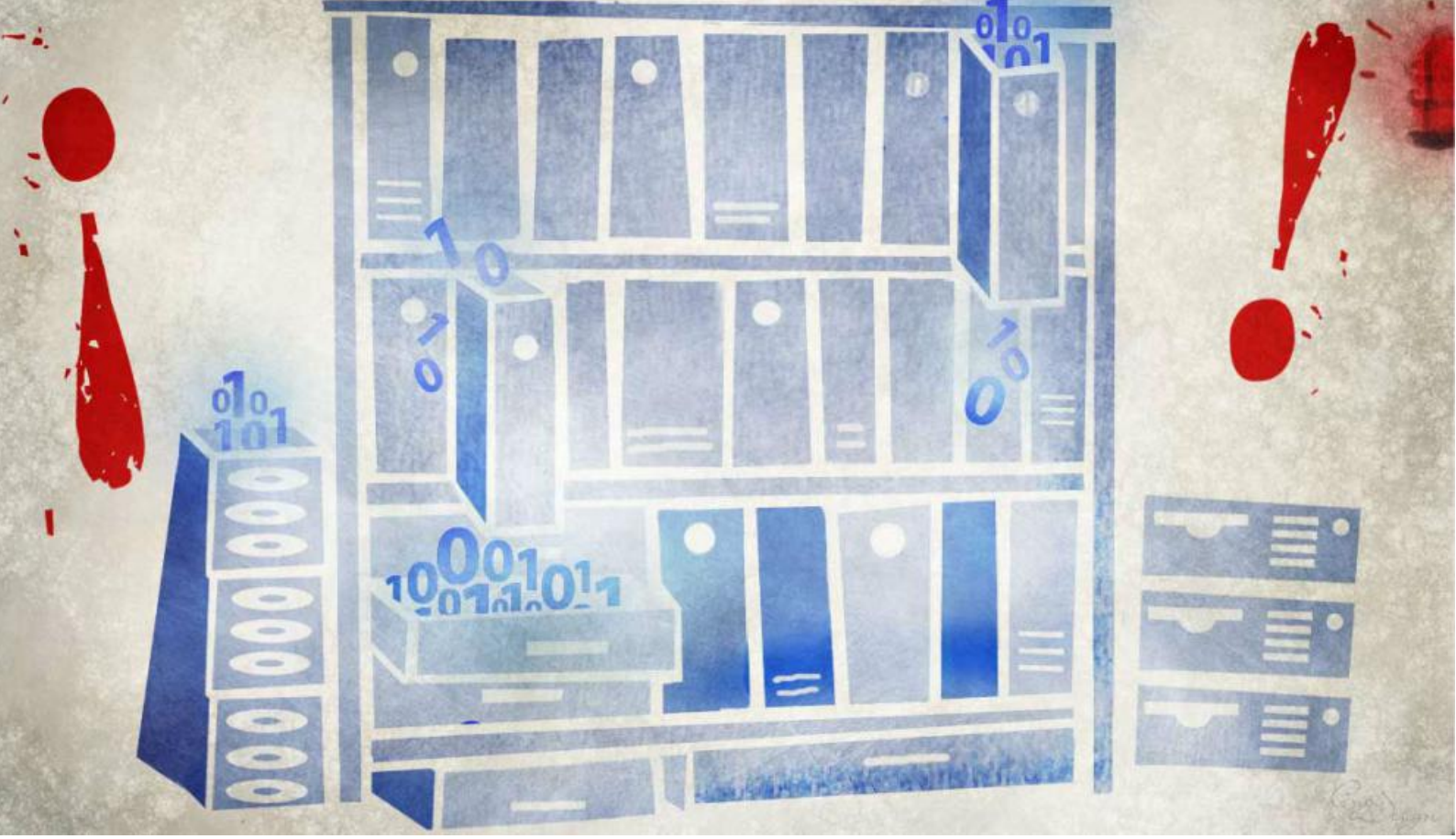
Reflexionando sobre esto, es que decidimos enfocar la publicación que lees en este momento hacia la protección de los datos, en todas sus formas y de todos sus tamaños. Confiamos en que después de revisar estas páginas, la idea de la protección de datos se vuelva quehacer de todos, de usuarios y de profesionales.

L.C.S Jazmín López Sánchez
Editora
Coordinación de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad Cultura de prevención TI M.R. / Número 22 / agosto - septiembre 2014 / ISSN No. 1251478, 1251477 /

Revista Bimestral, Registro de Marca 129829



# Lo que no debes pasar por alto para gestionar la seguridad de la información

H. Camilo Gutiérrez Amaya

La forma en que los usuarios intercambiamos información, sea personal o laboral, ha llevado a que los temas relacionados con su seguridad cobren gran relevancia dentro de las organizaciones, llevándola a ser parte fundamental para garantizar el cumplimiento de los objetivos de negocio.

Lo más complicado al momento de integrar temas relacionados con la seguridad de la información a la organización es que, generalmente, no se enfocan en las necesidades de negocio y sus intereses. Por esta razón revisaremos cuáles son los aspectos fundamentales que no deberíamos pasar por alto.

Cuando se refiere a seguridad de la información incluye el recurso humano y políticas claras que dirijen el accionar del sistema.

## ¿Qué debemos garantizar con nuestro Sistema de Gestión de Seguridad de la Información (SGSI)?

Lo primero es alinear la estrategia de seguridad con los objetivos del negocio, sucede al garantizar la protección de los sistemas y la información usada en los procesos.

Clásicamente se ha hablado de que un sistema de gestión de la seguridad debe garantizar en la información tres características: la integridad, la disponibilidad y la confidencialidad. Si bien estas tres características son fundamentales, hay otras tres que dado el crecimiento en el uso de la información y los nuevos tipos de ataques, no deben dejarse de lado: la verificación del origen

de los datos, la utilidad de los datos y el control de la información, este último enfocado a que la información no pueda ser revelada en caso de pérdida.

Procurar estas características debería ser el resumen de un modelo de gestión de la seguridad. Para lograrlo hay que apoyarse en algunos instrumentos como la política de seguridad, la identificación de activos y el análisis de riesgos, éstos deberían ser independientes a buscar certificaciones en alguna normativa.

## La piedra angular: política de seguridad

La política de seguridad debe convertirse en el punto de unión del negocio con los intereses de la seguridad de la información. Se logra a través del establecimiento de objetivos de seguridad, que no son más que la manifestación de las necesidades técnicas que debe satisfacer la información para garantizar el cumplimiento de los objetivos de negocio.

La política de seguridad debe darse a conocer a todos los niveles de la organización para garantizar que todos los empleados sepan cuál es la información crítica del negocio y cuáles son las características principales que le deben ser garantizadas. De esta forma, quien lea la política deberá tener claro cuáles son los límites que tiene con respecto a la seguridad de la información.

## Clasificar la información corporativa

Con la clasificación de la información se pueden priorizar y enfocar las acciones en materia de la gestión de la seguridad. La clasificación depende de la naturaleza del negocio pero en general deberían incluirse tres niveles: información pública, incluye todos los datos de dominio público. Ya que es información a la que pueden acceder los clientes y proveedores, sus características principales deben ser la precisión y la disponibilidad. En el siguiente nivel está la información de uso interno, comprende toda la información que se intercambia al interior de la empresa y entre los empleados, es la columna vertebral de las operaciones del negocio, por lo tanto las características que le aplican son la disponibilidad y la integridad. En el último nivel está la información de acceso restringido, está muy relacionada con el tipo de actividad que puede incluir, por ejemplo los planes de negocio, información de nuevos productos, resultados de investigaciones o estrategias de mercado. La principal característica de este tipo de información es su confidencialidad.

Al clasificar la información, la empresa tiene un panorama más claro de cuáles son los aspectos en los que debe enfocar su gestión. De esta forma se pueden identificar cuáles son los riesgos más relevantes dentro del SGSI y por tanto, determinar los controles más apropiados y acordes a la realidad de la empresa.

## Qué hacer y dónde enfocar esfuerzos: Análisis de riesgos

Es necesario para la empresa hacer una adecuada gestión de riesgos que le permita saber

cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar esas vulnerabilidades. En la medida que la empresa tenga clara esta identificación de riesgos podrá establecer las acciones preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

La identificación de controles es fundamental para permitir el análisis de riesgos, ya sea para mitigar la posibilidad de que ocurra la amenaza o para mitigar su impacto. Las medidas de control que puede asumir una empresa estarán relacionadas con el tipo de amenaza y el nivel de exposición que represente para la información corporativa.


## Lo que no se puede olvidar

Es muy importante no perder de vista que, cuando se refiere a seguridad de la información, no solamente se habla de garantizar la seguridad con equipos y aplicaciones, aún siendo una parte fundamental y prioritaria; sino que el panorama se extiende para incluir al recurso humano y a políticas claras que dirijan el accionar del sistema.
Finalmente, la gestión de la seguridad debe existir para soportar las operaciones del negocio y no para convertirse en parte de los objetivos. En otras palabras, a partir de la definición de su misión y su visión, una empresa debe establecer estrategias de negocio coherentes que la lleven a alcanzar sus objetivos, y como parte de esta estrategia, definir el sistema que garantice la seguridad de la información que le permita alcanzarlos.

**Si quieres saber más consulta:**

- Normatividad en organizaciones: Políticas de seguridad de la información - Parte I
- Riesgo tecnológico y su impacto para las organizaciones parte I
- Gestión de incidentes de seguridad informática con agentes inteligentes

*H. Camilo Gutiérrez Amaya*

Se desempeña actualmente como Especialista de Awareness & Research en ESET Latinoamérica. Es Ingeniero Electrónico egresado de la Universidad de Antioquia e Ingeniero Administrador graduado de la Universidad Nacional de Colombia.

Cuenta con una especialización en Sistemas de la Información en la Universidad EAFIT y actualmente opta al título de Magister en Data Mining en la Universidad de Buenos Aires.

# Modelo de autorregulación como parte del sistema de protección de datos personales – Parte II

Humberto David Rosales Herrera

En la primera parte de este documento se comentó sobre el marco jurídico en México para la protección de datos personales en posesión de los particulares, éste busca garantizar la privacidad de nuestros datos personales y el derecho y control sobre nuestra información personal frente a la posesión por terceros.

En particular se habló sobre el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) que establece que los particulares responsables de datos personales podrán convenir esquemas de autorregulación vinculante a través de los cuales crearán el compromiso de proteger los datos personales mediante el cumplimiento con lo dispuesto por la Ley, el Reglamento y demás disposiciones aplicables.

Se comentó que los esquemas deben estar constituidos por dos elementos básicos: el tipo de esquema de autorregulación vinculante (principios, normas, procedimientos a observar y cumplir) y los mecanismos de control necesarios para la aplicación de tales normas. Finalmente se describieron los objetivos mínimos que debe buscar el esquema de autorregulación:

- Consolidar una cultura de autoevaluación y autorregulación.
- Desarrollar un sistema de evaluación permanente.
- Fortalecer los mecanismos establecidos para la protección de datos.
- Dar a conocer las acciones encaminadas al cumplimiento de la ley y la protección de datos.
- Conocer las áreas de oportunidad o mejora

en esta materia.

- Análisis de brecha (gap analisys) sobre el cumplimiento.
- Mejora continua.
- Conocer la situación con relación al cumplimiento de la LFPDPPP y su reglamento.

Para alcanzar los objetivos del esquema de autorregulación es conveniente que éste se construya considerando tres fases principales:

## Autorregulación

Es el reconocimiento que debe realizar toda organización que tenga en su posesión datos de carácter personal (con base en un diagnóstico y una introspección o percepción interna de la organización) para desarrollar la capacidad reflexiva y así poder observar sus potencialidades, destrezas, habilidades, debilidades y oportunidades con relación a la protección de los datos personales y al cumplimiento de las disposiciones de la LFPDPPP.

## Autoevaluación

Constituye un acto consciente de apreciación y de valoración de las actividades realizadas. Está relacionada con los instrumentos y mecanismos orientados a identificar, conocer y analizar los elementos fundamentales utilizados para dar cumplimiento a la protección de datos personales, a la LFPDPPP y a su Reglamento.

Es por ello que la autoevaluación sobre la efectividad de las medidas de protección de datos personales se entiende como una forma tanto de retroalimentación como de control sobre la correcta aplicación de las medidas físicas, técnicas y administrativas establecidas para la protección de los datos personales, el cumplimiento de la LFPDPPP y su Reglamento, lo que resulta un requisito esencial para el proceso de toma de decisiones.
Durante la autoevaluación se identifica y evalúa la existencia de estos mecanismos y su relación con los propósitos u objetivos asociados a la protección de los datos, la capacidad para aplicar dichos mecanismos en forma sistemática y gestionada, así como el grado en que éstos permiten ejecutar planes para el cumplimiento de la LFPDPPP. Al mismo tiempo permite desarrollar procesos de aprendizaje institucional.

Su resultado es la emisión racional y consciente de un juicio acerca de su propio desenvolvimiento en relación a la protección de los datos personales y al cumplimiento de las disposiciones de la LFPDPPP.

## Acreditación

Un proceso voluntario mediante el cual una organización es capaz de medir la efectividad de sus mecanismos de protección de datos personales y los controles establecidos para el cumplimiento de las disposiciones de la LFPDPPP, además del rendimiento de los mismos frente a estándares reconocidos a nivel nacional o internacional. El proceso de acreditación implica la autoevaluación de la organización, así como una evaluación en detalle por un equipo de expertos externos.

El desarrollo de un esquema de autorregulación inicia con un proceso de autoevaluación en materia de protección de datos personales, permite establecer un sistema de aseguramiento integrado por mecanismos para medir la eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento. Este esquema corresponde a la autorregulación como máxima expresión del cumplimiento de la LFPDPPP.

El proceso de autorregulación comprende ocho aspectos previos a la autoevaluación propiamente dicha, los cuales se especifican a continuación:

- **Diagnóstico situacional**. Permite producir conocimientos para la acción y toma de decisiones adecuadas a la realidad y el contexto sobre la protección de los datos personales.
- **Acciones de mejora inmediata**. Son acciones

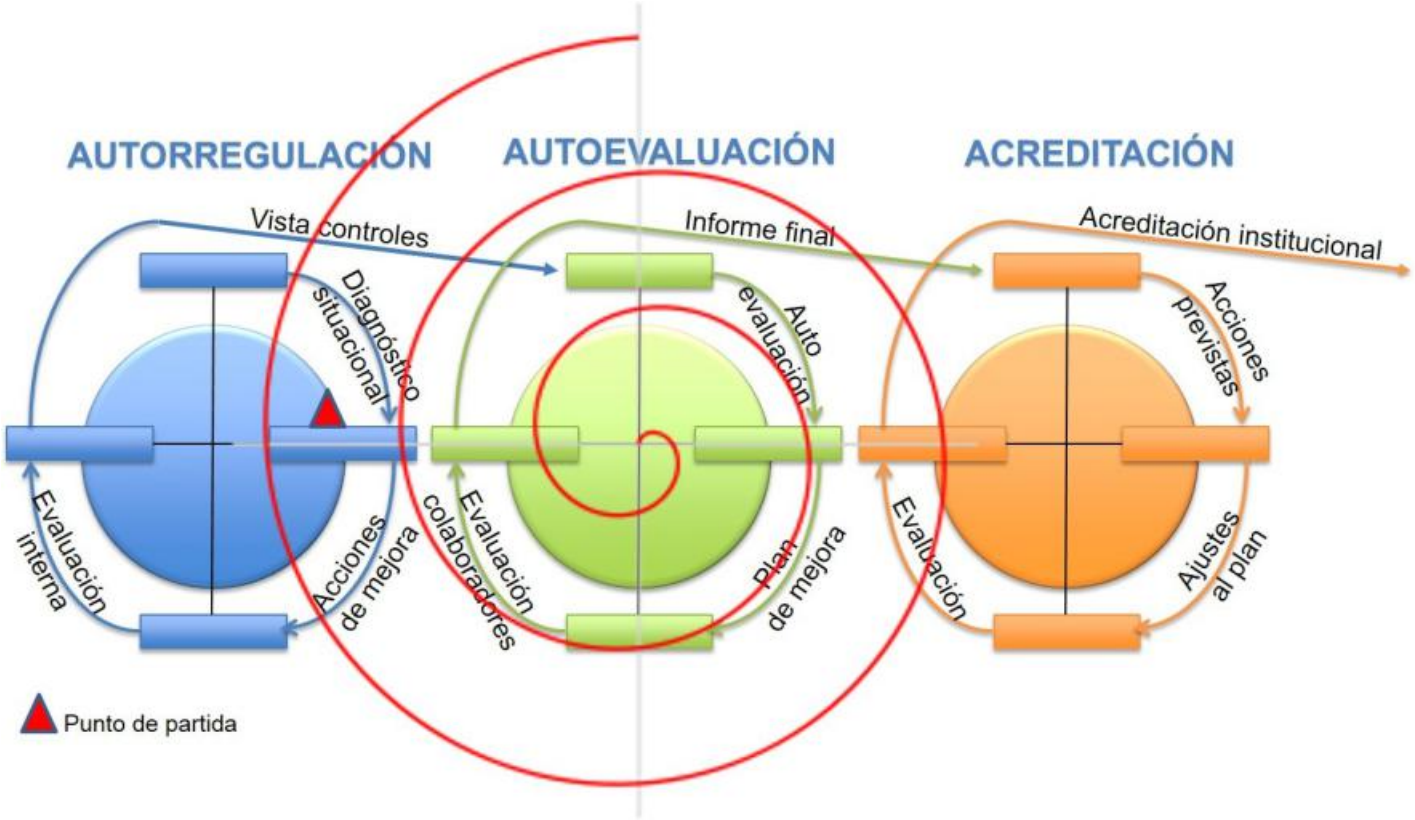



*Imagen 1. Ciclo de vida de un esquema de autorregulación vinculante*

que no requieren un proceso de análisis exhaustivo ni una programación detallada. Se desprenden por la sola aplicación del Instrumento de Autoevaluación, no necesitan recursos adicionales y pueden llevarse a cabo en el plazo inmediato. Sólo requieren la determinación de realizarse (decisión). Ejemplo de ello son: la formalización de un procedimiento, diseño y aplicación de un formulario, conformación de un equipo de tarea, etc.

- **Evaluación interna**. Se debe realizar en forma permanente y bajo supervisión.
- **Ponderación de factores**. Dan soporte para cumplir con la Ley.
- **Recolección de información**. Aviso de privacidad, derechos ARCO, medidas y gestión de protección de datos.
- **Juicios valorativos**. Basados en indicadores y métricas.
- **Elaboración de gap y plan director** (planes de mejora).
- **Evaluación interna y externa** (Auditoría).

El sistema de autorregulación debe proporcionar información para demostrar la eficacia en la protección de los datos personales y presentar las áreas de oportunidad donde éste puede ser mejorado. Los puntos de mejora de las medidas de protección de los datos personales pueden corresponder a dos tipos:

a) Acciones correctivas. Son las acciones encaminadas a eliminar las causas de fallas o incidentes ocurridos en las medidas de protección, su objetivo es prevenir que vuelvan a ocurrir. Las acciones deben ser proporcionales a la gravedad del incidente.

b) Acciones preventivas. Son las acciones encaminadas a eliminar las causas de fallas o incidentes posibles en las medidas de protección, dichas acciones deben ser proporcionales a las amenazas potenciales.

Para asegurar la obtención de dicha información es recomendable la asesoría de expertos especializados en la materia, existen en México empresas con experiencia en implementación de estos sistemas de autorregulación.

## Recomendaciones

- Convenir esquemas de autorregulación en grandes empresas o grupos de empresas.
- Focalizar el esfuerzo en la creación de un sistema y una cultura de autoevaluación para fortalecer los mecanismos de protección.
- Utilizarlo para conocer la situación sobre el cumplimiento de la Ley, su Reglamento y la

normatividad vigente al identificar áreas de oportunidad o mejora y desplegar planes de acción.

- Someter su instrumentación a un modelo de madurez.
- A mayor tratamiento de datos personales, mayor riesgo, para mitigar el impacto obtener los incentivos que establece el Reglamento.
- Extrapolar los esfuerzos hacia la seguridad de la información, entre otros.


## Conclusiones finales

- Aplicable en grandes empresas o grupos de empresas.
- Su objetivo, fortalecer los mecanismos de protección de datos.
- Autorregulación como instrumento de apoyo para la gestión del riesgo.
- La autorregulación incrementa la efectividad del sistema de gestión de protección de datos personales y el cumplimiento de la legislación en esta materia.
- Autorregulación como parte de la visión estratégica para crear valor.
- Utilizar la autorregulación como ventaja competitiva.

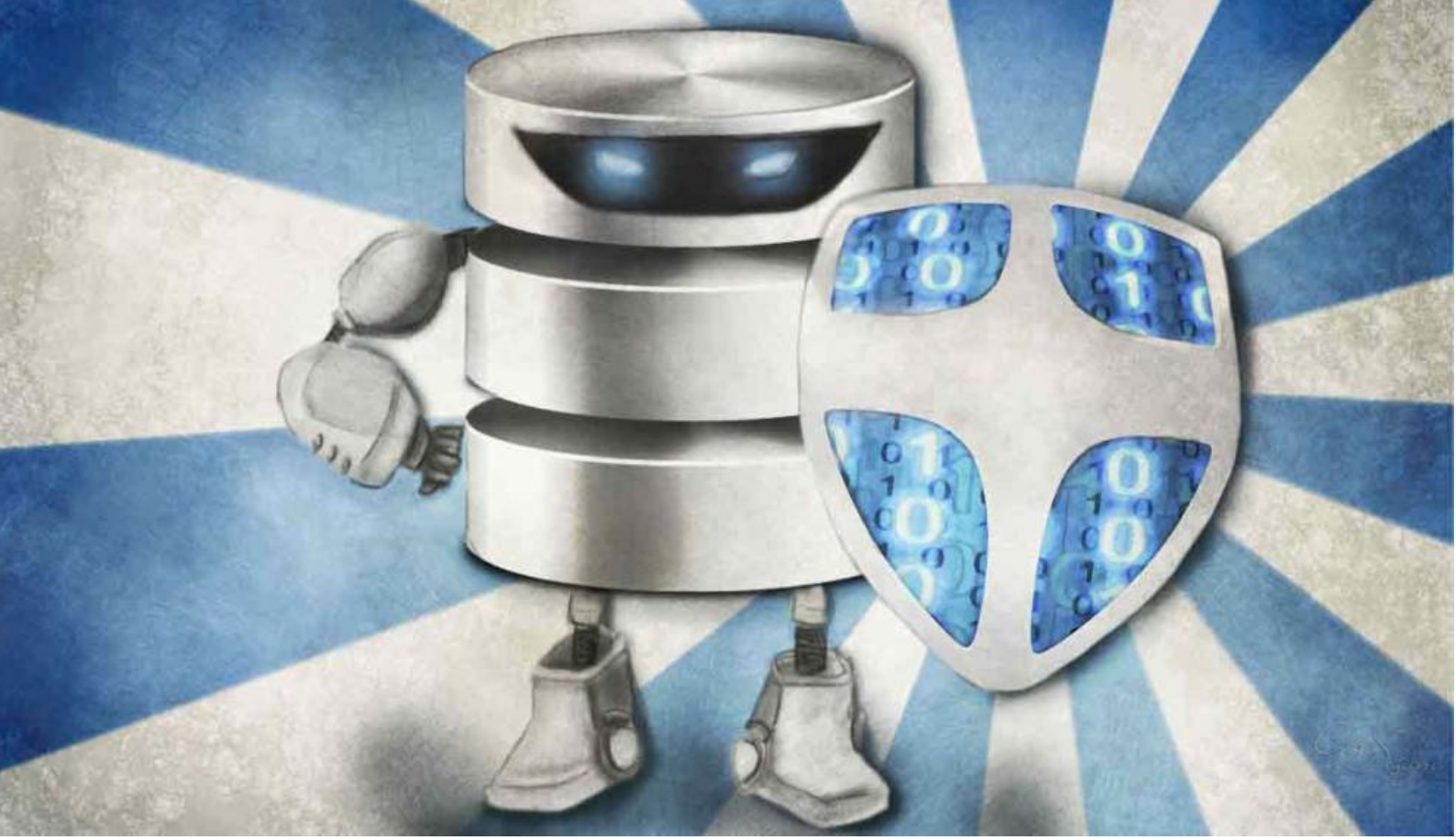
**Si quieres saber más consulta:**

- Modelo de autorregulación como parte del sistema de protección de datos personales I
- Acuerdos Internacionales para la Privacidad de la Información
- Implicaciones jurídicas y de ciberseguridad para la protección de bioinformación humana en su regulación legal, almacenamiento y uso – Parte I

*Humberto David Rosales Herrera*

Su experiencia profesional se ha enfocado en la administración áreas de tecnología de misión crítica y seguridad integral con más de veinticinco años de experiencia internacional como consultor, auditor, gerente y subdirector. Desarrollé un método para generar métricas sobre la evolución de efectividad en la administración de TI.

Cuenta con el PhD Computer Science (1990) de la Pacific Western University de Los Angeles, California y con las certificaciones CISSP, CCNA DE CISCO NETWORKS (instructor), MICROSOFT CERTIFIED PROFESSIONAL (instructor), PMP.



# Consideraciones para el uso del cifrado en las bases de datos

Johnny Villalobos Murillo

El cifrado de datos es una alternativa muy usada para el cumplimiento del requisito de confidencialidad de la información en las bases de datos, sin embargo, cuando se aplica en bases de datos heterogéneas y de gran tamaño, puede llevar a consecuencias no deseadas en su rendimiento.

En la primera sección de este artículo se habla sobre el proceso de cifrado y cómo se aplica en las bases de datos. La segunda sección explica las considera- ciones para el uso del cifrado con una base de datos y se proponen escenarios en donde puede ser adecuado el uso de este recurso. En la tercera sección se dan recomendaciones para diseñar aplicaciones que utilicen una base de datos cifrada.
Finalmente se presentan recomendaciones generales sobre cifrado en las bases de datos.

## El cifrado y las bases de datos

Para introducir al lector en los aspectos generales sobre el cifrado y su importancia como método de seguridad, veamos la siguiente definición:

"El cifrado es una operación criptográfica reversible que transforma datos significativos sin proteger, conocidos como texto sin formato, en datos ilegibles, cifrados, conocido como texto cifrado, utilizando una clave llamada clave de cifrado."[1]

En esta definición los datos significativos son el elemento fundamental, ya que por el carácter confidencial de los datos almacenados en las bases de datos, las organizaciones se ven

forzadas a implementar controles cada vez más sofisticados para protegerlas, uno de estos controles es el cifrado.

Sin embargo, la preocupación por la degradación del rendimiento, el soporte de aplicaciones y la forma de administrar las implementaciones de cifrado en bases de datos grandes originan barreras que hacen difícil adoptar esta importante medida de seguridad.

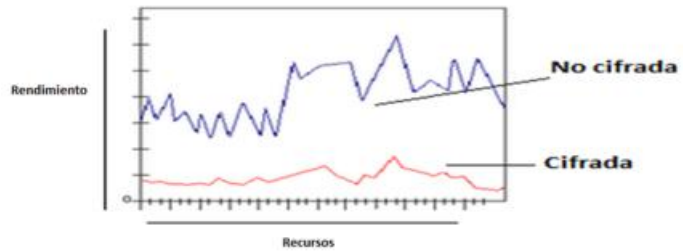



*Imagen 1. Rendimiento esperado en bases de datos cifradas.*

Existe una presunción sobre la afectación del rendimiento de la base de datos cifrada respecto a la no cifrada, como se muestra en la imagen 1. Si la organización desea aplicar el cifrado es importante conocer por qué se desea utilizar una base de datos cifrada, ya que esto ayuda a decidir la forma de conectarse, ejecutar transacciones y realizar consultas. Tener en cuenta esta pregunta ayudará a afectar al mínimo el rendimiento de la base de datos y el modo en que las aplicaciones de los usuarios crean, obtienen o almacenan la clave de cifrado para la base de datos.

Si todas las aplicaciones de la organización comparten el mismo motor de base de datos local y la base de datos está cifrada, al conectar cualquier aplicación o al leer y escribir en un archivo de la base de datos, ésta deberá proporcionar la clave de cifrado.

Para usar una base de datos cifrada debe crearse como cifrada, esto es una opción que existe en la mayoría de los sistemas gestores de bases de datos. Las técnicas para trabajar con una base de datos cifrada son las mismas que para el trabajo con una base de datos no cifrada. En concreto, la ejecución de declaraciones SQL es la misma independientemente de si una base de datos se encuentra o no cifrada.

## Claves de cifrado seguras

El proceso de creación de una base de datos cifrada es similar al proceso de creación de una base de datos no cifrada, la diferencia básica es el uso de una clave de cifrado. Esta clave debe ser generada antes de crear la base de datos mediante un proceso que asegure el nivel más elevado posible de privacidad y seguridad para los datos de los usuarios.

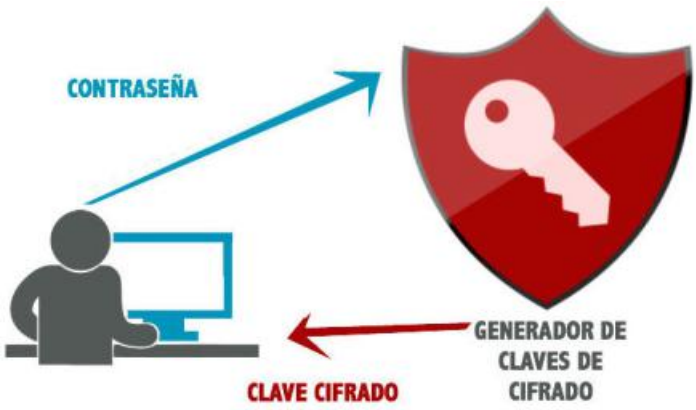



*Imagen 2. Generación de claves de cifrado por contraseña de usuario.*

El método deberá solicitarle al usuario una contraseña que sirva para crear esta clave de cifrado. Deberá utilizarse un método que compruebe que la contraseña introducida por el usuario cumple con los requisitos de longitud de contraseña. Se recomienda que la contraseña tenga entre 8 y 32 caracteres. Debe mezclar letras mayúsculas, minúsculas y al menos un número o caracter especial [2]. El usuario crea la base de datos cifrada indicando la clave de cifrado en el proceso, posteriormente, para conectarse y utilizarla deberá ingresar dicha clave.


*Imagen 3. Proceso de creación de base de datos cifrada.*

## Consideraciones para el uso del cifrado en una base de datos

La forma en que se plantea el uso del cifrado representa una parte importante en el control del nivel de privacidad de la información de una base de datos. Por ejemplo, si se está utilizando una base de datos cifrada para proteger la privacidad, incluso contra otros usuarios en el mismo equipo, la base de datos de cada usuario necesita su propia clave de cifradoincluso contra otros incluso contra otros usuarios en el mismo equipo, la base de datos de cada usuario necesita su propia clave de cifrado.

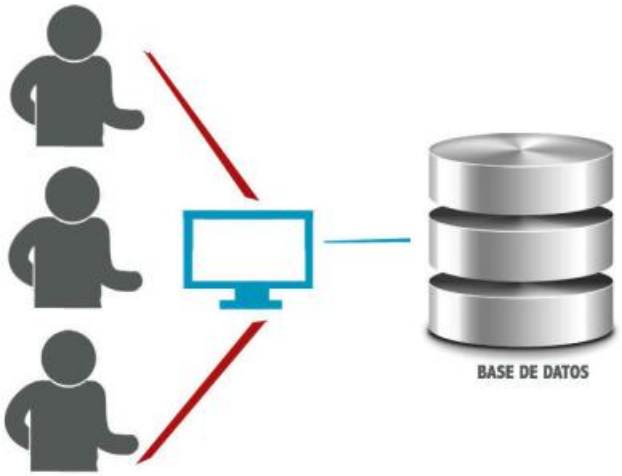



*Imagen 4. Acceso de usuarios a la base de datos por el mismo equipo.*

Para obtener la máxima seguridad, la aplicación puede generar una clave a partir de una contraseña introducida por el usuario. Si la clave de cifrado se basa en una contraseña, se garantiza que un usuario que pudiera suplantar la cuenta de otro en el equipo, no tenga posibilidad de acceder a los datos.

Tanto la aplicación como la técnica utilizada para generar la clave de cifrado se pueden diseñar según el nivel de privacidad que se desee. Las siguientes sugerencias se pueden aplicar para distintos niveles de privacidad de datos:

- Para que cualquier usuario con acceso a la aplicación pueda consultar una base de datos en cualquier equipo, utilice una sola clave que esté disponible en todas las instancias de la aplicación.

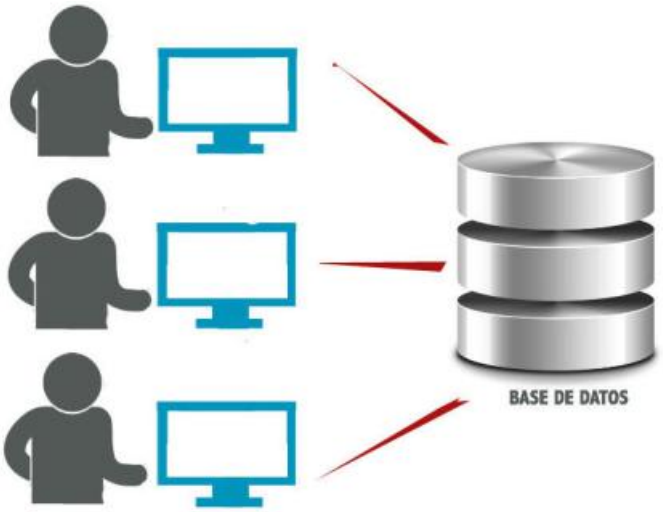



*Imagen 5. Acceso de usuarios a la base de datos desde cualquier equipo.*

Por ejemplo, la primera vez que se ejecute una aplicación puede descargar la clave de cifrado compartida de un servidor mediante un protocolo seguro, como SSL [3].

Para que un usuario pueda acceder a una base de datos desde cualquier equipo, genere la clave de cifrado a partir de una contraseña de usuario. No utilice algún valor que esté asociado a un equipo concreto.

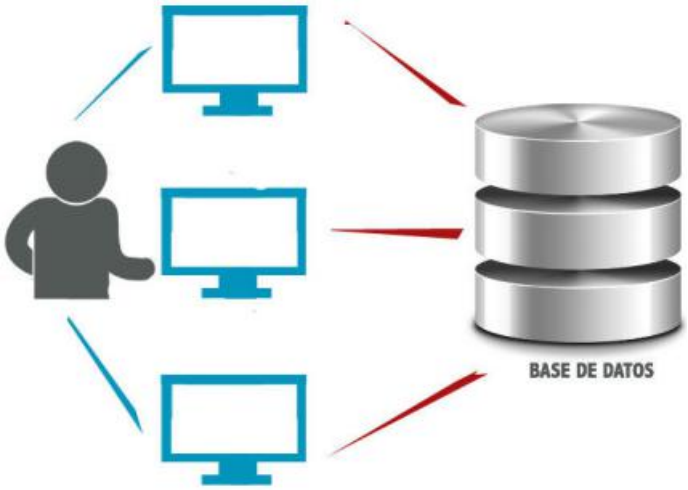



*Imagen 6. Acceso de un usuario a la base de datos desde cualquier equipo.*

Para que únicamente un usuario determinado pueda acceder a una base de datos en un solo equipo, genere la clave a partir de una contraseña y un valor salt generado [4].

## Recomendaciones generales sobre cifrado en las bases de datos

A continuación se incluyen consideraciones adicionales sobre seguridad que es importante tener en cuenta a la hora de diseñar una aplicación que utilice una base de datos cifrada:

- Un sistema sólo es seguro en su vínculo más débil.
- Si usa una contraseña introducida por el usuario para generar una clave de cifrado, tenga en cuenta la aplicación de restricciones de complejidad y longitud mínima en las contraseñas.
- Una contraseña corta que sólo utilice caracteres básicos se puede adivinar rápidamente.
- No ponga nunca una clave de cifrado en el código fuente, es preferible mantenerlas en un recurso externo.
- Tenga en cuenta que la técnica empleada para generar una clave de cifrado puede ser descubierta fácilmente por un atacante.
- Si opta por cifrar toda la base de datos, se cifrarán todos los objetos utilizados por el sistema gestor de base de datos junto con los datos de los usuarios.
- El sistema de base de datos retiene algunos datos en memoria interna para mejorar el rendimiento de lectura y escritura en las transacciones y estos datos no están cifrados.

**Si quieres saber más consulta:**

- El Cifrado Web (SSL/TLS)
- Principios Básicos de Seguridad en Bases de Datos
- Firewall de bases de datos

## Referencias


*[1] Ewow, Educación y Ciencia, Cifrado asimétrico, Recuperado de: http://www.ehowenespanol.com/cifrado-asimetrico-info_196286, 2014*

*[2] ESET, Contraseñas seguras, Recuperado de: http://www.eset.es/index.php/rss/245-el-uso-de-contrasewnwas-seguras 2014*

*[3] Sun Microsystem, Operating SSL Overview, Recuperado de: http://www.manualslib.com/manual/539752/Sun-Micro systems-Eway-5-1-1.html?page=27*

*[4] INTECO, Autenticación segura, Recuperado de: http://www.inteco.es/blogs/post/Security/SecurityBlog/Article_and_comments/autenticacion_passwords_srp9*



*Johnny Villalobos Murillo*

Licenciado en Informática, con énfasis en Sistemas de Información, por la Universidad Nacional de Costa Rica (UNCR), posee dos másters, uno en Auditoría de tecnologías de Información y otro en Ciencias de la Computación. Es catedrático de la UNCR y consultor en Administración de Bases de Datos, Tecnología de la Información y Auditoría.


# Instalando un Sistema de Detección de Intrusos Inalámbrico (WIDS) en Raspbian - I

José Luis Sevilla Rodríguez

Actualmente se han incrementado de forma considerable los ataques informáticos (*phishing*, *malware*, DDOS, accesos no autorizados, entre otros) dirigidos a medianas y pequeñas empresas así como a usuarios finales, según el Informe de Amenazas en Internet 2014 de Symantec. Existen soluciones para proteger la infraestructura tecnológica y la información de una organización contra diversas técnicas utilizadas por los atacantes, pero muy pocas veces podemos encontrar soluciones económicas y que estén orientadas a los usuarios finales.

El objetivo de este artículo es proporcionar una solución de detección de intrusos para redes inalámbricas que permita a un usuario identificar los ataques o intrusiones a dichas redes. Mediante esta publicación describiré todo lo necesario para instalar y configurar OpenWIPS sobre el sistema operativo Raspbian.

A continuación se listan los elementos técnicos:

- Raspberry Pi
- Raspbian
- OpenWIPS-ng

## Raspberry Pi

Es una computadora de dimensión pequeña, aproximadamente del tamaño de una tarjeta de crédito; tiene 2 puertos USB, una interfaz de red cableada, una interfaz HDMI (High-Definition Multimedia Interfaz), etc. Es utilizada en proyectos de electrónica y para realizar algunas tareas que se pueden hacer con una computadora de escritorio o un servidor dedicado. Una de las características principales es que el almacenamiento se lleva a cabo mediante una tarjeta de memoria flash SDHC

(Secure Digital High Capacity). El costo va de los $350 a los $600 pesos mexicanos. La imagen 1 corresponde al diagrama de una Raspberry Pi modelo B.

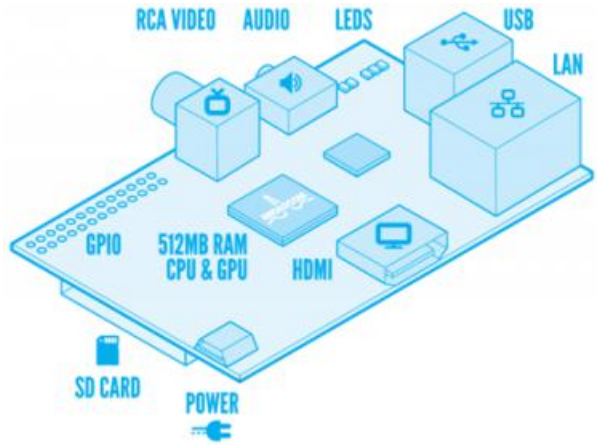



*Imagen 1. Raspberry Pi modelo B.*

## Raspbian

Es un sistema operativo (SO) libre basado en Debian (ver imagen 2) optimizado para Raspberry Pi. La imagen (un archivo que contiene la copia completa de un sistema operativo) de este SO se puede obtener desde su sitio oficial http://www.raspbian.org/


*Imagen 2. Raspbian.*

## OpenWIPS-ng

Es un IPS (Intrusion Prevention System) inalámbrico de código abierto. Está compuesto de tres partes principales:

- Sensor(es): Dispositivo silencioso que captura tráfico inalámbrico y lo envía al servidor para analizarlo. También responde a ataques aunque esta funcionalidad aún no está diseñada en la versión BETA.
- Servidor: Analiza los datos de todos los sensores y puede responder a ataques. También registra y genera una alerta en caso de detectar un ataque.
- Interfaz: Administra el servidor y despliega información acerca de las amenazas de la red inalámbrica detectadas por los sensores.

Actualmente se encuentra en la versión 0.1 beta1:

- Soporta sólo un sensor y, aunque se puedan conectar varios clientes (sensores), no se realiza reensamblaje de tramas (acción de eliminar tramas duplicadas y ponerlas en el orden correcto). Si los sensores se encuentran lejos físicamente entre ellos y no reciben el mismo tráfico, la probabilidad de detectar amenazas disminuye.
- Las credenciales predeterminadas para iniciar el sensor y al mismo tiempo conectarse al servidor son *sensor1:sensor1*.
- Detecta ataques de desasociación, es un tipo de ataque de denegación de servicio inalámbrico donde un atacante puede provocar la desconexión de uno o varios clientes conectados a un AP, así como de fragmentación.
- Sólo se necesita una tarjeta inalámbrica que se pueda poner en modo monitor la cual fungirá como sensor.
- Se lleva un registro de las alertas en tiempo real mediante la interfaz del servidor y se puede configurar OpenWIPS para almacenar una bitácora de eventos en un archivo del sistema.

## Requerimientos de hardware

- Una tarjeta SDHC de 8 GB o más, de preferencia de clase 10 (bus de datos de alta velocidad).
- Tarjeta de red inalámbrica, preferentemente con chipset RT8187L (si no se cuenta con una tarjeta con el chipset especificado, debe garantizarse que se pueda poner en modo monitor).

## Requerimientos de software

- Imagen del sistema operativo Raspbian.
- OpenWIPS-ng 0.1 beta 1.
- Conexión a Internet para descargar el software necesario para instalar OpenWIPS.

# Implementación

El objetivo del artículo no es explicar cómo se configura Raspbian en la memoria flash SDHC, sin embargo se recomienda el siguiente enlace al lector en donde se explica cómo poder hacerlo en Linux, Windows y Mac OS:

Una vez que esté instalado el SO en la Raspberry Pi, lo siguiente es descargar el código fuente de OpenWIPS:

```
root@OpenWIPS:~# wget http://www.openwips-ng.org/openwips-ng-0.1beta1.tar.gz
--2014-03-13 19:11:47--  http://www.openwips-ng.org/openwips-ng-0.1beta1.tar.gz
Resolviendo www.openwips-ng.org (www.openwips-ng.org)... 173.246.38.46
Conectando con www.openwips-ng.org (www.openwips-ng.org)[173.246.38.46]:80... co
nectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 177594 (173K) [application/x-gzip]
Grabando a: "openwips-ng-0.1beta1.tar.gz"

100%[======================================>] 177 594      677K/s   en 0.3s

2014-03-13 19:11:47 (677 KB/s) - "openwips-ng-0.1beta1.tar.gz" guardado [177594/
177594]
```

*Imagen 3. Descarga de OpenWIPS.*

Descomprimir y desempaquetar se puede hacer de la siguiente manera:

```
root@OpenWIPS:~# tar -xzvf openwips-ng-0.1beta1.tar.gz
```

*Imagen 4. Descompresión del archivo openwips-ng-0.1beta1.tar.gz.*

Ahora es necesario posicionarse en la carpeta que se generó cuando se descomprimió el paquete:

```
root@OpenWIPS:~# cd openwips-ng-0.1beta1/
root@OpenWIPS:~/openwips-ng-0.1beta1#
```

*Imagen 5. Cambio al directorio openwips-ng-0.1beta1.*

Visualizar el contenido del archivo INSTALL con el siguiente comando:

```
root@OpenWIPS:~/openwips-ng-0.1beta1# more INSTALL
Requirements
------------

        Hardware
        - A wireless capable of monitor mode

        Operating system
        - Linux

        Development software (build-essential package on Debian/Ubuntu based distro):
        - gcc
        - make

        Libraries
        - Openssl development package
        - libpcap
        - libz
        - m

Compilation
-----------

make
sudo make install

Configuration
-------------

Edit the configuration file /usr/local/etc/openwips-ng/openwips-ng-server.conf

Usage
-----
openwips-ng MONITOR_MODE_INTERFACE SERVER_IP SERVER_PORT LOGIN PASS
openwips-ng-server PATH_TO_CONFIGURATION_FILE
```

*Imagen 6. Visualización del archivo INSTALL.*

Como se puede observar en el archivo INSTALL, es necesario contar con software y bibliotecas adicionales, por lo tanto se deben instalar esos requerimientos:

```
root@OpenWIPS:~/openwips-ng-0.1beta1# apt-get install gcc make openssl libpcap-dev
```

*Imagen 7. Instalación de software necesario.*

Antes de compilar OpenWIPS es necesario que se borre la bandera –Werror debido a que lo toma como un error del archivo openwips-ng-0.1beta1/common.mak y obliga a terminar la compilación cuando se encuentra un warning o alerta, la eliminación se puede hacer mediante un editor de texto:

```
$(shell chmod 755 ../evalrev)

CC                      ?= gcc
CFLAGS          ?= -O0 -g3 -pthread -Wall -Werror

prefix          = /usr/local
sbindir         = $(prefix)/sbin
bindir          = $(prefix)/bin
confdir         = $(prefix)/etc/openwips-ng/

REVISION        = $(shell ../evalrev)
REV_DEFINE      = -D REVISION=$(REVISION)
```

*Imagen 8. Archivo openwips-ng-0.1beta1/common.mak antes de la modificación.*

```
$(shell chmod 755 ../evalrev)

CC                      ?= gcc
CFLAGS          ?= -O0 -g3 -pthread -Wall -Werror

prefix          = /usr/local
sbindir         = $(prefix)/sbin
bindir          = $(prefix)/bin
confdir         = $(prefix)/etc/openwips-ng/

REVISION        = $(shell ../evalrev)
REV_DEFINE      = -D REVISION=$(REVISION)
```

*Imagen 9. Archivo openwips-ng-0.1beta1/common.mak después de la modificación.*

Para compilar e instalar OpenWIPS se ejecuta lo siguiente:

```
root@OpenWIPS:~/openwips-ng-0.1beta1# make && make install
```

*Imagen 10. Compilación e instalación de OpenWIPST.*

Antes de configurar OpenWIPS, se recomienda instalar la suite Aircrack-ng para contar con herramientas complementarias de auditoría en redes inalámbricas. Descargar Aircrack-ng de la siguiente manera:

```
root@OpenWIPS:~/openwips-ng-0.1beta1# wget http://download.aircrack-ng.org/aircrack-ng-1.2
-beta1.tar.gz
--2014-03-13 20:17:20--  http://download.aircrack-ng.org/aircrack-ng-1.2-beta1.tar.gz
Resolviendo download.aircrack-ng.org (download.aircrack-ng.org)... 87.98.255.2, 2001:41d0:
1:1b00:87:98:255:2
Conectando con download.aircrack-ng.org (download.aircrack-ng.org)[87.98.255.2]:80... cone
ctado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 3457757 (3.3M) [application/x-gzip]
Grabando a: “aircrack-ng-1.2-beta1.tar.gz”

100%[=============================================>] 3 457 757    373K/s   en 8.5s

2014-03-13 20:17:29 (397 KB/s) - “aircrack-ng-1.2-beta1.tar.gz” guardado [3457757/3457757]
```

*Imagen 11. Descarga de Aircrack-ng.*

Para descomprimir y desempaquetar el archivo aircrack-ng-1.2-beta1.tar.gz se utiliza el siguiente comando:

```
root@OpenWIPS:~/openwips-ng-0.1beta1# tar -zxvf aircrack-ng-1.2-beta1.tar.gz
```

*Imagen 12. Descompresión del archivo aircrack-ng-1.2-beta1.tar.gz.*

Ubicarse en el directorio generado después del paso anterior:

```
root@OpenWIPS:~/openwips-ng-0.1beta1# cd aircrack-ng-1.2-beta1/
```

*Imagen 13. Cambio al directorio openwips-ng-0.1beta1.*

Para compilar e instalar aircrack-ng se debe ejecutar lo siguiente:

```
root@OpenWIPS:~/openwips-ng-0.1beta1/aircrack-ng-1.2-beta1# make && make install
```

*Imagen 14. Compilación e instalación de aircrack-ng.*

Para configurar la tarjeta de red en modo monitor se necesita instalar *iw* (es una utilidad de configuración para dispositivos inalámbricos sucesora de *iwconfig*):

```
root@OpenWIPS:~# apt-get install iw
```

*Imagen 15. Instalación de iw.*

Para comprobar que todo funcione correctamente se debe conectar una tarjeta de red inalámbrica que pueda configurarse en modo monitor (para el desarrollo de este artículo se usó una tarjeta de la marca ALFA Network). Se puede identificar la tarjeta de red inalámbrica de la siguiente manera:

```
root@OpenWIPS:~# iwconfig
wlan0     IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.
```

*Imagen 16. Verificar la existencia de la tarjeta de red inalámbrica.*

Para conocer el *chipset* de la tarjeta de red inalámbrica se utiliza el comando airmon-ng:

```
root@OpenWIPS:~# airmon-ng

Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
```

*Imagen 17. Identificación del chipset de la tarjeta de red inalámbrica.*

Para poner la tarjeta en modo monitor se debe ejecutar lo siguiente:

```
root@OpenWIPS:~# airmon-ng start wlan0

Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
1518    ifplugd
1522    ifplugd
1544    dhclient
2417    ifplugd
Process with PID 2417 (ifplugd) is running on interface wlan0

Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)
```

*Imagen 18. Configuración de la tarjeta en modo monitor.*

Para verificar la existencia de la interfaz *mon0* se puede utilizar *iwconfig*:

```
root@OpenWIPS:~# iwconfig
wlan0     IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

mon0      IEEE 802.11bg  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

eth0      no wireless extensions.
```

*Imagen 19. Verificación de la existencia de la tarjeta en modo monitor.*

Una vez comprobado que se puede configurar en modo monitor la tarjeta de red inalámbrica (se debe tener en cuenta que fungirá como sensor), se configurará OpenWIPS para poder ejecutarlo posteriormente.

Visualizar el archivo de configuración de OpenWIPS:

```
root@OpenWIPS:~# more /usr/local/etc/openwips-ng/openwips-ng-server.conf
```

*Imagen 20. Visualización del archivo de configuración de OpenWIPS.*

Como recomendación, se debe revisar detenidamente el archivo para que se comprenda todo lo que se puede configurar. Una de las partes importantes a modificar es agregar en una nueva línea la dirección MAC del punto de acceso inalámbrico (AP) que se quiera proteger (en este caso es f4:55:9c:cc:fb:3c) y comentar las líneas que contienen *allow_bssid=group1* y *allow_client=group1*:

```
# Allowed essid/bssid/clients (first item is the name of the group)
#allow_essid=group1 ap_with space and !
#allow_bssid=group1 00:11:22:33:4455 0077:21:53:48C5
#allow_client=group1 00:11:22:33:44:56 00:11:22:33:44:57 00:11:22:33:44:58
allow_bssid=group1 f4:55:9c:cc:fb:3c
# Ignored BSSID (if group is not in the value string, then this is a generic setting)
#ignore_bssid=11:22:33:44:55:66
```

*Imagen 21. Configuración del AP que se desea proteger.*

Asegurarse de que la protección de los dispositivos del grupo 1 esté habilitada:

```
# Do we actively protect our clients and AP? Send deauth, etc
protect_devices=group1 true
#protect_devices=groupX false
```

*Imagen 22. Configuración habilitada de protección de clientes del AP.*

Otra configuración importante es especificar la bitácora que registrará los eventos ocurridos, sobre todo las alertas de seguridad, por defecto se guardan en *syslog* de Raspbian pero se configurará una ubicación diferente:

```
# Define where everything is logged. It can be a path or 'syslog' or 'none'
# By default when it is not deamonized, it will also output the messages in stdout/stderr
log facility=/root/log openwips/log
```

*Imagen 23. Configuración de la ubicación de la bitácora.*

Se pueden realizar diferentes configuraciones según las necesidades de la red inalámbrica, tales como cambiar la contraseña de acceso de los sensores, agregar clientes que se conectarán al AP, habilitar o deshabilitar complementos, entre otras, pero debido al alcance del artículo, las configuraciones realizadas anteriormente son suficientes para iniciar OpenWIPS.

Para ejecutar el servidor y comenzar a probar el funcionamiento se debe ejecutar lo siguiente:

```
root@OpenWIPS:~# openwips-ng-server /usr/local/etc/openwips-ng/openwips-ng-server.conf
```

*Imagen 24. Ejecución del servidor OpenWIPS.*

Si la instalación fue correcta, se mostrará una salida como en la siguiente imagen

```
[*] Reading configuration file </usr/local/etc/openwips-ng/openwips-ng-server.conf>.
[*] Successfully read configuration.
Thu Mar 13 23:35:01 2014 -      INFO - OpenWIPS-ng server v0.1 beta1 starting
Thu Mar 13 23:35:01 2014 -      INFO - Plugin <FromDS_ToDS_bit_check> init: FromDS/ToDS
bits Check plugin - Initialized.
Thu Mar 13 23:35:01 2014 -      INFO - Successfully loaded plugin <FromDS_ToDS_bit_check
>
Thu Mar 13 23:35:01 2014 -      INFO - Plugin <Deauth_detect> init: Deauth (directed/bro
adcast) Attack Checker plugin - Initialized.
Thu Mar 13 23:35:01 2014 -      INFO - Successfully loaded plugin <Deauth_detect>
Thu Mar 13 23:35:01 2014 -      INFO - Plugin <Check_IEs> init: IE (Information Element)
 Check plugin - Initialized.
Thu Mar 13 23:35:01 2014 -      INFO - Successfully loaded plugin <Check_IEs>
Thu Mar 13 23:35:01 2014 -      INFO - Plugin <Frame_Subtype_check> init: Frame subtype
anomaly check.
Thu Mar 13 23:35:01 2014 -      INFO - Successfully loaded plugin <Frame_Subtype_check>
Thu Mar 13 23:35:01 2014 -      INFO - Plugin <Fragmentation_detection> init: Fragmentat
ion attack detection (with 1 frame) v1.0
Thu Mar 13 23:35:01 2014 -      INFO - Successfully loaded plugin <Fragmentation_detecti
on>
Thu Mar 13 23:35:01 2014 -      INFO - Successfully loaded plugins
Thu Mar 13 23:35:01 2014 -      INFO - Successfully started packet reassembly thread
Thu Mar 13 23:35:01 2014 -      INFO - Successfully started frame analysis thread
Thu Mar 13 23:35:01 2014 -      INFO - Listening for sensors on port 9477
```

*Imagen 25. Ejecución correcta de OpenWIPS.*

Para iniciar un sensor se ejecuta lo siguiente:

```
root@OpenWIPS:~# openwips-ng mon0 127.0.0.1 9477 sensor1 sensor1
```

*Imagen 26. Ejecución del sensor.*

En donde,

*127.0.0.1* es la dirección IP del servidor OpenWIPS,
*9477* es el puerto por donde se está ofreciendo el servicio de OpenWIPS,
*sensor1:sensor1* son las credenciales para conectarse con el servidor.

La salida de la instrucción anterior se ve de la siguiente manera:

```
root@OpenWIPS:~# openwips-ng mon0 127.0.0.1 9477 sensor1 sensor1
Trying to connect to 127.0.0.1:9477
Connected to server
[*] Trying to connect to 127.0.0.1:40000
Starting monitoring on interface mon0
[*] Connected to <127.0.0.1:40000>.
```

*Imagen 27. Ejecución correcta del sensor.*

Si la ejecución del servidor y el sensor es correcta, entonces ya se tiene instalado y configurado un sistema de detección de intrusos inalámbrico, aunque las siglas de OpenWIPS hacen creer que mitiga ataques, en esta fase del proyecto sólo puede detectar algunos, la parte de contención está planeada para la siguiente versión, sin embargo, la ventaja de que sea un proyecto de código abierto es que se pueden desarrollar varios complementos que permitan crear un IPS inalámbrico.

Una vez que OpenWIPS está instalado y configurado, el sensor comenzará a monitorizar la red inalámbrica y podrá detectar ataques de desasociación de clientes y fragmentación de paquetes. Para probar el funcionamiento, puedes simular ataques contra el AP protegido y se activarán las alertas de seguridad detectadas.

**Si quieres saber más consulta:**

- El nuevo paradigma de seguridad en redes inalámbricas
- Evolución de los sistemas de detección, prevención y análisis de incidentes
- The Honeynet Project Map

## Mesografía


*Imagen 1. Definición de Raspberry Pi. Recuperado el 21 de abril de 2014, de www.raspberrypi.org*

*Imagen 2. Características de Raspbian. Recuperado el 24 de abril de 2014, de www.raspbian.org*

*Imagen 3. Descripción de OpenWIPS-ng. Recuperado el 24 de abril de 2014, de www.openwips-ng.org*

*Imagen 4-27. Capturas de pantalla autoría de UNAM-CERT. 2014*



*José Luis Sevilla Rodríguez*

Egresado de la Facultad de Ingeniería de la carrera Ingeniería en Computación por la Universidad Nacional Autónoma de México con módulo de salida en Redes y Seguridad.

Desde mayo de 2012 labora en el Área de Auditoría y Nuevas Tecnologías de la CSI/UNAM-CERT, durante 2 años se desempeñó como especialista en pentest. Actualmente es Auditor Interno y está apoyando en la actualización de requerimientos de la revisión 2005 a 2013 del estándar ISO/IEC 27001. Cuenta con las certificaciones Ethical Hacker (CEH) y Hacking Forensisc Investigator (CHFI) de EC Council.

# Ciber-seguridad para la educación *online*

Galvy Ilvey Cruz Valencia

La demanda educativa en muchos países alrededor de mundo ha provocado que la educación a distancia, o la también llamada educación *online* o *e-learning*, sea una opción para miles de estudiantes. Esta condición ha marcado la necesidad de desarrollar plataformas cada vez mejores, que respondan a procesos formativos o de aprendizaje para lograr un propósito de éxito concreto entre estos particulares usuarios.

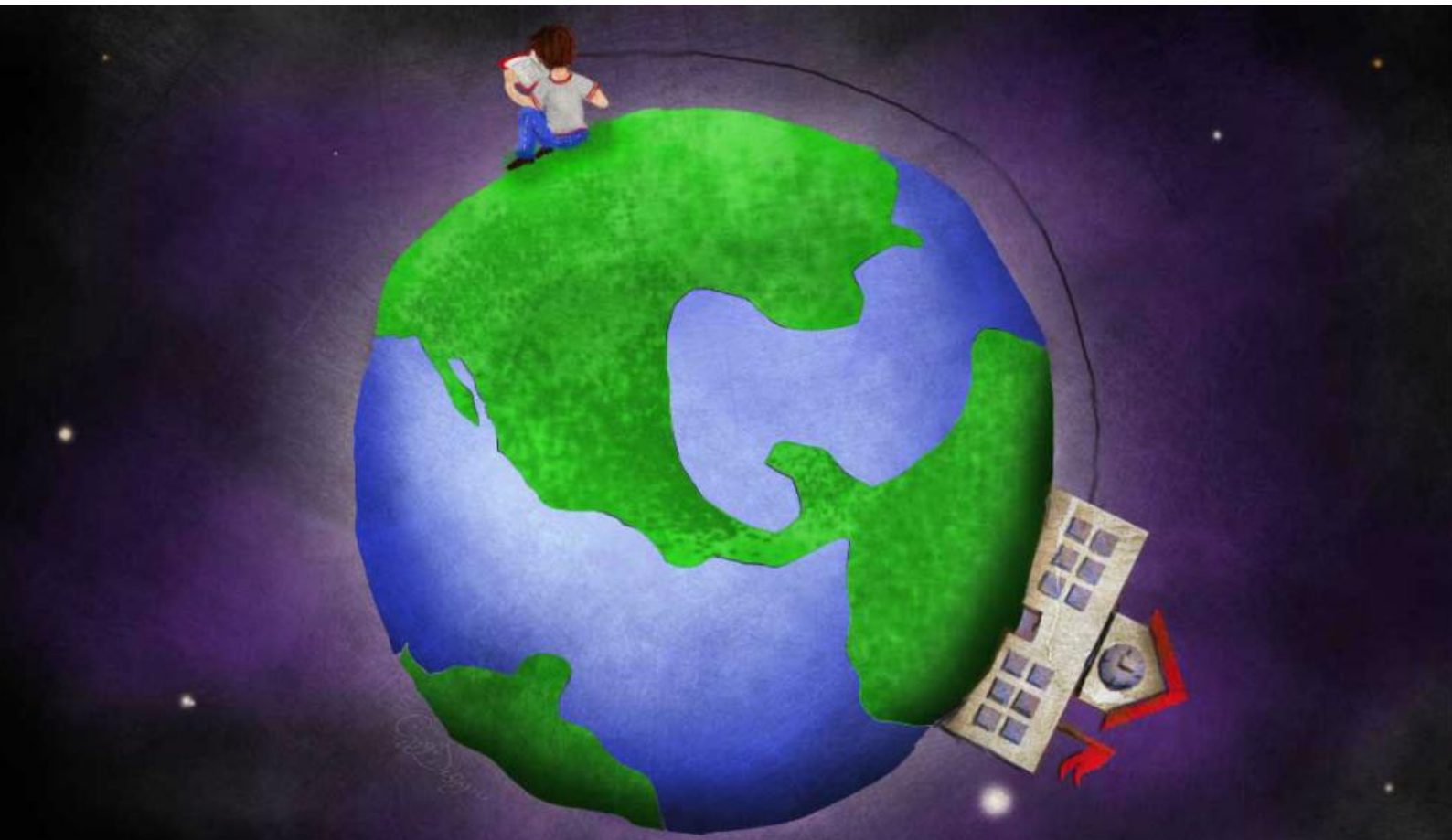
Ahora bien, si los recursos y posibilidades de estudio están dados, también es verdad que representan una oportunidad para los ataques cibernéticos. El ciberfraude y el robo de identidad, entre otros problemas de seguridad, no deben pasar por alto.

Dos analistas reconocidos en este tema específico son los académicos de la Nova Southeastearn University, Yair Levy y Michelle Ramim, quienes en 2006 publicaron el artículo *Seguridad en sistemas E-learning: Un caso de operaciones de ciberataques y administradores novatos de TI en una pequeña universidad*, el cual revela que las operaciones de ciberataques pueden darse tanto por la falta de políticas de tecnologías de información como por la ausencia de procesos para la contención de daños en las plataformas de educación en línea.

Pero, ¿qué es una plataforma *e-learning*, cómo opera y que parámetros debemos tomar en cuenta para cuidar la seguridad en ésta?

Una plataforma de este tipo consiste en un conjunto de recursos informáticos y web dispuestos para obtener conocimientos a distancia. Se basa en una serie de aplicaciones y contenidos accesibles a través de la computadora en la que forzosamente el usuario debe autenticarse para ingresar a la red.

Una vez que el usuario o participante ha ingresado a su cuenta personalizada (mediante



un usuario y contraseña comunmente), accede a *cursos* configurados a través de sesiones o módulos.

Desde esta perspectiva, sobresale que estas plataformas son capaces de desarrollar y producir conocimiento mediante un aprendizaje, si bien puede darse de manera presencial, lo es sobre todo a la distancia; y es aquí donde conviene hacer una revisión acerca de cómo es posible.

## Las plataformas paso a paso

Para revisar la arquitectura e ingeniería de las plataformas, debemos comenzar en primer término con su modelo, el cual está supeditado al dominio lógico antes que pedagógico; es decir, se trata de modelos más orientados a atraer la atención de los usuarios que a atender los problemas relacionados a escenarios pedagógicos, ya sea que estén planteados por su concepción, por su representación o por su planificación de actividades.

El segundo se refiere a las capacidades, aplicaciones y extensiones que pueden incorporar estas plataformas a fin de lograr sus objetivos pedagógicos; y más aún al interés que despiertan estos recursos informáticos para desarrollar contenidos y conocimientos que puedan dominar los usuarios, haciendo énfasis en que esto no es algo reducido, sino realmente exponencial.

El tercer aspecto a considerar acerca de estas plataformas se centra en un punto que acapara, en gran parte, la atención de este artículo: la utilización. Los problemas radican principalmente en la naturaleza convergente de disciplinas, pues pasa por el análisis de procesos de ejecución, el impacto de los contenidos, la organización de los módulos o sesiones y las acciones realizadas por los usuarios, las cuales hacen realmente la diferencia.

Si nos concentramos en caso de *Moodle*[1] sobresale el hecho de que se trata de una plataforma de características LAMP; cuyas siglas provienen, según señala Fernández [1] de la combinación de “Linux + Apache + Mysql +PHP. LAMP se ha convertido en uno de los ejes vertebrales de los servicios que pueden encontrarse en Internet”


De la descripción de Fernández sobresale un aspecto de seguridad en la configuración que no puede pasarse por alto: El servidor Apache concentra la gestión de páginas HTML; aunque vale la pena agregar que estas plataformas también pueden alojarse en sistemas Windows. Según señala Fernández, es necesario instalar una Socket Security Layer (SSL, también conocida como HTTPS) a fin de que las sesiones de los usuarios no se transfieran en modo abierto, esto sin duda nos llevará a la pregunta concreta:

## ¿Qué hacer por la seguridad de las plataformas educativas en línea?

Como todo sistema, desde el punto de vista de seguridad, las plataformas LAMP requieren evaluar aspectos internos y externos para garantizar su funcionalidad, según señalan Kouninef, Djelti y Rerbal [2].

Entre los principales criterios internos que los desarrolladores deben verificar en primera instancia, estamos frente a una plataforma con necesidades de mantenimiento, y dado que esto depende de los administradores, los usuarios están destinados a recurrir a respaldos continuos, ante la posibilidad de un “apagón”.

Plantear la seguridad de la plataforma desde un punto puramente informático, como filtros de IP que tendrán acceso al curso con autorización por medio del ingreso de credenciales (usuario/contraseña), nos llevará a no entender las posibilidades de riesgo en su totalidad.

Por ejemplo, causar una posible denegación de servicio por el número de solicitudes múltiples si no se tiene contemplado en el desarrollo la cantidad máxima de usuarios que podría soportar la plataforma. O un usuario con intenciones maliciosas que sube un archivo infectado, si éste es descargado por un usuario administrador, ¿cómo garantizar que no hay posibilidades de propagación?

Una de las posibilidades de incrementar las condiciones de seguridad es realizar, en cada uno de los lenguajes de programación utilizados, una rutina de actualización que permita lograr una evolución favorable del sistema y de su capacidad actual.

Otro aspecto interno es el relacionado con la gestión de envío de correos electrónicos a los distintos participantes en el curso *online*. Debemos garantizar, por un lado, la correcta distribución en las libretas de direcciones, y por el otro, los receptores deben verificar la autenticidad de los emisores; recordemos que hay posibilidades de enmascaramiento que podrían llevar a recibir correos falsos, limitando posibilidades de generar grupos de discusión.

Ahora revisemos los aspectos externos, los cuales podemos dividir en dos partes, aquellos que van propiamente de lado del ambiente del sistema y otro muy particular sobre el uso del sistema, lo cual involucra directamente al usuario.

En el primer caso, es preciso recordar que las plataformas funcionan en un medio y que este medio conlleva sus propios riesgos de seguridad. Por mencionar algo específico, consideremos los riesgos del navegador web y los problemas asociados a la viralidad de contenidos en aplicaciones de redes sociales como Facebook, YouTube y Twitter.

En el segundo caso, podemos evocar la extensa documentación que Levy [3] realizó en 2008, en la cual enlistó las 36 actividades que los estudiantes de plataformas e-learning consideran más valiosas durante su experiencia formativa, concluyendo que muchas de éstas podrían comprometer al sistema. Por considerar algunas:

a) Alteración de contenidos del curso
b) Distribución de contenidos maliciosos
c) Cambios no autorizados
d) Alteración de calificaciones
e) Destrucción de bases de datos
f) Robo de identidad

A esto, es necesario sumar que el entorno ofrece riesgos como:

a) El *spam*, es decir, correo basura.
b) *Phishing*, sitios falsos dedicados al robo de credenciales de acceso.
c) *Spyware*, software malicioso para recabar información del usuario e instalar publicidad molestosa sin consentimiento del usuario.
d) *Malware*, software creado con la intención de robar información o dañar la computadora.
e) Los *crackers*, expertos informáticos dedicados a intervenir los sistemas con propósitos malintencionados.

Si esto pareciera ya muy extenso, los expertos de Nova Southeastern University van más allá, en 2007 [4] ofrecieron la plática ¿Quién presenta realmente el examen?, en la cual presentaban un punto crítico, ya no sólo de la seguridad informática, sino de la seguridad de la información, arguyendo que los opositores a esta

modalidad de estudio justifican su postura respecto a la inoperatividad para autentificar al usuario que realiza las actividades y evaluaciones en las plataformas, por lo que el futuro de las plataformas pasará por las posibilidades de autentificación que hoy por hoy ofrecen las TIC, tales como la biometría; a fin de superar la mera autentificación con usuario y contraseña, como comúnmente se hace.

Finalmente, en cuanto a plataformas de e-learning se refiere, parece que la conducta ética de administradores, docentes y usuarios será determinante para la operatividad y concreción de propuestas educativas de esta naturaleza, atendiendo con sumo cuidado al hecho de que estas dinámicas están creciendo y respondiendo a necesidades educativas de un sector de la población caracterizado por su nivel educativo y adquisitivo; dos factores que se combinan en una suerte de gran atractivo para los delincuentes cibernéticos, por lo que indudablemente nos habituaremos a leer más acerca de estos temas.

**Si quieres saber más consulta:**

- Sugerencias de Seguridad para Sitios Web
- Aspectos Básicos de la Seguridad en Aplicaciones Web
- El Cifrado Web (SSL/TLS)

*[1] En palabras de Fernández, 2005, p.87: Modular Object - Oriented Dynamic Learning Environment (Entorno de Aprendizaje Dinámico Orientado a Objetos y Modular). sobresale el hecho de que se trata de una plataforma de características LAMP; cuyas siglas provienen, según señala Fernández [1] de la combinación de "Linux + Apache + Mysql +PHP. LAMP se ha convertido en uno de los ejes vertebrales de los servicios que pueden encontrarse en Internet".*

## Referencias


*[1] Fernández, J. (2005). La hora del e-aprendizaje. La plataforma educativa Moodle. Recuperado el 22 de junio de 2014, desde https://www.linux-magazine.es/issue/13/Educacion.pdf.*

*[2] Kouninef, B., Djelti, M. y Rerbal, S. (2007). Conception et réalisation d'une plate forme e-learning avec une migration au m-learning. Recuperado el 22 de junio de 2014, desde http://www.resatice.org/jour2007/communications/b-kouninef.pdf.*

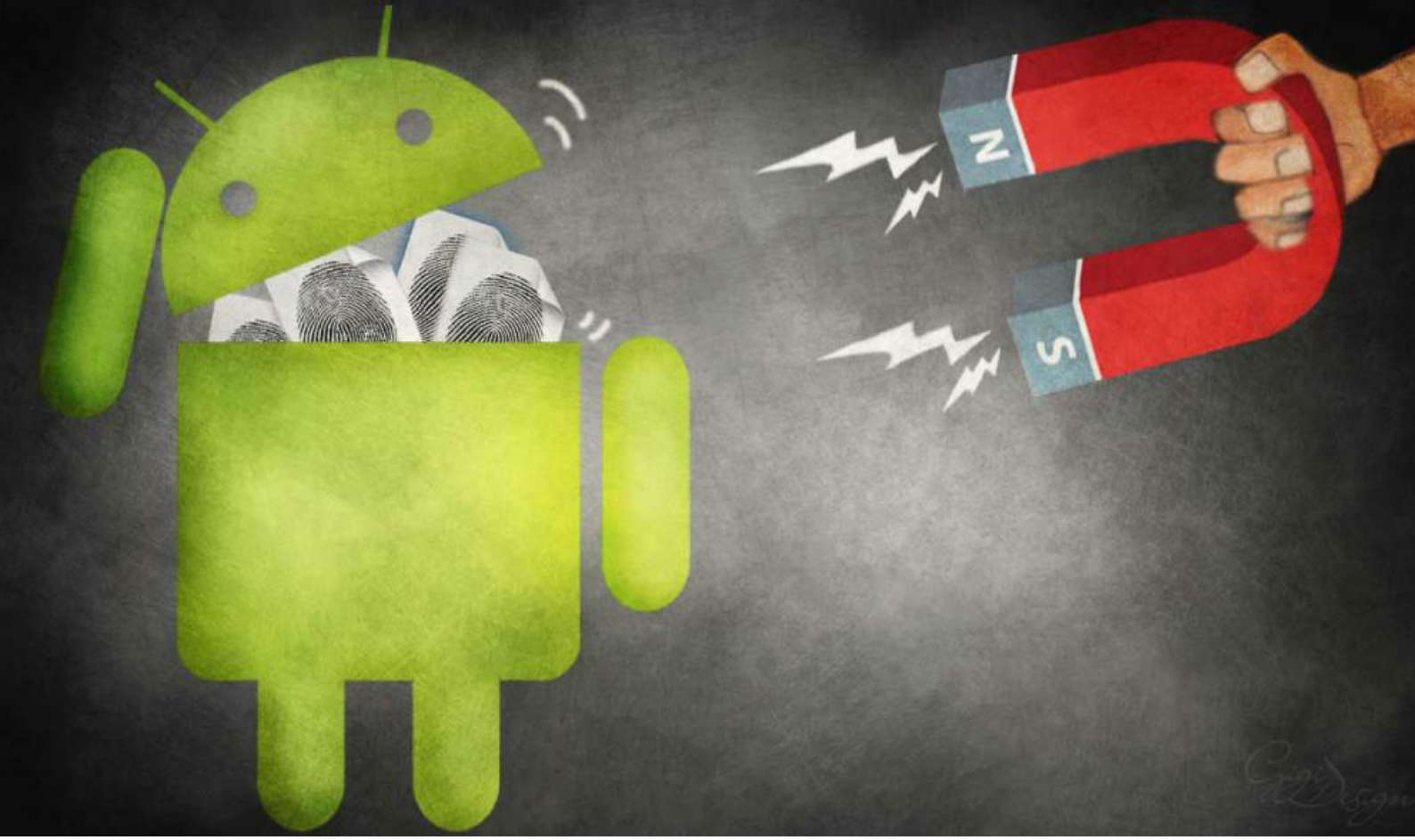
*[3] Levy, Y. & Ramim, M. (2006). Securing E-Learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University. Recuperado el 20 de junio de 2014, desde http://www.irmainternational.org/viewtitle/3187/.*

*[4] Levy, Y. & Ramim, M. (2007). Who is really taking the e-exam? What can we do about it? Nova Southeastern University, Recuperado el 20 de junio de 2014, desde http://bit.ly/1vuf4mk.*
*Levy, Y. & Ramim, M. (2009). Initial Development of a Learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM). Recuperado el 21 de junio de 2014, desde http://www.ijello.org/Volume5/IJELLOv5p379-397Levy672.pdf.14*



*Galvy Ilvey Cruz Valencia*

Licenciado en Ciencias de la Comunicación por la Facultad de Ciencias Políticas y Sociales de la UNAM. Es maestrando en Comunicación y Tecnologías Educativas por el Instituto Latinoamericano de la Comunicación Educativa, actualmente cursa el Módulo de Sistemas. Fue colaborador del UNAM-CERT como editor de su revista y hoy se desempeña como docente en CETACYS y coordinador editorial de la revista Integración360.




# Técnicas de protección de imágenes digitales capturadas con dispositivos móviles: fortalezas y debilidades

María del Rocío Sánchez Saavedra

Los dispositivos móviles, como tabletas digitales y teléfonos inteligentes, se han convertido en herramientas indispensables de uso cotidiano. Con ellos es posible realizar consultas a través de Internet, estar comunicados en todo momento gracias a las redes sociales y disfrutar de una gran cantidad de funciones multimedia, entre las que se destaca la posibilidad de capturar imágenes digitales en cualquier momento y lugar. Toda imagen capturada, desde las esporádicas fotografías artísticas hasta las populares selfies, son aunque a veces no seamos conscientes de ello, fruto de nuestra autoría. Los derechos de propiedad intelectual de dichas fotografías nos pertenecen. Esta situación no es algo que preocupe a la mayoría de los usuarios, pese a que muchos inmediatamente subimos nuestras capturas a las redes sociales o a algún sitio de Internet, donde son ampliamente vulnerables a cualquier uso que otros usuarios quieran darles.

En contraparte, existen algunos usuarios como fotógrafos, periodistas o empleados de compañías de seguros, por mencionar algunos, que dan una relevancia mayor a la protección de los derechos de autor en las imágenes que capturan. Muchos de ellos aprovechan la portabilidad, fácil acceso y alta resolución de captura de los dispositivos móviles. Además, son por excelencia, aparatos que nos acompañan en nuestro día a día y que traemos con nosotros prácticamente en cualquier momento. Sin embargo, las imágenes capturadas con estos dispositivos no cuentan con algún sistema de protección que permita validar los derechos de autor de las mismas. Una vez que ingresan a la red, no hay una manera fiable de demostrar nuestra propiedad intelectual sobre ellas.

Derivado de esta problemática, podemos encontrar algunas herramientas que pueden ser

útiles para tal fin, cada una de ellas con sus fortalezas y debilidades. En este artículo hablaremos en concreto del estado del arte existente para dispositivos móviles Android, que cuenta con cerca del 76% del mercado de teléfonos inteligentes y tabletas digitales [1-2].

| Sistema Operativo | Unidades vendidas 2013 | % | Unidades vendidas 2012 | % |
|---|---|---|---|---|
| Android | 879,681,345 | 76% | 504,962,250 | 63% |
| iOS | 221,186,059 | 19% | 191,598,832 | 24% |
| Microsoft | 34,874,702 | 3% | 18,103,135 | 2% |
| Otros | 27,468,698 | 2% | 81,792,300 | 10% |
| Total | 1,163,210,804 | 100% | 796,456,517 | 100% |

*Tabla 1. Distribución de sistemas operativos en los teléfonos inteligentes y tabletas digitales vendidos en 2012 y 2013*.

Al analizar el mercado de aplicaciones del sistema operativo Android es posible encontrar tres tipos de aplicaciones que favorecen la protección de derechos de autor en imágenes digitales: aplicaciones de marcado de agua digital, de cifrado y de ocultamiento de archivos. Revisaremos sus fortalezas y debilidades, dejando entrever que existen también técnicas que nos permiten obtener los medios digitales originales y sin protección alguna.

## Marcado de agua digital

El marcado de agua digital es una técnica que consiste en dejar un sello o huella en una imagen digital que permita su identificación o que cumpla con algún propósito específico. Podemos catalogarlas según su robustez y su perceptibilidad. Existen las marcas de agua frágiles, las semifrágiles y las robustas.

Las frágiles son sumamente fáciles de remover (se pierden con la más mínima manipulación de la imagen) y permiten validar que la imagen no haya sido modificada. Las semifrágiles cumplen la misma función e incluyen otras adicionales, como la posibilidad de recuperación de una determinada zona de la imagen (conocida como región de interés, que se almacena en otras zonas de la imagen). Esto permite recuperar una región específica de la imagen cuando ésta es modificada, evitando el uso fraudulento de dicha imagen. Finalmente están las marcas de agua robustas, las cuales son difíciles de eliminar y sirven principalmente para la protección de derechos de autor ya que generalmente son visibles, como se muestra en la imagen 1.

*Imagen 1. Imagen con una marca de agua visible.*

Entre las aplicaciones más populares que realizan este proceso se encuentran Add Watermark, iWatermark, Watermark! y Picture Watermark [3], algunas también están disponibles para otros sistemas operativos móviles, como iOS. Dichas aplicaciones permiten al usuario elegir alguna de sus imágenes para realizar el marcado, ya sea con un texto específico o con alguna otra imagen que fungirá como marca de agua.

**Fortalezas:**

- Los derechos de autor son directamente visibles en la imagen marcada.
- Las marcas de agua visibles ofrecen una gran resistencia ante ataques comunes a las marcas de agua, como lo son transformaciones geométricas (escalado, compresión, redimensionamiento), degradado de colores, aplicación de filtros, entre otros.
- Puede ser interpretada a simple vista, sin necesidad de procesos adicionales.

**Debilidades:**

- Al ser la marca de agua visible, el atacante conocerá de antemano la ubicación de la misma, por lo que puede hacer uso de aplicaciones de edición de imágenes para removerla manualmente, aunque esto representa bastante esfuerzo, tiempo y generalmente degradación de la imagen.
- Al realizarse la inserción de la marca de agua en un proceso posterior a la captura de la imagen,

es posible utilizar técnicas de recuperación de datos (muy utilizadas en la informática forense) para obtener la imagen original sin la marca de agua. Las aplicaciones existentes agregan la marca de agua en una copia de la imagen, el usuario puede eliminar la imagen original haciéndola vulnerable a las técnicas de recuperación (aunque esto requiere tener acceso al dispositivo de manera física y permisos de súper usuario).

## Cifrado

La criptografía constituye una disciplina de seguridad de la información cuyo objetivo es realizar, a partir de un proceso de cifrado, la conversión de un mensaje en caracteres completamente ininteligibles para aquellas personas o entidades que no tengan las credenciales necesarias para regresarlo a su estado normal. Entre las aplicaciones de Android que realizan dicho proceso encontramos a SSE - Universal Encryption, Encryption Manager y File encryption + [4], entre otras. Estas aplicaciones soportan una gran cantidad de algoritmos de cifrado y por lo general crean un nuevo archivo que contendrá los datos cifrados con la contraseña establecida por el usuario, respetando el archivo original.

**Fortalezas:**

- Al ser ininteligible, el medio es menos susceptible a que se le dé un uso indebido.
- Sólo podrá visualizar el contenido aquella persona que posea las credenciales necesarias para hacerlo.
- No puede ser publicado en redes sociales en su estado cifrado.

**Debilidades:**

- Aunque el cifrado protege el archivo, realmente no funciona como un mecanismo para validar los derechos de autor de una imagen, especialmente cuando ésta es descifrada.
- Una vez que un usuario obtiene las credenciales para descifrar el archivo (ya sea por criptoanálisis o cualquier otro método), la imagen queda completamente vulnerable a cualquier uso.
- Al crearse el nuevo archivo cifrado, es posible recuperar la imagen original a través de técnicas de recuperación de datos.

## Ocultamiento de archivos

Otra alternativa que se ha vuelto sumamente popular consiste en aplicaciones que funcionan como una caja fuerte, permitiendo al usuario elegir qué archivos desea ocultar dentro de su dispositivo.

Para entender su funcionamiento, hay que decir que Android está basado en un *kernel* de Linux, por lo que hereda el concepto de usuarios y grupos y lo ajusta al manejo de aplicaciones para determinar permisos. Las aplicaciones adquieren un identificador único para trabajar dentro de una sandbox en la cual puede ejecutarse, contando entre otras cosas, con un espacio de almacenamiento de archivos exclusivo al cual sólo es posible acceder con las credenciales de la misma aplicación o con permisos de súper usuario (*root*). Las aplicaciones de ocultamiento de archivos aprovechan este espacio de tal manera que sólo ellas puedan acceder a los archivos que se localizan allí, permitiendo al usuario elegir qué

archivos desea mantener ocultos para posteriormente hacer un proceso de segmentación del mismo y, en algunos casos, agregar alguna protección criptográfica. Entre las aplicaciones disponibles en el mercado de Google Play podemos encontrar a Hide pictures, Gallery Lock, Hide Pictures in Vaulty y Hide It Pro [5].

**Fortalezas:**

- Esconde los archivos de accesos no autorizados, especialmente cuando un tercero consigue acceso físico al dispositivo.

**Debilidades:**

- Es posible obtener permisos de súper usuario en los dispositivos a través de la explotación de algunas vulnerabilidades de Android, lo que permitiría al usuario acceder a cualquier directorio del sistema operativo y obtener los archivos protegidos.
- Una vez obtenido el archivo, no hay manera de validar la propiedad intelectual.
- Al igual que las anteriores, las técnicas de recuperación de archivos nos permitirán realizar un escaneo de la unidad de almacenamiento y encontrar el archivo original sin protección.

La gran variedad de apps existentes en este mercado, así como la cantidad de descargas correspondientes a cada una [3-5], nos permite inferir que este tipo de aplicaciones tienen una demanda interesante, reflejo de que existe una cantidad considerable de usuarios interesados en la protección de los medios digitales capturados desde sus dispositivos.

Las aplicaciones presentadas comparten la debilidad de ser vulnerables ante técnicas de recuperación de datos con el fin de obtener la imagen original. Siempre que el archivo sea procesado, existirá la posibilidad de obtener la primera versión del mismo a través del análisis de las unidades de almacenamiento, aun cuando sea necesario tener acceso físico al dispositivo y se requieran permisos de súper usuario para ello.

Actualmente en Google Play no existe un sistema de protección para las personas interesadas en preservar la propiedad intelectual sobre sus imágenes que sea confiable. Sin embargo, cabe destacar que el mercado de aplicaciones para Android es muy vasto y se encuentra constantemente ampliando su catálogo, por lo que tampoco podemos descartar del todo la posibilidad de encontrar alguna opción que considere esta problemática. Mientras tanto, el uso de varias de estas aplicaciones puede ayudar a completar el sistema de seguridad para ofrecer una mejor protección de las imágenes digitales.

**Si quieres saber más consulta:**

- Copyright prevent copy: Protocolo BPS
- Reputación en línea
- Dispositivos Móviles

## Referencias


*[1] Gartner. Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013. Recuperado el 27 de junio de 2014. Disponible: http://www.gartner.com/newsroom/id/2665715*

*[2] Gartner. Gartner Says Worldwide Tablet Sales Grew 68 Percent in 2013, With Android Capturing 62 Percent of the Market. Recuperado el 27 de mayo de 2014. http://www.gartner.com/newsroom/id/2674215*

*[3] Google Play. Watermark – Google Play. Recuperado el 28 de mayo de 2014. Disponible: https://play.google.com/store/search?q=watermark&c=apps*

*[4] Google Play. Cryptography – Google Play. Recuperado el 28 de mayo de 2014. Disponible: https://play.google.com/store/search?q=cryptography&c=apps*

*[5] Google Play. Vault – Google Play. Recuperado el 28 de mayo de 2014. Disponible: https://play.google.com/store/search?q=vault&c=apps.*

*Héctor Santoyo García*

Es egresado de la Universidad De La Salle Bajío de la carrera de Ingeniería en Tecnologías de la Información, obtuvo su título el 5 de noviembre de 2010.

Recibió el grado de Maestro en Ingeniería en Seguridad y Tecnologías de la Información el 10 de enero de 2014 por parte del Instituto Politécnico Nacional.

Ha trabajo con tecnologías web desde el año 2008, especializándose en la seguridad web.

Actualmente es aspirante de ingreso al Doctorado en Comunicaciones y Electrónica en la Sección de Estudios de Postgrado e Investigación de la Escuela Superior de Ingeniería Mecánica y Eléctrica Culhuacán del Instituto Politécnico Nacional.


DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN


Revista .Seguridad Cultura de prevención para TI
No.22 / agosto-septiembre 2014 ISSN: 1251478, 1251477