PLAN DE SEGURIDAD DE LA SOLUCIÓN
YO CUIDO LO PUBLICO ADMINISTRADOR SOLUCIONES MÓVILES 4
PROYECTO FÁBRICA DE SOFTWARE GRUPO 2

Soluciones y Servicios Tecnológicos
Dirección de Gobierno en línea

Bogotá, D.C, abril del 2014

FORMATO PRELIMINAR AL DOCUMENTO

Título:	**PLAN DE SEGURIDAD DE LA SOLUCIÓN**				
Fecha elaboración aaaa-mm-dd:	2014-02-25				
Sumario:	Plan de seguridad para la aplicación Yo Cuido Lo Público Administrador enmarcadas dentro del proyecto Soluciones Móviles 4.				
Palabras Claves:	Seguridad, confidencialidad				
Formato:	DOC		Lenguaje:		Español
Dependencia:	Ministerio de Tecnologías de la Información y las Comunicaciones: Dirección Gobierno en línea - Soluciones y Servicios Tecnológicos.				
Código:	GLFS2-SM4-PSS	Versión:	2.0	Estado:	Aprobado
Categoría:					
Autor (es):	Cristina Cortes Líder Técnico UT Software Works		Firmas:		
Revisó:	Mónica Monroy Gómez Consultor Procedimientos y Herramientas de Interventoría Consorcio S&M Jorge Santiago Moreno Dirección de Gobierno en línea Luisa Fernanda Medina. Dirección de Gobierno en línea Fernando Segura Asesor Secretaría de Transparencia				
Aprobó:	Luis Felipe Galeano Arquitecto IT Consorcio S&M Rafael Londoño Dirección Gobierno en línea				
Información Adicional:	No disponible				
Ubicación:	El archivo magnético asociado al documento está localizado en el repositorio de la solución 24 – SOLUCIONES MOVILES 4 en la siguiente ruta: 03. Fase de Ejecucion/02. Diseno/06. Plan de seguridad de la solución.				

CONTROL DE CAMBIOS

VERSIÓN	FECHA	No. SOLICITUD	RESPONSABLE	DESCRIPCIÓN
1.0	2014-02-25	No aplica	UT Software Works	Creación del documento
1.1	2014-04-07	No aplica	UT Software Works	Ajustes solicitados por interventoría, GEL y Entidad
2.0	2014-04-24	No aplica	UT Software Works	Aprobación del documento

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

DERECHOS DE AUTOR

CRÉDITOS

En un trabajo conjunto entre los consultores dela Dirección Gobierno en línea– Secretaría de Transparencia, las firmas Consorcio S&M y la UT Software Works, se ha generado el presente documento siguiendo los estándares establecidos por la Dirección de Gobierno en Línea, para el proyecto **IMPLEMENTACIÓN DE SOLUCIONES TECNOLÓGICAS BAJO EL MODELO DE FÁBRICA DE SOFTWARE PARA LAS INICIATIVAS DEL PLAN VIVE DIGITAL A CARGO DEL PROGRAMA AGENDA DE CONECTIVIDADY LA EVOLUCIÓN DE LAS SOLUCIONES QUE SOPORTAN LA ESTRATEGIA DE GOBIERNO EN LÍNEA GRUPO 2.**

Este documento fue revisado y aprobado por los consultores y profesionales dela Dirección de Gobierno en línea, previa validación de la empresa interventora del contrato Consorcio S&M.

1. AUDIENCIA

Este documento está dirigido a los integrantes de los equipos de la Dirección de Gobierno en línea, Secretaría de Transparencia, el Consorcio S&M y la Unión Temporal UT Software Works que participan en el proyecto Soluciones Móviles 4. Este documento es aplicable a la solución Yo Cuido Lo Publico Administrador el cuál debe ser conocido por los miembros de los equipos del proyecto: **IMPLEMENTACIÓN DE SOLUCIONES TECNOLÓGICAS BAJO EL MODELO DE FÁBRICA DE SOFTWARE PARA LAS INICIATIVAS DEL PLAN VIVE DIGITAL A CARGO DEL PROGRAMA AGENDA DE CONECTIVIDAD Y LA EVOLUCIÓN DE LAS SOLUCIONES QUE SOPORTAN LA ESTRATEGIA DE GOBIERNO EN LÍNEA GRUPO 2.**

2. INTRODUCCIÓN

El presente documento, busca describir el trabajo concertado de planificación de componentes de seguridad de la información, dentro de la arquitectura de la solución, describiendo los diferentes controles a implementar en las soluciones, que permitan mitigar los riesgos identificados en las mismas, la identificación de riesgos se hace basado en criterios determinados en el marco del proyecto OWASP. El documento, presenta una descripción clara de cada uno de estos controles y los principios de seguridad de la información que se busca proteger con la implementación de cada uno de ellos.

3. CARACTERIZACIÓN DEL SISTEMA

El objeto de esta sección es determinar las características del sistema que son relevantes para la seguridad de la información y no para la seguridad de la organización.

3.1 NOMBRE DEL SISTEMA

El nombre designado para el proyecto es Yo Cuido Lo Público.

3.2 TIPO DE SISTEMA

Yo Cuido Lo Publico es una aplicación WEB que corre bajo IIS (Internet Information Server) con S.O Windows Server 2008, los servicios web corren bajo Apache Tomcat 7.0.

3.3 ESTADO ACTUAL DEL SISTEMA

La aplicación se encuentra en su etapa de implementación, para esta etapa se encuentran definidos todos sus componentes de arquitectura, requerimientos funcionales y no funcionales.

3.4 DESCRIPCIÓN GENERAL DE LA APLICACIÓN

Corresponde a una aplicación especialmente diseñadas para cumplir las necesidades de una entidad del gobierno, con requerimientos funcionales específicos. La aplicación de administrador web se ha diseñado para su desarrollo con lenguaje C# que utiliza el framework 4.5 de Microsoft y la de los servicios con lenguaje Java que utiliza JDK 6.

3.5 ENTORNO DEL SISTEMA

A continuación se presenta el diagrama de los componentes mayores de las aplicaciones contenidas dentro del proyecto, en los que se evidencia su integración con el exterior, otros sistemas y los usuarios. Igualmente se evidencia el entorno de red e infraestructura sobre el cual se tiene diseñado para la aplicación.

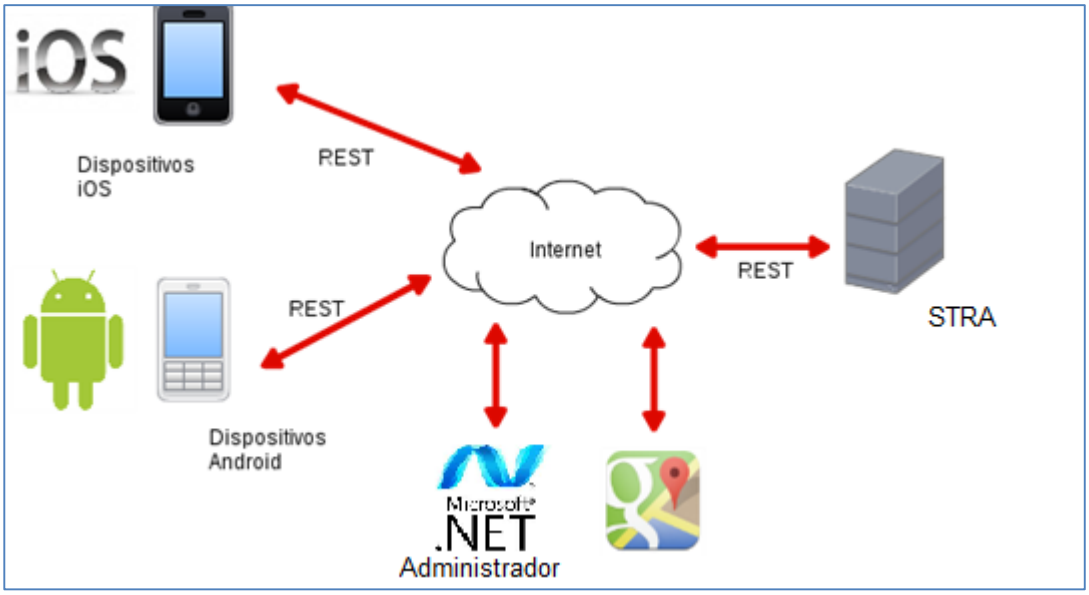

Figura 1. Componentes Básicos

3.6 INTERCAMBIO DE INFORMACIÓN DEL SISTEMA

Las interfaces de interoperabilidad fueron definidas de la siguiente manera:

La Secretaría de Transparencia expondrá Web Services, con la información específica necesaria para prestar la funcionalidad de las aplicaciones, el consumo de servicios Web, se realizará de manera controlada, solamente por las aplicaciones diseñadas, bajo un sistema de autenticación y autorización establecido en las peticiones generadas a los Web Services, desde las aplicaciones móviles desarrolladas para Android e iOS

3.7 PERFIL DE USUARIOS

La aplicación de administración contará con los usuarios gestores, los cuales son los encargados de revisar la información enviada por la ciudadanía y los perfiles de usuarios administradores para la aplicación, que tendrás la posibilidad de revisar y modificar los diferentes componentes propios de la aplicación.

4. ESTRATEGIA DE CUMPLIMIENTO DE PRINCIPIOS DE SEGURIDAD

La definición de la estrategia de seguridad para esta solución Yo Cuido Lo Publico Web la cual es una aplicación que administra información, se realiza basada en el análisis de la información que envían los diferentes componentes de la solución, en estos casos se busca asegurar componentes como autenticación que dan la oportunidad de administrar información mediante consultas y actualizaciones; teniendo en cuenta estos componentes de administración, se busca generar controles que permitan la confidencialidad, integridad y disponibilidad de la información, y que sean requerimientos necesarios en la programación de la presente aplicación.

4.1 AUTENTICACIÓN

Es necesario dentro de la seguridad de la aplicación, realizar un proceso de autenticación dentro de la misma, que permita la identificación de usuarios que tienen la posibilidad de acceder al sistema, en búsqueda de las denuncias generadas por los usuarios, el cuál asegure la identificación de cada uno de los usuarios en la plataforma.

El formulario de autenticación para la aplicación se debe encontrar restringido para su acceso desde las oficinas de la Secretaria de Transparencia de la Presidencia de la República y su acceso debe estar protegido a nivel de transporte.

El esquema de autenticación debe incluir una política, de uso de contraseñas complejas para la protección de las cuentas de gestores y administradores de la aplicación. Dicha política, basada en mejores prácticas o en el SGSI de la información de la entidad, debe ser establecida en el software y debe ser usado de manera obligatoria por los diferentes usuarios de la aplicación.

Se deben establecer tiempos máximos de validez de las sesiones, relacionados a los tiempos de revisión de los casos que soportados por la aplicación de Yo Cuido Lo Público, la autenticación de cada usuario que acceda a la plataforma de autenticación debe tener un tiempo máximo de validez no superior a ocho (8) horas.

4.2 AUTORIZACIÓN

La definición de controles a nivel de autorización, buscan que solamente usuarios que hayan comprobado su identidad, mediante el proceso de autenticación puedan hacer uso de la aplicación.

La autorización dentro del esquema de protección de la aplicación de administración se encuentra enfocada en las actividades que se encuentran permitidas para cada uno de los roles determinados.

Los usuarios gestores, solamente deben tener acceso a la comprobación y aceptación de las denuncias generadas por los ciudadanos, no deben poder generar actividades adicionales en la aplicación de administración.

Los usuarios administradores, deben poder acceder a la aplicación con los más altos privilegios, pudiendo realizar correcciones a la plataforma de denuncias, adicionalmente deben poder realizar la creación de nuevos usuarios en la plataforma y determinar los perfiles de los mismos. El usuario administrador debe tener la posibilidad de realizar tareas de mantenimiento de la plataforma, sin realizar modificaciones a los datos enviados por los ciudadanos.

4.3 AUDITORIA

El acceso de los usuarios dentro de la aplicación de administración, debe ser controlado desde el momento de su ingreso, hasta el momento de desconexión de la sesión en la aplicación. Cada una de las actividades realizadas debe ser guardada en un archivo que no pueda ser modificado por ningún usuario de la plataforma. Dentro del log, la información que debe ser registrada se resume a la siguiente:

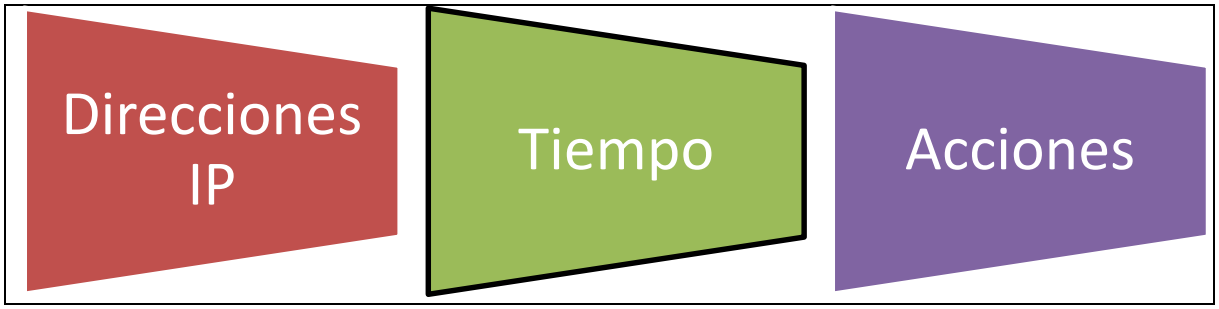

Figura 2. Auditoría

4.4 CONFIDENCIALIDAD

4.4.1 PROTECCIÓN DE DATOS ALMACENADOS

Los archivos de auditoría de la aplicación se deben proteger en almacenamiento, de cualquier modificación que puedan sufrir. El esquema de protección debe ir enfocado al cifrado de los mismos, el acceso a esta información se debe encontrar restringido y se recomienda el cálculo de un hash diario, que permita determinar cualquier posible cambio que exista fuera de horas de operación de la plataforma.

Es necesario asegurar un hash de los datos enviados originalmente por los ciudadanos, el cual resida en la aplicación y sea solamente verificable por el administrador de la misma.

4.4.2 PROTECCIÓN DE DATOS EN TRÁNSITO

En el esquema de seguridad para las credenciales de autenticación, es necesaria la definición de un mecanismo de protección a nivel de transporte, para la solución se ha establecido el uso de TLS.

Este esquema requiere de un certificado digital para que el servidor web pueda utilizar el protocolo seguro “https” y el puerto que generalmente se usa es “443”, con lo cual las aplicaciones que residan en dicho servidor web puedan asegurar las credenciales de autenticación. Con este tipo de certificado se asegura la información del sitio y se evita el riesgo de phishing[1], generando el máximo nivel de confianza y reconocimiento. Estos tipos de certificados son provistos por entidades de certificación autorizada por la Superintendencia de Industria y Comercio, como lo es Certicamara; para el caso específico de la aplicación el certificado debe ser provisto por la Secretaría de Transparencia o Gobierno en Línea.

TLS además de sus características propias de cifrado del canal, por medio de la generación de un túnel, ofrece características adicionales de seguridad dentro del túnel, entre las que sobresalen.

- Firmado de archivos para transmisión
- Comprobación de integridad de la información transmitida dentro del túnel

El establecimiento de TLS se realiza basado en el siguiente procedimiento.

[1] http://es.wikipedia.org/wiki/Phishing

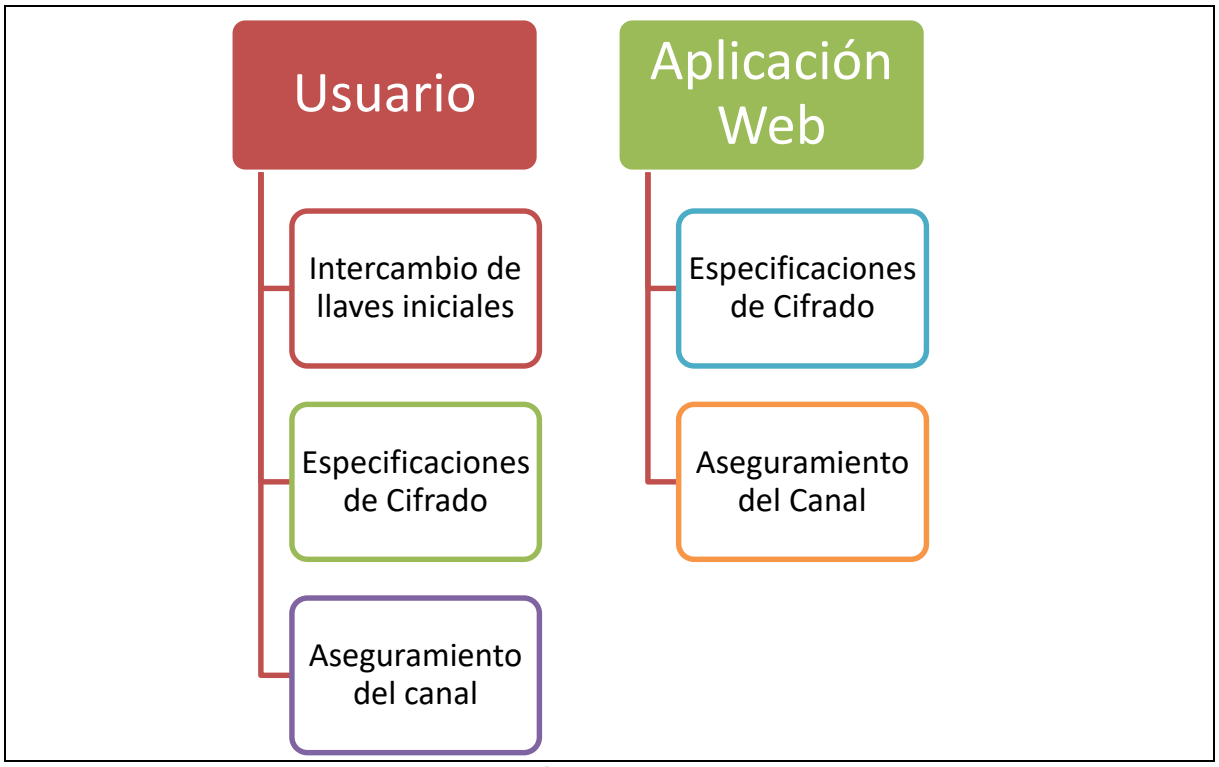

Figura 3. TLS

El intercambio de llaves se produce de manera segura y las especificaciones de cifrado se utilizan para la optimización del canal, frente a las necesidades propias de la comunicación, finalmente el aseguramiento del canal se realiza estableciendo el túnel por donde se transmiten los datos, la información sensible definida en la aplicación se transmite de manera segura, con el fin de proteger la confidencialidad e integridad de la misma.

En la figura se muestra el establecimiento de una sesión TLS normal, en primera instancia se realizar un intercambio de llaves entre el servidor y el cliente basado en información enviada por el servidor, posteriormente se establecen las especificaciones de cifrado en ambas partes, con la cual se genera el aseguramiento del canal por medio de un túnel cifrado.

4.5 INTEGRIDAD

Se debe asegurar por medio del cálculo de hashes, que ninguno de los archivos de los ciudadanos sea modificados por parte de los gestores o administradores de la aplicación de administración, también es necesario el cálculo de hashes de los archivos de logs de manera diaria, con el fin de realizar una comprobación de su estado a nivel de integridad.

4.6 DISPONIBILIDAD

Los mecanismos de disponibilidad, deben encontrase dispuestos en los servicios, que son los que ofrecerán la funcionalidad final a las aplicaciones enmarcadas en el proyecto. Los controles a nivel de disponibilidad de los servicios, deben ser planeados en soluciones de alta disponibilidad y balanceo de carga para las aplicaciones que, en funcionamiento, demuestren mayor consumo, la protección desde el diseño propuesto, se encuentra enfocado a que el consumo solamente podrá ser realizado por los usuarios que se encuentren autenticados, dentro de los mecanismos de control, descritos para este fin.

5. MATRIZ DE IDENTIFICACIÓN DE DEBILIDADES DE SEGURIDAD

El objeto de esta sección es evaluar de acuerdo a la tipología de vulnerabilidades, qué problemas (si aplica) puede tener la aplicación, así como definir si existe alguna estrategia técnica establecida en la solución para poder mitigar cada uno de los tipos de vulnerabilidades.

Tabla 1. Tipología de Vulnerabilidades

DESCRIPCIÓN	CATEGORÍA	PROBLEMAS POTENCIALES	SE CONTROLARÁ SI/NO
Autenticación	"¿Quién eres tú?". La autenticación es el proceso en el que una entidad demuestra la identidad de otra persona, típicamente a través de credenciales, tal como un nombre de usuario y contraseña.	Comprobación de usuarios que puedan acceder a la aplicación	SI. Autenticación a la aplicación por medio de nombres de usuario y contraseñas
Autorización	"¿Qué se puede hacer?". La autorización es cómo la aplicación proporciona controles de acceso a los recursos y operaciones.	Definición de alcance de cada rol	SI. Definición de roles.
Auditoria	Los datos sensibles se refieren a la forma en que su aplicación se encarga de todos los datos que deben ser protegidos, ya sea en la memoria, sobre el canal, o en almacenes persistentes.	Modificación de archivos de auditoría.	SI. Calculo de hashes y acceso restringido a dichos archivos.
Auditoría y registro	¿Quién hizo qué y cuándo? La Auditoría y registro se refiere a cómo las aplicaciones registran los acontecimientos relacionados con la seguridad.	Determinación de elementos que deben ser tenidos en cuenta dentro de la generación de logs	SI. Definición de componentes como dirección IP, timestamp y petición generada al web service.

6. TERMINOLOGÍA

AES: AdvancesEncryptionStandards, es una especificación para cifrado de datos electrónicos establecida por el Instituto Nacional de Estados Unidos de Estándares y Tecnología (NIST).

Android: Sistema Operativo diseñado para dispositivos móviles desarrollado por AndroidInc, bajo el apoyo de Google.

C#: es un lenguaje de programación orientado a objetos desarrollado y estandarizado por Microsoft como parte de su plataforma .NET, que después fue aprobado como un estándar por la ECMA (ECMA-334) e ISO (ISO/IEC 23270). C# es uno de los lenguajes de programación diseñados para la infraestructura de lenguaje común.

Cache: Es un componente que de manera transparente, almacena información para que en operaciones posteriores pueda ser obtenida de manera más eficiente.

Cookies: Son una pequeña pieza de información enviada por un sitio o aplicación, las cuales son almacenadas en una ubicación predeterminada, permitiendo que el sitio o la aplicación puedan acceder a ellas para determinar información específica del sistema.

Cross Site Scripting: Se refiere a un ataque que permite la manipulación de funciones en la aplicación, generando la ejecución de sentencias que no se encuentran dentro de la programación original de la aplicación.

FRAMEWORK .NET: es un framework de Microsoft que hace un énfasis en la transparencia de redes, con independencia de plataforma de hardware y que permita un rápido desarrollo de aplicaciones. Basado en ella, la empresa intenta desarrollar una estrategia horizontal que integre todos sus productos, desde el sistema operativo hasta las herramientas de mercado.

HMAC: Hash MessageAuthenticationCode: Es un código que me permite la comprobación de las peticiones realizadas a un servicio o aplicación web.

IMEI: International Mobile StationEquipmentIdentify: Es un número especialmente diseñado para identificar estaciones móviles.

Inyección: Método de ataque en el cual se intenta introducir contenido no permitido a una aplicación o sistema.

IIS: es un servidor web y un conjunto de servicios para el sistema operativo Microsoft Windows.

iOS: Sistema operativo usado en los teléfonos Apple.

Java: Es un lenguaje de programación de propósito general, concurrente, orientado a objetos y basado en clases que fue diseñado específicamente para tener tan pocas dependencias de implementación como fuera posible.

JDK: Java Development Kit o (JDK), es un software que provee herramientas de desarrollo para la creación de programas en Java. Puede instalarse en una computadora local o en una unidad de red.

OWASP: Open Web Application Security Project

SecureRandom: Clase de Java la cual genera números pseudo-aleatorios criptográficamente seguros

Sistema de Archivos: Son las estructuras de información guardad, que se definen en los dispositivos de almacenamiento, para su acceso y procesamiento.

Timestamp: Mecanismo de firmado de tiempo para peticiones y respuestas generadas desde diferentes fuentes

TLS: TransportLayerSecure: Es un protocolo criptográfico que permite el cifrado de canales inseguros para transmisión de datos.

Token de autenticación: Es la representación de una credencial de autenticación, que puede estar descrita dentro de diferentes componentes o archivos.

Tomcat: Apache funciona como un contenedor de servlets desarrollado bajo el proyecto Jakarta en la Apache Software Foundation. Tomcat implementa las especificaciones de los servlets y de JavaServerPages (JSP) de Sun Microsystems.

UDID: UniqueDeviceIdentifier: Es una cadena de cuarenta (40) caracteres de longitud asignada a ciertos dispositivos Apple, incluyendo el iPad, iPhone y iPod.