# Como asegurar el canal de transmisión de los datos

Por: Andrés Felipe Diaz G.

Proyecto aplicado en TIC[[1]](#footnote-1)

Universidad Pontificia Bolivariana

Medellín

2020

Índice

[Como asegurar el canal de transmisión de los datos 1](#_Toc39081374)

[Resumen 3](#_Toc39081375)

[Objetivos 4](#_Toc39081376)

[Objetivo general 4](#_Toc39081377)

[Objetivos específicos 4](#_Toc39081378)

[Android Developers 5](#_Toc39081379)

[Certificado SSL 6](#_Toc39081380)

[Creación del certificado auto firmado 6](#_Toc39081381)

[Cibergrafía 9](#_Toc39081382)

# Resumen

En este documento expondremos ideas acerca de cómo podemos resolver el tema de un canal seguro de una forma completamente diferente a la que implementamos en el proyecto educativo EduApps[[2]](#footnote-2).

# Objetivos

## Objetivo general

* El objetivo de este documento no es menos que el de informar diferentes vías que pudimos haber tomado como equipo a la hora de asegurar nuestro canal de transmisión de datos.

## Objetivos específicos

* Profundizar en el área de seguridad móvil enfocándonos, en primera medida, en asegurar la integridad de los datos en el momento en que viajan a través de la red
* Documentar brevemente las diferentes soluciones encontradas a la necesidad que teníamos.

# Android Developers

Android en todas sus versiones tiene cierto “tips”[[3]](#footnote-3) de seguridad que harán que sus aplicaciones sean más seguras y que se implementan al momento de desarrollar.

Las siguientes especificaciones de seguridad te ayudaran a ello:

* La aplicación de Android, SandBox, la cual aísla los datos y el código de tu aplicación de otras aplicaciones
* Un framework de aplicación con gran cantidad de implementaciones de funcionalidades de seguridad comunes tales como criptografía, permisos, y un IPC seguro
* Tecnologías como ASLR[[4]](#footnote-4), NX[[5]](#footnote-5), ProPolice[[6]](#footnote-6), safe\_iop[[7]](#footnote-7), OpenBSD[[8]](#footnote-8) dlmalloc, OpenBSD calloc, y Linux mmap\_min\_addr[[9]](#footnote-9) para mitigar el riesgo asociado a problemas de manejo de memoria comunes.
* Un sistema de cifrado de archivos que puede ser activado para proteger datos en dispositivos perdidos o robados.
* Permisos suministrados por el usuario que restringen el acceso a especificaciones y datos de usuario.
* Permisos definidos por la aplicación para controlar los datos en cada aplicación.

Estas recomendaciones vienen seguidas de una basta cantidad de contenido sobre implementación en Android (excepto los programas anteriormente mencionados, esos son externos) que será adjuntada como link bibliográfico

# Certificado SSL

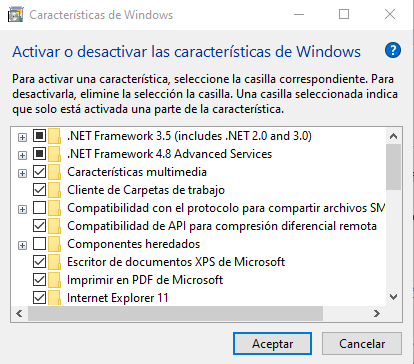
La otra forma, la forma que implementamos, es esta. Al momento de terminar con la implementación de FTPS en el servidor, nos dimos cuenta de que el flujo de datos hacia conexión mediante un registro HTTP; pero no quedamos convencidos con el resultado, por lo que buscamos formas de volver ese registro un HTTPS y decidimos crear un certificado auto firmado de tipo HTTPS.

## Creación del certificado auto firmado

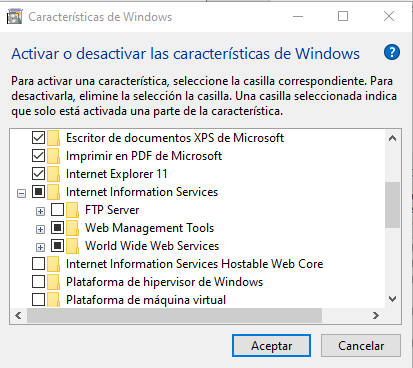
Primero debemos activar el complemento IIS (Internet information Services), para eso solo hay que seguir estas instrucciones:

1. Abrir “Panel de control”
2. Ir a “Programas”
3. Buscar la opción de “Activar o desactivar características de Windows”

Y te saldrá lo siguiente:



1. Buscamos la opción que dice “Internet information Services”



Lo marcamos y le damos “Aceptar”

Y listo, así de fácil se habilita esa característica

Para la creación del certificado auto firmado, solo es necesario seguir estas instrucciones:

1. Abrir el Administrador de IIS y selecciona el nodo. A continuación, haz click en abrir Certificados de servidor.
2. Seleccionar la opción Crear un certificado auto firmado. Una vez allí, el sistema solicitará el nombre del dominio al que deseamos poner el certificado.
3. Ir al sitio web donde quieres que se instale el certificado, en este paso debemos indicar el nombre denuestro dominio.
4. A continuación, vamos a Enlaces.
5. Hacer click en Agregar.
6. Escoger el tipo de HTTPS, ten en cuenta que por defecto el puerto siempre será el 443. A continuación, puedes escoger el nombre del certificado.
7. Cuando hayamos aceptado, en el panel de acciones veremos que aparece una nueva opción. Esta nueva pestaña nos permitirá enlazar al sitio seguro. Recuerda que, si quieres que siempre se requiera el acceso a través de HTTPS, deberás especificarlo en la Configuración de SSL.
8. Cuando ya hayamos introducido todos los cambios solicitados, hacer click en Requerir SSL y el certificado auto firmado ya estará listo.

Tan sencillo como eso, claro, si lo estas haciendo en Windows 10, pero ¿qué pasa cuando es otro sistema operativo?

No hay necesidad de preocuparse por eso, pues hay opciones gratuitas que hacen todo el trabajo de generar el certificado auto firmado, esto se debe a que son entidades Open Source[[10]](#footnote-10) por lo cual es gratis, y no hay que descargar nada, solo habilitarlo según lo requiera el sistema operativo.

A continuación, un ejemplo de una entidad que realiza certificados de forma gratuita

* [Let’s Encrypt](https://linube.com/blog/que-es-ssl-lets-encrypt/)

# Cibergrafía

* <https://linube.com/blog/certificado-ssl-autofirmado/>
* <https://developer.android.com/training/articles/security-tips>
* <https://luisperis.com/instalar-iis-windows-10-5-minutos/>
* <https://developer.android.com/privacy/best-practices>

1. TIC: Tecnologías de la información y la comunicación [↑](#footnote-ref-1)
2. “EduApps” es un proyecto educativo que se quiere implementar en el Urabá Antioqueño para ayudar a los estudiantes y profesores de las instituciones educativas a mejorar la eficiencia de las clases desde un entorno TIC [↑](#footnote-ref-2)
3. “Tips”: Concejos en inglés [↑](#footnote-ref-3)
4. La aleatoriedad en la disposición del espacio de direcciones es una técnica de seguridad informática relacionada con la explotación de vulnerabilidades basadas en la corrupción de memoria [↑](#footnote-ref-4)
5. ofrece un conjunto integrado de herramientas que coordina distintas disciplinas, preserva la integridad de los datos y la intención de diseño y optimiza el proceso al completo [↑](#footnote-ref-5)
6. Es una aplicación que implementa varias técnicas usadas durante el desarrollo de software para mejorar la seguridad en aplicaciones detectando desbordamientos del buffer [↑](#footnote-ref-6)
7. Es un programa que se encarga de ocultar su dirección IP, evitando así posibles ataques o suplantaciones [↑](#footnote-ref-7)
8. OpenBSD es un sistema operativo libre multiplataforma enfocado en la seguridad y la criptografía [↑](#footnote-ref-8)
9. Es una instrucción que especifica la dirección virtual mínima que un proceso tiene permitido escanear, esto con el fin de procesar con direcciones inferiores e incrementar la seguridad. [↑](#footnote-ref-9)
10. Open Source, o fuente abierta, hace referencia a entidades que fueron hechas por diferentes personas y en la que cada una de ellas aportó en cuestiones de código, en la realización de dicha entidad. [↑](#footnote-ref-10)