



## SEGURIDAD EN INTERNET

### Protección en Internet

#### Sitio Web Protegido

Un sitio web protegido es aquel que presenta un protocolo de seguridad, es decir una función que dificulta la instalación de software malintencionado en el equipo, además de autorizar la instalación de ciertos controles que permiten mejor navegabilidad cuando se inicia sesión como administrador.

El modo protegido está activado de forma predeterminada en zonas de Internet, Intranet y Sitios restringidos, y se muestra un icono en la barra de estado para indicar que se está ejecutando.

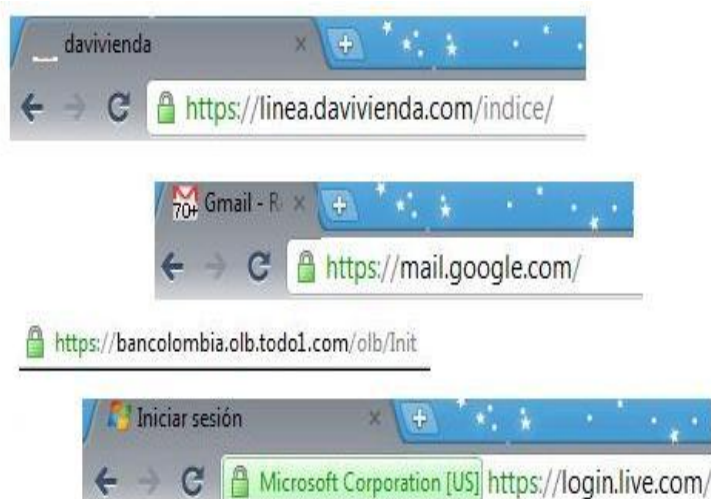


Figura. Ejemplos de sitios web protegidos

La mayoría de cuentas en las que se requiere de un usuario y contraseña, cuentan con un protocolo de seguridad, tal es el caso de cuentas de correo electrónico y entidades bancarias, entre otros. Todas ellas inician la escritura de su URL así: https (la "s" después del "http" significa "seguro"). También se observa un pequeño candado en la barra de navegación.



### Certificado digital

Un certificado digital es un documento o información que se obtiene en la red, mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública. Estos certificados incrementan los niveles de seguridad ofrecidos, son equivalentes a un segundo nivel de seguridad para proteger algunas operaciones o transacciones realizadas en la web.



**Figura. Certificado Digital.** Tomado de: <http://servelegovernment.blogspot.com/2010/05/certificado-digital.html>

La existencia de firmas en los certificados aseguran por parte del firmante del certificado (una autoridad de certificación, por ejemplo) que la información de identidad y la clave pública perteneciente al usuario o entidad referida en el certificado digital están vinculadas.

Un aspecto fundamental es que el certificado para cumplir la función de identificación y autenticación necesita del uso de la clave privada (que sólo el titular conoce).

Los certificados son unos archivos que permiten identificar a las dos partes que se conectan vía Internet, intercambiar una clave con la que se codifican los datos que se transmiten entre los dos extremos y garantizar la confidencialidad de esa clave.

### Cifrado o Encriptación

El proceso del cifrado consiste en convertir la información original (en el caso de documentos escritos el texto original viene a ser el "texto plano") en otra secuencia sin sentido (en el caso del texto se convierte en otro ilegible), mediante la aplicación de un algoritmo de cifrado, ya sea sustituyendo los caracteres por otros de manera predeterminada o aplicando alguna fórmula matemática para determinar la sustitución o resultado.



**Figura. Acceso restringido**

Mediante este proceso se vuelve ilegible determinada información que es considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

El texto plano que está encriptado o cifrado se llama criptograma. Este procedimiento de cifrado digital es que el que utilizamos sin darnos cuenta en el mundo actual, por ejemplo en los chips internos de ciertas tarjetas de crédito, al ingresar a la página web de nuestro banco, en la telefonía celular.

### Precauciones Informáticas

Cuando navegamos en red obtenemos mucha información, recursos y archivos entre otros. En algunas oportunidades, estos archivos son considerados “virus” ya que ocasionan daños al equipo.

Un virus informático es un malware o software malicioso, que altera el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus se diseminan transfiriendo archivos infectados de una computadora a otra. Esto puede ocurrir transfiriendo archivos en discos removibles, accediendo o descargando archivos de internet o de una red o a través de archivos enviados por correo electrónico. Los virus pueden ser archivos ejecutables o en otros formatos, como de procesador de texto que contengan macros. Al correr estos archivos ejecutables o abrir aquellos que contienen macros infectados se puede activar el virus que puede provocar daños considerables.

# Ruta de formación docente

## TIC con sentido pedagógico

Vicerrectoría Académica / Univirtual / Universidad Tecnológica de Pereira



Existen diversos tipos de virus, varían según su función o la manera en que éste se ejecuta en el computador alterando la actividad del mismo, entre los más comunes están:

- Troyanos,
- Gusanos,
- Bombas lógicas o de tiempo
- Hoax
- Joke.



**Figura. Peligros en Internet.** Tomado de <http://gatitangie.blogspot.com/2009/09/proteccion-contra-virus.html>