
GPG

# HERRAMIENTAS DESEGURIDADLIBRES

La seguridad es fundamental a la hora de afrontar tareas que se realizan en sistemas informáticos, ya que son las únicas medidas que pueden garantizar que éstas se realicen con cierta garantía. Y la posibilidad de modificar libremente el software, para adaptarlo a sus propias necesidades, tiene claras ventajas

**POR: LIC. CLAUDIO RAFAEL ARIAS**

**FUNDACIÓN DOMINICANA DE SOFTWARE LIBRE**

> SEGÚN EXPERTOS, LA SEGURIDAD NO EXISTE COMO TAL, Y MUCHO MENOS EN LOS SISTEMAS DE INFORMACIÓN DIGITAL, SINO QUE SOLO CONTAMOS CON NIVELES DE CONFIABILIDAD, Y ESTA DEPENDERÁ EN GRAN MEDIDA DE LAS PRECAUCIONES QUE CADA USUARIO TOME CON RELACIÓN A LA INFORMACIÓN QUE MANEJA"

La seguridad es un tema que bordea el planeta en un momento en que la tecnología lo domina prácticamente todo, en un mundo donde los delitos informáticos han crecido y controlar a los delincuentes informáticos es casi imposible. Redes sociales, correo electrónico, mensajería instantánea, páginas web, almacenamiento en la nube, comunicaciones por voz y vídeo, son algunos de los servicios a los que millones de personas acceden diariamente en Internet y se han convertido en parte importante de sus estilos de vida, a los cuales acceden desde distintos dispositivos y aplicativos.

¿Cuáles son los riesgos con la información que intercambiamos diariamente y los documentos que almacenamos en nuestros equipos? ¿Qué tan seguros están los datos que manejamos a diario en las redes? Entendemos la creciente ola de personas desaprensivas, maliciosas, que crece de manera descomunal en el mundo cibernético, siendo estos seducidos por diversión, por dinero o por simple deseo de probar sus conocimientos.

Según expertos, la seguridad no existe como tal, y mucho menos en los sistemas de información digital, sino que solo contamos con niveles de confiabilidad, y esta dependerá en gran medida de las precauciones que cada usuario tome con relación a la información que maneja.

De acuerdo con diversas fuentes, la seguridad de la información es el conjunto de medidas preventivas y reactivas que buscan mantener los

niveles de confidencialidad, disponibilidad e integridad de la misma, siendo estos tres un conjunto de principios a los que profesionales de este campo le llamamos el "triangulo de la seguridad". Solo si se cuenta con mecanismos y una conducta apropiada que procure mitigar la pérdida de unos de estos tres elementos, entonces podríamos estar acercándonos a niveles aceptables de fiabilidad.

**CONFIDENCIALIDAD**

La confidencialidad es el principio de la seguridad que garantiza que cierta información solo sea conocida por la persona a quien corresponda o se le autorice, la misma está vinculada a la privacidad y a la autorización.
Para esto, deben definirse controles de acceso adecuados para poder reducir los riesgos de acceso no autorizados a equipos o lugares en donde se encuentre información sensitiva.
Uno de los métodos más comunes de autenticación es utilizar un nombre y una contraseña.
Esta última normalmente suele ser fácil de adivinar, ya que los usuarios utilizan palabras predecibles basadas en diccionarios, números, fechas importantes, nombres de hijos y otros familiares, e incluso sus propios nombres.
Algunos consejos que podrían ayudar a mejorar los niveles de confidencialidad es utilizar contraseñas fuertes. Una sugerencia es crear una nomenclatura que permita la utilización de caracteres en mayúscula, minúscula, números, caracteres especiales, y una longitud considerable, por ejemplo: 3dMp@R1cDm0@, la cual dice "El dia Menos pensado @lguien Robara 1a contraseña De mi 0rdenador @ctual".
Otra recomendación es utilizar redes anónimas para navegar en Internet. La red Tor (torproject.org) es la más conocida. Tor es un proyecto que procura proteger su privacidad y defenderlo contra análisis de tráfico y vigilancia masiva en Internet.
Otra herramienta importante es GnuPG (gnupg.org). Esta le permite codificar y firmar (digital) su información y comunicación, haciéndolos legible solo a los destinatarios.
La codificación protege el contenido contra terceros (no pueden leerlo) y la firma digital se asegura de que no se modificó y proviene del remitente correcto. El proyecto Gpg4win (gpg4win.org) provee una versión estable para Windows.
Combinar GnuPG con un gestor de correo electrónico es el principio del inicio para proteger la confidencialidad de las comunicaciones este medio tan popular. Recomendamos seguir la guía "Defensa Personal del Correo Electrónico" en https://emailselfdefense.fsf.org/es/. Esta guía utiliza el cliente Thunderbird y el complemento Enigmail. Explica paso a paso todo el proceso, tanto para el sistema GNU/Linux como para Windows. Otra medida inteligente que podemos utilizar para evitar la pérdida de confidencialidad, es cifrar el contenido importante que almacenamos en nuestros computadores, tabletas o dispositivos móviles, ya que estos podrían ser sustraídos y cualquiera puede tener acceso a información importante contenida en las unidades de almacenamiento.
Todas estas herramientas están disponibles en sus respectivos portales de manera libre, y su código fuente está disponible para su estudio y posterior modificación. El uso de estos aplicativos libres es un buen inicio que nos ayuda significativamente para proteger la confidencialidad de nuestros datos.
En una próxima entrega escribiremos sobre la integridad de la información y los consejos prácticos de cómo evitar su pérdida haciendo uso de aplicaciones libres.

"COMBINAR GNUPG CON UN GESTOR DE CORREO ELECTRÓNICO ES EL PRINCIPIO DEL INICIO PARA PROTEGER LA CONFIDENCIALIDAD DE LAS COMUNICACIONES ESTE MEDIO TAN POPULAR"