Publicado en CDMX el 11/07/2022

# [9 riesgos de ciberseguridad que toda empresa debería conocer: Hillstone Networks](http://www.notasdeprensa.es)

## Hillstone Networks comparte los principales riesgos de seguridad que vuelven más vulnerables a todo tipo de empresas

 Hillstone Networks, proveedor líder de soluciones de seguridad de red y gestión de riesgos, aseguró que para garantizar la seguridad en la información, es necesario cumplir con tres principios fundamentales: confidencialidad, integridad y disponibilidad. A estos criterios se les conoce también como la “Triada CID”. Confidencialidad: Garantiza que la información no sea divulgada ni tenga acceso a personas o entidades no autorizadas. Integridad: Mantener a salvo la exactitud de los datos o la información almacenada. Disponibilidad: Garantizar la accesibilidad a la información en cualquier momento a los usuarios autorizados. Riesgos que amenazan la informaciónUna vez identificados cuáles son los criterios con los que se mide la seguridad, es más fácil determinar cuáles son los posibles riesgos que pueden amenazar la información de una empresa, por ejemplo: Correos no deseado: Se refiere a cualquier tipo de correo tipo spam que contenga phishing o pharming y que pueda introducir malware en el sistema para robar o modificar la información. Uso de aplicaciones online: Algunas aplicaciones de almacenamiento de datos online, como, por ejemplo, Dropbox, Google Drive o OneDrive, pueden exponer la información y poner en peligro cualquiera de los principios CID. Copias de seguridad: La falta de copias de seguridad es un error grave. No hacerlo implica la posibilidad de pérdida de información. Debilidad en las contraseñas: Aunque parezca obvio, una contraseña segura hace realmente la diferencia. Nunca se debe dejar una contraseña asignada por defecto o utilizar algún término demasiado fácil de escribir. Lo más recomendable es utilizar una combinación de mayúsculas y minúsculas, números y caracteres especiales. Permisos de administrador: Otorgar permisos de administrador a todos los trabajadores de la empresa puede poner en serios problemas la seguridad de la información. Es importante restringir el acceso a la información a todas las personas que no deberían manipularla. Puede ocurrir que, o accidental o intencionalmente, se instale algún software malicioso en la red interna de la empresa. Acciones para evitar riesgos innecesarios: Con base en el análisis de riesgos, se puede mencionar algunas acciones que, aunque no protegerían un 100 % la información, sí reducirían considerablemente la exposición a las amenazas a la información. Capacitación: Muchas veces, la falta de conocimiento por parte de los trabajadores contribuye a poner en riesgo la información confidencial de una empresa. Por ello, una buena idea sería ofrecer una capacitación a los empleados que les permita conocer cómo funciona la ciberseguridad. Acceso limitado: Es esencial limitar el acceso a la información exclusivamente a las personas que lo necesiten. No hay motivos para exponerse al mal uso de los datos. Cuidados en la red: El intercambio de datos online debe restringirse en la medida de lo posible. La red siempre representa un riesgo alto para la información. En definitiva, la posibilidad de riesgo siempre va a existir, sin embargo, está en cada empresa tomar acciones para evitarlos.

**Datos de contacto:**

Carlos Soto

5532322068

Nota de prensa publicada en: [https://www.mexicopress.com.mx/9-riesgos-de-ciberseguridad-que-toda-empresa](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Software Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)