# Blinda a tu negocio **contra amenazas digitales**

*El trabajo híbrido se impone en las organizaciones, pero no todas están preparadas para enfrentar las amenazas que supone almacenar y manejar su información en un entorno digital. Aplica estos tips de ciberseguridad y evita que los delincuentes se aprovechen de tus vulnerabilidades tecnológicas.*

Las empresas, actualmente, se exponen a tres amenazas digitales principales:

1. Ransomware o secuestro de información.
2. Fraude electrónico a través de suplantación de identidad.
3. Robo de información al hacer click en correos o links desconocidos.

## ¿Por qué les sucede eso?

- Tienen una cultura en torno a la seguridad informática poco desarrollada.
- Sus colaboradores están poco capacitados para identificar amenazas.
- Los criminales sacan partido de esta situación y ejecutan acciones como el secuestro de información y el cobro de un “rescate” para “liberarla”.

## ¿Cómo evitar ciberataques?

Aplica estos tips de ciberseguridad que da Luis Fernando Garzón, líder de ciberseguridad para Cisco Colombia y participante en el Bootcamp en Ciberseguridad 2022, realizado por la Cámara de Comercio de Cali:

| | | |
|---|---|---|
| 1 | Desarrolla en tu empresa una cultura organizacional o un proceso de enseñanza continua. Así: | ▪ Todos los empleados aprenden a usar los recursos tecnológicos acertadamente.<br>▪ Saben a qué sitios web ingresan, a qué le dan click o qué tipo de programa están ejecutando. |
| 2 | Promueve el uso diferenciado de los recursos tecnológicos de la organización y los de uso personal. De esta forma: | ▪ Evitas que se usen implementos de la compañía para actividades personales y así proteges la información corporativa. |
| 3 | Mantén actualizados todos los sistemas o software que usa todo el personal. Gracias a esto: | ▪ Cuentas con la protección que ofrecen esos sistemas con cada actualización.<br>▪ Reduces las vulnerabilidades a nivel tecnológico de la organización. |
| 4 | Identifica quién se está conectado a las redes o equipos de la empresa, ya sea dentro de la misma o de forma remota para: | ▪ Cerciorarte acerca de quién está intentando acceder a la información confidencial.<br>▪ Verificar si cada persona es quien dice ser y saber si se le debe otorgar un permiso de acceso a la información o no. |
| 5 | Concibe a la nube como un acelerador del negocio. Esto significa: | ▪ Usar la nube no solo como repositorio de archivos o aplicaciones, sino como un entorno seguro.<br>▪ Considerar la nube como un elemento que permita llevar un control de las actividades que cada empleado realiza. |
| 6 | Implementa una cultura de análisis previo a realizar click en links atractivos: | ▪ Enseña a tu equipo que debe evitar hacer click en correos que no está esperando o que parezcan sospechosos.<br>▪ La curiosidad no debe poner en riesgo la información del negocio. |
| 7 | Mantén unificadas y actualizadas las políticas de seguridad tecnológica corporativas: | ▪ Lo que se tiene escrito en el papel debe llevarse a la práctica. |
| 8 | Brinda tanto conexiones seguras, como espacios seguros a los usuarios corporativos: | ▪ Trabajar desde un café internet pone en riesgo la información porque los delincuentes pueden escuchar datos para usarlos a su favor. |
| 9 | Ten un panorama de tus riesgos tecnológicos para tomar acciones correctivas y mitigar los problemas: | ▪ En el campo de la ciberseguridad se tiene la premisa de que solo se puede proteger lo que se ve. |
| 10 | Ante cualquier duda sobre posibles amenazas cibernéticas, busca la asesoría de fabricantes, proveedores de seguridad o expertos: | ▪ Así puedes resolver inquietudes y saber cómo proceder en caso de un ciberataque. |

*“La alta dirección de la organización debe estar comprometida con la ciberseguridad, pues no es un asunto exclusivo del área tecnológica, sino un tema relativo al negocio. En esta época, conectividad y seguridad deben ir de la mano”.*

**Luis Fernando Garzón,** líder de ciberseguridad para Cisco Colombia

Cámara de Comercio de Cali