RECOMENDACIONES BÁSICAS DE SEGURIDAD

Recomendaciones básicas de seguridad

Las nuevas tecnologías han permitido que la información sea fácil de manejar para mejorar la productividad de las empresas, pero al mismo tiempo, ha incrementado la exposición a nuevas amenazas que permiten la fuga de información confidencial, ya sea por agentes internos (errores, empleados descontentos, etc.) o externos (ataques con malware o de ciberdelincuentes).

Por más esfuerzos que una compañía realice para proteger la información confidencial, la responsabilidad recae principalmente en la práctica de sus colaboradores. El eslabón más débil de la cadena de la seguridad siempre es el humano, ya que en ocasiones no seguimos las reglas establecidas o no tomamos las precauciones necesarias.

Por eso es importante que todas las personas se responsabilicen de su papel como protectores de información y se encarguen de conocer, comprender y difundir las normas básicas de seguridad de la información.

Los expertos en ciberseguridad de la compañía Panda recomiendan llevar a cabo las siguientes acciones:

Confirma la identidad de todo aquel que solicite información:
Antes de brindar cualquier información a través de algún medio, tienes que estar seguro de que la persona que la solicita es quien dice ser.

Evita compartir información laboral en redes sociales:
Además de la disminución de la productividad en horas laborales, cada vez más personas publican información y fotografías que ponen en riesgo la seguridad de la empresa.

Evita instalar software en equipos institucionales:
Evita navegar en sitios sospechosos y, sobre todo, jamás instales software sin autorización del equipo de soporte de sistemas.

Instala un buen antivirus:
Asegúrate de tener un antivirus de buena reputación y mantenerlo actualizado constantemente, para proteger los equipos y datos de la organización.

Aplica el sentido común:
Siempre mantén un equilibrio en las medidas de seguridad, no deben ser tan estrictas ni tampoco tan sencillas.

Realiza copias de seguridad:
Las computadoras y dispositivos de almacenamiento no son a prueba de ataques. Lleva a cabo copias de seguridad en diferentes sitios, para recuperar la información si es necesario.

Protege tus copias de seguridad:
Tan importante es realizar copias de seguridad, como protegerlas. Evita transportar tu equipo de cómputo y el medio de respaldo juntos.

Utiliza la nube:
Los espacios de almacenamiento virtual son una buena alternativa para llevar a cabo respaldos de información. Solo recuerda seguir las indicaciones correctas, con respecto al cuidado de tus contraseñas y conexiones seguras.

Cuida tu correo electrónico:
Siempre evita abrir correos de usuarios desconocidos y, sobre todo, jamás ejecutar archivos o hacer clic sobre enlaces sospechosos, aun y cuando parezcan venir de una organiza

ción reconocida. Las cuentas de correo institucionales no se deben utilizar para acceder a páginas web.

Crea una buena contraseña:
Las contraseñas deben formarse a partir de una combinación de letras en mayúsculas y minúsculas, números y símbolos que sean difíciles de descifrar, así como evitar utilizar la misma contraseña para varios sitios. Jamás reveles tu contraseña. ¡A nadie!