




Recomendaciones para la protección de la información






Copias de seguridad

Para minimizar el impacto que podría tener la pérdida masiva de datos. Se recomienda crear copias de seguridad, que consisten en una copia de todos los datos que se deseen conservar guardada en un dispositivo separado del sistema central.

Existen alternativas en la actualidad que facilitan esta mecánica, como los dispositivos USB o los discos duros extraíbles, son cada vez más económicos y de mayor capacidad. Además, es posible acceder al almacenamiento en la nube, especialmente útil para guardar información de menor tamaño si no se espera destinar muchos recursos en membresías de pago.





Instalación de antivirus


Si bien en la actualidad los sistemas operativos ofrecen aplicativos integrados que aportan a la seguridad informática, contar con mecanismos adicionales, como antivirus, puede otorgar más tranquilidad para el manejo de datos.

En el mercado, existen innumerables alternativas que garantizan proteger la información de todo tipo de ataque informático, por lo que, con una asesoría adecuada, se pueden encontrar alternativas robustas y de confianza.

Cifrado de información

Esta estrategia funciona como un excelente complemento a las demás listadas en esta sección. El cifrado consiste en la modificación de los datos en un lenguaje que obedezca a unos parámetros determinados, pero que, para quien no posea la guía para su traducción, resultará ilegible.

De esta forma, si la información es violentada a través de cualquier **programa malicioso**, no podrán hacer uso de su contenido; no obstante, este sistema **no evita que corrompan los archivos o eliminen datos sensibles para la empresa.**




Uso de contraseñas efectivas

La creación de contraseñas es una de esas actividades a las que no se les suele prestar la atención suficiente. Generalmente, constituyen la primera barrera para acceder a la información, por lo que una contraseña extensa, no asociable al usuario de la información y con una cantidad suficiente de caracteres que no sigan ningún patrón, puede dificultar exponencialmente el acceso no autorizado a los datos.







Capacitación del personal

Como estrategia preventiva, capacitar al personal puede evitar que se cometan malas prácticas que pongan en riesgo las bases de datos de la empresa. La falta de conocimiento puede llevar a excesos de confianza o faltas en la aplicación de los protocolos de seguridad definidos por la empresa.

Situaciones lamentablemente comunes, como el acceso a páginas web sin certificados de seguridad o la descarga de contenido de páginas de dudosa reputación, pueden terminar otorgando acceso al contenido de los equipos informáticos a personas malintencionadas que se aprovechan de estas brechas.