Información importante

Tips de Seguridad

Como la seguridad es muy importante para nosotros, te hacemos llegar algunas mejores prácticas y consejos para que tengas en cuenta y apliques en tus entornos y servidores virtuales.

Usá contraseñas seguras en todos tus servidores: Más de 8 caracteres + Letras mayúsculas y minúsculas + Números + Símbolos.

Abrí sólo los puertos que vas a utilizar y **creá** reglas para no permitir tráfico por los que no uses (Ej. FTP o RDP).

Cambiá el protocolo de conexión a puertos "no conocidos". Esto te dejará fuera de típicos ataques. Por ejemplo, si vas a usar puertos de acceso remoto como RDP o SSH, te dejamos instrucciones:

- En Windows: <click aquí para más información>
- En Linux Debian y Ubuntu: <click aquí para más información>
  y Centos: <click aquí para más información>

Evitá que tu entorno tenga reglas de tipo PERMITIR ANY, la cual permite tráfico saliente / entrante de cualquier origen.
Es importante restringir las direcciones IP origen para el acceso a puertos RDP, SSH y FTP. Tener expuestos estos puertos hace que seas vulnerable a posibles ataques.

Instalá un antivirus y anti-spyware. Es altamente recomendable contar con antivirus en tus máquinas virtuales. Si no contás con uno, podés adquirir ***"Seguridad Empresas"*** desde tu portal Claro Cloud en muy pocos pasos <encontralo aquí>

Aplicá actualizaciones de parches de seguridad en sistemas operativos y aplicaciones (Apache, JAVA, Linux, Windows, etc.)

Realizá chequeos periódicos de vulnerabilidades.

Respaldá tus servidores frecuentemente. Realizá backups de la información relevante, y así poder tener una recuperación rápida ante fallas. Si usás servidores en Nube Pública ya contás con una herramienta de backup integrada, y si usás Data Centers Virtuales podés consultar por el servicio de backup AVAMAR a tu ejecutivo de cuentas o al 0800-12-CLOUD.

Consultá las páginas oficiales de Microsoft y Linux para ampliar las mejores prácticas de seguridad:

- Microsoft:https://docs.microsoft.com/es-es/windows-server/security/security-and-assurance
- Linux: https://www.debian.org/security/ - https://wiki.centos.org/TipsAndTricks - https://ubuntu.com/security

Tené en cuenta que en la actualidad los entornos de cómputo en la nube pueden estar expuestos a diferentes vulnerabilidades, por eso es muy importante que trabajemos juntos para minimizar los riesgos y que tu infraestructura Claro Cloud esté segura.