

12 Consejos de Ciberseguridad para Home Office.



Consejo #1



Habilita

el acceso remoto a la red a través de un canal seguro, solo cuando sea necesario (por ejemplo: VPN).

Consejo #2



Exige

doble factor de autenticación, cuando sea posible.

Consejo #3



Utiliza

servicios remotos solo por protocolos seguros (HTTPS).

Consejo #4



Limita

los accesos remotos únicamente a los servicios permitidos y a zonas aisladas en la red.

Consejo #5



Valida

los controles en equipos remotos
(por ejemplo: antivirus,
actualizaciones, configuraciones de
seguridad, etc.)

Consejo #6



Valida

las capacidades de borrado y bloqueo remoto en los equipos.

Consejo #7



Asegura

que los equipos personales cuenten con cifrado de disco y valida los controles de prevención de fuga de información.

Consejo #8



Realiza

un backup de la información crítica.



MARSH

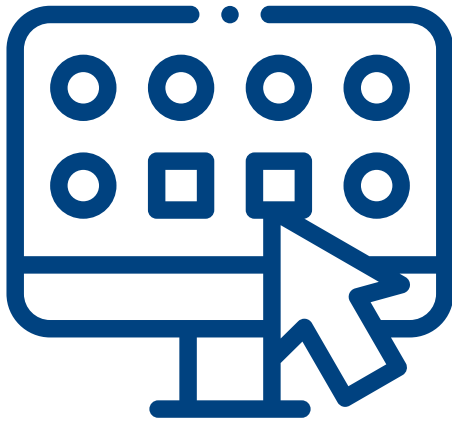
Consejo #9



Concientización, concientización, concientización

por ejemplo: cómo detectar un phishing, correos maliciosos, etc.

Consejo #10



Definir

a los usuarios los protocolos para reportar cualquier situación anómala o sospechosa.

Consejo #11

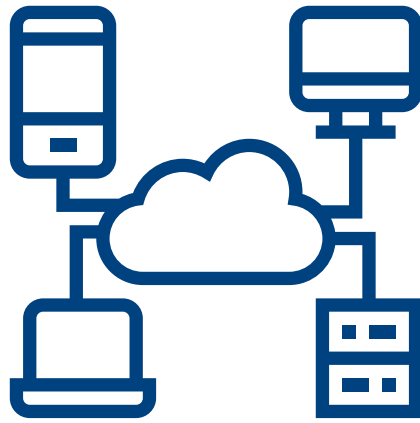


Incrementar

los niveles de monitoreo de eventos de seguridad. Algunos ejemplos:

- Intentos de autenticación fallidos y luego exitosos.
- Acceso con un mismo usuario desde múltiples direcciones IP.
- Tráfico de red sospechoso.
- Conexiones desde ubicaciones anómalas (por ejemplo: países inusuales).

Consejo #12



Aconseja

evitar el uso de redes públicas o inseguras para la conexión.

Ten en cuenta que la aplicación de políticas de Home Office pueden saturar los enlaces a Internet.

Revisa la capacidad y monitorea constantemente los enlaces para asegurar la continuidad de los servicios.

