System kopii zapasowych

1. Wykonanie przeglądu czy system kopii zapasowych działa prawidłowo i czy wykonuje swoje zadanie zgodnie z zadanym harmonogramem.
2. Wykonywanie kopii bezpieczeństwa zgodnie z harmonogramem - raz dziennie kopia różnicowa lub przyrostowa oraz raz w tygodniu pełna kopia.
3. Weryfikację czy wykonane kopie zapasowe faktycznie pozwolą na odtworzenie całych systemów wraz z danymi i konfiguracją.
4. Wykonywane kopie zapasowe nie mogą być podłączone jako zasób sieciowy.
5. Wykonanie testów odtworzenia systemów w izolowanym środowisku. Działanie takie powinno odbywać się cyklicznie.
6. Stosowanie strategii 3-2-1:
   a. Należy przechowywać co najmniej 3 kopie zapasowe.
   b. Co najmniej 2 z nich powinny być przechowywane na różnych nośnikach.
   c. Co najmniej 1 z nich powinna być odizolowana od pozostałych oraz sieci lokalnej (odmiejscowienie)
7. Przygotowanie planu działania na scenariusz utraty systemu kopii zapasowych razem z kopiami – powołanie nowej maszyny, instalacja OS oraz systemu kopii, wgranie kopii konfiguracji systemu kopii, podłączenie kopii zapasowych.
8. System kopii zapasowych powinien być w dedykowanej podsieci. Przepuszczony ruch pomiędzy hostami i systemem kopii powinien być minimalny, niezbędny – określone porty. System kopii powinien działań na dedykowanych kontach bez praw administratora domenowego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706