	- distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd); - demagnetizzazione ad alta intensità.

5.2 Sicurezza dei Sistemi Operativi

Di seguito viene fornita una vista delle principali minacce e delle relative contromisure da adottare.

Sono fornite dapprima una serie di indicazioni generiche, valide per qualsiasi sistema operativo moderno ma con un focus particolare per sistemi destinati ad un ruolo di server, e successivamente una serie di indicazioni specifiche (in paragrafi dedicati) per i sistemi operativi più diffusi, ovvero Windows, Mac OS X e Linux.

5.2.1 Architettura

Architettura	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	- Utilizzare un sistema di protezione del perimetro (Firewall). - Segmentare la rete: creare segmenti di rete distinti per le diverse tipologie di sistemi dotate di caratteristiche diverse di sensibilità e tipologia. Ad es. creare un segmento o layer dati, un layer per i server di front-end, un layer per le postazioni di lavoro, un segmento per la rete di amministrazione (da cui gli amministratori accedono alle interfacce amministrative dei server e degli apparati di rete e di sicurezza). - Non usare le VLAN per separare i layer: attestare ogni layer/segmento su una diversa interfaccia del firewall. - Installare un IDS (intrusion detection system) o IPS (intrusion prevention system) - Impiegare VPN terminate sul firewall perimetrale (o su host specifici e dedicati, attestati su una apposita DMZ), per la connessione di utenti remoti e di altre reti appartenenti a diverse sedi dell'ente/organizzazione. - Utilizzare un sistema di controllo accessi alla rete (NAC basato su protocollo 802.1x e Server RADIUS) per prevenire l'accesso tramite cavo da parte di sistemi fraudolenti. - Individuare e rimuovere eventuali punti di accesso wireless non autorizzati e utilizzare su quelli leciti il sistema di protezione Wi-Fi Protected Access versione 2 (WPA2) per la massima protezione dagli attacchi wireless, avendo cura di aggiornare il firmware all'ultima versione disponibile (fine Ottobre 2017 o successiva), in grado di eliminare la vulnerabilità denominata KRACK (Key Reinstallation Attacks) (cfr. https://www.krackattacks.com/). - Collocare i computer e i supporti esterni di memorizzazione dei dati in luoghi sicuri. - Adottare sistemi di controllo basato su ruolo per l'accesso ai computer e ai dati, separando gli utenti in più gruppi con distinto livello di autorizzazione per la lettura e la scrittura dei dati.

Architettura	
Minaccia	- Negazione dei servizi. - Cancellazione di informazioni (accidentale).
Contromisure	Al fine di garantire la continuità operativa del sistema, configurare i dischi in modalità RAID-1 o RAID-5, in modo che i dati presenti su ciascun disco siano replicati. In questo modo in caso di guasto di un disco, sarà possibile continuare ad utilizzare il