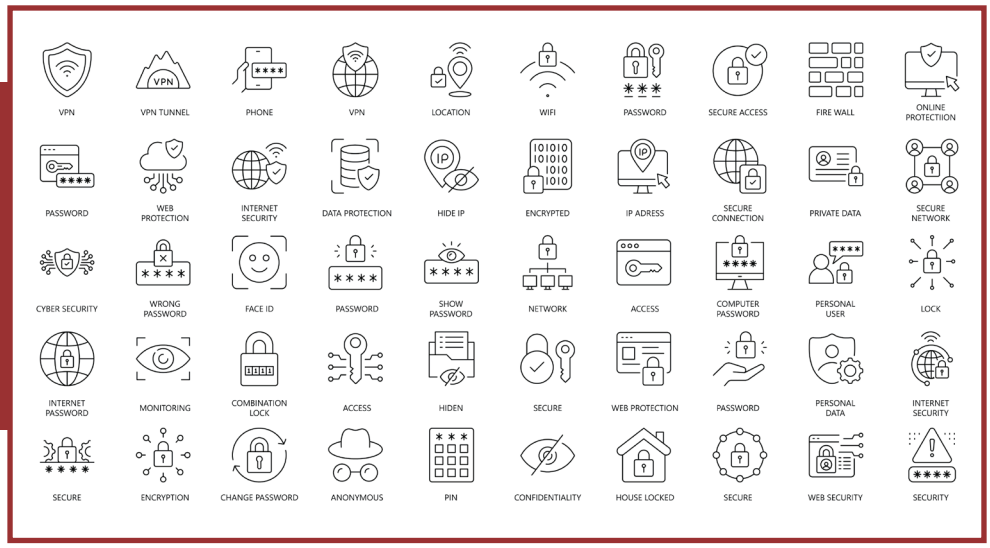
Fabrizio Di Crosta
Libero professionista
Consulente di direzione e Informatica,
Socio AIAS

Le misure di sicurezza tecniche e organizzative nel GDPR

Il Regolamento UE 2016/679 (GDPR) ha introdotto un nuovo paradigma nella protezione dei dati personali, basato non più su un elenco di misure "minime" da rispettare, ma su un approccio dinamico e contestualizzato. Il principio guida è la "adeguatezza" delle misure di sicurezza, stabilite in funzione dei rischi specifici derivanti dai trattamenti effettuati.

L'art. 32 del GDPR richiede che titolari e responsabili del trattamento implementino misure tecniche e organizzative idonee a garantire un livello di sicurezza proporzionato al rischio.

Questo approccio richiede che ogni organizzazione valuti la probabilità e la gravità di eventuali eventi negativi, considerando natura, contesto, finalità del trattamento e tipologia di dati.



L'obiettivo è proteggere i diritti e le libertà delle persone fisiche da accessi non autorizzati, perdite, modifiche o divulgazioni indebite di dati personali. È importante comprendere che la valutazione dei rischi deve essere "altruistica", focalizzandosi sui diritti dell'interessato, non sugli interessi del business.

Tra le misure tecniche, rientrano strumenti come la pseudonimizzazione e la cifratura, ma anche sistemi anti-malware, firewall, controllo degli accessi, backup, monitoraggio dei log, e la protezione delle comunicazioni di rete. Ad esempio, la cifratura dei dati, a riposo e/o in transito, riduce il rischio che un eventuale furto di informazioni comporti un impatto concreto. L'autenticazione a due fattori per l'accesso ai sistemi critici è ormai una misura largamente consigliata, soprattutto per gli account con privilegi amministrativi e per i *login* su applicativi web.

Le misure organizzative riguardano invece la struttura operativa dell'organizzazione: nomine formali al personale, formazione del personale, policy interne sull'uso dei dispositivi, procedure per la gestione degli incidenti, accordi con i fornitori (responsabili del trattamento dati personali ex art. 28 GDPR). È fondamentale che i dipendenti siano consapevoli delle proprie responsabilità in materia di protezione dei dati: una password lasciata incustodita o un link malevolo cliccato per errore possono compromettere l'intero sistema di sicurezza.

Un elemento centrale è la valutazione dei rischi: non si tratta di un adempimento isolato, ma di un processo da aggiornare periodicamente e ogni volta che cambiano i trattamenti, gli strumenti o il contesto. Il principio di *accountability* impone di documentare tutte le scelte effettuate, in modo da poter dimostrare, anche a posteriori, l'adeguatezza delle misure adottate. Questo include i registri dei trattamenti, i risultati del *risk assessment*, le DPIA (ove richiesto) e la descrizione dettagliata delle misure di sicurezza implementate. Dichiarare in modo riduttivo, ad esempio, che si adottano credenziali con password per accedere ai sistemi, che si usa un antivirus e si fa il backup non basta. Occorre dettagliare meglio i criteri di complessità delle password, l'eventuale adozione della MFA, la configurazione di anti-malware e firewall, il tipo di backup che si effettuano, come sono protetti e dove sono conservati.
Il GDPR, pur non prescrivendo soluzioni specifiche, promuove il ricorso a standard riconosciuti, come la ISO/IEC 27001-27002, che forniscono un *framework* completo per la sicurezza delle informazioni. Altri schemi adottabili sono le Linee Guida ENISA, il *Cybersecurity Maturity Model*, il *Cybersecurity Framework* del NIST, le Misure di Sicurezza AGID (specifiche per la P.A.). L'adozione di tali standard aiuta le organizzazioni a strutturare il proprio sistema di gestione della sicurezza in modo coerente e verificabile, migliorando la resilienza e facilitando eventuali audit interni ed esterni.

Un altro punto chiave è la distinzione tra misure di sicurezza per la privacy e quelle generali per la protezione delle informazioni. Ad esempio, in una fabbrica la perdita di progetti tecnici può essere critica per il business, mentre la perdita dei dati personali dei dipendenti potrebbe avere un impatto minore. In un ospedale, invece, la perdita delle cartelle cliniche

può avere gravi conseguenze sia per l'organizzazione sia per i pazienti. Questo dimostra che anche misure tecniche simili devono essere calibrate in base alla finalità e alla sensibilità dei dati trattati, nell'ottica dell'interessato per il GDPR.

Da non dimenticare sono i principi di "*privacy by design*" e "*privacy by default*". Il primo impone che la sicurezza sia prevista sin dalla fase di progettazione dei trattamenti, mentre il secondo richiede che, per impostazione predefinita, siano trattati solo i dati strettamente necessari. Ciò implica che i sistemi informativi debbano essere configurati per garantire il massimo livello di protezione, riducendo al minimo la discrezionalità dell'utente. L'implementazione concreta di questi principi richiede un coinvolgimento interdisciplinare: legale, tecnico, organizzativo.
Infine, è bene ricordare che anche le organizzazioni più piccole, che si affidano a consulenti esterni per la gestione IT, restano pienamente responsabili delle misure adottate. Il coinvolgimento della direzione aziendale nella scelta e documentazione delle misure è fondamentale, così come la condivisione delle responsabilità con i fornitori. Senza un accordo chiaro, il rischio è che in caso di violazione dei dati nessuno si assuma la responsabilità delle scelte fatte, lasciando il titolare esposto a sanzioni e contenziosi (può essere accusato di *culpa in eligendo* e/o *culpa in vigilando*).

CONCLUSIONI

La sicurezza nel GDPR non è un requisito tecnico, ma una responsabilità gestionale e culturale. Le misure tecniche e organizzative devono essere coerenti, proporzionate, integrate nei processi e documentate. Inoltre, la loro efficacia dovrà essere periodicamente verificata. Solo con un approccio integrato, consapevole e costantemente aggiornato è possibile proteggere realmente i dati personali e costruire una fiducia duratura con clienti, dipendenti e cittadini.