Tutela dei dati personali

- Cosa è
- Informativa
- Consenso
- Nomine
- Le diverse realtà
- Individuazione dei dati
- Nomina dpo
- verifiche
- Accontabiliy
- DPIA

Reg. europeo e Sicurezza

- GDPR 679/2016
- D.Lgs 196/2003
- D. Lgs 101/2018
- Cod. deontologici
- direttiva (UE) 2016/1148
- D.L 14 giugno 2021, n. 82

Privacy è Sicurezza

- Adeguamento
- Protezione
- Anonimizzazione
- Crittografazione
- Dati
- Dati sensibili
- Dati giudiziari

1995

Direttiva 95/46/CE

1996

L. 675/96

2003

D. Lgs. 196/2003

2016

Reg. Europeo

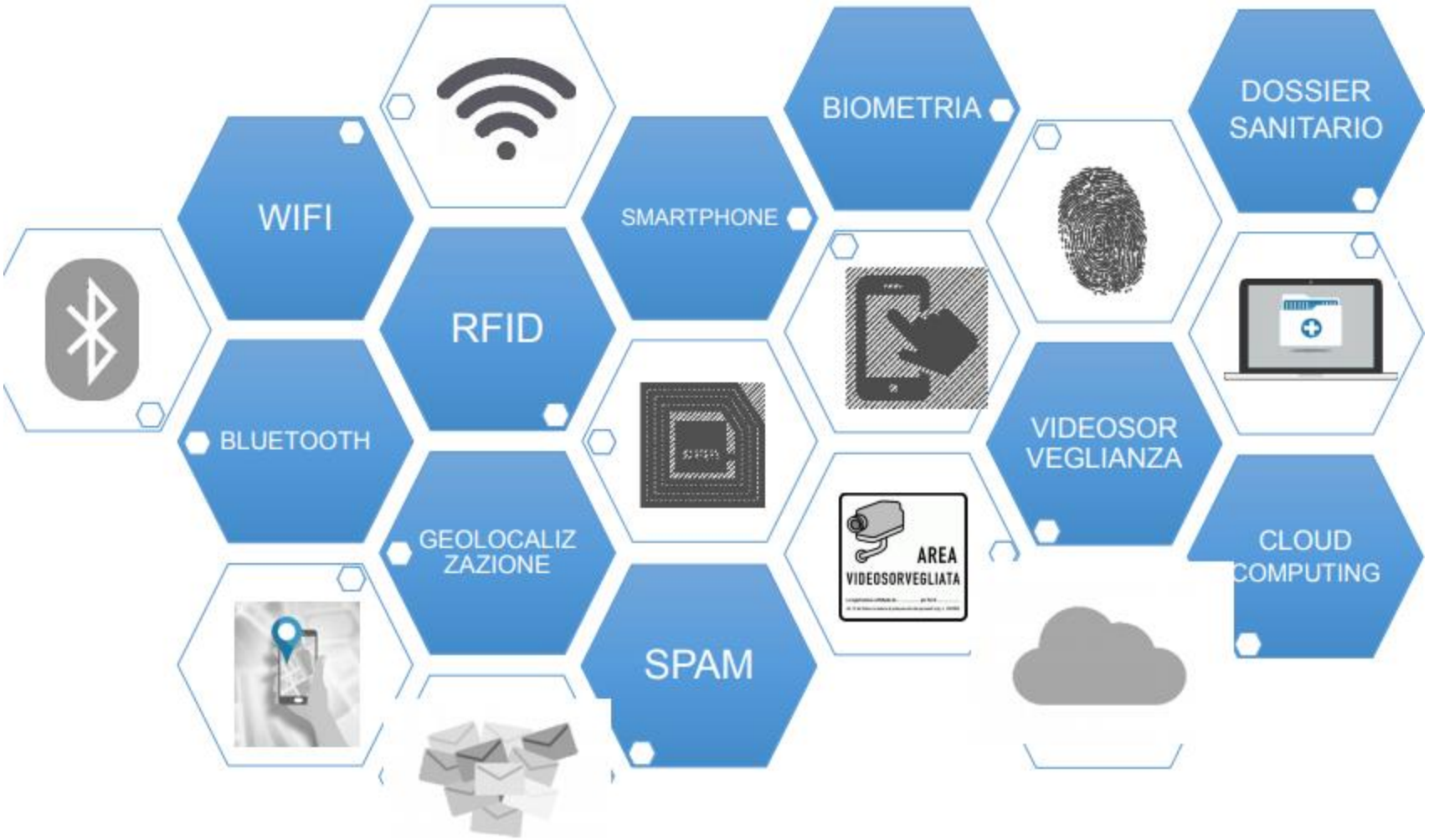
2018

Avvio Reg. EU

2021

D.L 14/06/21, n. 82

La tecnologia da mettere in sicurezza



Cosa si intende per misure di sicurezza

Le misure di sicurezza ICT devono rappresentare un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti.

Le misure consistono in controlli di natura

- **tecnologica,**
- **organizzativa**
- **procedurale**

utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.

A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa della P.A., le misure minime possono essere implementate in modo graduale seguendo tre livelli di attuazione.

Minimo: è quello al quale ogni P.A., indipendentemente dalla sua natura e dimensione, deve necessariamente rendersi conforme.

Standard: è il livello, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana.

Avanzato: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

Le misure minime sono un importante supporto metodologico, oltre che un mezzo attraverso il quale le Amministrazioni, soprattutto quelle più piccole e che hanno meno possibilità di avvalersi di professionalità specifiche, possono verificare autonomamente la propria situazione e avviare un percorso di monitoraggio e miglioramento. Le misure minime:

- **forniscono un riferimento operativo direttamente utilizzabile (checklist),**
- **stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili;**
- **forniscono uno strumento utile a verificare lo stato di protezione contro le minacce informatiche e poter tracciare un percorso di miglioramento;**
- **responsabilizzano le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica.**

Responsabilità della PA

L'adeguamento alle misure minime (AGID) è a cura del responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie, come indicato nel CAD (art. 17) o, in sua assenza, del dirigente designato. Il dirigente responsabile dell'attuazione deve compilare e firmare digitalmente il "Modulo di implementazione" allegato alla Circolare 18 aprile 2017, n. 2/2017.

Secondo la circolare, le misure minime di sicurezza devono essere adottate da parte di tutte le pubbliche Amministrazioni entro il 31 dicembre 2017.

La legge 109/2021 definisce l'architettura nazionale di cybersicurezza, introduce diverse novità in materia e istituisce:

- **L'Agenzia Nazionale per la Cybersecurity;**
- **Il Comitato interministeriale per la cybersicurezza;**
- **Il Nucleo per la cybersicurezza.**

Il Governo, intende promuovere la cultura della sicurezza cibernetica e aumentare la consapevolezza sul tema all'interno del settore pubblico, accendendo i riflettori sui rischi e sulle minacce cyber.

Infatti, l'accresciuta esposizione alle minacce cibernetiche ha evidenziato la necessità di sviluppare, idonei e sempre più stringenti meccanismi di tutela e Cyber Security

La Cyber Security, si concentra sugli aspetti legati alla sicurezza delle informazioni, rese accessibili da sistemi informatici, ed è spesso utilizzato come sinonimo di Information Security. In realtà, si tratta di una sottoclasse della Sicurezza Informatica, ovvero l'insieme dei mezzi, delle tecnologie e delle procedure utili a proteggere i sistemi informatici in termini di disponibilità, riservatezza e integrità dei dati e degli asset informatici.

Il termine Cyber Security viene utilizzato anche per indicare le qualità di resilienza, robustezza e reattività che una tecnologia deve possedere per fronteggiare gli attacchi informatici che possono colpire singoli individui, imprese private, enti pubblici e organizzazioni governative.

La cyber sicurezza costituisce uno degli interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021. Inoltre, è uno dei 7 investimenti della Digitalizzazione della pubblica amministrazione.

Nel Regolamento non esiste più una specifica definizione per

- **dati personali “sensibili”**
- **dati personali “giudiziari”**

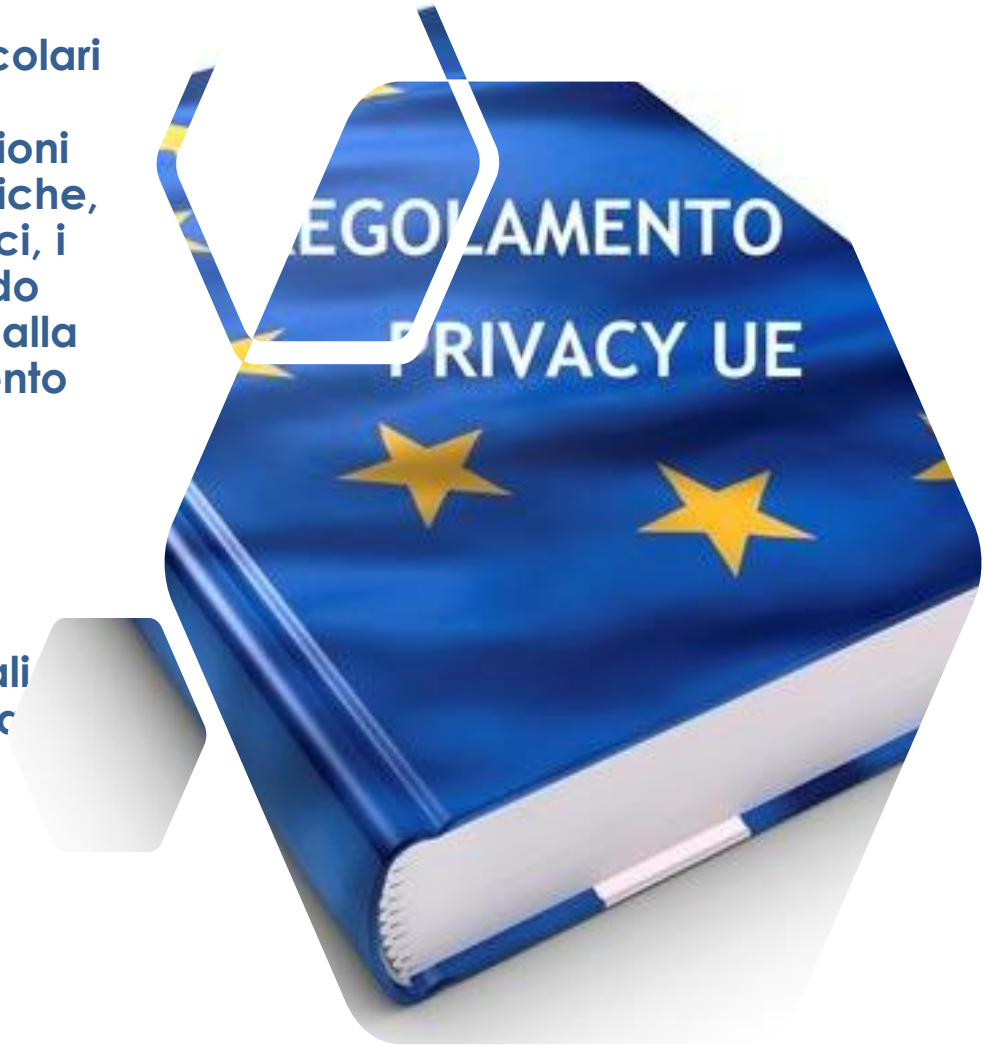
però la definizione è ricavabile dagli articoli generali dedicati a queste categorie di informazioni.

Art. 9

individua in generale le “categorie particolari di dati personali” nelle informazioni “che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona fisica”.

Art. 10

disciplina il trattamento dei “dati personali relativi alle condanne penali e ai reati o c connesse misure di sicurezza”.



Vulnerability assesment

Nell'era informatica in cui viviamo, dove gli attacchi informatici sia alle aziende che ai privati aumentano in modo esponenziale, effettuare correttamente un Vulnerability Assessment consente di proteggere i nostri dati e la nostra privacy (o almeno tentare di farlo) e sapere se la nostra azienda o il sito web presentino delle vulnerabilità che qualcuno potrebbe sfruttare per prenderne il controllo o rubare dei dati.

La maggior parte delle intrusioni ad un server avviene tramite lo sfruttamento di vulnerabilità, che si conoscono e i cui rimedi sono già conosciuti.

In ambito informatico, per Vulnerability Assessment si intende quel processo finalizzato a identificare e classificare i rischi e le vulnerabilità, in termini di sicurezza, dei sistemi informativi aziendali.

Il Vulnerability Assessment è un'analisi di sicurezza che ha come obiettivo l'identificazione di tutte le vulnerabilità potenziali dei sistemi e delle applicazioni valutando il danno potenziale che l'eventuale "attaccante" può infliggere all'unità produttiva.

Queste attività hanno lo scopo di scovare all'interno o all'esterno di un'organizzazione gli eventuali errori di programmazione o di errate configurazioni, commessi durante un'installazione o un upgrade dei sistemi informativi. Uno degli aspetti chiave di questa tipologia è l'isolamento tempestivo delle vulnerabilità evidenziate che potrebbero causare un blocco temporale o una grave perdita di dati.

Un buon strumento di Vulnerability Assessment permette all'utente di avere una situazione aggiornata del livello di sicurezza degli asset IT. Ovviamente, questo è il punto di partenza per ottimizzare tutti gli sforzi di security management.

La vulnerabilità è intesa come una componente di un sistema, in corrispondenza della quale le misure di sicurezza sono assenti, ridotte o compromesse, il che rappresenta un punto debole che consente a un aggressore di iniettare del codice malevolo compromettendo la sicurezza dell'intero sistema.

Se questo avviene, l'attaccante avrà la chiave universale per accedere all'intera infrastruttura o quasi, permettendo l'esfiltrazione di dati sensibili che possono causare una danno reputazionale importante.

IAM - IDENTITY ACCESS MANAGEMENT

La gestione dell'identity access management (IAM) assicura che le persone e le entità con identità digitali dispongano del livello di accesso adeguato a risorse aziendali quali reti e database. I ruoli degli utenti e i privilegi di accesso sono definiti e gestiti tramite un sistema IAM.

Una soluzione IAM consente agli amministratori IT di gestire in modo sicuro ed efficace le identità digitali degli utenti e i relativi privilegi di accesso. Con IAM, gli amministratori possono configurare e modificare i ruoli utente, monitorare e segnalare le attività degli utenti e applicare policy aziendali e di conformità normativa per la tutela della sicurezza dei dati e della privacy.

Una soluzione IAM è una raccolta di numerosi processi e strumenti. Gli amministratori IT usano le soluzioni IAM per il controllo dell'accesso alle reti tramite funzionalità quali la gestione del ciclo di vita della policy, l'accesso di networking dell'utente ospite e controlli sulla sicurezza.

In termini più tecnici, l'IAM è un mezzo per gestire le identità digitali di un determinato gruppo di utenti e i privilegi associati a ciascuna identità. È un termine generico che raggruppa una serie di prodotti diversi che assolvono tutti la stessa funzione di base. All'interno di un'organizzazione, l'IAM potrebbe essere un singolo prodotto oppure una combinazione di processi, software, servizi cloud e hardware che fornisce agli amministratori la visibilità e il controllo dei dati organizzativi a cui possono accedere i singoli utenti.