Casarosa Ultra Sintetizzato

Riservatezza: prevenzione della divulgazione non autorizzata di informazioni.
Integrità: garantisce che il messaggio inviato sia identico a quello ricevuto e che il messaggio non sia stato alterato durante il transito Disponibilità: garantisce che le informazioni siano disponibili all'utente in modo tempestivo e ininterrotto quando sono necessarie, indipendentemente dalla posizione dell'utente.

L'Unione europea (UE) opera in base al principio del conferimento, il che significa che può agire solo nei limiti delle competenze concesse dagli Stati membri nei trattati per raggiungere gli obiettivi prefissati. I poteri non conferiti all'UE rimangono agli Stati membri. L'Unione deve rispettare l'uguaglianza, l'identità nazionale e le funzioni statali essenziali degli Stati membri, tra cui l'integrità territoriale, l'ordine pubblico e la sicurezza nazionale, che restano di loro esclusiva competenza.

Base giuridica della legislazione dell'UE in materia di sicurezza informatica:

- **Articolo 114 del TFUE (Mercato interno):** Consente l'armonizzazione delle leggi tra gli Stati membri per garantire il corretto funzionamento del mercato interno, allineando le normative ed eliminando gli ostacoli al commercio e alla concorrenza.
- **Articoli 62 e 53(1) del TFUE (diritto di stabilimento e libertà di servizio):** Prevede norme che garantiscono la libertà di stabilimento e di prestazione di servizi in tutta l'UE.
- **Articoli 127, paragrafo 2, e 132, paragrafo 1, del TFUE (sistemi di pagamento):** Conferisce al Sistema europeo di banche centrali (SEBC) e alla Banca centrale europea (BCE) l'autorità di sostenere la stabilità dei prezzi, le politiche economiche e i compiti di regolamentazione.
- **Articolo 83, paragrafo 1, del TFUE (libertà, sicurezza e giustizia):** Consente di stabilire norme minime sui reati transfrontalieri gravi, compresa la criminalità informatica.

Per quanto riguarda le competenze non esclusive dell'UE, si applica il **principio di sussidiarietà**, che impone all'Unione di agire solo quando gli obiettivi non possono essere sufficientemente raggiunti dagli Stati membri da soli e possono essere affrontati meglio a livello di Unione. Il **principio di proporzionalità** garantisce che l'azione dell'UE sia limitata a quanto necessario per raggiungere gli obiettivi del Trattato. Entrambi i principi sono regolati da protocolli e monitorati dai parlamenti nazionali.

La struttura di governance dell'UE per la sicurezza informatica è decentralizzata e assegna le responsabilità a tre aree chiave: sicurezza delle reti e delle informazioni, criminalità informatica e difesa informatica.

Per quanto riguarda la **sicurezza delle reti e dell'informazione**, l'Agenzia dell'Unione europea per la sicurezza informatica (ENISA), istituita nel 2004 e dotata di un mandato permanente nel 2019 dalla legge sulla sicurezza informatica, svolge un ruolo centrale nel miglioramento della resilienza, nella sensibilizzazione e nella preparazione di schemi europei di certificazione della sicurezza informatica. Lavora insieme al CERT-EU, ai CSIRT e alle reti di cooperazione.

Per quanto riguarda la **criminalità informatica**, il Centro europeo per la criminalità informatica (EC3) fornisce supporto operativo, formazione e competenze agli Stati membri per combattere le attività dei criminali informatici.

Per quanto riguarda la **difesa cibernetica**, enti come l'Agenzia europea per la difesa (EDA) e lo Stato maggiore dell'UE svolgono funzioni di consulenza, mentre gli Stati membri mantengono il controllo operativo sulle attività di difesa.

L'ecosistema di sicurezza informatica dell'UE è strutturato attorno a quattro pilastri: resilienza, applicazione della legge, difesa informatica e diplomazia informatica. Questi pilastri comportano il coordinamento tra le organizzazioni dell'UE e i meccanismi per migliorare la sicurezza. L'Unità Cibernetica Congiunta sostiene gli sforzi operativi come la creazione di inventari di capacità, la produzione di rapporti sulla situazione, l'attuazione di piani di risposta alle crisi e la mobilitazione di squadre di reazione rapida. Una sicurezza informatica efficace si basa anche su una maggiore condivisione delle informazioni tra pubblico e privato per affrontare attacchi informatici sempre più complessi.

Regolamenti e direttive:

I regolamenti, come il GDPR, sono direttamente applicabili in tutti gli Stati membri, garantendo l'uniformità senza richiedere l'adozione di norme nazionali. recepimento. Le direttive, come la NIS2, fissano gli obiettivi che gli Stati membri devono raggiungere, ma consentono una certa flessibilità nell'attuazione, adattandosi ai contesti locali.

La legge sulla cibersicurezza (regolamento 2019/881) pone l'accento sul miglioramento delle capacità di cibersicurezza, sulla promozione della cooperazione e sul rafforzamento delle risposte a livello di Unione agli incidenti su larga scala. L'ENISA ha il compito di sostenere la cooperazione pubblico-privato e la protezione delle infrastrutture critiche, anche facilitando la condivisione delle informazioni all'interno dei settori.

La **direttiva NIS2 (2022/2555)** rafforza le capacità degli Stati membri di gestire gli incidenti di sicurezza informatica, imponendo la creazione di CSIRT dotati di risorse adeguate e capaci. Sottolinea la necessità di un'efficace condivisione delle informazioni su minacce e
vulnerabilità per migliorare la prevenzione, il contenimento e il recupero, nonostante le barriere esistenti, come la concorrenza e i problemi di responsabilità.

PPP

I partenariati pubblico-privati (PPP) nel campo della cybersecurity mirano a migliorare la sicurezza attraverso la collaborazione tra governi ed enti privati. Queste partnership affrontano la riluttanza degli attori privati a condividere volontariamente informazioni sensibili con le autorità pubbliche creando modelli di cooperazione strutturati.

L'ENISA definisce i PPP come relazioni contrattuali in cui soggetti pubblici e privati condividono rischi, responsabilità e risorse per raggiungere obiettivi comuni, come il miglioramento della resilienza della cybersecurity. Il livello di interazione tra attori pubblici e privati dipende dal settore; ad esempio, gli enti privati che forniscono servizi ai consumatori hanno spesso un rapporto più stretto con le autorità pubbliche rispetto a quelli che gestiscono infrastrutture fisiche.

Motivazioni e vantaggi:

Per le entità private, i PPP forniscono accesso a finanziamenti pubblici, approfondimenti normativi e opportunità di influenzare la legislazione e la standard. Per i governi, offrono una comprensione più approfondita delle esigenze del settore, l'accesso a risorse private e l'allineamento con le leggi e i regolamenti internazionali. I PPP favoriscono la fiducia, promuovono la condivisione delle informazioni e migliorano la resilienza complessiva della cybersecurity.

Tipi di PPP:

- **PPP istituzionali:** Stabiliti nell'ambito di quadri giuridici per la protezione delle infrastrutture critiche, coinvolgono gruppi di lavoro e comunità a lungo .
- **PPP orientati agli obiettivi:** Si concentrano sulla creazione di una cultura della cybersicurezza e sullo scambio di conoscenze.
- **Esternalizzazione dei servizi di sicurezza informatica:** I governi e i settori privati collaborano come fornitori di terze parti per soddisfare le esigenze del settore e definire le politiche.
- **PPP ibridi:** Spesso includono CSIRT incaricati di fornire servizi di cybersecurity a livello nazionale sotto la supervisione del governo.

Sfide:

I PPP devono affrontare ostacoli come la carenza di professionisti qualificati, i bilanci pubblici limitati, le difficoltà nel promuovere il dialogo tra i settori e la scarsa consapevolezza delle PMI. Le lacune a livello di leadership e i quadri giuridici poco chiari ostacolano ulteriormente una collaborazione efficace.

Per affrontare queste sfide, gli studi dell'ENISA raccomandano di promuovere la fiducia, migliorare la condivisione delle conoscenze e creare strutture legali e organizzative chiare per sostenere lo sviluppo dei PPP in Europa.

ECSO

L’European Cyber Security Organization (ECSO) è un’entità senza scopo di lucro creata nel 2016 per agire come la Commissione europea.
in un partenariato pubblico-privato nell'ambito di Horizon 2020. I suoi 250 membri comprendono principalmente attori dell'industria della cybersecurity e degli istituti di ricerca, con una certa rappresentanza del settore pubblico e delle industrie dal lato della domanda. L'ECSO si concentra sulla creazione di comunità, sullo sviluppo industriale e sulla formulazione di raccomandazioni sui programmi europei di cybersecurity.

Il Regolamento (UE) 2021/887 ha istituito il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza (ECCC) e una rete di centri nazionali di coordinamento (NNCC). Con sede a Bucarest, l'ECCC mira a sviluppare un'agenda comune per lo sviluppo e la diffusione delle tecnologie di cibersicurezza, concentrandosi sulle aree di interesse pubblico e sulle imprese, in particolare le PMI. Questa iniziativa rafforza la sovranità tecnologica europea facilitando gli investimenti congiunti in progetti strategici di cybersecurity.

L'ECCC si concentra sul coordinamento e sulla facilitazione, non su compiti operativi di cybersicurezza come la gestione degli incidenti. Sostiene lo sviluppo delle infrastrutture TIC per le industrie, le PMI e il settore pubblico, collaborando con gli NNCC per allineare gli sforzi. Gli NNCC
sono costituiti da un centro per ogni Stato membro, riconosciuto dalla Commissione europea per la sua capacità di gestire i fondi e di realizzare gli obiettivi di cybersecurity. Questi centri, tipicamente enti pubblici, devono possedere competenze in materia di cybersecurity e impegnarsi efficacemente con l'industria, la ricerca e il settore pubblico per realizzare la loro missione.

La direttiva sulle infrastrutture critiche europee (ECI) del 2008 si concentra sull'energia e sui trasporti, identificando le infrastrutture la cui interruzione interessa almeno due Stati membri. Stabilisce i requisiti di protezione per gli operatori e le autorità, anche se gli sforzi dell'UE ora includono azioni settoriali e intersettoriali più ampie, come la protezione del clima, la protezione civile e la sicurezza informatica. Gli Stati membri applicano misure nazionali diverse e sono state designate 94 ICE, soprattutto nei settori dell'energia e dell'Europa centrale e orientale.

La politica delle infrastrutture critiche si è evoluta per affrontare i rischi moderni, tra cui i rischi naturali, le minacce ibride, il terrorismo, le pandemie e le nuove tecnologie come il 5G. La maggiore interdipendenza tra i settori significa che le interruzioni possono avere effetti a cascata su più Paesi. L'ambito di applicazione abbraccia ora dieci settori, tra cui energia, trasporti, salute, finanza e spazio, con gli Stati membri che identificano le entità critiche attraverso valutazioni nazionali del rischio.

La politica enfatizza ora la resilienza rispetto alla protezione, incorporando misure sia preventive che reattive e accettando che gli incidenti si verifichino. Si è passati a un approccio più ampio, dal basso verso l'alto, che copre 11 settori critici e affronta le interdipendenze tra sistemi fisici e digitali.

Il coordinamento della sicurezza informatica si allinea alla direttiva NIS 2, che rafforza la resilienza delle entità essenziali e importanti. Le autorità responsabili delle entità critiche e della NIS 2 collaboreranno per affrontare i rischi informatici e non informatici, integrando la sicurezza fisica nella gestione del rischio di cybersecurity per le infrastrutture digitali critiche.

NIS

La Direttiva UE 2016/1148 mira a stabilire un livello elevato di sicurezza comune per i sistemi di rete e di informazione in tutta l'Unione per sostenere il mercato interno. Essa impone misure di sicurezza agli operatori di servizi essenziali (OES) e ai fornitori di servizi digitali (DSP); gli atti giuridici specifici del settore hanno la precedenza se soddisfano obblighi di sicurezza equivalenti.

La direttiva affronta le sfide della sicurezza informatica, come le capacità insufficienti, le disparità di preparazione degli Stati membri e la mancanza di requisiti di sicurezza comuni per gli OES e i DSP. Tra i suoi obiettivi principali vi è il rafforzamento della cooperazione a livello dell'Unione attraverso un gruppo di cooperazione per il coordinamento strategico e una rete di CSIRT per la collaborazione operativa.

Gli Stati membri devono adottare strategie nazionali per definire obiettivi, quadri di governance e misure per la preparazione, la risposta e il recupero, oltre a iniziative di educazione, sensibilizzazione e ricerca. L'ENISA può fornire assistenza nello sviluppo di queste
strategie.

Ogni Stato membro deve designare uno o più CSIRT per gestire i rischi e gli incidenti nei settori critici, assicurando risorse adeguate, infrastrutture resilienti e una cooperazione efficace all'interno della rete di CSIRT. L'ENISA fornisce supporto ai CSIRT nazionali, devono aderire a processi strutturati per la gestione degli incidenti.

La direttiva si applica agli OES e ai DSP, che sono tenuti a rispettare gli obblighi di sicurezza e di notifica degli incidenti per migliorare la resilienza della sicurezza informatica in tutta l'UE.

La direttiva richiede agli operatori di servizi essenziali (OES) e ai fornitori di servizi digitali (DSP) di implementare misure tecniche e organizzative proporzionate per gestire i rischi di sicurezza della loro rete e dei loro sistemi informativi. Tali misure devono essere in linea con lo stato dell'arte e garantire la continuità dei servizi essenziali riducendo al minimo l'impatto degli incidenti.

Per quanto riguarda la notifica degli incidenti, l'OES deve informare l'autorità competente o il CSIRT senza ritardi ingiustificati sugli incidenti in modo significativo. che incidono sulla continuità del servizio. Le notifiche devono consentire una valutazione degli impatti transfrontalieri senza aumentare la responsabilità. La rilevanza di un incidente è determinata da parametri quali il numero di utenti interessati, la durata e la diffusione geografica. Le autorità hanno la responsabilità di bilanciare l'interesse del pubblico a essere informato con i rischi commerciali e di reputazione degli operatori.

Allo stesso modo, i DSP devono implementare misure per gestire i rischi e garantire la continuità del servizio. Sono tenuti a notificare tempestivamente gli incidenti significativi, considerando fattori quali l'impatto sugli utenti, la durata, la diffusione geografica e l'interruzione della società. Gli obblighi di notifica si applicano solo se il fornitore è in grado di valutare adeguatamente l'impatto dell'incidente.

NIS2

La Direttiva NIS 2 (UE) 2022/2555 amplia il suo campo di applicazione per includere più settori critici per l'economia e la società, eliminando la distinzione tra operatori di servizi essenziali (OES) e fornitori di servizi digitali (DSP). Rafforza i requisiti di sicurezza con un approccio di gestione del rischio, garantendo che le entità implementino misure appropriate per mitigare efficacemente i rischi di cybersecurity. La direttiva si applica alle entità che forniscono servizi critici che, se interrotti, potrebbero avere un impatto significativo sulla sicurezza pubblica, la protezione, la salute o l'economia.

Requisiti di sicurezza

Gli Stati membri devono garantire che le entità essenziali e importanti adottino misure tecniche, operative e organizzative proporzionate ai rischi. Queste misure dovrebbero includere l'analisi del rischio, la gestione degli incidenti, la continuità operativa (ad esempio, backup, gestione delle crisi), la sicurezza della catena di approvvigionamento, le politiche di crittografia e l'autenticazione sicura. Per proteggere i sistemi e gli ambienti fisici è necessario utilizzare un approccio all-hazards.

Notifica dell'incidente

Le entità devono notificare tempestivamente ai CSIRT o alle autorità competenti gli incidenti significativi. Le notifiche devono valutare gli incidenti transfrontalieri
e includono avvisi tempestivi (entro 24 ore), notifiche di incidenti (entro 72 ore), rapporti intermedi (se richiesti) e rapporti finali (entro un mese). Le entità devono anche informare i destinatari dei servizi sulle minacce significative e sulle misure di mitigazione.

Vigilanza e applicazione

Le entità essenziali sono soggette a una supervisione proattiva, che comprende audit, ispezioni e scansioni di sicurezza. Le entità importanti sono sottoposte a una vigilanza ex post, con misure applicate solo dopo che sono emerse prove di non conformità. Le misure di vigilanza devono essere efficaci, proporzionate e dissuasive.

Sanzioni

Le sanzioni amministrative per la mancata conformità possono raggiungere i 10 milioni di euro o il 2% del fatturato globale per le entità essenziali e i 7 milioni di euro o l'1,4% per le entità importanti, a seconda della gravità della violazione.

Agenzia per l’Italia Digitale

La legge 134/2012 ha istituito l’Agenzia per l’Italia Digitale” per coordinare le iniziative di innovazione e promuovere le tecnologie ICT nelle pubbliche amministrazioni, in linea con l’Agenda Digitale Europea. Il Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013 ha centralizzato gli sforzi di cybersecurity tra le amministrazioni pubbliche e la comunità di intelligence.

Il Decreto Legislativo 65/2018 ha recepito la Direttiva UE 2016/1148 per rafforzare la sicurezza delle reti e delle informazioni a livello nazionale e comunitario. Gli Operatori di Servizi Essenziali (OES) e i Fornitori di Servizi Digitali (DSP) devono segnalare gli incidenti significativi al CSIRT italiano, con sanzioni pecuniarie in caso di inadempienza.

Il Decreto Legge 105/2019 ha ampliato le misure di cybersecurity attraverso il Perimetro Nazionale di Cybersecurity (PSNC), includendo entità pubbliche e private critiche per la sicurezza nazionale. Il DPCM 131/2020 ha definito le funzioni e i servizi essenziali coperti, come ad esempio
continuità del governo, difesa, sicurezza pubblica, infrastrutture e settori high-tech, concentrandosi sulla protezione dei sistemi la cui interruzione potrebbe minacciare la sicurezza nazionale.

Il DPCM 81/2021 prevede che le entità all'interno del PSNC prevengano, segnalino e rispondano agli incidenti, mantenendo inventari aggiornati di
reti, sistemi e servizi IT. Le valutazioni dei rischi e le misure di mitigazione devono essere in linea con gli standard europei e internazionali, come il framework NIST. La gravità degli incidenti determina le tempistiche di segnalazione al CSIRT italiano, con sanzioni in caso di non conformità.

Il Decreto presidenziale 54/2021 prevede che le entità del PSNC notifichino al Centro nazionale di valutazione e certificazione (CVCN) i prodotti o i servizi TIC esternalizzati. Il CVCN conduce valutazioni di sicurezza ed emette linee guida per il loro utilizzo.

ACN

L'Agenzia Italiana per la Cybersecurity (ACN) è un ente autonomo responsabile dell'impegno nazionale in materia di cybersecurity, che opera in modo indipendente pur attenendosi alle direttive del Presidente del Consiglio e alla supervisione del COPASIR per il mantenimento della politica.
imparzialità. I suoi obiettivi comprendono la salvaguardia della sicurezza informatica nazionale, lo sviluppo di capacità di prevenzione, monitoraggio, rilevamento e risposta alle minacce informatiche. L'ACN redige la strategia nazionale di cybersecurity, coordina le attività del settore pubblico-privato, migliora la sicurezza dell'industria digitale, fornisce pareri consultivi e promuove la collaborazione internazionale. Inoltre, fa rispettare la conformità alla cybersecurity all'interno del perimetro nazionale di cybersecurity (PSNC) e funge da autorità di vigilanza nazionale e da contatto per
sicurezza della rete.

Il CSIRT italiano monitora gli incidenti di cybersecurity, condivide avvisi e informazioni, interviene negli incidenti, conduce analisi dei rischi e partecipa alla collaborazione internazionale attraverso la rete di CSIRT con l'ENISA.

Il Decreto Legislativo n. 138 del 4 settembre 2024 attua la Direttiva UE 2022/2555 (NIS 2), aggiornando gli standard di cybersecurity. L'ACN identificherà le entità essenziali e importanti entro aprile 2025, con obblighi di sicurezza specifici basati sull'esposizione al rischio.
Le sanzioni per la mancata conformità includono multe per le entità essenziali e importanti, con multe aggiuntive per la mancata registrazione e comunicazione. Le violazioni ripetute possono comportare un aumento delle multe e la sospensione delle certificazioni.

La legge europea sulla cibersicurezza (regolamento 2019/881) istituisce l'ENISA e mira a far sì che l'UE guidi il mercato globale della cibersicurezza, affronti le lacune nella risposta agli attacchi informatici e si allinei alla strategia geopolitica dell'UE sulla sicurezza dei sistemi e delle reti di informazione.

Legge sulla sicurezza informatica

La legge sulla cibersicurezza rafforza il ruolo dell'ENISA nel migliorare la sicurezza informatica in tutta l'UE. L'ENISA fornisce supporto, consulenza e competenze agli Stati membri, alle istituzioni dell'UE e alle parti interessate, con l'obiettivo di ridurre la frammentazione delle normative in materia di cibersicurezza e garantire il coordinamento con gli sforzi nazionali. Opera in modo indipendente, promuovendo al contempo lo sviluppo di risorse per sostenere i compiti di cybersecurity, con particolare attenzione allo sviluppo di capacità, alla cooperazione operativa e alle soluzioni affidabili.

Il quadro di certificazione della sicurezza informatica dell'UE mira a creare un sistema unificato per la certificazione di prodotti, servizi e processi ICT in tutta l'UE. Questo quadro mira a creare fiducia, a ridurre le certificazioni nazionali in conflitto e a diminuire i costi aziendali nel mercato digitale. Il processo di certificazione prevede l'utilizzo di schemi nazionali e internazionali esistenti e la definizione di procedure tecniche di certificazione.
standard.

Esistono due tipi principali di schemi di certificazione: lo Schema europeo di certificazione della cibersicurezza, definito a livello di UE, e gli Schemi nazionali di certificazione della cibersicurezza, definiti dai singoli Stati membri. La certificazione può prevedere l'autovalutazione per
prodotti a basso rischio, con dichiarazione di conformità da parte dei produttori. Queste certificazioni sono riconosciute in tutti gli Stati membri dell'UE e possono influenzare l'accesso al mercato, la responsabilità e la conformità.

Un sistema centralizzato prevede un'autorità che supervisiona le certificazioni, mentre un sistema granulare utilizza più livelli per valutazioni personalizzate. La proposta dell'UE di modificare il Cybersecurity Act include i servizi di sicurezza gestiti negli schemi di certificazione, concentrandosi su obiettivi di sicurezza quali la garanzia di personale qualificato, il mantenimento di procedure interne, la protezione dei dati e la garanzia di resilienza e sicurezza del servizio.

EUCC

Gli standard di sicurezza informatica definiscono procedure, linee guida e specifiche per garantire la sicurezza, la coerenza e l'affidabilità delle attività.
prodotti, servizi e sistemi. Nel campo della cybersecurity, questi standard si concentrano sulle caratteristiche di sicurezza, sui controlli, sui processi e sulle linee guida che riducono i rischi e prevengono gli attacchi informatici. I vantaggi degli standard sono il risparmio di tempo e di costi, la maggiore consapevolezza degli utenti, la continuità operativa e la conformità alle best practice. Inoltre, consentono di confrontare i sistemi di sicurezza a livello internazionale.

Gli standard di cybersecurity forniscono metodi specifici per i processi, mentre i framework di cybersecurity offrono linee guida più ampie senza specificare le fasi. Esempi di standard di cybersecurity sono le serie ISO 27000, NIST e SOX.

Il sistema EUCC (European Cybersecurity Certification), proposto nel 2020, mira a sostituire il riconoscimento reciproco SOG-IS.
Accordo e miglioramento della sicurezza dei prodotti ICT, in particolare per i prodotti con funzioni di sicurezza integrate come firewall e dispositivi di crittografia. Offre due livelli di garanzia di sicurezza, "sostanziale" ed "elevato", esclusi i livelli di base e l'autovalutazione. Lo schema EUCC mira ad armonizzare gli standard di sicurezza in tutti gli Stati membri dell'UE, aumentando la fiducia dei consumatori nei prodotti certificati. Segue lo standard Common Criteria (CC), riconosciuto a livello mondiale e utilizzato da schemi nazionali in paesi come Francia, Germania e Italia.

Per ottenere un certificato EUCC, i richiedenti devono fornire una documentazione sull'uso del prodotto e sui rischi associati, che l'organismo di certificazione verifica. I domini tecnici per la certificazione includono AVA_VAN.4, per smart card e dispositivi che si basano su elementi hardware personalizzati, e AVA_VAN.5, per dispositivi hardware con involucri fisici di protezione, come i terminali di pagamento.

Nella cybersecurity, valori chiave come la sicurezza, la privacy, l'equità e la responsabilità sono essenziali per proteggere le informazioni da accessi non autorizzati, modifiche, distruzione e altre minacce.

La sicurezza si riferisce alla protezione da pericoli o danni, distinguendosi dalla sicurezza, che implica la protezione da minacce non intenzionali. La privacy riguarda il modo in cui le informazioni personali vengono condivise o mantenute riservate, concentrandosi sul controllo di quali dati vengono divulgati. L'equità riguarda l'uguaglianza, la giustizia e la non discriminazione nell'impatto delle misure di cybersecurity, garantendo un trattamento equo.

per tutti gli individui. La responsabilità si riferisce alla trasparenza e alla responsabilità, assicurando che i danni o gli squilibri di potere siano affrontati.

Il rapporto tra sicurezza e privacy è complesso, poiché il raggiungimento di una di esse ha spesso un impatto sull'altra. La sicurezza è necessaria per la privacy, ma il raggiungimento della privacy può richiedere sacrifici in termini di sicurezza.

GDPR

Il Regolamento generale sulla protezione dei dati (GDPR) definisce gli standard legali per la protezione dei dati personali e per garantire la privacy delle persone all'interno dell'Unione Europea. Si applica ai dati personali trattati sia all'interno che all'esterno dell'UE, a condizione che il trattamento riguardi l'offerta di beni o servizi agli interessati dell'UE o il monitoraggio del loro comportamento.

I dati personali comprendono tutte le informazioni che possono identificare o rendere identificabile un individuo, come ad esempio dettagli sulla sua salute, sul suo stile di vita o sulla sua situazione economica. I dati sensibili, come quelli di carattere sanitario o giudiziario, sono soggetti a ulteriori tutele.

Gli attori principali del trattamento dei dati sono l'interessato, i cui dati personali vengono trattati, il responsabile del trattamento, che determina le finalità e i mezzi del trattamento, e l'incaricato del trattamento, che tratta i dati per conto del responsabile.

Il GDPR garantisce agli interessati diversi diritti, tra cui il diritto di accedere ai propri dati, di richiedere la rettifica, la cancellazione o la limitazione del trattamento e di opporsi al trattamento, in particolare per il marketing diretto. Il diritto all'oblio garantisce alle persone la possibilità di cancellare i propri dati e i responsabili del trattamento sono tenuti a informare della richiesta di cancellazione i soggetti che hanno ricevuto tali dati.

Il trattamento dei dati deve essere conforme a principi quali la liceità, la limitazione delle finalità, la minimizzazione dei dati, l'accuratezza e la limitazione della conservazione. Il trattamento deve essere sicuro e i dati personali devono essere conservati solo per il tempo necessario. È inoltre necessaria una base legale, che può includere il consenso, gli obblighi contrattuali o l'interesse pubblico. Il consenso deve essere dato liberamente, informato e specifico per ogni finalità, e gli interessati devono ricevere informazioni chiare e trasparenti sulle modalità di trattamento dei loro dati.

Il GDPR enfatizza la responsabilità e la trasparenza, garantendo che le persone siano ben informate su come vengono utilizzati i loro dati e dando loro il controllo sui loro dati.

Il GDPR regolamenta il trasferimento di dati personali verso Paesi al di fuori dell'UE, consentendolo solo quando il Paese ricevente è stato ritenuto adeguato dalla Commissione europea, oppure quando si applicano garanzie o eccezioni appropriate.

Le autorità di controllo della protezione dei dati, compresi gli organismi nazionali come l'Autorità italiana per la protezione dei dati, vigilano sulla conformità. Hanno il potere di monitorare, consigliare, indagare, gestire i reclami e imporre azioni correttive. I reclami possono portare a sanzioni amministrative, con multe basate sulla gravità della violazione.

Il principio di responsabilità richiede che i responsabili e gli incaricati del trattamento dei dati garantiscano la conformità al GDPR e siano in grado di . Le misure da adottare a tal fine comprendono la tenuta di registri delle attività di trattamento, l'implementazione di misure di sicurezza e la conduzione di valutazioni d'impatto sulla protezione dei dati (DPIA).

Il GDPR stabilisce anche il diritto al risarcimento per le persone danneggiate dalla non conformità. I responsabili e gli incaricati del trattamento dei dati possono essere ritenuti responsabili dei danni, anche se possono essere esonerati se possono dimostrare di non essere responsabili della violazione.

Le valutazioni del rischio sono fondamentali nel GDPR, e i responsabili del trattamento devono implementare misure di sicurezza adeguate in base alla natura, alla portata e ai rischi del trattamento. Ciò include la protezione dei dati per progettazione e per impostazione predefinita, e misure come la crittografia e la pseudonimizzazione per proteggere i dati. Se il trattamento può comportare rischi elevati per i diritti delle persone, è necessaria una DPIA prima di iniziare il trattamento.

I rischi nel trattamento dei dati possono portare a conseguenze significative, come discriminazioni, frodi, perdita di reputazione o danni alla salute. privacy. Il GDPR considera i rischi legati alle categorie di dati sensibili e al trattamento dei dati su larga scala, in particolare quando sono coinvolti soggetti vulnerabili, come i bambini.

Gli effetti del trattamento dei dati possono portare a conseguenze negative significative per le persone, come ad esempio danni alla reputazione, discriminazione, furto di identità, perdite finanziarie e danni fisici o psicologici. Le persone possono anche perdere il controllo sui propri dati personali o incontrare difficoltà nell'esercitare i propri diritti, nell'accedere ai servizi o nel trarre vantaggio dalle opportunità a causa di un uso improprio dei dati. elaborazione.

La valutazione del rischio comporta l'identificazione e il controllo dei rischi all'interno di un'organizzazione. Gli elementi chiave includono la valutazione dell'origine, della natura, della gravità, della probabilità e dell'impatto dei rischi sui diritti e sulle libertà degli individui. La gravità dei rischi è classificata in quattro livelli: basso, medio, alto e molto alto, con conseguenze che vanno da piccoli inconvenienti a danni irreversibili.

La valutazione d'impatto sulla protezione dei dati (DPIA) è richiesta solo quando il trattamento può comportare un rischio elevato per i diritti e le libertà delle persone. Anche se la DPIA non è obbligatoria, i responsabili del trattamento devono comunque valutare i rischi e attuare misure adeguate per , garantendo che i rischi per i diritti degli interessati siano ridotti al minimo.

La DPIA (Data Protection Impact Assessment) è uno strumento previsto dal GDPR utilizzato per valutare i rischi delle operazioni di trattamento dei dati personali e garantire la conformità. Il suo scopo è quello di identificare i rischi potenziali per i diritti e le libertà delle persone, valutare la necessità e la proporzionalità delle attività di trattamento e definire le garanzie per mitigare tali rischi.

Quando è richiesta una DPIA?

È obbligatorio per le operazioni di trattamento che possono comportare rischi elevati, come esempio:

- Processo decisionale automatizzato o profilazione con effetti significativi sulle persone.
- Trattamento su larga scala di dati sensibili o di casellari giudiziari.

- Monitoraggio sistematico delle aree accessibili al pubblico su larga scala.

Le DPIA non sono necessarie quando il trattamento non presenta rischi significativi, quando un trattamento simile è già stato valutato o quando è regolato da leggi specifiche per le quali è già stata eseguita una DPIA.

Chi conduce una DPIA?

Il titolare del trattamento è responsabile dell'della DPIA, anche se può delegare il compito internamente o esternamente. Gli incaricati del trattamento devono contribuire a fornire le informazioni pertinenti. I responsabili della protezione dei dati (RPD) devono essere consultati e, se del caso, è necessario chiedere il parere degli interessati.

Come condurre una DPIA?

Il processo inizia prima dell'avvio dell'operazione di elaborazione dei dati e deve essere aggiornato durante tutto il ciclo di vita. Comprende:

1. Descrivere le operazioni di trattamento e le finalità.
2. Valutare i rischi per i diritti e le libertà delle persone.
3. Valutare la necessità e la proporzionalità del trattamento.
4. Identificare le misure tecniche e organizzative per ridurre i rischi.

Conseguenze della non conformità:

La mancata o scorretta esecuzione di una DPIA può comportare multe fino a 10 milioni di euro o al 2% del fatturato mondiale annuo.

Violazioni dei dati e GDPR:

Una violazione dei dati personali comporta l'accesso non autorizzato, la perdita o la divulgazione di dati personali. Non tutti gli incidenti di sicurezza sono violazioni di dati, ma solo quelli che hanno un impatto sulla riservatezza, l'integrità o la disponibilità dei dati personali.

Gestione delle violazioni:

- **Prevenire**: Ridurre al minimo la raccolta dei dati, proteggere i dispositivi, utilizzare la crittografia e aggiornare regolarmente i sistemi.
- **Rilevare**: Utilizzare strumenti di registrazione, monitoraggio e forensi per identificare tempestivamente le violazioni.
- **Valutare**: Determinare l'impatto della violazione sui dati personali e sui diritti delle persone. Informare le autorità entro 72 ore se c'è un rischio per le persone.
- **Comunicare**: Informare le persone interessate se la violazione presenta un rischio elevato, a meno che le misure di protezione (come la crittografia) non attenuino rischio.

La trasparenza è essenziale per la fiducia e la responsabilità organizzativa. I responsabili del trattamento dei dati devono documentare le violazioni e dimostrare la conformità alle autorità di vigilanza, mentre per le violazioni significative può essere richiesta una comunicazione pubblica.

La Strategia europea sui dati sottolinea la creazione di uno spazio unificato dei dati all'interno dell'UE che promuova il libero flusso dei dati, l'adesione alle leggi europee e l'accesso equo ai dati, garantendo al contempo una solida governance e il mantenimento dei valori europei. Riconosce il valore del riutilizzo dei dati nei settori pubblico e privato, evidenziando sfide come gli squilibri del mercato, l'interoperabilità e la governance per massimizzare l'utilità dei dati, in particolare nell'IA.

La legge sui dati mira ad armonizzare le norme sull'accesso e la condivisione dei dati e riguarda i produttori, i fornitori di servizi e le istituzioni pubbliche dell'UE. Garantisce un uso equo dei dati, protegge dall'accesso non autorizzato, facilita il passaggio da un dato all'altro.
servizi e sviluppa standard di interoperabilità. Il regolamento si applica in modo ampio, includendo i produttori, gli utenti, le istituzioni pubbliche e i responsabili del trattamento dei dati.

In casi di eccezionale necessità, come emergenze pubbliche o compiti critici di interesse pubblico, la legge prevede che i titolari dei dati forniscano i dati alle autorità pubbliche, comprese la Commissione europea e la Banca centrale europea, se non sono disponibili alternative. Tale
Le richieste devono essere precise, giustificate, proporzionate e rispettare i principi della protezione dei dati, con garanzie come la pseudonimizzazione o l'anonimizzazione quando si tratta di dati personali.

La legge affronta anche i problemi di sicurezza informatica, in particolare nelle emergenze come gli attacchi ransomware, affermando che l'interesse pubblico ad accedere ai dati può superare il controllo del titolare dei dati. Stabilisce le condizioni per la condivisione dei dati, garantendo la protezione dei segreti commerciali e la conformità con i quadri giuridici, imponendo al contempo trasparenza e responsabilità nel processo di richiesta.

Veicoli a guida autonoma

Per funzionare efficacemente, i veicoli a guida autonoma (AV) si affidano in larga misura alla connettività, utilizzando sistemi come Vehicle-to-Network (V2N), Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Infrastructure-to-Vehicle (I2V), Vehicle-to-Person (V2P) e una più ampia comunicazione Vehicle-to-Everything (V2X). Mentre le attuali funzioni AV assistono principalmente i conducenti con avvisi o controlli limitati, i progressi futuri mirano a integrare completamente queste funzioni nel processo di guida, sostituendo completamente il conducente.

L'intelligenza artificiale svolge un ruolo cruciale nella realizzazione di veicoli autonomi, con capacità fondamentali quali il rilevamento, la localizzazione, la rappresentazione della scena, la pianificazione e il controllo. Le principali tecnologie di IA includono il riconoscimento degli oggetti, la segmentazione (classificazione delle regioni dell'immagine in categorie), la localizzazione del veicolo (stima della posizione nel) e il tracciamento della dinamica degli oggetti in movimento.