PRATICA GUIDA GDPR

SICUREZZA DEL DATI PERSONALI

Versione 2024

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

L'obiettivo di questa guida è supportare le organizzazioni nell'implementazione delle misure di sicurezza al fine di garantire la protezione dei dati personali che trattano.

Si rivolge in particolare ai responsabili della protezione dei dati (DPO), al responsabile della sicurezza delle informazioni (CISO) e agli informatici. Anche i consulenti privacy potranno trovare elementi utili.

Questa guida è uno strumento vivo arricchito da pratiche all'avanguardia ed elementi dottrinali dell'autorità francese per la protezione dei dati (CNIL) sulla questione della sicurezza dei dati.

Sul sito web della CNIL è disponibile un registro delle modifiche per aiutare gli attori a identificare le evoluzioni di cui tenere conto per adattare il proprio livello di sicurezza.

SOMMARIO

PREFAZIONE

La sicurezza è una parte essenziale della protezione dei dati personali. È vincolante per qualsiasi titolare del trattamento e responsabile del trattamento ai sensi dell'articolo 32 del Regolamento generale sulla protezione dei dati1 (GDPR). In linea di principio, ogni operazione di trattamento deve essere sottoposta ad un insieme di misure di sicurezza decise in base al contesto, vale a dire ***"precauzioni utili, avuto riguardo alla natura dei dati e ai rischi*** *presentati).* Il GDPR specifica che il *trattamento"* l'adozione di *"misure* L'articolo 121 del francese Dati Protezione Atto2 (la protezione dei dati personali richiede *tecniche e organizzative adeguate per garantire un* ***livello di sicurezza adeguato al rischio"*** per i diritti e le libertà delle persone fisiche, compresa la loro riservatezza.

Per valutare le misure da attuare è necessario adottare due approcci complementari:

– la creazione di una base di sicurezza che incorpori buone pratiche derivanti da anni di capitalizzazione sull'igiene e sulla sicurezza informatica (ad esempio: regolamenti, standard, guide). Questa base mira ad affrontare i rischi più comuni;

– l'analisi dei rischi3 per gli interessati dal trattamento, che mira a identificare e valutare i rischi specifici del trattamento. Tale analisi supporta un processo decisionale obiettivo sul trattamento di questi rischi e l'identificazione delle misure necessarie e adeguate al contesto.

Tuttavia, è difficile per i non specialisti in sicurezza informatica attuare un simile approccio e garantire che il livello di sicurezza del trattamento di cui sono responsabili sia sufficiente.

Per facilitare la conformità, questa guida presenta una serie di raccomandazioni raggruppate per schede tematiche. Ogni scheda informativa è strutturata in tre sezioni:

– precauzioni di base, che incorporano buone pratiche essenziali;
– cattive pratiche di tendenza, che dovrebbero essere evitate;
– misure aggiuntive, da fare ulteriormente4 .

Ogni scheda può essere letta separatamente dalle altre: i riferimenti sono riportati in occasione di un'altra scheda.

1 "Regolamento generale sulla protezione dei dati – GDPR", eur-lex.europa.eu
2 "Legge sulla protezione dei dati", cnil.fr
3 In particolare, è essenziale quando il trattamento deve essere sottoposto a una valutazione d'impatto sulla protezione dei dati o a una DPIA (vedi "Cosa devi sapere sull'analisi d'impatto sulla protezione dei dati (AIPD)", cnil .Fr).
4 Queste misure potrebbero col tempo e con la pratica diventare precauzioni di base.

SCHEDA 1 – GESTIONE DELLA SICUREZZA DEI DATI

Attuare e mantenere la protezione dei dati personali richiesta dal GDPR e dalle normative settoriali.

L'integrazione della protezione dei dati nei processi decisionali dell'organizzazione garantisce che se ne tenga conto nel tempo e nei momenti chiave in cui vengono decisi budget e progetti.

Precauzioni di base

• **Coinvolgere il management** e formalizzare gli obiettivi generali in termini di sicurezza e protezione dei dati personali, approvati dal management dell'organizzazione.

• **Identificare** (attraverso il registro5) **il trattamento dei dati personali,** automatizzato o meno, i dati trattati (es: fascicoli clienti, contratti) e i supporti su cui si basano:

– l'hardware (es: server, laptop, dischi rigidi);
– il software (es.: sistemi operativi, software aziendali);
– le risorse di cloud computing utilizzate (es: SaaS, PaaS, IaaS);
– i canali di comunicazione logici o fisici (es.: connessioni cablate, Wi-Fi, Internet, scambi verbali, corrieri);

– i documenti cartacei (es: documenti stampati, fotocopie);
– i locali e le strutture fisiche in cui sono ubicati gli elementi di cui sopra (es.: sale informatiche, uffici).

Formalizzare le interconnessioni e i diagrammi di flusso dei dati tra i diversi componenti dei sistemi informativi. Il registro e gli schemi devono essere aggiornati ogniqualvolta si verifichi una modifica strutturale dei processi o delle componenti dei sistemi informativi.

• **Definire un piano d'azione per la sicurezza informatica e implementare le misure tecniche e organizzative definite** per garantire la protezione dei dati. A tal fine si possono attuare due approcci complementari: da un lato, attuare le precauzioni di base elencate nella presente guida (vedi checklist di valutazione) e, dall'altro, integrarle con misure specifiche individuate mediante l'analisi dei rischi6 (vedi scheda informativa 20 – Analisi dei rischi).

Ogni nuova misura decisa deve incorporare il piano d'azione, i cui progressi sono monitorati regolarmente.

• **Controllare periodicamente l'efficacia delle misure tecniche e organizzative** per garantire che raggiungano lo scopo previsto (ad esempio stabilendo indicatori). Dare priorità alle misure implementate per affrontare le vulnerabilità identificate o prevenire incidenti che si sono già verificati.

• **Garantire che la direzione sia tenuta informata** sulla gestione del rischio IT attraverso un riesame della direzione almeno una volta all'anno. Dovrebbe consentire di adottare decisioni e di produrre una sintesi di produrre una sintesi e di prendere decisioni tenendo presente:

– il contesto in evoluzione, le sfide e le aspettative degli stakeholder (es: clienti, partner, autorità di vigilanza);

– il cambiamento degli obiettivi e delle missioni dell'organizzazione;
– l'evoluzione delle minacce informatiche;
– lo sviluppo di nuove tecnologie o soluzioni di sicurezza;

5 "Il registro dei trattamenti", cnil.fr

6 L'articolo 35 del GDPR richiede una valutazione d'impatto sulla protezione dei dati (DPIA) per determinati tipi di trattamento (vedi "Che cosa devi sapere sulla valutazione d'impatto sulla protezione dei dati (AIPD)", cnil.fr).

– la natura evolutiva dei sistemi informativi e del trattamento dei dati;
– l'evoluzione dei rischi per la sicurezza dei dati e la privacy;
– lo stato di avanzamento del piano d'azione legale (es: rispetto dei contratti) e del piano d'azione tecnico (misure di sicurezza);
– gli incidenti e le violazioni riscontrati, con il loro impatto sull'organizzazione e sull'interessato;

– le richieste ed i reclami ricevuti e trattati riguardanti i dati personali.

• **Migliorare la protezione dei dati personali nel tempo.** In particolare, il riesame della gestione dovrebbe consentire di decidere in merito all'assegnazione delle risorse umane e di bilancio necessarie per le misure da attuare e per il miglioramento continuo della sicurezza.

Cosa dovrebbe essere evitato

• Considerare la sicurezza come un aspetto secondario che può essere affrontato in una fase successiva, una volta che l'elaborazione dei dati è già operativa.
• Concentrarsi su misure avanzate senza adottare le precauzioni di base.
• Limitarsi ad azioni una tantum e non considerare il trattamento dei dati nel suo complesso (ad esempio raccolta dei dati, partner, fine vita) al momento di decidere sulle misure di sicurezza da attuare.
• Basarsi esclusivamente su misure tecniche senza supportarle con un'organizzazione coerente le misure.
• Definire un piano d'azione senza assegnare una scadenza e responsabile dell'implementazione di ciascuna azione.

• Delegare la gestione di tutta la sicurezza informatica a un fornitore.

ANDARE OLTRE

• Per il monitoraggio quotidiano della sicurezza e della protezione dei dati, è molto utile (o addirittura obbligatorio a seconda della natura dell'organizzazione) **nominare un responsabile della sicurezza delle informazioni (CISO) e un responsabile della protezione dei dati7 (DPO).** Essi devono:

- essere qualificati per **riferire direttamente al più alto livello di gestione;**
- **disporre delle risorse e delle condizioni di lavoro necessarie** per svolgere i propri compiti;
- **essere coinvolti** (se stessi o il proprio team) sistematicamente e in una fase iniziale nelle discussioni su questioni relative alla propria area di responsabilità, al fine di garantire che i sistemi informativi siano sicuri e che i dati personali siano protetti **by design e by default.**

• Gli obiettivi generali per la protezione dei dati personali possono essere registrati in una politica generale di protezione dei dati, approvata dalla direzione e comunicata a tutti i soggetti coinvolti (personale, subappaltatori, partner). Tale politica potrà poi essere specificata a livello operativo sotto forma di politiche tematiche e procedure dettagliate per adattare le misure di protezione dei dati personali al contesto delle attività dell'organizzazione.

• **Gli audit di sicurezza sono uno strumento essenziale per valutare il livello di sicurezza dei sistemi su cui si basa il trattamento dei dati personali.** Eseguiti periodicamente, consentono di tenere conto dei cambiamenti nei processi e delle minacce. Ogni audit deve produrre un piano d'azione, la cui attuazione dovrebbe essere monitorata al livello più alto dell'organizzazione.

• Per strutturare la governance nel tempo è possibile impostare un sistema di gestione basato su un approccio di miglioramento continuo. Lo standard internazionale ISO/IEC 277018 descrive i processi e le misure organizzative e tecniche per implementare un sistema di gestione delle informazioni sulla privacy (PIMS), basato sul sistema di gestione della sicurezza delle informazioni (ISMS) coperto dallo standard ISO/IEC 27001.

• L'Agenzia nazionale francese per la sicurezza informatica (ANSSI) ha pubblicato la propria guida9 sulle migliori pratiche in materia di sicurezza informatica.

7 "Diventa delegato alla protezione dei dati", cnil.fr
8 "ISO 27701, uno standard internazionale per la protezione dei dati personali", cnil.fr
9 "Linee guida per un sistema informativo sano in 42 misure", cyber.gouv.fr

UTENTI

SCHEDA 2 – DEFINIRE UN QUADRO PER GLI UTENTI

Dare valore vincolante alle principali regole per l'utilizzo degli strumenti informatici.

Gli utenti utilizzano spesso quotidianamente gli strumenti IT. Le loro pratiche possono avere un impatto diretto sulla sicurezza dei dati personali e pertanto devono essere inquadrate.

Precauzioni di base

- **Elaborare una carta informatica e darle valore vincolante** (es.: annessione al Regolamento).
- **Includere nella carta** almeno quanto segue:

1. Un richiamo alle norme sulla protezione dei dati e alle sanzioni previste per il mancato rispetto di tali norme.

2. Il campo di applicazione della Carta, che dovrebbe includere in particolare:
   - le modalità di intervento dei team responsabili della gestione delle risorse informatiche dell'organizzazione;
   - le modalità di autenticazione utilizzate dall'organizzazione e la password policy che l'utente – deve rispettare;

   - le regole di sicurezza che gli utenti devono rispettare tra cui:
     - segnalare al dipartimento IT interno qualsiasi sospetta violazione o tentativo di violazione del proprio account informatico, qualsiasi smarrimento o furto di apparecchiature e, in generale, qualsiasi malfunzionamento;
     - non affidare mai la propria password (o equivalente) a terzi;
     - non installare, copiare, modificare, distruggere o configurare software senza autorizzazione;
     - bloccare (o spegnere) il computer non appena ci si allontana dalla propria postazione di lavoro;
     - non accedere, tentare di accedere o cancellare le informazioni se ciò non è di responsabilità del utente;
     - rispettare le procedure preventivamente definite dall'organizzazione al fine di regolamentare le operazioni di copia dei dati su supporti rimovibili, in particolare ottenendo la preventiva approvazione del superiore gerarchico e rispettando le norme di sicurezza.
3. Le modalità di utilizzo delle apparecchiature informatiche e delle risorse telematiche messe a disposizione tali come:
   - postazioni di lavoro;
   - attrezzature mobili (soprattutto nel contesto del telelavoro);
   - spazi di stoccaggio individuali;
   - reti locali;
   - dispositivi personali (in particolare le condizioni per l'utilizzo di tali dispositivi);
   - Internet;
   - messaggistica elettronica;
   - telefonia.
4. Le condizioni che regolano l'amministrazione del sistema informativo e l'esistenza, ove applicabile, di:

   - sistemi di filtraggio automatici;
   - sistemi di registrazione automatica;
   - sistemi di gestione delle postazioni di lavoro.
5. Le responsabilità e le sanzioni previste in caso di mancato rispetto della Carta.

Cosa dovrebbe essere evitato

• Non dare forza vincolante alla Carta o non applicarla e farla rispettare in caso di inosservanza.
• Non considerare le pratiche reali degli utenti, le loro aspettative e le loro esigenze definendo le regole per l'uso dell'IT significa: lo shadow IT a volte rivela bisogni essenziali che non vengono soddisfatti dall'organizzazione o un malfunzionamento strutturale.
• Non supportare gli utenti nelle loro pratiche.

ANDARE OLTRE

• Prevedere la sottoscrizione **di un impegno di riservatezza** (vedi clausola di esempio di seguito), oppure inserire nei contratti di lavoro una **specifica clausola di riservatezza** relativa ai dati personali.
• Prevedere una carta specifica per gli amministratori che dettagli i requisiti aggiuntivi che questa popolazione particolarmente a rischio deve rispettare.

Esempio di clausola di impegno di riservatezza per soggetti destinati a manipolare dati personali

Io sottoscritto Sig./Sig.ra. esercitando le funzioni di_____ all'interno della società_____(di seguito "Società"), essendo pertanto tenuto ad accedere ai dati personali, dichiara di riconoscere la riservatezza di tali dati.

Mi impegno pertanto, ai sensi dell'articolo 32 del Regolamento generale sulla protezione dei dati del 27 aprile 2016, ad adottare tutte le precauzioni conformi allo stato dell'arte e alle norme interne nell'ambito delle mie competenze al fine di tutelare la riservatezza delle informazioni a cui ho accesso, ed in particolare per evitare che gli stessi siano comunicati a soggetti non espressamente autorizzati a ricevere tali informazioni.

In particolare mi impegno a:

- non utilizzare i dati a cui posso accedere per scopi diversi da quelli previsti dai miei poteri;
- comunicare tali dati solo a soggetti debitamente autorizzati, in ragione delle loro funzioni, a ricevere tali informazioni, ove privato, pubblico, naturale o giuridico;
- non fare copie di questi dati se non per quanto necessario per lo svolgimento dei miei compiti;
- adottare tutte le misure coerenti con lo stato dell'arte e le regole interne nell'ambito dei miei poteri al fine di evitare l'uso improprio o fraudolento di questi dati;
- adottare tutte le precauzioni conformi allo stato dell'arte e alle norme interne per preservare la sicurezza fisica e logica di tali dati;
- garantire, nell'ambito dei miei poteri, che per trasferire questi dati verranno utilizzati solo mezzi di comunicazione sicuri;
- in caso di cessazione dall'incarico restituire integralmente i dati, gli archivi informatici ed ogni supporto informatico relativi a tali dati.

Tale impegno di riservatezza, in vigore per tutta la durata del mio incarico, resterà efficace, dopo la cessazione dall'incarico, qualunque ne sia la causa e fino a quando i dati non saranno resi pubblici da parte della Società, a condizione che tale impegno riguardi l'utilizzo e la comunicazione di dati personali dati.
Sono stato informato che qualsiasi violazione di questo impegno mi espone a sanzioni disciplinari e penali ai sensi della normativa vigente, in particolare per quanto riguarda gli articoli 226-13 e da 226-16 a 226-24 del Codice Penale.

Fatto a xxx, xxx, in xxx esemplari

Nome:
Firma:

SCHEDA 3 – COINVOLGERE E FORMARE GLI UTENTI

Rendere ogni utente consapevole delle sfide relative alla privacy e alla sicurezza.

Gli errori umani e gli attacchi di ingegneria sociale sono responsabili di un numero significativo di incidenti di sicurezza. Le soluzioni tecniche non sono sufficienti per garantire la protezione dei dati personali detenuti dalle organizzazioni.

Precauzioni di base

• **Sensibilizzare gli utenti (sia interni che esterni all'organizzazione) che lavorano con dati personali sui rischi per la privacy, informandoli delle** misure implementate per affrontare tali rischi e delle potenziali conseguenze in caso di non conformità. Concretamente può essere:

  – organizzare sessioni di sensibilizzazione sui rischi, sulle principali tipologie di attacchi (es: phishing, ransomware, furto di identità), sulla vigilanza necessaria (es: prima di aprire un allegato o cliccare su un collegamento in un messaggio, quando si risponde al telefono), e cosa cosa fare in caso di incidente o sospetto (misure di protezione e di allerta);

  – inviare regolarmente promemoria di istruzioni in base agli eventi attuali dell'organizzazione (es: recente tentativo di phishing, arrivo di un nuovo provider).

• Implementare diverse campagne di sensibilizzazione il cui **contenuto e linguaggio siano adattati ai ruoli dei destinatari.** Ad esempio, il personale delle risorse umane deve essere informato dei dati che gestisce e i dipendenti che lavorano fuori sede devono essere informati dei rischi specifici del nomadismo.

• Garantire che il personale incaricato del trattamento dei dati personali (es.: addetti alla gestione dei reclami o dei documenti amministrativi) abbia pienamente recepito le buone pratiche relative alla protezione dei dati personali da attuare quotidianamente (es: valutazione delle conoscenze).

• Formare il personale addetto agli strumenti informatici (es: addetti alla progettazione e alla manutenzione) in materia di sicurezza informatica e protezione dei dati personali.

• **Documentare le procedure operative,** mantenerle aggiornate e renderle disponibili a tutti gli utenti interessati. In concreto, qualsiasi azione sui dati personali, sia che si tratti di un'operazione di amministrazione o del semplice utilizzo di un'applicazione, deve essere spiegata con un linguaggio chiaro e adatto a ciascuna categoria, in documenti ai quali gli utenti possono fare riferimento.

Cosa dovrebbe essere evitato

• Imporre strumenti informatici senza accompagnarne l'adozione da parte dei team.

• Non rendere obbligatorio per i nuovi assunti la partecipazione alla sessione sulla protezione dei dati personali, quando l'attività principale dell'organizzazione comporta il trattamento dei dati personali (es: struttura sanitaria, servizio clienti).

• Sottovalutare l'impatto positivo che dipendenti ben informati possono avere sulla sicurezza IT dell'organizzazione.

• Non garantire la consapevolezza dei fornitori di servizi esterni (mediante azione diretta o impegno contrattuale) quando il loro impatto sulla sicurezza dei dati può essere altrettanto significativo di quello dei dipendenti interni.

ANDARE OLTRE

- Implementare una politica e strumenti **di classificazione delle informazioni** che definiscano diversi livelli (ad esempio: pubblico, interno, confidenziale) e richiedano di contrassegnare i documenti, i media e le e-mail contenenti dati riservati.
- Apporre un avviso visibile ed esplicito su ogni pagina dei documenti cartacei o informatici che contengono dati sensibili10 .
- Organizzare **esercitazioni e simulazioni di incidenti o crisi di sicurezza informatica** (previa organizzazione e supervisione necessarie per qualsiasi esercitazione di sicurezza). Questi esercizi consentono di verificare il grado di applicazione delle istruzioni e l'efficacia delle procedure di gestione degli incidenti e delle crisi in atto. Il consolidamento del feedback derivante da questi esercizi consente di identificare i messaggi da rafforzare e le procedure da migliorare.

10 I dati sensibili sono descritti nell'articolo 6 della legge francese sulla protezione dei dati e sulle libertà e nell'articolo 9 del GDPR.

SCHEDA 4 – AUTENTICARE GLI UTENTI

Riconoscere gli utenti in modo che possano ottenere gli accessi necessari.

Prima di qualsiasi utilizzo delle risorse informatiche, l'utente deve ricevere un **proprio identificativo e deve autenticarsi** in modo da poter verificare la sua identità e gli accessi ai dati di cui ha bisogno.

I meccanismi per effettuare l'autenticazione delle persone sono classificati a seconda che coinvolgano:

- un fattore di conoscenza (ciò che si sa), ad esempio una password;
- un fattore di possesso (cosa si ha), ad esempio una smart card;
- un fattore intrinseco (che cosa si è), ad esempio un'impronta digitale o la dinamica della pressione dei tasti[11] . Si ricorda che il trattamento di dati biometrici finalizzato a identificare in modo univoco una persona fisica sulla base delle sue caratteristiche fisiche, fisiologiche o comportamentali costituisce un trattamento di dati sensibili che dà luogo all'applicazione dell'articolo 9 del GDPR [12].

L'autenticazione dell'utente è definita **multifattoriale** quando utilizza una **combinazione di almeno due fattori** di categorie distinte. Si dice **forte** se si basa su un meccanismo crittografico i cui parametri e sicurezza sono considerati robusti (es: chiave crittografica).

Precauzioni di base

• **Definire un identificatore univoco per utente e vietare account condivisi** tra più utenti. Nel caso in cui l'uso di identificatori generici o condivisi sia inevitabile, richiedere una convalida della gerarchia, implementare misure per registrare le azioni associate a questi identificatori e rinnovare la password non appena una persona non ha più bisogno di accedere all'account.

• **Rispettare la raccomandazione CNIL13 in caso di autenticazione degli utenti basata su password,** in particolare by applicando le seguenti regole:

- memorizzare solo le impronte digitali delle password, ottenute mediante tecniche all'avanguardia;
- non richiedere il rinnovo periodico delle password per gli utenti semplici (a differenza degli amministratori);
- richiedere all'utente, al primo accesso, la modifica dell'eventuale password attribuita automaticamente o da un amministratore in fase di creazione dell'account o di reimpostazione della password;
- imporre la complessità della password in base ai casi d'uso:
  - **per impostazione predefinita, entropia14** (imprevedibilità teorica) **minimo di 80 bit** (es: minimo 12 caratteri con maiuscole, minuscole, cifre e caratteri speciali; minimo 14 caratteri con maiuscole, minuscole e cifre, senza caratteri speciali obbligatori);
  - Entropia a 50 bit (ad esempio: minimo 8 caratteri di 3 tipi diversi; 16 cifre) nel caso in cui siano in atto misure aggiuntive (restrizione dell'accesso all'account come ritardare l'accesso dopo diversi errori, impostare "Captcha" o bloccare l'account dopo 10 fallimenti);
  - Entropia a 13 bit (es: 4 cifre) nel caso di apparecchiature di proprietà dell'utente (es: SIM card, dispositivo contenente un certificato) con blocco dopo 3 guasti.

11 La biometria comportamentale (ad esempio: dinamica della pressione dei tasti) è meno matura della biometria fisiologica (ad esempio: scansione delle impronte digitali).

12 Per quanto riguarda l'autenticazione sul posto di lavoro, qualsiasi titolare del trattamento che desideri effettuare tale trattamento deve rispettare i requisiti del quadro normativo sull'accesso mediante autenticazione biometrica sul posto di lavoro (vedi "Le contrôle d'accès sur les lieux de travail", cnil.fr).

13 "Password: una nuova raccomandazione per controllare la vostra sicurezza", cnil.fr

14 L'entropia, applicata ad una password, corrisponde alla sua capacità di resistere ad un attacco di forza bruta.
Ad esempio, per il codice segreto di una carta di credito, il numero di combinazioni possibili è pari a 10 (cifre possibili) elevato a 4 (104). In binario, per ottenere un numero equivalente di combinazioni, è necessario utilizzare 13 bit, perché 2 (bit possibili) elevato alla potenza 13 (213) vale 8192, che è dello stesso ordine di grandezza di 10 4. Ciò dà un'entropia di 13 bit.

• **Supportare gli utenti nella scelta di una password complessa:**
  – sensibilizzando sui **metodi mnemonici15** – incoraggiando ;
  l'uso dei **gestori di password16** e fornendo formazione sul loro utilizzo:
    – consente di registrare in modo sicuro tutte le password necessarie richiedendo la memorizzazione di una sola password principale;
    – la password principale deve quindi essere particolarmente forte;
    – particolare attenzione deve essere posta nella scelta della soluzione.
• **Comunicare pratiche vietate17** (es: comunicare la propria password a chiunque altro, utilizzare una password desumibile dal contesto in cui viene utilizzata, salvare le password in un browser privo di master password). **In caso di cattive pratiche, una password che rispetti l'entropia richiesta può sempre essere facilmente utilizzata da un utente malintenzionato.**

Cosa dovrebbe essere evitato

• Utilizzando le password predefinite di apparecchiature e software.
• Memorizzazione delle password in testo non crittografato, non come impronte digitali crittografiche.
• Utilizzo di una funzione di hash crittografico obsoleta, come MD5 o SHA-1 (vedi scheda 21 – Crittografia, hash, firma) per generare l'impronta della password da archiviare, o progettata internamente, che quindi non è riconosciuta o provata.

• Prevenire l'uso della funzione "Incolla" o di completamento automatico nei moduli per evitare di influenzare l'uso di un gestore di password.

15 "Generare una password complessa", cnil.fr
16 "5 argomenti a favore dell'adozione del gestore di password", cnil.fr
17 "'Consigli della CNIL per una buona password'", cnil.fr

ANDARE OLTRE

• **Privilegiare, ove possibile, l'autenticazione a più fattori ,** soprattutto quando la connessione è accessibile dall'esterno della rete dell'organizzazione.
• **Limitare il numero di tentativi di accesso** agli account utente sulle workstation e bloccare temporaneamente o meno l'accesso all'account quando viene raggiunto il limite.
• **Richiedere agli amministratori di utilizzare password con entropia più elevata e di rinnovarle con una frequenza ragionevole e pertinente.**
• Implementare misure tecniche per **applicare le regole di autenticazione** (ad esempio: blocco dell'account di un amministratore se la password non viene aggiornata).
• Sul suo sito web, la CNIL mette a disposizione uno strumento18 per calcolare la complessità delle password richieste agli utenti, a seconda dei casi d'uso (password sola, con restrizioni di accesso o con materiale in possesso della persona).

• Se possibile, evitare di rendere gli identificatori (o login) di utenti e amministratori uguali agli account definiti per impostazione predefinita dalle società di software e disattivare gli account predefiniti.
• **Conservare le password in modo sicuro,** elaborate con una funzione (hash) appositamente progettata a questo scopo e utilizzando sempre un salt o una chiave19 (vedi scheda 21 – Crittografia, hash, firma). Una chiave non deve essere archiviata nello stesso database delle impronte digitali delle password.
• L'ANSSI in collaborazione con la CNIL20 autenticazione e , ha pubblicato raccomandazioni sull'approccio multifattoriale password. Fare riferimento anche alle guide21 pubblicate dall'ANSSI per aiutare gli sviluppatori e gli amministratori nella scelta degli algoritmi crittografici, nel dimensionamento e nell'implementazione.
• Per le autorità amministrative, gli Allegati al " *quadro generale di sicurezza* " (RGS22) si applicano, in particolare gli allegati B1 e B2 riguardanti rispettivamente i meccanismi crittografici e la gestione delle chiavi.

18 "Politica di verifica della password", cnil.fr
19 Il random utilizzato si chiama "salt" quando è diverso per ogni password memorizzata e "key" quando è comune alla trasformazione di un insieme di password (es. per un intero database).
20 "Raccomandazioni relative all'autenticazione a più fattori e alle password", cyber.gouv.fr
21 "Meccanismi crittografici", cyber.gouv.fr
22 "Il quadro generale di sicurezza versione 2.0: i documenti", cyber.gouv.fr

SCHEDA 5 – GESTIONE DEGLI ACCESSI

Consenti l'accesso solo ai dati di cui l'utente ha realmente bisogno.

Il rispetto del principio del privilegio minimo, attraverso la gestione dei profili di autorizzazione, consente di limitare le conseguenze di un'usurpazione dell'account o di un errore di manipolazione.

Precauzioni di base

• **Definire profili di autorizzazione** nei sistemi separando compiti e aree di responsabilità, in modo da limitare l'accesso degli utenti ai soli dati strettamente necessari per adempiere alle proprie responsabilità.
• **Ottenere la validazione di tutte le richieste di autorizzazione** da parte di un responsabile (es: manager di linea, project manager).
• **Revoca del diritto di accesso degli utenti non appena questi non sono più autorizzati ad accedere ad un locale o ad una risorsa informatica** (ad es. cambio di missione o posto) **nonché alla scadenza del loro contratto.**
• **Effettuare una revisione regolare, almeno annuale, delle autorizzazioni al fine** di identificare ed eliminare gli account non utilizzati e riallineare i diritti concessi alle responsabilità di ciascun utente. I manager aziendali dovrebbero essere coinvolti in questa revisione in modo che possano garantire la legittimità operativa dei diritti concessi.

Cosa dovrebbe essere evitato

• Creare o utilizzare account condivisi da più persone senza ricondurre queste eccezioni alle regole di sicurezza, senza farli convalidare dai gestori competenti e senza verificarli regolarmente.

• Concedere i diritti di amministratore agli utenti che non ne hanno bisogno.
• Concedere a un utente più privilegi del necessario.
• Dimenticare di rimuovere le autorizzazioni temporanee concesse ad un utente (es: per una sostituzione).
• Dimenticare di eliminare gli account utente di persone che hanno lasciato l'organizzazione o cambiato le loro funzioni.

ANDARE OLTRE

• Stabilire, documentare e rivedere regolarmente **una politica di controllo degli accessi** in relazione alle operazioni di trattamento implementate dall'organizzazione, che deve includere:
– le procedure da applicare automaticamente all'arrivo e alla partenza o al cambio di ruolo per una persona con accesso ai dati personali;
– le conseguenze previste per i soggetti legittimati ad accedere ai dati in caso di mancato rispetto delle misure di sicurezza (es.: abuso del diritto di legittimo accesso);
– le misure che consentono di limitare e controllare la concessione e l'utilizzo dell'accesso al trattamento (vedi scheda 16 – Operazioni di registrazione).

LE MIE INFORMAZIONI LA TECNOLOGIA E LA MIA ATTREZZATURE

SCHEDA 6 – SICUREZZA DELLE POSTAZIONI DI LAVORO

Previeni l'accesso fraudolento e l'esecuzione di programmi dannosi (es: virus) o di controllo remoto, anche tramite Internet.

I rischi di intrusione IT sono numerosi e le workstation rappresentano uno dei principali punti di ingresso.

Precauzioni di base

- Fornire un meccanismo **di blocco automatico della sessione** attivato ogni volta che la workstation non è stata utilizzata per un determinato periodo.
- Installare sulla postazione un software **firewall** e limitare l'apertura delle porte di comunicazione a quelle strettamente necessarie al corretto funzionamento delle applicazioni installate sulla postazione.
- Utilizzare **un antivirus regolarmente aggiornato.**
- **Correggere le violazioni della sicurezza con gli aggiornamenti di sicurezza appropriati il prima possibile** dopo averli testati. Gli aggiornamenti che correggono i difetti critici divulgati pubblicamente devono essere installati senza ritardi.
- Mantenere i diritti degli utenti al minimo indispensabile in base alle loro esigenze di utilizzo delle loro postazioni di lavoro.
- **Abilitare e promuovere l'archiviazione dei dati degli utenti su uno spazio di archiviazione online regolarmente sottoposto a backup e accessibile attraverso la rete interna dell'organizzazione** piuttosto che sulle postazioni di lavoro reali. Se i dati sono archiviati localmente, fornire mezzi di sincronizzazione o backup agli utenti e addestrarli a utilizzarli.
- **Cancellare in modo sicuro i dati su qualsiasi workstation prima di riassegnarla** a un'altra persona.
- Per quanto riguarda i supporti rimovibili (es: chiavette USB, hard disk esterni):
  - sensibilizzare gli utenti sui rischi associati ai dispositivi rimovibili, soprattutto se provengono dall'esterno;
  - **limitare la connessione di supporti rimovibili** allo stretto necessario;
  - disabilitare l'"esecuzione automatica" dai supporti rimovibili.
- Per **assistenza sulle postazioni di lavoro:**
  - gli strumenti di amministrazione remota devono **ottenere il consenso** dell'utente prima di qualsiasi intervento sul suo la sua posizione (es: ogni volta che viene concordato un appuntamento, mostrando all'utente un messaggio che lo invita ad accettare);
  - l'utente deve inoltre essere in grado di **distinguere se il controllo remoto è ancora in corso** e se è terminato (es: visualizzando un messaggio sullo schermo).

Cosa dovrebbe essere evitato

- Utilizzo di sistemi operativi obsoleti il cui supporto non è più fornito dall'editore.
- Fornire privilegi di amministrazione, sia in locale che in rete, agli utenti la cui posizione non lo richiede (es: amministratori).

ANDARE OLTRE

- **Consentire solo l'esecuzione di applicazioni scaricate** da fonti sicure (lista bianca).
- **Limitare l'uso** delle applicazioni che richiedono diritti di amministratore per la loro esecuzione.
- Fornire un ambiente sicuro (es: ambiente temporaneo virtualizzato) per lo svolgimento delle operazioni necessarie che comportano un rischio particolare (es: navigazione su un sito Web non attendibile).
- Configurare una soluzione per analizzare e **decontaminare i supporti rimovibili** prima di ogni utilizzo. L'ANSSI ha pubblicato una guida23 per aiutare nella scelta di questo tipo di soluzioni.
- **In caso di compromissione di una postazione di lavoro, ricercare la fonte e qualsiasi traccia di intrusione** nel sistema informativo dell'organizzazione per rilevare la compromissione di altri elementi.
- **Monitorare il software e l'hardware utilizzati nel sistema informativo dell'organizzazione.** Il CERT-FR, il centro di monitoraggio governativo francese incaricato di allertare e rispondere agli attacchi informatici, pubblica sul suo sito web24 avvisi e avvisi sulle vulnerabilità scoperte nei software e nell'hardware. Quando possibile, fornisce anche i mezzi per prevenirli.

- Distribuire **tempestivamente gli aggiornamenti critici ai sistemi operativi** (se applicabile dopo averli testati) pianificando un controllo automatico settimanale.
- Fornire una politica di aggiornamenti funzionali.
- Fissare le postazioni di lavoro a mobili specifici o difficili da spostare (es: utilizzare cavi antifurto).
- Assicurarsi che tutti gli utenti siano ben informati sulle **azioni da intraprendere e sull'elenco delle persone da contattare in caso di incidente di sicurezza o di evento insolito** che incida sui sistemi informativi e di comunicazione dell'organizzazione.
- Consultare25 la pagina del CERT-FR sui buoni riflessi in caso di intrusione in un sistema informativo.

23 “Funzionalità e profilo di sicurezza - Airlock e stazione bianca (reti non classificate)”, cyber.gouv.fr
24 “CERT-FR – Centro governativo per il monitoraggio, l'allarme e la risposta agli attacchi informatici”, cert.ssi.gouv.fr
25 “Buoni riflessi in caso di intrusione in un sistema informativo”, cert.ssi.gouv.fr

SCHEDA INFORMATIVA 7 – PROTEZIONE DEL MOBILE COMPUTING

Anticipare la violazione della sicurezza dei dati al di fuori dei propri locali, incluso il furto o la perdita di apparecchiature mobili.

Sono aumentate un'ampia varietà di pratiche di lavoro a distanza, al di fuori delle sedi delle organizzazioni (ad esempio: viaggi, telelavoro), nonché l'uso di attrezzature personali per scopi lavorativi, con conseguente aumento di rischi specifici, in particolare con l'uso di laptop, chiavette USB o smartphone: presidiare tali rischi è fondamentale.

Precauzioni di base

• **Sensibilizzare gli utenti sui rischi specifici legati all'utilizzo degli strumenti informatici mobili** (es. furto di apparecchiature, connessione a reti non controllate e rischi legati alle apparecchiature, in particolare apparecchiature pubbliche, utilizzo di apparecchiature personali) e sulle procedure per limitarli.
• **Fornire il controllo degli accessi** attraverso opportuni dispositivi di autenticazione (es: certificato elettronico, smart card). Tutti i flussi di informazioni dovrebbero essere crittografati (ad esempio VPN per accesso esterno).
• Fornire agli utenti **spazi di archiviazione condivisi accessibili da remoto.** Incoraggiali a conservare lì tutti i loro dati per mitigare i danni causati dalla perdita o dal furto dei loro dispositivi.
• **Implementare o integrare una soluzione di crittografia per dispositivi di archiviazione nomadi o rimovibili** (ad esempio: laptop, unità USB, disco rigido esterno, CD-R, DVD-RW) come:
  – crittografia del disco rigido (molti sistemi operativi supportano tale funzionalità);
  – crittografia file per file;
  – creazione di contenitori crittografati (cartella che può contenere più file).
• **Per quanto riguarda gli smartphone,** oltre all'utilizzo del PIN della SIM card, **abilitano il blocco automatico del terminale e richiedono un segreto per sbloccarlo** (es: password, sequenza).
• **Assicurarsi che agli utenti siano forniti i recapiti corretti** del dipendente incaricato in caso di smarrimento o furto dei propri dispositivi.
• **Valutare e affrontare i rischi specifici associati all'utilizzo delle apparecchiature personali da parte degli utenti** (bring your own device o BYOD) **e autorizzarli solo per quanto riguarda i rischi identificati.** Tali dispositivi che non sono controllati dall'organizzazione devono essere di conseguenza limitati nell'accesso ai dati e alle applicazioni per quanto riguarda la loro criticità. Assicurarsi che la carta informatica copra e formalizzi le responsabilità di tutti i soggetti coinvolti nonché le precauzioni da seguire (vedere scheda informativa 2 – Definire un quadro per gli utenti).

Cosa dovrebbe essere evitato

• Utilizzo di servizi cloud predefiniti installati per impostazione predefinita su un dispositivo per scopi di backup o sincronizzazione senza un'analisi approfondita dei termini di utilizzo e dei requisiti di sicurezza rispettati da tali fornitori di servizi. Questi generalmente non rispettano le raccomandazioni riportate nella scheda 14 – Gestione dei responsabili del trattamento.
• Applicare misure di sicurezza (ad esempio: impostando in modo restrittivo un sistema di gestione dei dispositivi mobili, MDM, su un telefono personale) che impediscano l'uso domestico di apparecchiature personali sulla base del fatto che il dispositivo viene utilizzato in un contesto professionale (ad esempio vietare l'installazione di applicazioni sul dispositivo).

• Violare il diritto alla privacy dell'utente accedendo a dati o elementi archiviati nello spazio di archiviazione personale dell'utente del proprio dispositivo utilizzato in
• Accesso agli elementi relativi alla privacy delle persone archiviati nello spazio personale dell'utente

ANDARE OLTRE

apparecchiature utilizzate in ambito professionale (BYOD).

- Consultare la scheda dedicata26 all'utilizzo delle attrezzature personali da parte degli utenti sul sito web della CNIL.
- **Predisporre un sistema di gestione dei dispositivi mobili (MDM),** anche sui dispositivi personali utilizzati in contesto professionale (BYOD) se la pratica è consentita, al fine di standardizzare le configurazioni e controllare il livello di garanzia della sicurezza dei dispositivi che si connettono alla rete dell'organizzazione.
- **Fornire un filtro per la privacy** per gli schermi delle postazioni di lavoro se devono essere utilizzati in spazi pubblici.
- Sensibilizzare sulle cattive pratiche nei luoghi pubblici:
  - **non lasciare attrezzature o documenti incustoditi;**
  - non discutere (es: chat di gruppo, telefonate) o condividere informazioni sensibili (es: dati personali, informazioni che possano rivelare violazioni della sicurezza).
- **Limitare l'archiviazione locale dei dati** sulle postazioni di lavoro nomadi allo stretto necessario, in particolare per le attrezzature personali, ed eventualmente vietarlo durante i viaggi all'estero27 .
- **Proteggersi dai furti** (es: cavo di sicurezza, marcatura visibile delle apparecchiature) **e mitigarne gli impatti** (es: blocco automatico, crittografia, cancellazione remota). Se deve essere utilizzato un meccanismo di cancellazione su un dispositivo personale (BYOD), il datore di lavoro deve incorporarne le condizioni di utilizzo nella Carta informatica (vedi scheda informativa 2 – Definire un quadro per gli utenti).
- Parti divisorie di attrezzature personali destinate all'uso in ambito professionale.

26 "BYOD: quali sono le migliori pratiche?", cnil.fr

27 "Migliori pratiche per chi viaggia per affari", cyber.gouv.fr

SCHEDA 8 – PROTEGGERE LA RETE INFORMATICA

Limitare le funzionalità di rete alla misura strettamente necessaria all'esecuzione dei Suoi trattamenti.

La rete interna interconnette tutti i componenti dei sistemi informativi di un'organizzazione e spesso offre punti di connessione con l'esterno. È tanto un punto di ingresso quanto un mezzo per la propagazione degli attacchi. Pertanto, proteggere la rete interna è fondamentale.

Precauzioni di base

• **Limitare l'accesso a Internet** bloccando i servizi non necessari (ad esempio VoIP, peer to peer).
• **Gestire le reti Wi-Fi.** Devono utilizzare la crittografia più moderna (WPA3 o WPA2 secondo le raccomandazioni di configurazione dell'ANSSI28). Inoltre, le reti aperte agli ospiti devono essere separate dalla rete interna.

• **Applicare l'uso della VPN per l'accesso remoto** implementando, se possibile, una forte autenticazione dell'utente (ad esempio: smart card, password monouso basata sul tempo (TOTP).
• **Assicurarsi che nessuna interfaccia di amministrazione sia direttamente su Internet.** Le operazioni di amministrazione e manutenzione devono essere effettuate tramite VPN.
• Per scopi di amministrazione della rete, la procedura migliore consiste nel configurare e implementare (correttamente) il protocollo SSH o accedere fisicamente all'apparecchiatura.
• **Limitare i flussi di rete allo stretto necessario** filtrando i flussi in entrata/uscita sugli apparati (es: firewall, server proxy). Ad esempio, se un server Web è in modalità solo HTTPS, dovresti consentire solo i flussi in entrata su quella macchina sulla porta 443 e bloccare tutte le altre porte.
• **Partizionare la rete** per mitigare gli impatti potenziali delle violazioni della sicurezza. Implementare almeno due aree di rete distinte: **una rete interna dove non è consentita la connessione a Internet e una DMZ** (zona demilitarizzata) **accessibile da Internet,** separata da gateway.

Cosa dovrebbe essere evitato

• Utilizzo del protocollo Telnet per la connessione di apparati di rete attivi (es.: firewall, router, gateway).

• Fornire agli utenti un accesso a Internet non filtrato.
• Configurazione di una rete Wi-Fi utilizzando la crittografia WEP.

28 “Protezione dell'accesso Wi-Fi”, cyber.gouv.fr

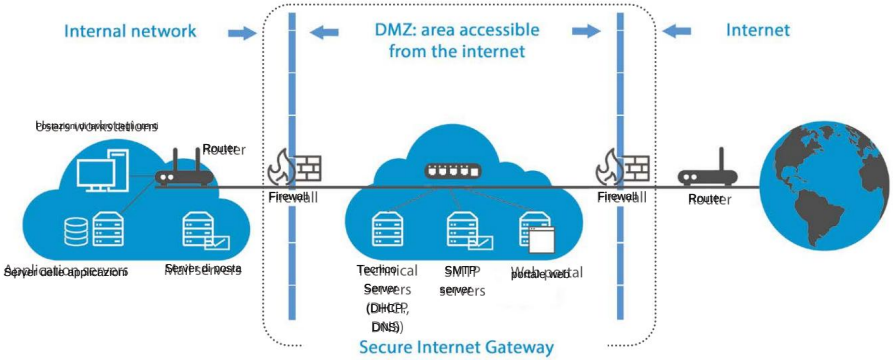
ANDARE OLTRE

• Le operazioni di amministrazione e manutenzione dovrebbero essere eseguite da apparecchiature sotto il controllo esclusivo del responsabile del trattamento dei dati o dei suoi subappaltatori.

• **L'identificazione automatica dell'hardware può essere implementata** configurando l'autenticazione hardware (protocollo 802.1X) o, almeno, definendo una lista bianca di identificatori aggiornata dei controller dell'interfaccia di rete (indirizzi MAC) per limitare una connessione di dispositivi non elencati.

• **I sistemi di rilevamento delle intrusioni** (IDS) e **di prevenzione delle intrusioni** (IPS) possono analizzare il traffico di rete per rilevare e persino rispondere ad alcuni attacchi. **Informare gli utenti** sull'implementazione di tali sistemi nella Carta informatica (vedi scheda 2 – Definire un quadro per gli utenti), dopo aver informato e consultato i rappresentanti sindacali del personale.

• **L'ANSSI ha pubblicato un manuale di buone pratiche29,** per aiutare a decidere, ad esempio, come definire l'interfaccia per connettere un sistema informativo a Internet30 (che si ispira allo schema seguente), la scelta dei firewall31 o l'implementazione del protocollo 802.1X32 .



29 “Pubblicazioni dell’ANSSI”, cyber.gouv.fr

30 “Raccomandazioni relative all'interconnessione di un IS a Internet”, cyber.gouv.fr

31 “Raccomandazioni per la scelta di firewall controllati in aree esposte a Internet”, cyber.gouv.fr

32 “Raccomandazioni per l'implementazione del protocollo 802.1X per il controllo degli accessi alle reti locali”, cyber.gouv.fr

Rafforzare le misure di sicurezza dei server.

Poiché i server centralizzano una grande quantità di dati e ospitano servizi che consentono l'accesso o la manipolazione di tali dati, la sicurezza dei server deve essere una priorità.

Precauzioni di base

• **Disinstallare o disattivare i servizi e le interfacce non necessari.**
• **L'accesso agli strumenti e alle interfacce di amministrazione sarà limitato al solo personale autorizzato.** Utilizza gli account utente senza privilegi per le operazioni di routine.
• **Adottare una politica di password specifica** per gli amministratori. Cambiare le password, almeno, durante ogni partenza di un amministratore e in caso di sospetto di compromissione.
• **Installare senza indugio gli aggiornamenti critici** (se applicabile dopo averli testati), in particolare le patch di sicurezza, sia per i sistemi operativi che per le applicazioni, programmando un check-up automatico settimanale.
• **Utilizzare software di rilevamento e rimozione malware** (ad esempio antivirus), aggiornandoli regolarmente.
• **Utilizzare account registrati** per l'accesso ai database e creare account tecnici specifici dell'applicazione.
• **Eseguire il backup e verificare regolarmente l'integrità dei file di backup e la possibilità di ripristinarli** (vedere scheda 17 – Salvataggio).
• **Implementare il protocollo TLS** (invece di SSL33), ovvero un protocollo che garantisca la crittografia e l'autenticazione, almeno per ogni scambio di dati su Internet e verificarne la corretta attuazione mediante strumenti adeguati34 .

• Non consentire l'uso di algoritmi di crittografia obsoleti per le comunicazioni del server.
• **Configurare un sistema di registrazione degli eventi** (vedi scheda informativa 16 – Operazioni di registrazione).

Cosa dovrebbe essere evitato

• Trattare i dati personali su server obsoleti senza sostituirli.
• Utilizzo di protocolli di scambio dati non sicuri (ad esempio autenticazione non crittografata, flussi di testo in chiaro).
• Utilizzare i server per funzioni diverse da quelle a cui sono dedicati, come la navigazione su siti web o l'accesso alla posta elettronica.
• Posizionamento dei database su un server direttamente accessibile da Internet.
• Utilizzo di account generici (cioè condivisi tra più utenti).

33 Il protocollo TLS viene talvolta erroneamente chiamato SSL o SSL/TLS. Il protocollo SSL, predecessore del TLS, è ormai obsoleto e da bandire.

34 Per TLS esistono diversi strumenti a questo scopo (es: “SSL Server Test”, ssllabs.com, “SSL-Tools”, ssl-tools.net).

ANDARE OLTRE

- Qualsiasi sistema che tratti dati sensibili35 deve essere implementato in un **ambiente dedicato** (logicamente isolato).
- **Le operazioni di amministrazione del server dovrebbero essere effettuate attraverso una rete dedicata e isolata,** con accesso con autenticazione forte (vedi scheda 5 – Gestione degli accessi) per una migliore tracciabilità (vedi scheda 16 – Operazioni di logging).
- Oltre ai flussi esterni, **i flussi interni devono essere crittografati** il più possibile (ad esempio utilizzando i protocolli TLS, IPsec o SSH).
- Isolare i server obsoleti ma essenziali e limitare il trattamento dei dati personali su di essi in attesa della loro sostituzione con sistemi aggiornati.
- Per quanto riguarda il software in esecuzione sui server, utilizzare **strumenti di rilevamento delle vulnerabilità** (software di scansione delle vulnerabilità come nmap36, nessus37 o nikto38) o fare affidamento su audit per l'elaborazione più critica per rilevare possibili vulnerabilità della sicurezza. Possono essere utilizzati anche sistemi di rilevamento e prevenzione degli attacchi su sistemi o server critici.
- Limitare l'accesso fisico e vietare l'accesso logico remoto alle porte di diagnosi e configurazione.

- Dovrebbe essere implementato e/o integrato TLS v1.3 o, almeno, v1.2, in conformità alle raccomandazioni pubblicate dall'ANSSI sull'argomento39 .
- **L'ANSSI ha pubblicato varie40 raccomandazioni,** tra cui la sicurezza dell'amministrazione dei sistemi informativi41 e l'impostazione del partizionamento del sistema42 .

35 I dati sensibili sono descritti nell'articolo 6 della legge sulla protezione dei dati e nell'articolo 9 del GDPR.

36 “Nmap”, nmap.org

37 “Tenable Nessus”, tenable.com

38 “Nikto2”, cirt.net

39 “Raccomandazioni di sicurezza per TLS”, cyber.gouv.fr

40 “Pubblicazioni dell’ANSSI”, cyber.gouv.fr

41 “Raccomandazioni per l’amministrazione sicura dei sistemi informatici”, cyber.gouv.fr

42 “Raccomandazioni per l’impostazione del partizionamento del sistema”, cyber.gouv.fr

SCHEDA INFORMATIVA 10 – PROTEZIONE DEI SITI WEB

Garantire che ai siti web vengano applicate buone pratiche minime.

Ogni sito web deve garantire la propria identità ai terminali ad esso collegati e la riservatezza delle informazioni trasmesse.

Precauzioni di base

- **Flussi di scambio dati sicuri attraverso l'** uso di TLS:
  - **ottenere certificati** ai livelli appropriati (di dominio, di organizzazione o esteso) da un ente di certificazione e gestirli in modo appropriato;
  - implementare il protocollo **TLS** (in sostituzione di SSL43) su tutti i siti web, utilizzando solo le versioni più recenti e verificandone la corretta implementazione;
  - **rendere obbligatorio l'uso di TLS** per tutte le pagine di autenticazione o le pagine su cui vengono visualizzati o trasmessi dati personali.
- **Limitare le porte di comunicazione** a quelle strettamente necessarie per il corretto funzionamento delle applicazioni installate. Se l'accesso a un server Web avviene solo tramite HTTPS, è necessario consentire solo il traffico di rete IP in entrata per quella macchina sulla porta 443 e bloccare tutte le altre porte.
- **Limitare l'accesso agli strumenti amministrativi e alle interfacce solo al personale autorizzato.** In particolare, limitare l'uso degli account amministratore ai team IT interni e solo per le azioni amministrative che li richiedono.

- Implementare le opzioni "HttpOnly" e "secure" per tutti i cookie utilizzati.
- **Se vengono utilizzati cookie non necessari per il servizio, raccogliere il consenso dell'utente** dopo aver informato l'utente e prima che il cookie venga memorizzato.
- **Limitare il numero di componenti utilizzati,** monitorarli regolarmente e aggiornarli.
- **Limitare le informazioni restituite durante la creazione di un account utente o durante la reimpostazione di una password,** per non informare un utente malintenzionato dell'esistenza – o meno – di un account associato a un identificatore (es. indirizzo e-mail).
- **Adottare le migliori pratiche per lo sviluppo IT** (vedere la scheda informativa 11 – Gestione degli sviluppi IT). In particolare, **proteggersi dagli attacchi più comuni ai siti Web indicati nella OWASP Top 10**[44]
(ad esempio: iniezioni SQL[45] , iniezioni XSS[46] , manipolazioni URL[47]).

Cosa dovrebbe essere evitato

- Trasmissione di dati personali in un URL (es: credenziali, password).
- Utilizzo di servizi non protetti (es.: autenticazione non crittografata, flusso non crittografato).
- Utilizzo di server che ospitano siti Web come postazioni di lavoro (ad esempio: navigazione nei siti Web, accesso alla posta elettronica).
- Posizionamento dei database su un server direttamente accessibile da Internet.
- Utilizzo di account utente generici (cioè condivisi tra più utenti).

43 Il protocollo TLS viene talvolta chiamato erroneamente SSL o SSL/TLS. Il protocollo SSL, predecessore del TLS, è ormai obsoleto e da bandire.

44 L'Open web application security project (OWASP) pubblica regolarmente un elenco dei dieci rischi più critici per le applicazioni web (vedi "OWASP Top Ten", owasp.org).

45 "SQL Injection", owasp.org

46 "Cross Site Scripting (XSS)", owasp.org

47 "Attraversamento del percorso", owasp.org

ANDARE OLTRE

- Per quanto riguarda l'implementazione dei cookies, si consiglia di consultare il dossier dedicato sul sito della CNIL48 .

- In generale, rispettare i livelli L1 e L2 delle raccomandazioni prodotte da OWASP. Per i software49 in esecuzione sui server, è consigliabile utilizzare **strumenti di rilevamento delle vulnerabilità** (software di scansione delle vulnerabilità come OWASP ZAP50, nmap51 o nikto52) per l'elaborazione più critica, al fine di rilevare possibili falle di sicurezza. Possono essere utilizzati anche sistemi per rilevare e prevenire attacchi a sistemi o server critici. Questi test devono essere eseguiti regolarmente e prima che qualsiasi nuova versione del software venga messa in produzione.

- **L'ANSSI ha pubblicato raccomandazioni specifiche sul proprio sito web53** per l'implementazione di TLS54 o per la protezione di un sito web55 .

48 “Sito web, cookie e altri traccianti”, cnil.fr
49 “Lista di controllo OWASP MAS”, mas.owasp.org
50 “Zed Attack Proxy (ZAP)”, zaproxy.org
51 “Nmap”, nmap.org
52 “Nikto2”, cirt.net
53 “Pubblicazioni dell’ANSSI”, cyber.gouv.fr
54 “Raccomandazioni di sicurezza per TLS”, cyber.gouv.fr
55 “Proteggere un sito web”, cyber.gouv.fr

SCHEDA 11 – GESTIONE DEGLI SVILUPPI IT

Integrare la sicurezza e la protezione dei dati personali il prima possibile nei progetti.

La protezione dei dati personali deve essere integrata nel ciclo di sviluppo informatico fin dalla fase di progettazione e per le configurazioni predefinite al fine di fornire agli interessati un migliore controllo sui propri dati e limitare errori, perdite, modifiche non autorizzate o usi impropri dei propri dati in applicazioni.

Precauzioni di base

• **Integrare la protezione dei dati, compresi i requisiti di sicurezza dei dati, fin dalla progettazione** dell'applicazione o del servizio. Questi requisiti possono comportare una varietà di scelte di architettura (decentralizzata o centralizzata), di funzionalità (ad esempio: anonimizzazione effettuata subito dopo la raccolta, minimizzazione dei dati), di tecnologie (ad esempio: crittografia delle comunicazioni), ecc.
• Utilizzare componenti o strumenti **riconosciuti e sicuri dalla comunità** (ad esempio: biblioteche).
• Implementare misure contro attacchi comuni contro i database (ad esempio: iniezioni di codice SQL, script).
• **Per qualsiasi sviluppo rivolto al grande pubblico, considerare attentamente i parametri che influenzano la privacy e il suo rispetto,** in particolare le impostazioni predefinite.
• **Evitare l'uso di caselle di testo libero o commenti,** che sono fonti di raccolta di dati personali aggiuntivi non necessari o sproporzionati.
• **Eseguire test completi** (ad esempio: test di unità, integrazione, funzionalità, sicurezza) prima che un prodotto venga reso disponibile o aggiornato. Durante un aggiornamento, assicurarsi che i test utilizzati siano sempre appropriati.
• Effettuare lo sviluppo e il test del computer in un ambiente informatico distinto da quello di produzione (ad esempio su computer o macchine virtuali diversi) e su dati fittizi o anonimizzati.
• **Assicurarsi che non vi siano segreti (autenticazione o crittografia)** quando si invia il codice a uno strumento di gestione delle versioni (ad esempio: Git o svn). **Cambia i segreti quando entri in produzione.**
• **Eseguire un test di non regressione e/o una revisione del codice prima che qualsiasi aggiornamento vada in produzione,** al fine di evitare l'emergere di fonti di violazione dei dati personali.

Cosa dovrebbe essere evitato

• Utilizzo di dati personali reali per le fasi di sviluppo e test. Dovrebbero essere utilizzati il più possibile set di dati fittizi.

• Sviluppare un'applicazione e poi pensare alle misure di sicurezza o protezione da mettere in atto riguardo ai dati personali.

ANDARE OLTRE

• La CNIL ha pubblicato una **guida GDPR56 specificatamente rivolta ai team di sviluppo** per aiutarli ad allineare i loro sviluppi informatici alla normativa in materia di protezione dei dati personali.

• **Mettere in atto una difesa approfondita dei sistemi,** vale a dire una combinazione di diverse misure e controlli di sicurezza (ad esempio controllare i dati inseriti in un modulo online ma anche proteggere le query del database). In particolare, le misure in atto sulla parte "frontend" di un'applicazione possono essere aggirate e dovrebbero essere rafforzate da misure sulla parte "backend".

• Lo sviluppo deve imporre **formati di immissione e registrazione dei dati che riducano al minimo i dati raccolti.** Se ad esempio si vuole raccogliere solo l'anno di nascita di una persona, il campo del modulo corrispondente non deve consentire l'inserimento del mese e del giorno di nascita. Ciò può significare, in particolare, l'implementazione di un menu a tendina che limiti le scelte per un campo modulo.

• Un articolo dedicato alle zone di testo libero o di commento è disponibile sul sito CNIL .57

• Le convenzioni o regole di codifica e la documentazione sono essenziali per mantenere l'applicazione o il servizio nel tempo senza introdurre nuove vulnerabilità e per correggere efficacemente i malfunzionamenti.

• I formati dei dati devono essere compatibili con l'attuazione del periodo di conservazione scelto. Ad esempio, se un documento digitale deve essere conservato per 20 anni, potrebbe essere rilevante favorire formati aperti che hanno maggiori probabilità di essere mantenuti a lungo termine.

• La **creazione e gestione di profili utente** con diritti di accesso ai dati differenziati a seconda delle categorie di utenti deve essere integrata fin dalla fase di progettazione.

• I test effettuati su dati fittizi o resi anonimi talvolta non sono sufficienti per garantire che un nuovo servizio o funzionalità funzioni correttamente. È quindi possibile testare in un ambiente di pre-produzione con dati reali. L'ambiente di pre-produzione deve essere configurato e messo in sicurezza allo stesso livello dell'ambiente di produzione stesso e il nuovo servizio o il suo aggiornamento deve essere già stato sottoposto a tutti i test (unitari, di integrazione e funzionali) negli ambienti di sviluppo e test.

• A seconda della natura dell'applicazione, potrebbe essere necessario garantirne l'integrità utilizzando firme di codici eseguibili per garantire che non abbia subito alcuna alterazione.

56 "Guida GDPR per il team di sviluppo", lincnil.github.io
57 "Blocco note e aree commenti: buoni riflessi per evitare di scivolare", cnil.fr

SCHEDA 12 – PROTEGGERE I LOCALI

Rafforzare la sicurezza dei locali che ospitano server e hardware di rete.

L'accesso ai locali deve essere controllato per impedire o rallentare l'accesso diretto non autorizzato, sia ad archivi cartacei che ad apparecchiature informatiche, compresi i server. I locali devono essere protetti anche da altri tipi di minacce (es. incendio, allagamento).

Precauzioni di base

- Limitare l'accesso ai locali tramite porte chiuse.
- Installare **allarmi anti-intrusione** e verificarne periodicamente il corretto funzionamento.
- **Installare rilevatori di fumo e attrezzature antincendio** e ispezionarli annualmente.
- Proteggere le chiavi di accesso ai locali nonché i codici di allarme.
- **Distinguere le aree dell'edificio in base al rischio** (es: prevedere un controllo accessi dedicato per la sala computer).

- Mantenere un elenco aggiornato delle persone o delle categorie di persone autorizzate ad accedere a ciascuna area e rivedere periodicamente tale elenco.
- **Stabilire regole e modalità per controllare l'accesso dei visitatori,** almeno mediante **l'accompagnamento dei visitatori58 fuori dalle aree di accoglienza del pubblico** da parte di una persona appartenente all'organizzazione.
- Proteggere l'accesso alla rete (ad esempio: prese da ufficio, patch bay) e consentire solo alle apparecchiature autorizzate di connettersi ad essi.
- Proteggere fisicamente le apparecchiature informatiche con misure specifiche (es.: sistema antincendio dedicato, elevazione contro possibili allagamenti, ridondanza dell'alimentazione elettrica, ridondanza del sistema di condizionamento).

Cosa dovrebbe essere evitato

- Scarsa progettazione o trascurata manutenzione degli ambienti delle sale computer (es: aria condizionata, alimentazione elettrica ininterrotta). Un guasto a questi impianti comporta spesso lo spegnimento delle macchine o l'apertura degli accessi ai locali (per favorire la circolazione dell'aria) che neutralizza di fatto gli elementi che contribuiscono alla sicurezza fisica dei locali.

- Lasciare visibili (es: schermi della segreteria facilmente leggibili dai visitatori, sale riunioni con schermi visibili dall'esterno) o accessibili (es: documenti stampati critici posti in vista del pubblico nelle aree di accoglienza) dati che dovrebbero rimanere riservati.

58 Dal loro ingresso, durante la loro visita e fino all'uscita dai locali.

ANDARE OLTRE

• Tenere un registro degli accessi ai locali o agli uffici che potrebbero contenere materiale di trattamento di dati personali che potrebbe avere un grave impatto negativo sugli interessati in caso di incidente. **Informare gli utenti** dell'attuazione di tale sistema, previa informazione e consultazione degli organi di rappresentanza del personale.

• Garantire che solo il personale debitamente autorizzato sia ammesso nelle aree ad accesso limitato. Per esempio:

– all'interno delle aree regolamentate, imporre a tutte le persone di indossare un visibile mezzo di identificazione (es: badge);
– i visitatori (es: personale di supporto tecnico) devono avere un accesso limitato. Dovranno essere registrate la data e l'ora del loro arrivo e della loro partenza;
– rivedere e aggiornare regolarmente i permessi di accesso alle aree protette e cancellarli se necessario.

IL MIO CONTROLLO SOPRA DATI

SCHEDA INFORMATIVA 13 – GARANTIRE GLI SCAMBI CON IL MONDO FUORI

Rafforzare la sicurezza di qualsiasi trasmissione di dati personali.

Senza misure aggiuntive, i canali di trasmissione dei dati dei consumatori (ad esempio posta elettronica, messaggistica istantanea, piattaforme di archiviazione di file) **sono raramente un mezzo di comunicazione sicuro** per la trasmissione dei dati personali. Un semplice errore imprudente può indurre persone non autorizzate ad accedere ai dati personali, violando così il diritto alla privacy degli interessati. Inoltre, le entità che hanno accesso ai server attraverso i quali transitano le informazioni possono avere accesso al loro contenuto o metadati.

Precauzioni di base

- **Crittografare i dati prima che vengano archiviati su un supporto fisico per essere trasmessi a terzi** (ad esempio unità USB, disco rigido portatile, disco ottico).
- **Quando si invia tramite una rete:**
  - **crittografare le parti sensibili** da trasmettere. A questo proposito si rimanda alle raccomandazioni contenute nella scheda 21 – Crittografia, hash, firma;
  - utilizzare un protocollo che garantisca la riservatezza e l'autenticazione del server di destinazione per i trasferimenti di file (es. **SFTP** o **HTTPS),** utilizzando le **versioni più recenti dei protocolli;**
  - **garantire la riservatezza dei segreti** (es: chiave di crittografia, password) trasmettendoli tramite un canale separato dai dati protetti (es: invio del file crittografato tramite e-mail e comunicazione della password tramite telefono o SMS).

- Aprire un file dall'esterno solo se si conosce il mittente e solo dopo aver effettuato una **scansione antivirus .**

- Quando si utilizza un apparecchio **fax ,** adottare le seguenti misure:
  - installare il facsimile in un locale fisicamente controllato e accessibile solo al personale autorizzato;
  - visualizzare l'identità del destinatario del fax durante l'invio dei messaggi;
  - raddoppiare l'invio via fax con l'invio dei documenti in originale al destinatario;
  - preregistrare i numeri dei potenziali destinatari nella rubrica fax (se esiste la funzione).

Cosa dovrebbe essere evitato

- Trasmissione di file contenenti dati personali non crittografati tramite messaggistica o altre piattaforme consumer.
- Non pianificare la cancellazione (preferibilmente automatica) dei file trasmessi utilizzando una piattaforma di trasferimento file.

ANDARE OLTRE

- Utilizzare algoritmi a chiave pubblica, quando diversi attori hanno messo in atto **un'infrastruttura di gestione della chiave pubblica** per garantire la riservatezza e l'integrità delle comunicazioni, nonché l'autenticazione dell'emittente.
- Far **firmare elettronicamente i dati** dall'emittente prima della loro trasmissione per garantire che sia lui l'autore della trasmissione (vedi scheda 21 – Crittografia, hash, firma).
- Potrebbe essere appropriato anche l'uso di un **server di archivio di file temporanei .** In questo caso, assicurarsi di:
  - fissare un tempo limitato per rendere disponibili i file;
  - limitare l'accesso ai file solo ai destinatari debitamente autorizzati;
  - crittografare i file prima di caricarli sul servizio qualora la soluzione utilizzata non preveda questa possibilità in modo integrato.
- Alcuni strumenti e soluzioni di comunicazione proteggono anche i metadati relativi agli elementi scambiati e possono essere utilizzati quando questi sono particolarmente sensibili.
- Per i sistemi più sensibili, confinare i file provenienti dall'esterno in aree isolate dal resto del sistema per impedire la diffusione di malware.

SCHEDA 14 – GESTIONE DEI RESPONSABILI DEL TRATTAMENTO

Gestire la sicurezza dei dati con i processori.

trattamento dei dati effettuato da un responsabile del per conto del titolare del trattamento deve essere soggetto al trattamento con garanzie sufficienti, in particolare in termini di sicurezza. Il titolare del trattamento deve essere a conoscenza dei dettagli delle misure di sicurezza adottate dai suoi responsabili del trattamento per poterne dimostrare il rispetto60 .

Precauzioni di base

• **Utilizzare solo processori con garanzie sufficienti** (in particolare in termini di conoscenze specialistiche, affidabilità e risorse).

• **Prevedere un contratto con i responsabili del trattamento61,** che definisca in particolare l'oggetto, la durata, lo scopo del trattamento nonché gli obblighi delle parti, in particolare in termini di sicurezza.

Garantire che contenga, in particolare, disposizioni che stabiliscano:

- la ripartizione delle responsabilità e degli obblighi relativi alla riservatezza dei dati personali affidati;
- requisiti minimi di autenticazione dell'utente;
- le condizioni per la restituzione e la distruzione dei dati al termine del contratto;
- le regole per la gestione e la notifica degli incidenti. Ciò dovrebbe includere l'informazione al titolare del trattamento nel caso in cui venga scoperta una violazione o un incidente di sicurezza, e ciò dovrebbe essere fatto il prima possibile in caso di violazione dei dati ;

personali62 – assistenza da fornire al responsabile del trattamento per garantire il rispetto degli obblighi di sicurezza63 ;

- il riesame periodico delle misure di sicurezza e, se del caso, le condizioni per la loro revisione.

• **Fornire i mezzi per verificare l'efficacia delle garanzie di protezione dei dati offerte dal responsabile del trattamento** (ad esempio: controlli di sicurezza, visite in loco). Tali garanzie includono, ma non sono limitate a:

- la crittografia dei dati in base alla loro sensibilità o, in mancanza, l'esistenza di procedure che garantiscano che la società di servizi non abbia accesso ai dati ad essa affidati se ciò non è necessario per l'esecuzione del suo contratto;
- crittografia delle trasmissioni dati (es: connessione HTTPS, implementazione VPN);
- garanzie in termini di protezione della rete, tracciabilità, gestione delle autorizzazioni, autenticazione, pratiche amministrative, audit, ecc.

Cosa dovrebbe essere evitato

• Iniziare il trattamento dei dati senza aver sottoscritto con il responsabile del trattamento un contratto che preveda i requisiti previsti dall'articolo 28 del GDPR.

• Utilizzo di servizi cloud senza garanzia circa l'effettiva ubicazione geografica dei dati e senza garantire le condizioni legali e le eventuali formalità per il trasferimento dei dati al di fuori dell'Unione Europea.

---

59 Inteso ai sensi del GDPR.

60 Articoli 5.2 e 24.1 del GDPR.

61 La Commissione Europea ha pubblicato le clausole contrattuali tipo su cui può basarsi il presente contratto (vedi " Clausole contrattuali tipo tra titolare del trattamento e subappaltatore", cnil.fr).

62 Un incidente di sicurezza è definito "violazione dei dati personali" quando riguarda dati personali.

63 Si rinvia all'articolo 32 del GDPR e al § 41 delle Linee guida 07/2020 adottate dal Comitato europeo per la protezione dei dati (EDPB)

PER ULTERIORI

- La CNIL ha pubblicato una guida per i responsabili del trattamento64.
- Consultare e attuare le disposizioni dell'articolo 28 GDPR.
- Prestare particolare attenzione alla scelta di un fornitore di servizi cloud (vedi scheda 22 – Cloud computing).
- Va considerata tutta la filiera del subtrattamento (responsabili del trattamento) e non solo diretta processori.
- Quando si sceglie un trasformatore, l'ottenimento di una certificazione è un primo indice per valutarne l'affidabilità. Ad esempio, lo standard internazionale ISO/IEC 2700165 richiede misure organizzative e tecniche per l'istituzione di un sistema di gestione della sicurezza delle informazioni (ISMS), mentre ISO/IEC 27701 copre i sistemi di gestione della privacy (PIMS).

- Per quanto riguarda i dati sanitari, un fornitore di hosting deve disporre di una certificazione di hosting di dati sanitari (HDS) 66. La Digital Health Agency (ANS) pubblica un elenco di hosting provider certificati. Vale la pena notare che un processo di certificazione ha progressivamente sostituito le autorizzazioni HDS a partire dal 2018 e che alcuni hosting provider67 dispongono ancora di un'autorizzazione68 valida.
- Ove opportuno, richiedere al fornitore del servizio di comunicare le proprie certificazioni e di verificarle scopo.

64 “Regolamento europeo sulla protezione dei dati: una guida a sostegno dei subappaltatori”, cnil.fr
65 “ISO 27701, uno standard internazionale per la protezione dei dati personali”, cnil.fr
66 “Hosting di dati sanitari (HDS)”, esante.gouv.fr
67 “Elenco degli host certificati”, esante.gouv.fr
68 “Elenco degli host approvati”, esante.gouv.fr

SCHEDA 15 – SUPERVISIONE DELLA MANUTENZIONE E FINE VITA DI HARDWARE E SOFTWARE

Garantisci la sicurezza dei dati in ogni fase del ciclo di vita dell'hardware e del software.

Le operazioni di supporto devono essere supervisionate per controllare l'accesso ai dati da parte dei fornitori di servizi. I dati dovranno essere preventivamente cancellati dalle apparecchiature destinate allo smaltimento.

Precauzioni di base

- **Registrare** gli interventi di manutenzione **su un registro.**
- **Aprire l'accesso necessario** per la manutenzione remota **su richiesta del fornitore di servizi,** per un periodo di tempo predefinito adeguato all'intervento. Tali accessi dovranno essere nuovamente chiusi allo scadere di tale periodo.

- Includere clausole di sicurezza nei contratti di manutenzione con i fornitori di servizi per controllare il loro accesso ai sistemi informativi (vedi clausola di esempio a fianco).
- **Garantire che gli interventi di terzi siano supervisionati da un responsabile dell'organizzazione.**
- **Non lasciare soli gli appaltatori esterni,** soprattutto in locali sensibili (ad es. sale server).
- **Cancellare in modo sicuro i dati dall'apparecchiatura prima del suo smaltimento, del suo invio a terzi per la riparazione** o al termine di un contratto di noleggio.

Cosa dovrebbe essere evitato

- Installazione di applicazioni di manutenzione remota con vulnerabilità note (es: applicazioni che non crittografano le comunicazioni).
- Riutilizzare, rivendere o eliminare supporti che contengono dati personali senza che i dati siano stati cancellati in modo sicuro.

- Consentire l'accesso completo o permanente ai sistemi per la manutenzione remota.

ANDARE OLTRE

- Scrivere e implementare una procedura sicura di cancellazione dei dati.
- Utilizzare un software dedicato all'eliminazione dei dati senza distruzione fisica che sia stato qualificato o certificato. L'ANSSI rilascia certificazioni di primo livello69 a tali software.
- Implementare strumenti di monitoraggio in tempo reale oa posteriori (es. registrazione) (es. sessioni “4-eye”) per interventi di manutenzione remota da parte di terzi70 .
- L'ANSSI dedica un capitolo della sua guida71 sull'amministrazione sicura alla manutenzione da parte di terzi.

69 “Prodotti certificati”, cyber.gouv.fr

70 Come i sistemi di registrazione, tali sistemi devono essere impostati in conformità con le disposizioni legali applicabili e con le informazioni degli interessati.

71 “Raccomandazioni per l'amministrazione sicura dei sistemi informatici”, cyber.gouv.fr

Esempio di clausola utilizzabile in caso di manutenzione da parte di terzi:

Ogni intervento di manutenzione deve essere oggetto di una descrizione che specifichi le date, la natura degli interventi e i nominativi dei soggetti coinvolti, trasmessa a X.

In caso di manutenzione remota che consente l'accesso remoto ai file di X, Y potrà intervenire solo dopo che X avrà autorizzato l'accesso. L'accesso deve essere chiuso al termine di ogni intervento Y.

[Formulazione alternativa in base alla natura della manutenzione:

In caso di manutenzione remota che consente l'accesso remoto ai file di X, Y potrà intervenire solo dopo che X sarà stato informato, consentendo a X di identificare e monitorare l'accesso al suo sistema informativo.
]
Verranno redatti dei registri sotto le rispettive responsabilità di X e Y, indicanti la data e la natura dettagliata degli interventi di manutenzione remota e i nomi dei loro autori.

Nota: tale clausola di mantenimento deve necessariamente essere accompagnata da una clausola di riservatezza per i trasformatori.

PREPARAZIONE PER UN INCIDENTE

SCHEDA 16 – OPERAZIONI DI LOGGING

Registrare le operazioni per il rilevamento di anomalie, malfunzionamenti o incidenti e disporre delle informazioni utili al loro trattamento o in caso di contenzioso.

Per poter **identificare l'accesso fraudolento** o **l'uso improprio** dei dati personali, o per determinare l'origine di un incidente, è necessario registrare determinate azioni eseguite sui sistemi IT. I log poi raccolti costituiscono anche una prova utile per la dimostrazione della conformità[72] .

Precauzioni di base

• **Prevedere un sistema di logging** (ovvero sistema di registrazione in file di log) delle attività aziendali degli utenti (log applicativi), degli interventi tecnici (anche da parte degli amministratori), delle anomalie e degli eventi legati alla sicurezza (log tecnici o di sistema).

• **Conservare questi registri per un periodo compreso tra sei mesi e un anno** (tranne, ad esempio, nel caso di un obbligo legale relativo a questo periodo di conservazione, la necessità di gestione del contenzioso, di controllo interno o un'esigenza identificata di post-incidente analisi).

• **Effettuare, per i log delle applicazioni, una registrazione della creazione, consultazione, condivisione, modifica e cancellazione** dei dati conservando l'identificativo dell'autore, la data, l'ora e la natura dell'operazione nonché il riferimento dei dati interessati (per evitare duplicazione).

• **Informare gli utenti,** ad esempio al momento dell'autenticazione o dell'accesso al sistema, della predisposizione del sistema di registrazione, dopo aver informato e consultato gli organi di rappresentanza del personale.

• **Proteggere l'attrezzatura di registrazione e le informazioni registrate** da operazioni non autorizzate (ad esempio rendendole inaccessibili alle persone la cui attività è registrata), uso improprio da parte di account autorizzati (ad esempio: creando una carta d'uso o avvisi specifici) e la frantumazione dei registri generati dalle applicazioni interessate.

• Garantire il corretto funzionamento del sistema di registrazione **integrando l'attrezzatura in uno strumento di monitoraggio e controllando regolarmente la presenza di registri sfruttabili.**

• **Garantire che i responsabili del trattamento siano contrattualmente obbligati** a implementare la registrazione in conformità con queste raccomandazioni e a notificare al più presto possibile qualsiasi anomalia o incidente di sicurezza al responsabile del trattamento.

• **Analizzare attivamente, in tempo reale oa breve termine, i log raccolti per poter rilevare il verificarsi di un incidente** (vedi scheda 9 – Gestione degli incidenti e delle violazioni).

Cosa dovrebbe essere evitato

• Duplicare e memorizzare eccessivamente i dati personali interessati dal trattamento all'interno dei log (es: salvataggio delle password o del loro hash durante l'autenticazione degli utenti).

• Utilizzare le informazioni provenienti dai sistemi di registrazione per scopi diversi da quelli di garantire il corretto utilizzo del sistema informatico (ad esempio, utilizzare i registri per contare le ore lavorate è un abuso di scopo, punibile dalla legge).

• Conservazione dei registri senza limiti di tempo.

72 Articoli 5.2 e 24.1 del GDPR.

ANDARE OLTRE

- Cfr. la raccomandazione CNIL sul disboscamento73 .
- **Coinvolgere l'utente nel monitoraggio delle transazioni effettuate** sul suo conto e sui suoi dati (es: fornire un riepilogo delle ultime tre connessioni). Focus sul monitoraggio automatico dei log, abbinato a un'adeguata configurazione degli avvisi.
- **Istituire un'enclave di raccolta** che centralizzi i registri degli eventi in tutto il sistema informativo al fine di prevenirne qualsiasi alterazione.
- L'ANSSI ha pubblicato raccomandazioni sulla creazione di un sistema di registrazione74 e più specificamente raccomandazioni nell'ambiente Active Directory75 .

73 “La CNIL pubblica una raccomandazione relativa alle misure di disboscamento”, cnil.fr

74 “Raccomandazioni di sicurezza per l'architettura di un sistema di registrazione”, cyber.gouv.fr

75 “Raccomandazioni sulla sicurezza per la registrazione dei sistemi Microsoft Windows in un ambiente Active Directory”, cyber.gouv.fr

SCHEDA 17 – RISPARMIARE

Esegui backup regolari per limitare l'impatto di una perdita o alterazione indesiderata dei dati.

Le copie di backup devono essere create e testate regolarmente per essere disponibili quando necessario.

Precauzioni di base

- **Effettuare frequenti backup dei dati,** sia in formato cartaceo che elettronico. Potrebbe essere opportuno fornire backup incrementali giornalieri[76] e backup completi a intervalli regolari.
- Archiviare almeno un backup in un sito geograficamente separato dal sito operativo.
- **Isolare almeno un backup offline,** disconnesso dalla rete aziendale.
- **Proteggere i dati archiviati allo stesso livello di sicurezza di quelli archiviati sui server operativi** (ad esempio crittografando i backup, garantendo l'archiviazione in un luogo sicuro, prevedendo contrattualmente un servizio di esternalizzazione dei backup).
- Crittografare il canale di trasmissione, se non è interno all'organizzazione, quando i backup vengono trasmessi attraverso la rete.
- Testare regolarmente l'integrità dei backup e la capacità di ripristinarli.

Cosa dovrebbe essere evitato

- Garantire un livello di sicurezza inferiore sul sistema di backup (es: non salvare il sistema stesso) solo su altri sistemi informativi.
- Mantenere i backup sugli stessi sistemi dei dati sottoposti a backup senza isolarli. Una minaccia (ad esempio: ransomware) potrebbe quindi colpire sia i dati che i relativi backup.
- Conservare i backup nello stesso posto in cui si trovano le macchine che ospitano i dati. Un grave disastro che si verificasse lì comporterebbe una perdita definitiva di dati.
- Non controllare mai se i backup sono disponibili e rendersi conto che non è così nel giorno in cui sono necessari.

ANDARE OLTRE

- Proteggere almeno un backup (es: quello geograficamente distinto dal luogo operativo) in casseforti ignifughe e impermeabili.
- Se i requisiti di disponibilità dei dati e del sistema sono elevati, è consigliabile implementare la replica dei dati su un sito secondario.
- Si consiglia di applicare la regola denominata “3 – 2 – 1”, lo stato dell'arte in termini di backup, che consiste nell'avere 3 copie dei dati, archiviandoli su 2 supporti diversi, di cui 1 offline.
- L'ANSSI ha pubblicato raccomandazioni[77] sulla salvaguardia dei sistemi informativi.

76 Un backup incrementale consiste nel salvare solo le modifiche apportate rispetto ad un backup precedente.

77 “Backup dei sistemi informativi”, cyber.gouv.fr

SCHEDA 18 – PREVISIONE CONTINUITÀ E RE-PREVISIONE DI ATTIVITÀ

Prevedere il funzionamento degradato dei sistemi informativi ed essere in grado di riavviarli senza incidere sulla sicurezza dei dati.

Per limitare i tempi di inattività del sistema è necessario anticipare gli incidenti più comuni.
Garantire la continuità aziendale significa pianificare le modalità per continuare a operare, in generale in modo degradato, nonostante i malfunzionamenti. La ripresa delle attività, invece, racchiude tutte le azioni necessarie per rilanciare un sistema costituito.

Precauzioni di base

• **Scrivere un piano di continuità operativa (BCP) e un piano di disaster recovery (DRP),** anche riassuntivo, per l'attività IT, compreso l'elenco delle parti interessate. Il livello di protezione dei dati non dovrebbe essere ridotto dalle modalità operative previste.
• **Garantire che utenti, fornitori di servizi e subappaltatori sappiano chi allertare in caso di incidente.**
• **Testare regolarmente il ripristino dei backup e l'applicazione del piano di continuità aziendale o del piano di ripristino di emergenza.**
• Informazioni sui materiali:

– utilizzare un inverter per proteggere le apparecchiature utilizzate per i trattamenti essenziali;
– prevedere la ridondanza materiale delle apparecchiature di storage (es.: utilizzo della tecnologia RAID 78).

Cosa dovrebbe essere evitato

• Considerarsi al sicuro.
• Ridurre il livello di sicurezza dei dati quando si implementa una procedura degradata, senza tenere conto dei nuovi rischi generati per mantenere l'attività.
• Non prevedere un ritorno alla normalità.
• Non testare la continuità aziendale o le misure di ripristino a monte.

ANDARE OLTRE

• Il Segretariato Generale per la Difesa e la Sicurezza Nazionale (SGDSN) ha pubblicato79 una guida sulla creazione di un piano di continuità aziendale o di ripresa aziendale.
• Definire un'organizzazione per la gestione della crisi.
• Svolgere esercitazioni con tutte le parti interessate per verificare l'efficacia e l'assimilazione delle procedure messe in atto.
• Si possono preferire test mirati su alcuni componenti o parti del sistema per limitare l'impatto sulla produzione. Occorre però testare di volta in volta la continuità e la ripresa degli elementi più critici. Dovrebbe essere presa in considerazione anche una prova di spegnimento completo del sistema informativo.

78 RAID (array ridondante di dischi indipendenti) si riferisce a tecniche di distribuzione dei dati su più supporti di memorizzazione (ad esempio: dischi rigidi) per prevenire la perdita di dati in seguito al guasto di uno dei supporti.
79 “Benvenuti nella guida alla continuità aziendale”, guide-continuite-activite.sgdsn.gouv.fr.

SCHEDA 19 – GESTIONE INCIDENTI E VIOLA-ZIONI

Fornire procedure per la gestione degli incidenti e la risposta alle violazioni dei dati (violazione della riservatezza, dell'integrità o della disponibilità).

È necessario essere preparati all'eventualità di un incidente per intervenire in modo tempestivo e adeguato, incorporando l'obiettivo di limitare gli effetti per le persone i cui dati sono interessati. Il responsabile del trattamento può essere tenuto a notificare l'incidente alla CNIL o a informare gli interessati dell'incidente a seconda del rischio per loro.

Precauzioni di base

• **Analizzare regolarmente i log raccolti** (vedi scheda 16 – Operazioni di logging).
• Garantire che **i gestori del sistema di gestione del logging** (sia interni che esterni) **avvisare il titolare del trattamento, nel più breve tempo possibile, in caso di anomalia o incidente di sicurezza.**
• Diffondere a tutti gli utenti, sia interni che esterni, **i comportamenti da tenere e l'elenco delle persone da contattare in caso di incidente di sicurezza o di evento insolito** che incida sui sistemi informativi e di comunicazione dell'organizzazione. **Sensibilizzare gli utenti** sull'importanza di segnalare eventi sospetti.

• Stabilire procedure che dettaglino i sistemi per generare e sollevare avvisi da diverse fonti (es.: automatici, da parte degli utenti), il loro trattamento e le azioni da intraprendere in caso di incidente accertato (es.: persone da contattare, azioni per limitare l'incidente in base alla sua natura). Includere la gestione della violazione dei dati nel processo di gestione degli incidenti. **Definire i criteri per classificare un incidente come violazione dei dati.**

• **Valutare il rischio per le persone causato dalla violazione,** tenendo conto della gravità e della probabilità delle conseguenze che la violazione potrebbe avere sui loro diritti e libertà.
• **Mantenere un registro interno di tutte le violazioni dei dati personali.**
• **Notificare80 alla CNIL, entro 72 ore (come previsto dal GDPR), le violazioni che mettono a rischio i diritti e le libertà delle persone fisiche** e, in caso di rischio elevato e salvo diversa disposizione del GDPR81, **informare gli interessati** affinché possano limitarne le conseguenze 82.

Cosa dovrebbe essere evitato

• In attesa che gli interessati o terzi rilevino e segnalino un incidente.
• Omettere l'analisi dei rischi che una violazione dei dati personali potrebbe comportare per i diritti e le libertà delle persone.

• Attendere informazioni precise per notificare alla CNIL quando è chiaramente accertato che si è verificata una violazione. Le notifiche dei dati possono essere trasmesse in due fasi: una iniziale, entro 72 ore, poi un'ulteriore se necessario.

80 La procedura di notifica è dettagliata sul sito web della CNIL (vedi "Notificare una violazione di dati personali", cnil.fr).

81 Articoli 33 e 34 del GDPR.

82 L'obbligo di notificare le violazioni dei dati personali non esonera la persona responsabile dai suoi eventuali altri obblighi di segnalazione degli incidenti (vedi "Notifiche di incidenti di sicurezza alle autorità di regolamentazione: come organizzarsi e chi contattare?", cnil.fr).

ANDARE OLTRE

- Focus sul **monitoraggio automatico dei log,** abbinato ad un'adeguata configurazione degli avvisi.
- Stabilire una formazione obbligatoria per tutto il personale sull'identificazione e la segnalazione delle violazioni, nonché su cosa fare in questo caso.
- Il GEPD83 ha pubblicato linee guida84 che descrivono in dettaglio 18 esempi di violazioni dei dati, basati su pratiche pratiche casi riscontrati dalle autorità europee per la protezione dei dati.
- Il Gruppo di lavoro (denominato “Articolo 29”) che ha preceduto il GEPD sulla protezione dei dati ha pubblicato anche linee guida85 sulla notifica delle violazioni dei dati personali per accompagnare gli organismi nell'adempimento dei loro obblighi.

- In caso di incidente o per prepararsi ad esso, consultare l'assistenza per la sicurezza digitale e sito web sulla prevenzione86 .

83 Comitato europeo per la protezione dei dati.

84 “Linee guida 01/2021 su esempi riguardanti la notifica di violazione dei dati personali”, edpb.europa.eu

85 “Linee guida sulla notifica di violazione dei dati personali ai sensi del Regolamento 2016/679 (wp250rev.01)”, ec.europa.eu

86 “Assistenza e prevenzione del rischio digitale a beneficio del pubblico”, cybermalveillance.gouv.fr

MESSA A FUOCO

SCHEDA 20 – ANALISI DEI RISCHI

Identificare i rischi e valutarne la probabilità e la gravità al fine di implementare le misure di sicurezza adeguate.

Oltre a rispettare le precauzioni di base presentate in questa guida, è rilevante, se non obbligatorio in base alla criticità del trattamento, effettuare analisi dei rischi legati alla protezione dei dati. Tali analisi forniscono la base per decidere ulteriori misure di sicurezza, adeguate al contesto, per limitare l'impatto sugli interessati coinvolti nel trattamento dei dati.

Precauzioni di base

• Individuare i trattamenti di dati personali per i quali è **necessaria una valutazione d'impatto sulla protezione dei dati (DPIA)87 dovrà essere effettuato in conformità al GDPR88 .** Una PIA comprende non solo una parte dedicata all'analisi dei rischi, argomento di questa scheda, ma anche una parte dedicata agli aspetti legali del trattamento dei dati.

• Effettuare un'analisi dei rischi89 , anche minima, basata sui seguenti tre passaggi:

1. Identificare il trattamento dei dati personali, automatizzato o meno, i dati trattati (ad esempio: file dei clienti, contratti) e i media su cui si basano:

– l'hardware (es: server, laptop, dischi rigidi);
– il software (es.: sistemi operativi, software aziendali);
– le risorse di cloud computing utilizzate (es: SaaS, PaaS, IaaS);
– i canali di comunicazione logici o fisici (es.: connessioni cablate, Wi-Fi, Internet, scambi verbali, corrieri);

– i documenti cartacei (es: documenti stampati, fotocopie);
– i locali e le strutture fisiche in cui sono ubicati gli elementi di cui sopra (es.: sale informatiche, uffici).

Questo passaggio merita di essere effettuato indipendentemente da qualsiasi analisi dei rischi (vedi scheda 1 – Gestione della sicurezza dei dati).

2. Valutare i rischi generati da ciascuna operazione di trattamento:

UN. **Identificare i potenziali effetti** sui diritti e sulle libertà degli interessati, per i tre seguenti eventi temuti:

– **accesso illegittimo ai dati** (es.: furto d'identità a seguito della divulgazione delle buste paga di tutti i dipendenti di un'azienda);
– **modifica indesiderata dei dati** (es: accusa ingiusta di colpa o di illecito a seguito della modifica dei log di accesso);
– **perdita temporanea o permanente di dati** (es: mancata rilevazione di un'interazione farmacologica per impossibilità di accedere alla cartella clinica del paziente).

87 "Cosa c'è da sapere sulla valutazione d'impatto sulla protezione dei dati (AIPD)", cnil.fr
88 Articolo 35 del GDPR.
89 Il vocabolario utilizzato nella seguente descrizione è tratto dalle guide AIPD pubblicate dalla CNIL (cfr. "Privacy Impact Assessment (PIA)", cnil.fr).

B. Identificare le fonti di rischio (chi o cosa potrebbe essere all'origine di ogni evento temuto?), tenendo conto delle fonti umane interne ed esterne (es. amministratore informatico, utente, aggressore esterno, concorrente) nonché di fonti non interne ed esterne -fonti umane (ad esempio acqua, epidemie, materiali pericolosi, virus informatici non mirati).

C. Identificare le possibili minacce (cosa potrebbe consentire il verificarsi di ciascun evento temuto?). Tali minacce si verificano su supporti precedentemente identificati (hardware, software, canali di comunicazione, documenti cartacei, ecc.), che possono essere:

– utilizzati in modo inappropriato (es.: abuso di diritti, errore di gestione);

– modificati (es.: software intrappolati o hardware-keylogger, installazione di software dannoso);

– smarrimento (es: furto di un computer portatile, smarrimento di una chiavetta USB);

– osservato (es: osservazione di uno schermo su un treno, geolocalizzazione di apparecchiature);

– danneggiati (es: atti vandalici, degrado dovuto alla naturale usura);

– sovraccarico (es: unità di storage piena, attacco Denial of Service).

D. Identificare le misure esistenti o pianificate per ridurre ciascun rischio (es: controllo degli accessi, backup, tracciabilità, sicurezza dei locali, crittografia, anonimizzazione).

e. Valutare la gravità (impatto o potenziale danno per gli interessati) e la probabilità (probabilità di accadimento) dei rischi rispetto agli elementi precedenti (un esempio di scala utilizzabile per la valutazione: trascurabile, moderato, ampio, massimo).

Evento temuto	Effetti su individui	Principali fonti di rischio	Principali minacce	Esistenti o pianificate le misure	Gravità	Probabilità
Accesso illegittimo ai dati						
Modifica indesiderata dei dati						
Perdita di dati						

Per formalizzare questa riflessione è possibile utilizzare la seguente tabella:

3. Implementare e verificare le misure pianificate. Se le misure esistenti e previste sono ritenute adeguate, è necessario garantirne l'attuazione e il monitoraggio (vedi scheda informativa 1 – Gestione della sicurezza dei dati). In caso contrario, dovranno essere identificate e implementate misure aggiuntive per ridurre la gravità e/o la probabilità dei rischi associati.

• **Riesaminare regolarmente l'analisi dei rischi** e, in particolare, in caso di modifica del sistema o del contesto di trattamento.

Cosa dovrebbe essere evitato

• Dimenticando l'impatto per gli interessati e considerando solo l'impatto per l'organizzazione.
• Omettere parte del trattamento dei dati (es: raccolta, partner, dati di fine vita) per condurre l'analisi.

• Adeguare le scale di probabilità e gravità durante l'analisi del rischio, anziché definirle a monte in base al contesto generale dell'organizzazione.

ANDARE OLTRE

• Il GDPR introduce **le Valutazioni di Impatto sulla Protezione dei Dati** (DPIA) e specifica che esse contengano almeno "una […] descrizione delle […] operazioni e delle finalità del trattamento […], una valutazione della necessità e della proporzionalità [...], una valutazione dei rischi [...] e le misure previste per affrontare i rischi [...] e dimostrare la conformità al regolamento" (articolo 35.7).

• La CNIL ha pubblicato delle guide[90] per condurre una DPIA. La CNIL ha inoltre pubblicato un software per facilitare lo svolgimento e la formalizzazione della DPIA[91] • La CNIL ha .
inoltre pubblicato elenchi di trattamenti per i quali è richiesta o meno una DPIA[92][93].

• **Gli audit di sicurezza sono uno strumento essenziale per valutare il livello di sicurezza dei sistemi su cui si basa il trattamento dei dati personali.** Eseguiti periodicamente, consentono di tenere conto dei cambiamenti nei trattamenti e delle minacce. Ogni audit deve produrre un piano d'azione, la cui attuazione dovrebbe essere monitorata al livello più alto dell'organizzazione.

• **La valutazione del rischio per la sicurezza delle informazioni[94] può essere condotta contemporaneamente alla valutazione del rischio privacy.** Questi approcci sono compatibili.

• La valutazione del rischio fornisce una base per determinare le misure di sicurezza da attuare.
È necessario **stanziare un budget** per la loro attuazione.

90 "Valutazione dell'impatto sulla privacy (PIA)", cnil.fr

91 "Il software open source PIA aiuta a effettuare la valutazione dell'impatto sulla protezione dei dati", cnil.fr

92 "Analisi d'impatto relativa alla protezione dei dati: pubblicazione di un elenco di trattamenti per i quali è necessaria un'analisi", cnil.fr

93 "Analisi d'impatto relativa alla protezione dei dati: pubblicazione di un elenco di trattamenti per i quali non è richiesta un'analisi", cnil.fr

94 Ad esempio, utilizzando il metodo EBIOS RM (vedi "EBIOS Risk Manager – Il metodo", cyber.gouv.fr), il metodo di gestione del rischio pubblicato dall'ANSSI, un'agenzia collegata al Segretariato Generale della Difesa e della Sicurezza Nazionale (" Secrétariat général de la défense et de la sécurité nationale" o SGDSN). EBIOS è un marchio registrato di SGDSN.

SCHEDA 21 – CRITTOGRAFIA, HASH, FIRMA

Garantire l'integrità, la riservatezza e l'autenticità delle informazioni.

Le funzioni hash garantiscono **l'integrità dei dati. Le firme digitali,** oltre a garantire l'integrità, permettono di verificare l'autenticità dell'identità del firmatario e di assicurarne la non ripudiabilità. Infine, **la crittografia95** garantisce **la riservatezza** di un messaggio.

Precauzioni di base

- **Utilizzare un algoritmo riconosciuto e sicuro,** ad esempio i seguenti algoritmi:
  - SHA-296 o SHA-397 come famiglie di funzioni hash;
  - bcrypt, scrypt, Argon2 o PBKDF2 per memorizzare le password;
  - AES98 con una modalità di costruzione appropriata (CCM, GCM o EAX) o ChaCha20 99 (con Poly1305) per la crittografia simmetrica;
  - RSA -OAEP100 , ECIES-KEM101 o DLIES-KEM101101 per crittografia asimmetrica;
  - RSA-SSA-PSS100100 o ECDSA102 per le firme.
- **Utilizzare tasti sufficientemente lunghi:**
  - per AES si considerano sufficienti chiavi da 128, 192 o 256 bit;
  - per algoritmi basati su RSA si consiglia di utilizzare modulo segreto ed esponenti di almeno 2048 bit oppure 3072 bit, con esponenti pubblici, per cifratura maggiore di 65536 bit.
- **Applicare raccomandazioni rilevanti per l'uso,** specifiche per l'algoritmo scelto. Gli errori di implementazione hanno un impatto significativo sulla sicurezza del meccanismo crittografico.
- **Proteggere le chiavi private,** almeno attraverso l'implementazione di diritti di accesso limitati e una password sicura.

- **Scrivere una procedura che indichi come verranno gestite chiavi e certificati** considerando i casi di password dimenticate per il loro sblocco.

Cosa dovrebbe essere evitato

- Utilizzo di algoritmi obsoleti, come la crittografia DES e 3DES o le funzioni hash MD5 e SHA-1.
- Confondere le funzioni hash con le funzioni di crittografia e considerare che una funzione hash da sola sia sufficiente a garantire la riservatezza dei dati. Sebbene le funzioni hash siano funzioni “unidirezionali”, cioè funzioni difficili da invertire, i dati possono essere recuperati dalla sua impronta digitale. Infatti, poiché queste funzioni sono veloci nell'esecuzione, è spesso possibile testare automaticamente tutte le possibilità e quindi riconoscere l'impronta.

- Hashing delle password senza utilizzarne alcuna sale103 .

95 Talvolta chiamata impropriamente crittografia.

96 Come definito nello standard NIST FIPS 180-4.

97 Come definito nel NIST FIPS 202.

98 Come definito nel NIST FIPS 197.

99 Come definito nella RFC 8439.

100 Come definito in RSA PKCS#1 v2.2.

101 Come definito nella norma ISO/IEC 18033-2.

102 Come definito nel NIST FIPS 186-5.

103 Chiamiamo “sale” un pericolo diverso utilizzato per ciascuna password memorizzata.

ANDARE OLTRE

- Consultare la pagina dedicata sul sito web della CNIL[104] .
- ANSSI ha pubblicato **guide105** per assistere **sviluppatori e amministratori nella scelta degli algoritmi crittografici, nel dimensionamento e nell'implementazione.**
- Quando si riceve un certificato elettronico, **verificare che il certificato** contenga un'indicazione di utilizzo conforme a quanto previsto, **che sia valido e non revocabile e che abbia una corretta catena di fiducia** a tutti i livelli.

- **Utilizzare software o librerie di crittografia verificati da terze parti con comprovata esperienza.**

- È possibile utilizzare diverse soluzioni di crittografia, come ad esempio:
  - soluzioni certificate o qualificate da ANSSI[106] ;
  - software VeraCrypt, che consente l'implementazione di contenitori crittografati[107] ;
  - software GNU Privacy Guard, che consente l'implementazione della crittografia asimmetrica (firma e crittografia)[108] .
- Per le autorità amministrative, gli Allegati al General Security Repository (GSR)[109] si applicano, in particolare, gli allegati B1 e B2 riguardanti rispettivamente i meccanismi crittografici e la gestione delle chiavi.

104 “Comprensione dei principi fondamentali della crittografia e della crittografia”, cnil.fr
105 “Meccanismi crittografici”, cyber.gouv.fr
106 “VISTO DI SICUREZZA”, cyber.gouv.fr
107 Un contenitore è un file che può contenere diversi altri file.
108 “La guardia della privacy di Gnu”, gnupg.org
109 “Il quadro generale di sicurezza versione 2.0: i documenti”, cyber.gouv.fr

SCHEDA 22 – CLOUD COMPUTING

Proteggi i dati e l'elaborazione in un ambiente cloud.

Il cloud computing è percepito come un modo più rapido e flessibile per implementare nuovi servizi. Tuttavia, l'attuazione del trattamento dei dati tiene sempre conto dei rischi specifici relativi al cloud computing.
Il fornitore di servizi cloud deve fornire garanzie sufficienti per garantire che le misure di sicurezza siano state implementate correttamente. Tuttavia, anche il cliente deve essere coinvolto nella sicurezza dei propri dati e del loro trattamento nel cloud, non solo per proteggerli da terzi malintenzionati, ma anche dallo stesso fornitore di servizi cloud.

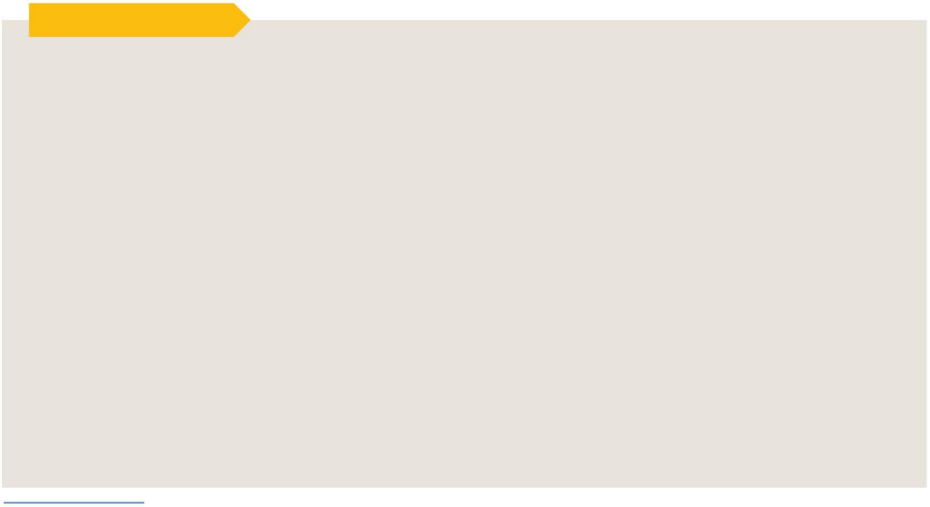
Precauzioni di base

• **Mappare dati ed elaborazioni nel cloud** e mantenere aggiornata questa mappatura. Mappa anche i servizi cloud in uso (comprese le applicazioni SaaS). Identifica le risorse cloud inutilizzate o non monitorate e, se applicabile, rimuovile.

• Valutare le esigenze di sicurezza per il trattamento dei dati implementato, quindi scegliere:
  – il **metodo** appropriato di implementazione del servizio (pubblico, privato, ibrido, comunitario, multi-cloud);
  – il fornitore di servizi cloud dopo aver valutato il livello di sicurezza garantito (in particolare per backup, ridondanza, crittografia, sicurezza fisica, sicurezza di manutenzione) secondo le specifiche riconosciute di sicurezza cloud.

• **Includere i servizi cloud nell'analisi dei rischi** (vedi scheda 20 – Analisi dei rischi), ma anche nel PCA/PRA (vedi scheda 18 – Prevedere la continuità e la ripresa dell'attività), considerando le loro specificità.
• **Assicurarsi che i requisiti di sicurezza e l'allocazione delle responsabilità siano coperti da un contratto tra il fornitore e il cliente** (vedi scheda informativa 14 – Gestione dei responsabili del trattamento dei dati).
• Garantire che **tutte le parti coinvolte** nella fornitura del servizio cloud **mantengano effettivamente il livello di sicurezza concordato** (il fornitore stesso e i suoi potenziali subappaltatori).
• **Se pertinente, configurare gli strumenti di sicurezza forniti dal fornitore** (ad esempio: crittografia, gestione degli accessi e dell'identità, firewall, strumento anti-DDoS) in conformità con la politica di sicurezza dei sistemi informativi interni.
• Applicare le **precauzioni di base** di questa guida all'elaborazione cloud. In particolare:
  – crittografare i dati dormienti nonché quelli in transito e utilizzare l'apposita gestione delle chiavi crittografiche (cfr. scheda 21 – Crittografia, hash, firma). Si noti che l'utilizzo dei servizi di gestione delle chiavi offerti dal fornitore di servizi implica che anche il fornitore di servizi abbia la possibilità di accedere ai dati;

  – assicurarsi che **solo al personale autorizzato siano assegnati i** diritti di accesso e di autorizzazione pertinenti per l'accesso alle risorse (dati e applicazioni) nel cloud e applicare il principio dei privilegi minori (vedere scheda 5 – Gestione degli accessi);
  – autenticare gli utenti per l'accesso ai servizi cloud (vedi scheda 4 – Autenticazione utenti) e concedere solo le autorizzazioni necessarie (vedi scheda 5 – Gestione degli accessi);
  – gestire e configurare i permessi delle risorse cloud;
  – esegui i backup (vedi scheda 17 – Salvataggio) e verifica che il tuo provider disponga effettivamente di più data center di backup geograficamente distanti tra loro.



SCHEDA 23 – APPLICAZIONI MOBILI: DESIGN E SVILUPPO

Applicare i principi di sicurezza di base allo sviluppo di applicazioni mobili.

Le applicazioni mobili rappresentano uno dei principali mezzi per accedere a contenuti e servizi digitali e comportano nella maggior parte dei casi il trattamento di dati personali. È necessario che gli editori garantiscano questo trattamento e offrano la massima trasparenza possibile agli utenti.

Precauzioni di base

• **Ridurre al minimo il trattamento dei dati personali** garantendo che ogni tipo di dati raccolti sia effettivamente necessario per il funzionamento dell'applicazione.
• Scegliere, in fase di selezione, i permessi rilevanti per il funzionamento dell'applicazione e che comportano una raccolta minima aggiuntiva, o anche proporre alternative all'utente non basate sui permessi (es: la geolocalizzazione può semplificare una ricerca geografica, ma può essere sostituita dall'indirizzo manuale iscrizione).
• **Proteggere le comunicazioni,** almeno con i server, incapsulandoli in un canale TLS, rispettandoli la guida ANSSI TLS121 .
• **Memorizzare i segreti crittografici in modo sicuro** tramite API che consentono l'utilizzo delle suite crittografiche incluse nel telefono, favorendo protezioni hardware come Hardware Keystore122 di Android o Secure Enclave123 di Apple .
• **Prendere in considerazione la possibilità che il sistema operativo effettui backup automatici di eventuali dati personali.** Disabilita i backup indesiderati o crittografa i dati senza includere la chiave di crittografia nei backup.
• **Utilizzare un mezzo di autenticazione corrispondente al livello di sicurezza ricercato** quando è richiesta l'autenticazione (ad esempio se una persona deve essere autenticata con certezza, non utilizzare l'autenticazione biometrica se il dispositivo utilizzato consente la registrazione di modelli biometrici di più persone).

Cosa dovrebbe essere evitato

• Contrattare con uno sviluppatore per la realizzazione di un'applicazione senza definire adeguatamente con lui gli obiettivi e le misure tecniche previste in termini di sicurezza dei dati e senza specificare che tali requisiti sono applicabili ai successivi subappaltatori (vedi scheda 14 – Gestione dei responsabili del trattamento).

• Integrare o consentire al proprio subappaltatore di integrare nella propria applicazione elementi di codice esterno (o SDK), compresi quelli proposti dagli editori di sistemi operativi mobili, senza garantire che essi stessi rispettino le precauzioni di sicurezza più moderne.

121 “Raccomandazioni di sicurezza per TLS”, cyber.gouv.fr

122 “Archivio chiavi supportato da hardware”, source.android.com

123 “Secure Enclave”, support.apple.com

ANDARE OLTRE

- In generale, rispettare i livelli L1 e L2 delle raccomandazioni prodotte dall'OWASP124.
- **Il modello di sicurezza delle applicazioni mobili non dovrebbe basarsi sull'integrità del terminale (tramite un'attestazione resa disponibile dal sistema operativo),** tranne in alcuni casi giustificati. Il servizio dovrebbe essere progettato in modo tale da mantenere il livello di sicurezza anche con terminali considerati danneggiati. Dovrebbero essere applicate **le migliori pratiche in termini di API** (vedi scheda informativa 25 – API: interfacce di programmazione dell'applicazione) **per proteggere i server utilizzati dall'applicazione e proteggerli da possibili tentativi di abuso.**
- Privilegiare il trattamento e l'archiviazione dei dati dell'utente direttamente sul suo terminale.
- È auspicabile che **l'editore di un'applicazione istituisca un processo di validazione di tutte le modifiche apportate ai trattamenti attuati, in particolare in termini di sicurezza,** al fine di evitare cambiamenti (es: operazioni di manutenzione, modifica di componenti esterni) che potrebbero impattare la sicurezza complessiva del trattamento.
- È importante implementare processi che garantiscano il mantenimento della sicurezza dell'applicazione nel tempo, tra cui:
  - adottare una metodologia di integrazione e distribuzione continua (CI/CD) per consentire aggiornamenti frequenti delle applicazioni, soprattutto nel caso di aggiornamenti di sicurezza;
  - informando gli utenti della disponibilità di aggiornamenti critici (es: un banner informativo), o anche bloccando alcune funzionalità a livello di server per versioni non sicure dell'applicazione;
  - mantenere la vigilanza sugli elementi esterni incorporati nelle applicazioni, in particolare di fronte al rischio di evoluzione dannosa negli SDK o nelle librerie utilizzate, attraverso le pratiche di sicurezza della catena di approvvigionamento descritte nelle analisi dell'ANSSI125 ;
  - garantire che il livello di sicurezza atteso possa rimanere lo stesso, il più a lungo possibile, indipendentemente dalla versione del sistema operativo utilizzato. In modo che un utente che non vuole o non può accedere a un dispositivo recente possa beneficiare di un livello di sicurezza sufficiente.

124 Progetto aperto sulla sicurezza delle applicazioni web (vedi “OWASP MAS Checklist”, mas.owasp.org).

125 “Catena di attacco ai fornitori di servizi e agli uffici di progettazione: un nuovo rapporto di analisi delle minacce”, cyber.gouv.fr

SCHEDA 24 – INTELLIGENZA ARTIFICIALE: DESIGN E IMPARARE

Dotati delle risorse e degli strumenti necessari per sviluppare un sistema di intelligenza artificiale robusto, affidabile ed efficiente.

Che si tratti di addestrare un nuovo modello o di integrare un modello esistente in un software o in un ecosistema applicativo, lo sviluppo di un sistema di intelligenza artificiale (AI) richiede l'implementazione di alcune misure di sicurezza specifiche. **L'elevato volume di dati di addestramento,** nonché la **complessità di questi sistemi,** aumentano la superficie di attacco e il rischio di guasto che può avere gravi conseguenze sull'affidabilità **del sistema.** In questa scheda informativa sono elencate alcune raccomandazioni **tecniche e organizzative** per raggiungere un primo livello di sicurezza.

Precauzioni di base

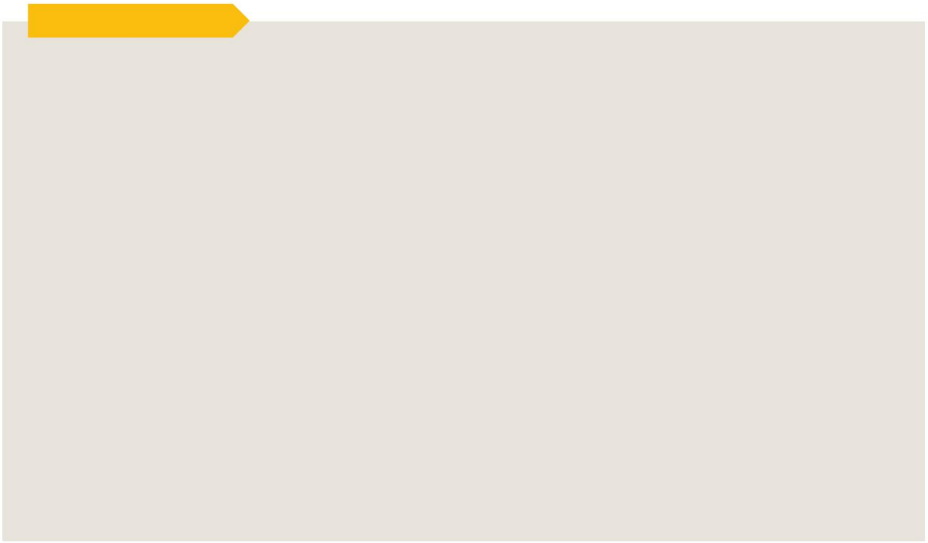
• Costituire un **team di sviluppo con competenze multidisciplinari** (analisi e ingegneria dei dati, interfaccia utente ed esperienza utente, controllo qualità, amministrazione dell'infrastruttura IT, team aziendali), garantirne la formazione sulle buone pratiche di sicurezza e aumentare la consapevolezza sulle vulnerabilità dell'IA.
• Implementare una procedura obbligatoria per lo sviluppo e l'integrazione continui, basata su **test completi e robusti, accesso soggetto ad autorizzazione e autenticazione adattata ai profili** (vedi scheda 4 – Autenticazione degli utenti), in particolare per le modifiche al codice di produzione (vedi scheda 11 – Gestione degli sviluppi IT).

• **Verificare la qualità dei dati e delle annotazioni, l'eventuale presenza di errori, l'affidabilità delle fonti dei dati,** in particolare per evitare che i dati vengano manipolati da terzi (ad esempio avvelenamento).

• **Evitare copie parziali o totali dei database** e limitare l'accesso e l'uso dei database solo alle persone autorizzate nei casi che lo richiedono. **Utilizza dati fittizi o sintetici** in altri casi, come test di sicurezza, integrazione o alcuni controlli.

• **Costruire una raccolta di documenti** per sviluppatori e utenti del sistema, tra cui:
  – la progettazione del sistema, compresi i dati e i modelli utilizzati e le analisi che hanno portato alla loro selezione e convalida, nonché i risultati di tali analisi;
  – il funzionamento del sistema durante tutto il suo ciclo di vita, le sue prestazioni, l'analisi dei suoi errori e dei risultati ottenuti, le sue condizioni e limitazioni d'uso, come i casi in cui le prestazioni potrebbero essere insufficienti;
  – l'attrezzatura materiale necessaria per l'utilizzo del sistema, la latenza prevista o la capacità massima per i sistemi accessibili in SaaS.
• **Verificare la legittimità degli utenti** del sistema quando viene reso disponibile come servizio, al fine di evitare un tentativo di attacco come un **attacco per inversione del modello126** • **Fornire un piano di audit del sistema,** che comprenda software, hardware e misure organizzative quali **le procedure per il controllo umano del sistema di IA.** **o negazione del servizio.**

126 Gli attacchi con inversione di modello mirano a ricostruire i dati utilizzati per addestrare il sistema.



SCHEDA 25 – API: PROGRAMMAZIONE DELLE APPLICAZIONI INTERFACCE

Garantire che i dati condivisi siano protetti tramite l'implementazione di un'API.

L'uso delle interfacce di programmazione delle applicazioni (API) è una buona pratica per molti casi di scambio di dati personali, poiché le API possono contribuire a rendere questi scambi più affidabili, minimi e sicuri. Per fare ciò, la gestione delle API deve far parte della politica di sicurezza dei sistemi informativi ed essere coordinata tra fornitori di API e consumatori.

Precauzioni di base

Individuare gli attori e il loro **ruolo funzionale** (titolare dei dati, API manager, organizzare il perimetrore-user130) al fine di: • di allocazione di ciascuno in **termini di accesso alle API e ai dati.**

• Limitare la condivisione ai **dati strettamente necessari,** solo alle **persone fisiche e per le finalità previste,** nel rispetto del principio di minimizzazione.

• Creare una separazione tra le chiamate alle funzioni comuni dell'API e quelle dedicate alla sua amministrazione, per le quali appare necessaria un'autenticazione robusta.

• Disporre **di registri pertinenti** per tenere traccia degli scambi (vedere la scheda informativa 16 – Operazioni di registrazione) e per rilevare e reagire in caso di uso improprio dell'API, accesso illegittimo ai dati, superamento della capacità di accesso o qualsiasi altro comportamento insolito (vedere scheda informativa 19 – Gestione degli incidenti e violazioni).

• **Mantenere aggiornata la documentazione.** Ciò deve includere il **formato delle query e dei dati** coinvolti nella condivisione al fine di limitare il rischio di interpretazioni errate.

Cosa dovrebbe essere evitato

• Mantenere **attive le vecchie versioni di un'API** che non consentono di mantenere il livello di sicurezza atteso.

• Trascurare la sicurezza delle **chiavi di accesso API,** mentre esistono soluzioni di sicurezza segrete, come una cassaforte digitale.

130 Il riutilizzatore dei dati è qualsiasi organizzazione che considera di accedere o ricevere dati tramite un'API per utilizzarli per proprio conto.

ANDARE OLTRE

- Prima del lancio di un'API, verificarne la resistenza ai rischi pubblicati dall'OWASP nel suo **Le 10 migliori API** 131.
- Consultare la raccomandazione CNIL132 sulla condivisione sicura dei dati tramite API.
- L'implementazione dell'API deve essere conforme a misure di sicurezza standard come l'implementazione di un **adeguato meccanismo di autenticazione** (vedi scheda 4 – Autenticazione degli utenti), la gestione periodica delle autorizzazioni (vedi scheda 5 – Gestione degli accessi) o la **crittografia delle comunicazioni** allo stato dell'arte.
- Dovrebbe essere resa disponibile una versione sandbox dell'API per consentire esperimenti e testare i risultati attesi da dati fittizi.

131 "OWASP API Security Top 10", owasp.org
132 "API: raccomandazioni CNIL sulla condivisione dei dati", cnil.fr

VALUTARE IL LIVELLO DI SICUREZZA DELLA MIA ORGANIZZAZIONE DATI PERSONALI

Hai pensato a...

SCHEDE INFORMATIVE		LE MISURE	
1	**Gestire la sicurezza dei dati**	Rendere la sicurezza una questione condivisa e coinvolgere il management	☐
		Verificare regolarmente l'efficacia delle misure tecniche e organizzative e adottare un approccio di miglioramento continuo	☐
2	**Definire un quadro per gli utenti**	Elaborare una carta informatica comprendente le procedure per l'utilizzo delle apparecchiature informatiche e delle risorse di telecomunicazione, le norme di sicurezza e i mezzi di amministrazione in atto	☐
		Dare forza vincolante alla Carta e ricordare le sanzioni previste in caso di mancato rispetto	☐
3	**Coinvolgente e formazione utenti**	Sensibilizzare gli utenti (sia interni che esterni all'organizzazione) che lavorano con dati personali sui rischi per la privacy	☐
		Adattare il contenuto e il linguaggio delle campagne di sensibilizzazione ai ruoli del destinatario	☐
4	**Autenticazione utenti**	Concedere un identificatore univoco a ciascun utente	☐
		Adottare una politica di password in linea con le raccomandazioni della CNIL	☐
		Richiedere all'utente di modificare la password assegnata automaticamente o da un amministratore	☐
5	**Gestione degli accessi**	Definire i profili di autorizzazione	☐
		Ritirare i permessi di accesso obsoleti	☐
		Effettuare, almeno annualmente, una revisione delle autorizzazioni	☐
6	**Garantire postazioni di lavoro**	Fornire un meccanismo di blocco automatico della sessione	☐
		Installa un software firewall	☐
		Utilizzare un antivirus regolarmente aggiornato	☐
		Ottenere il consenso dell'utente prima di qualsiasi intervento sulla sua posizione	☐
7	**Protezione del mobile computing**	Sensibilizzare gli utenti sui rischi legati all'utilizzo degli strumenti informatici mobili	☐
		Implementa o integra una soluzione di crittografia per dispositivi di archiviazione nomadi o rimovibili	☐
		Richiedere un segreto (es: password, sequenza) per lo sblocco degli smartphone	☐
8	**Protezione della rete informatica**	Limitare i flussi Internet allo stretto necessario	☐
		Gestire le reti Wi-Fi, anche implementando il protocollo WPA3	☐
		Imponi l'uso della VPN per l'accesso remoto	☐
		Partizionare la rete, creando almeno una DMZ (zona demilitarizzata)	☐
9	**Protezione dei server**	Disinstallare o disabilitare servizi e interfacce non necessari	☐
		Limitare l'accesso agli strumenti e alle interfacce di amministrazione solo al personale autorizzato	☐
		Installa gli aggiornamenti critici senza indugio dopo averli testati, ove appropriato	☐

FOGLI		LE MISURE	
10	Protezione dei siti web	Flussi di scambio dati sicuri	☐
		Assicurati che nessun segreto o dato personale venga trasmesso tramite URL	☐
		Verificare che le voci dell'utente corrispondano a quanto previsto	☐
11	Gestire Sviluppi informatici	Integrare la protezione dei dati fin dalla progettazione	☐
		Fornire impostazioni rispettose della privacy per impostazione predefinita	☐
		Eseguire un test di non regressione e/o una revisione del codice prima che qualsiasi aggiornamento venga messo in produzione	☐
		Utilizzo di dati fittizi o resi anonimi per lo sviluppo e il test	☐
12	Protezione dei locali	Limitare l'accesso ai locali mediante porte chiuse	☐
		Installare allarmi antintrusione e verificarne periodicamente il corretto funzionamento	☐
13	Garantire gli scambi con il mondo esterno	Crittografare i dati prima di trasmetterli	☐
		Assicurati che sia il destinatario giusto	☐
		Garantire la riservatezza dei segreti trasmettendoli tramite un canale separato	☐
14	Gestione dei dati processori	Prevedere clausole specifiche nei contratti dei trasformatori	☐
		Stabilire le condizioni per la restituzione e la distruzione dei dati	☐
		Fornire i mezzi per verificare l'efficacia delle garanzie sulla protezione dei dati	☐
15	Supervisionare la manutenzione e fine vita di hardware e software	Registrare gli interventi di manutenzione su un registro	☐
		Garantire che gli interventi di terze parti siano supervisionati da un responsabile dell'organizzazione	☐
		Eliminare in modo sicuro i dati dall'apparecchiatura prima del suo smaltimento	☐
16	Operazioni di registrazione	Fornire un sistema di registrazione	☐
		Informare gli utenti sul sistema di registrazione	☐
		Proteggi le apparecchiature di registrazione e le informazioni registrate	☐
		Analizza attivamente i log per rilevare il verificarsi di un incidente	☐
17	Salvataggio	Effettua frequenti backup dei dati	☐
		Proteggi i backup, sia durante l'archiviazione che durante il trasporto	☐
		Testare regolarmente l'integrità dei backup e la capacità di ripristinarli	☐

SCHEDE INFORMATIVE		LE MISURE	
18	**Prevedere continuità e ripresa dell'attività**	Scrivere un piano di continuità aziendale e un piano di ripristino di emergenza	☐
		Eseguire regolarmente i test	☐
19	**Gestione degli incidenti e delle violazioni**	Avvisi di processo generati dal sistema di registrazione	☐
		Fornire procedure interne e responsabilità per la gestione degli incidenti, inclusa la notifica alle autorità di regolamentazione delle violazioni dei dati personali	☐
20	**Analisi dei rischi**	Effettuare un'analisi dei rischi, anche minimi, sul futuro trattamento dei dati	☐
		Garantire che le misure pianificate siano implementate e monitorate	☐
		Rivedere regolarmente l'analisi dei rischi	☐
21	**Crittografia, hash, firma**	Utilizza algoritmi, software e librerie riconosciuti e sicuri	☐
		Proteggi i segreti e le chiavi crittografiche	☐
22	**Il cloud computing**	Includere i servizi cloud nell'analisi dei rischi	☐
		Valutare il livello di sicurezza garantito impostato dal fornitore di servizi cloud	☐
		Assicurarsi che i requisiti di sicurezza e l'allocazione delle responsabilità siano coperti da un contratto tra il fornitore e il cliente	☐
		Garantisci lo stesso livello di sicurezza nel cloud e in locale	☐
23	**Applicazioni mobili: Design e sviluppo**	Considerare le specificità del sistema operativo al fine di ridurre i dati personali raccolti e limitare i permessi richiesti	☐
		Proteggi le comunicazioni incapsulandole in un canale TLS	☐
		Utilizza le suite crittografiche incluse nel sistema operativo e le protezioni hardware dei segreti	☐
24	**Intelligenza artificiale: progettazione e apprendimento**	Adottare buone pratiche di sicurezza per lo sviluppo	☐
		Garantire la qualità e l'integrità dei dati e delle annotazioni utilizzate per l'apprendimento e l'inferenza	☐
		Fornire un piano di audit del sistema	☐
25	**API: interfacce di programmazione delle applicazioni**	Organizzare e documentare il perimetro di allocazione delle API in termini di sicurezza e accesso ai dati	☐
		Limitare la condivisione dei dati ai dati strettamente necessari e agli individui per gli scopi previsti	☐

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS