**CYBERYOUTH**

**Formazione non formale per la sicurezza informatica e la resilienza delle organizzazioni giovanili e dei giovani**

***Accademia online per la cybersecurity giovanile***

****

**Governance, Rischi e Conformità**

Indice

[Introduzione](#_heading=h.fpb3yt6tcffi)

[Potrebbe essere successo anche a te...](#_heading=h.c7zxm1r80lor)

[Cosa imparerai](#_heading=h.bd1t10x6k115)

[Perché è importante](#_heading=h.1fqj6c1n3ygs)

[Come può aiutarti nella vita di tutti i giorni](#_heading=h.bddh90wxykhs)

[Quale carriera puoi intraprendere](#_heading=h.l25siuf1d90q)

[Pre-requisiti](#_heading=h.obikvf4haym5)

[Materiale](#_heading=h.wlxlanfpyu9n)

[6.1 Leggi e Regolamentazione](#_heading=h.2yz7x8bu8zb5)

[Leggi sul Data Protection](#_heading=h.oo7qhy4nz301)

[GDPR](#_heading=h.mxx776cq98gz)

[Leggi Europee](#_heading=h.gpht6cntx8cg)

[Leggi Nazionali/Statali](#_heading=h.jo5y0jx0953s)

[Conclusioni](#_heading=h.q7y4utybp22l)

[6.2 Quadri chiave per la protezione dei dati](#_heading=h.wv8lmqsplpdd)

[ISO](#_heading=h.se3v82rotiu3)

[CSF](#_heading=h.xa9iyn2x8esy)

[6.3 Gestione del Personale](#_heading=h.g98km9urykdd)

[Personale Introduzione](#_heading=h.d7j3sia9a2ue)

[Onboarding](#_heading=h.4rgr0sqkydi2)

[Politiche di Sicurezze Basilari](#_heading=h.yqucjs90vwi5)

[Training](#_heading=h.uu16mwe9cyzf)

[Politiche Comportamentali e di Condotta](#_heading=h.aymlrjsxfl61)

[Gestione dei rischi interni](#_heading=h.ls5c88is89uy)

[6.4 Gestione dei rischi da parti terze](#_heading=h.7pii0khen2cd)

[Conclusioni](#_heading=h.8fgh3pvuc4s3)

[6.5 Dati sensibili](#_heading=h.azw51npc11fy)

[Conclusioni](#_heading=h.scbfee5behhv)

[L’angolo del Geek](#_heading=h.floxyjcfjlz3)

[Conclusioni](#_heading=h.umqq3lf4f2yk)

[Quiz](#_heading=h.35btfg6prjdy)

[Fonti](#_heading=h.ioedg3ublhq7)

# 

# **Introduzione**

## **Potrebbe essere successo anche a te...**

Nel 2022, il NHS, il sistema sanitario socializzato del Regno Unito, è stato vittima di un attacco di phishing che ha portato alla disponibilità di centinaia di email dei dipendenti e dati personali e a una violazione dei dati nel sistema interno.

Si è scoperto che i dipendenti avevano ricevuto una richiesta di accesso fasulla ai loro account interni, e accedendo a tali account, i malintenzionati hanno potuto ottenere l'accesso ai loro account e ai dati privilegiati senza alcun problema.

Sfortunatamente, situazioni come questa (attacchi dovuti a errori umani o formazione inadeguata) sono molto più comuni del tipo di attacco informatico mostrato nei media come in TV o nei film, motivo per cui non si può sottolineare a sufficienza l'importanza di una corretta formazione iniziale e di un addestramento del personale, nonché di politiche rigorose sulla gestione dei dati.

Forse dovresti pensarci due volte quando ricevi una email da un'azienda che afferma che devi effettuare l'accesso immediatamente!

## **Cosa imparerai**

In questo modulo, impareremo le restrizioni legali e governative per mantenere sicuri i dati e, di conseguenza, le persone. Approfondiremo anche la valutazione e la gestione dei rischi, dalla formazione del personale al trattamento dei dati altamente sensibili, nonché il processo per identificare e agire su questi rischi e prevenire che i rischi diventino incidenti o che gli incidenti diventino crisi. Discuteremo alcuni dei principali quadri e standard coinvolti nello scambio e nel trattamento dei dati, sia storicamente che soprattutto attualmente. Durante questo modulo, un aspetto fondamentale da tenere in considerazione, forse il più importante e spesso ignorato, è la **conformità normativa**. Dopotutto, possiamo sviluppare il piano o la politica più sicura possibile, ma senza la conformità, tutto ciò va in fumo!

## **Perché è importante**

Questo modulo è essenziale per te e per la tua organizzazione poiché fornisce una base per comprendere l'importanza della governance dei dati e la conformità alle linee guida, alle leggi e ai regolamenti stabiliti nella mitigazione dei rischi legati alla sicurezza informatica che possono mettere a repentaglio i dati organizzativi e personali. Attraverso il completamento di questo modulo, comprenderemo i rischi associati alla gestione di dati personali o sensibili e, attraverso ciò, l'importanza delle normative e della governance per stabilire come gestire tali dati. Dopotutto, queste leggi o regolamenti possono sembrare superflui a prima vista, ma sono la chiave per assicurare che tutte le organizzazioni e/o le imprese seguano linee guida rigorose anziché lasciare queste decisioni alla discrezione personale.

## **Come può aiutarti nella vita di tutti i giorni**

I materiali trattati in questo modulo potrebbero non sembrare tali a prima vista, ma sono fondamentali per mantenere al sicuro i dati e collaborare con gli standard stabiliti nella protezione dei dati, nonché per capire perché essi esistono in primo luogo. Acquisiremo una conoscenza più approfondita sulla governance dei dati digitali e fisici e sull'importanza della conformità alle linee guida locali, nazionali e internazionali e ai quadri giuridici, imparando come ridurre il rischio di incidenti e violazioni della sicurezza o problemi seguendo e conformandosi alle leggi stabilite, nonché mantenendo registrazioni e documentazione dei quadri seguiti per garantire una copertura legale in caso di incidenti o qualsiasi forma di attacco informatico.

## **Quale carriera puoi intraprendere**

Completando questo modulo e l'intero corso online, acquisirai una maggiore comprensione delle complessità della regolamentazione e della conformità dei dati, nonché dei rischi associati a non seguirle, acquisendo nel contempo ulteriori conoscenze sui punti chiave relativi all'integrazione e alla preparazione dei nuovi dipendenti, preparandoti per posizioni come:

* Specialista dell'integrazione
* Agente di valutazione del rischio
* Esperto junior della regolamentazione

## **Pre-requisiti**

Per trarre il massimo beneficio dal contenuto di questo modulo, ti consigliamo di completare i moduli precedenti del corso online per seguire i comuni fili conduttori importanti e comprendere meglio i concetti discussi. Non avrai bisogno di conoscenze precedenti sulla regolamentazione dei dati, se non una conoscenza di base dei concetti, quindi questo modulo è ottimo sia per imparare da zero che per migliorare le tue conoscenze esistenti.

# 

# **Materiale**

## **6.1 Leggi e Regolamentazione**

### Leggi sul Data Protection

Una delle chiavi per la sicurezza digitale è regolare la protezione dei dati al fine di standardizzare il trattamento dei dati. In questo modo, esistono leggi sulla protezione dei dati e vengono attuate per regolamentare i modi in cui i dati possono essere gestiti.

### GDPR

Chiunque lavori nell'industria della sicurezza informatica deve essere familiarizzato con il Regolamento Generale sulla Protezione dei Dati (GDPR). Un ampio quadro di protezione dei dati chiamato GDPR è stato messo in atto nel 2018 con l'obiettivo di preservare il diritto alla privacy delle persone all'interno dell'Unione Europea (UE). Esso stabilisce una serie di linee guida, requisiti e diritti relativi alla raccolta, gestione e conservazione dei dati personali. Come esperto di sicurezza informatica, è necessario comprendere le idee fondamentali del GDPR, tra cui i concetti di liceità, correttezza e trasparenza, nonché i diritti dei soggetti dei dati, le responsabilità organizzative e le sanzioni per la mancata conformità.

Comprendere il GDPR può aiutarti a migliorare la sicurezza e la privacy dei dati sia per singoli individui che per le imprese, fornendoti utili informazioni sulla protezione dei dati personali e garantendo che le tue attività di sicurezza informatica siano conformi agli standard legali.

### Leggi Europee

Lo sviluppo dei metodi di sicurezza informatica e la protezione della privacy dei dati sono significativamente influenzati dalla legislazione europea. Gli esperti di sicurezza informatica dovrebbero essere informati su altre leggi e direttive significative all'interno dell'Unione Europea, oltre al GDPR. Gli operatori di servizi vitali e i fornitori di servizi digitali devono attenersi ai criteri di sicurezza informatica e segnalazione degli incidenti stabiliti dalla Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS Directive). Tale direttiva mira ad aumentare la resilienza complessiva dei servizi Internet e dell'infrastruttura critica.

La Direttiva sull'ePrivacy è incentrata sulla tutela della privacy di coloro che utilizzano comunicazioni elettroniche e contiene regolamenti relativi ai cookie, ai messaggi di marketing e alla riservatezza di tali dati. Il Regolamento UE sulla cibersicurezza stabilisce inoltre un quadro per l'accreditamento di beni, servizi e procedure correlati alla sicurezza informatica. Gli esperti di sicurezza informatica possono mantenere la conformità e contribuire a creare un ambiente digitale sicuro e rispettoso della privacy all'interno dell'Unione Europea rimanendo informati sulla legislazione europea.

### Leggi Nazionali/Statali

Oltre alla legislazione europea, è fondamentale che i professionisti della cybersecurity comprendano le regolamentazioni nazionali che disciplinano la protezione dei dati e le pratiche di sicurezza informatica. Ogni paese all'interno dell'Unione Europea può avere leggi e regolamenti specifici che integrano il GDPR e forniscono ulteriori orientamenti sulle responsabilità in materia di sicurezza informatica. Ad esempio, nel Regno Unito, il Data Protection Act 2018 integra il GDPR e stabilisce requisiti aggiuntivi per la protezione dei dati. Allo stesso modo, paesi come Germania, Francia e Spagna hanno adottato leggi nazionali per integrare e chiarire le disposizioni del GDPR.

Queste regolamentazioni nazionali possono affrontare aree specifiche come i requisiti di notifica delle violazioni dei dati, le normative settoriali o ulteriori misure di sicurezza per il trattamento dei dati personali. Come professionista della cybersecurity, rimanere aggiornati sulle regolamentazioni nazionali è essenziale per garantire la conformità e proteggere efficacemente i dati all'interno delle giurisdizioni nazionali specifiche. Comprendendo sia la legislazione europea che quella nazionale, i professionisti della cybersecurity possono navigare nel complesso panorama regolamentare e implementare misure robuste di sicurezza informatica in linea con i requisiti regionali e locali.

In tutti i casi relativi alla cybersecurity e alla regolamentazione, è fondamentale consultare i quadri giuridici nazionali, regionali e locali per comprendere come essi differiscano rispetto alla regolamentazione dell'UE e al GDPR al fine di capire come conformarsi correttamente alle regolamentazioni a livello dell'UE e locale.

### **Conclusioni**

Per riassumere quanto abbiamo discusso, l'UE sta guidando il mondo nella protezione dei dati personali e nel diritto alla privacy in un mondo sempre più pubblico. Le normative sulla protezione dei dati, come il GDPR, sono fondamentali per mantenere la sicurezza online e la privacy per l'intera popolazione, e la conformità ad esse è essenziale per trattare i dati in modo etico, legale e responsabile. Sebbene le linee guida del GDPR siano rigorose e chiare, la loro applicazione può variare da paese a paese, pertanto è sempre importante essere il più cauti e rispettosi possibile della privacy, mentre si comprendono le basi giuridiche nel paese dell'organizzazione per avere una migliore conoscenza del trattamento dei dati.

## **6.2 Quadri chiave per la protezione dei dati**

Con l'importanza della sicurezza dei dati e la protezione delle informazioni sensibili o personali, l'uso di linee guida standardizzate al di là dei quadri legali attuati a livello nazionale o europeo è diventato più comune in molte organizzazioni e aziende. Diamo un'occhiata a due quadri chiave che affrontano la gestione dei rischi e la protezione dei dati per le organizzazioni e gli individui.

### **ISO**

Il quadro ISO (Organizzazione internazionale per la normazione) è un insieme di norme internazionali che fornisce linee guida e migliori pratiche per vari aspetti della gestione organizzativa, compresa la sicurezza informatica. Ecco alcuni punti chiave sul quadro ISO:

* **ISO 27001:** Sistema di gestione della sicurezza delle informazioni (ISMS): ISO 27001 è lo standard principale per la gestione della sicurezza delle informazioni. Fornisce un approccio sistematico per stabilire, implementare, mantenere e migliorare continuamente l'ISMS di un'organizzazione. Lo standard comprende vari controlli di sicurezza e processi di gestione dei rischi per proteggere la confidenzialità, l'integrità e la disponibilità delle informazioni.
* **ISO 27002:** Codice di pratica per i controlli di sicurezza delle informazioni: ISO 27002 fornisce un insieme completo di controlli di sicurezza che possono essere implementati per affrontare rischi specifici per la sicurezza delle informazioni. Offre orientamenti sulla selezione, implementazione e gestione dei controlli in vari ambiti come il controllo degli accessi, la crittografia, la sicurezza fisica, la gestione degli incidenti e altro ancora.
* **ISO 27005:** Gestione dei rischi per la sicurezza delle informazioni: ISO 27005 si concentra sulla gestione sistematica dei rischi per la sicurezza delle informazioni all'interno di un'organizzazione. Fornisce linee guida per la valutazione dei rischi, il trattamento dei rischi e i processi di accettazione dei rischi. Lo standard enfatizza l'importanza dell'individuazione e della valutazione dei rischi per prendere decisioni informate in merito all'implementazione dei controlli di sicurezza.
* **ISO 31000:** Gestione dei rischi: ISO 31000 è uno standard di gestione dei rischi più ampio applicabile a vari settori, compresa la sicurezza informatica. Fornisce principi, quadro e processi per gestire efficacemente i rischi. Mentre ISO 27005 si concentra specificamente sui rischi per la sicurezza delle informazioni, ISO 31000 fornisce un approccio più generale che può essere applicato ad altre aree della gestione dei rischi all'interno di un'organizzazione.
* **ISO 22301:** Sistema di gestione della continuità aziendale (BCMS): ISO 22301 si concentra sulla creazione e sul mantenimento di un BCMS per garantire che le organizzazioni possano rispondere ed riprendersi efficacemente da incidenti disruptivi. Fornisce un quadro per la pianificazione della continuità aziendale, compresa la valutazione dei rischi, l'analisi dell'impatto aziendale e lo sviluppo di strategie di continuità.
* **ISO 20000:** Gestione dei servizi IT: ISO 20000 delinea le migliori pratiche per la gestione dei servizi IT, inclusa la fornitura, la gestione e il supporto dei servizi IT. Pur non essendo specificamente focalizzato sulla sicurezza informatica, enfatizza l'importanza della fornitura sicura dei servizi IT, della gestione degli incidenti e del miglioramento continuo dei processi IT.

Queste norme ISO forniscono alle organizzazioni quadri e linee guida riconosciuti a livello internazionale per stabilire pratiche efficaci di sicurezza informatica e di gestione dei rischi. L'implementazione di queste norme può aiutare le organizzazioni a migliorare la propria postura di sicurezza, dimostrare la conformità alle migliori pratiche del settore e costruire fiducia con gli stakeholder.

### **CSF**

Il quadro CSF, noto anche come NIST Cybersecurity Framework, è un insieme di linee guida e migliori pratiche sviluppate dal National Institute of Standards and Technology (NIST) negli Stati Uniti. Il CSF fornisce un quadro flessibile e volontario per le organizzazioni al fine di gestire ed attenuare efficacemente i rischi legati alla sicurezza informatica.

Il quadro CSF è composto da tre componenti principali: il Core, gli Implementation Tiers e il Profilo.

1. **Core:** Il Core del quadro CSF include cinque funzioni chiave: Identificare, Proteggere, Rilevare, Rispondere e Recuperare. Queste funzioni rappresentano le attività fondamentali di sicurezza informatica che le organizzazioni dovrebbero intraprendere per stabilire una solida postura di sicurezza informatica. Ciascuna funzione è ulteriormente suddivisa in categorie e sottocategorie che forniscono orientamenti più specifici sulle attività di sicurezza informatica.
2. **Implementation Tiers:** Gli Implementation Tiers nel quadro CSF forniscono un modo per le organizzazioni di valutare e comunicare il loro livello di maturità in materia di sicurezza informatica. Ci sono quattro livelli: Parziale, Basato sul Rischio, Ripetibile e Adattivo. Questi livelli aiutano le organizzazioni a comprendere il loro stato attuale della sicurezza informatica e a stabilire obiettivi di miglioramento.
3. **Profilo:** Il componente Profilo del quadro CSF consente alle organizzazioni di allineare le loro attività di sicurezza informatica con le esigenze aziendali e la tolleranza al rischio. Le organizzazioni possono creare un Profilo selezionando le categorie e le sottocategorie pertinenti del Core in base alle loro esigenze specifiche, priorità e risorse disponibili.

Il quadro CSF enfatizza un approccio basato sul rischio alla sicurezza informatica, concentrandosi sull'innovazione continua e sulla collaborazione tra diverse funzioni aziendali. Fornisce un linguaggio e un quadro comuni per le organizzazioni per gestire e comunicare efficacemente i rischi legati alla sicurezza informatica, sia internamente che esternamente. Il quadro CSF può essere adottato da organizzazioni di qualsiasi dimensione, settore o livello di maturità per potenziare la loro postura di sicurezza informatica e resilienza.

## **6.3 Gestione del Personale**

Un'altra chiave per la regolamentazione e la conformità è una corretta comprensione da parte dei membri di un'organizzazione. Dopotutto, se i membri del nostro team non comprendono le loro obbligazioni nel trattare i dati, come possiamo aspettarci che si conformino? Ecco perché l'importanza di una formazione adeguata prima di iniziare a lavorare in un nuovo luogo di lavoro è fondamentale, ed è per questo che la preparazione adeguata dei nuovi dipendenti o membri del team è un pilastro fondamentale per garantire che le leggi e i regolamenti vengano rispettati. Come si suol dire, inizia come intendi proseguire!

### **Personale Introduzione**

Come menzionato, la chiave per garantire che un'organizzazione stia seguendo la procedura corretta è formare i dipendenti e i membri del team sin dall'inizio. Ciò significa assicurarsi che tutte le regole, i regolamenti o le leggi pertinenti vengano spiegate e che venga fornita formazione ai nuovi membri, e idealmente, dovrebbe essere offerta supervisione durante un breve periodo mentre i nuovi membri si familiarizzano con l'organizzazione e gli sviluppi.

#### Onboarding

La parte più importante per preparare adeguatamente un nuovo dipendente o membro del team per il successo, sia in senso di sicurezza che in senso lato, è un processo di inserimento dettagliato e chiaro. In molti casi, questo può essere sviluppato attraverso video, presentazioni di diapositive o talvolta persino attraverso un breve percorso di apprendimento online. Qualunque sia il metodo di sviluppo, i pilastri chiave rimangono gli stessi; il processo di inserimento dovrebbe informare il nuovo membro del team su tutto ciò che deve sapere, offrendo anche risorse per consultazioni future, per consentire ai membri di integrarsi senza problemi in un'organizzazione senza diventare un rischio né per la produttività, né, cosa più importante, per la sicurezza informatica dell'organizzazione. Un corretto processo di inserimento dovrebbe lasciare il dipendente o il membro del team pronto per iniziare in modo sicuro e responsabile.

#### Politiche di Sicurezze Basilari

Oltre a preparare i membri attraverso un inserimento dettagliato, come abbiamo discusso nei moduli precedenti, uno dei punti più cruciali in materia di sicurezza informatica di un'organizzazione è avere regole e regolamenti interni chiari e definiti, non solo legalmente. Sviluppando una Politica di Sicurezza chiara e concisa, possiamo garantire la conformità in tutta l'organizzazione nel mantenere al sicuro i dati, nonché assicurarci che i dipendenti e i membri del team rimangano al sicuro nella comunicazione.

### **Training**

Oltre alle politiche interne e all'inserimento, è importante assicurarsi che i membri dell'organizzazione abbiano accesso a opportunità di formazione coerenti e significative per sviluppare le loro conoscenze e competenze in materia di sicurezza informatica all'interno dell'organizzazione al fine di garantire le capacità dei membri del team e dei lavoratori.

### **Politiche Comportamentali e di Condotta**

In un contesto di sicurezza informatica, l'istituzione di politiche comportamentali solide è essenziale per promuovere una cultura di comportamento responsabile e sicuro all'interno di un'organizzazione. Le politiche di condotta in questo contesto dovrebbero sottolineare l'importanza di salvaguardare informazioni sensibili, proteggere sistemi e reti e attenersi a standard etici. Dovrebbero delineare chiaramente linee guida per l'uso accettabile delle risorse tecnologiche, compresa la corretta gestione dei dati, l'adesione ai protocolli di sicurezza e il rispetto delle leggi e dei regolamenti applicabili. Inoltre, le politiche di condotta dovrebbero affrontare i potenziali rischi associati all'ingegneria sociale, agli attacchi di phishing, al malware e ad altre minacce alla sicurezza informatica. Sottolineare l'importanza degli aggiornamenti regolari del software, delle password robuste e della segnalazione di attività sospette contribuirà a creare una cultura consapevole della sicurezza. Mediante l'istituzione e l'applicazione di solide politiche di condotta, le organizzazioni possono ridurre la probabilità di incidenti di sicurezza e migliorare l'insieme della loro postura di sicurezza informatica.

### **Gestione dei rischi interni**

La gestione interna del rischio in un contesto di sicurezza informatica è fondamentale affinché le organizzazioni identifichino, valutino e mitigano i potenziali rischi per i loro sistemi informativi e per i dati sensibili. Questo implica un approccio sistematico alla comprensione e alla gestione delle vulnerabilità interne, delle minacce e degli impatti potenziali sulla sicurezza informatica. Una gestione interna efficace del rischio comporta la conduzione periodica di valutazioni del rischio per identificare le debolezze, valutare la probabilità e l'impatto potenziale di diverse minacce e prioritizzare di conseguenza gli sforzi di mitigazione. Comprende anche l'istituzione di controlli interni robusti, come controlli di accesso, crittografia e sistemi di monitoraggio, per rilevare e rispondere tempestivamente agli incidenti di sicurezza. Inoltre, le organizzazioni devono educare e formare i propri dipendenti sulle migliori pratiche di sicurezza informatica, promuovendo una cultura di consapevolezza e responsabilità in tutta l'organizzazione. Mediante l'attuazione di una strategia completa di gestione interna del rischio, le organizzazioni possono proteggere in modo proattivo i propri asset, mitigare i potenziali rischi di sicurezza informatica e garantire la continuità delle proprie operazioni di fronte alle minacce in evoluzione.

## **6.4 Gestione dei rischi da parti terze**

La gestione dei rischi legati ai fornitori esterni è un aspetto critico della sicurezza informatica, poiché le organizzazioni spesso si affidano a fornitori, partner e collaboratori esterni che possono avere accesso ai loro sistemi, reti o dati sensibili. Una gestione efficace dei rischi legati ai fornitori esterni comporta la valutazione e la mitigazione dei potenziali rischi di sicurezza informatica associati a queste entità esterne. Le organizzazioni dovrebbero stabilire un quadro completo che includa processi di dovuta diligenza per valutare le pratiche di sicurezza informatica dei fornitori esterni, accordi contrattuali che delineino requisiti e responsabilità in materia di sicurezza e meccanismi di monitoraggio e audit continui per garantire la conformità.

Per gestire efficacemente il rischio legato ai fornitori esterni, le organizzazioni dovrebbero iniziare identificando e categorizzando i fornitori e i partner critici in base al loro livello di accesso e alla sensibilità dei dati da loro gestiti. Dovrebbe essere condotta una dovuta diligenza per valutare i controlli di sicurezza, le politiche e le pratiche di questi fornitori esterni. Ciò potrebbe includere la revisione delle certificazioni di sicurezza, la conduzione di audit in loco o la richiesta di documentazione sulle politiche di sicurezza informatica e i piani di risposta agli incidenti. Inoltre, le organizzazioni dovrebbero stabilire accordi contrattuali chiari che delineino requisiti specifici in materia di sicurezza, misure di protezione dei dati, protocolli di risposta agli incidenti e disposizioni in materia di responsabilità.

Dovrebbero essere condotti monitoraggi continui e valutazioni periodiche per garantire che i fornitori esterni continuino a rispettare gli standard di sicurezza concordati e per affrontare tempestivamente eventuali vulnerabilità o violazioni identificate. Mediante l'attuazione di un solido programma di gestione dei rischi legati ai fornitori esterni, le organizzazioni possono rafforzare la propria posizione complessiva in materia di sicurezza informatica e mitigare i potenziali rischi introdotti da entità esterne.

In conclusione, la gestione dei rischi legati ai fornitori esterni è una componente essenziale della sicurezza informatica. Attraverso una dovuta diligenza approfondita, la stipula di accordi contrattuali chiari e l'attuazione di processi di monitoraggio e audit continui, le organizzazioni possono valutare ed affrontare in modo efficace i potenziali rischi di sicurezza informatica posti dai propri fornitori e collaboratori esterni. Questo approccio proattivo aiuta a proteggere i sistemi, le reti e i dati sensibili dell'organizzazione, garantendo la sicurezza e l'integrità complessiva delle proprie operazioni.

### **Conclusioni**

In sintesi, la gestione, compresa la formazione adeguata e l'onboarding dei membri del team e dei dipendenti, è un punto chiave nella sicurezza di un'organizzazione e nella conformità alla governance dei dati e alle normative, insieme alla sicurezza dei clienti o degli utenti, nonché dei dipendenti o dei membri del team.

## **6.5 Dati sensibili**

Considerando tutto ciò di cui abbiamo discusso, possiamo comprendere l'importanza di trattare i dati in modo appropriato e di seguire la governance e la legislazione che dettaglia il trattamento dei dati personali. Pertanto, quando si tratta di dati sensibili o potenzialmente dannosi (dati che includono nomi di utenti minorenni, dettagli relativi al codice fiscale, indirizzi, password, ecc.), tali regole e regolamenti dovrebbero essere seguiti ancor di più "alla lettera" per così dire.

La gestione dei dati sensibili è un aspetto critico della sicurezza informatica, poiché le organizzazioni gestiscono grandi quantità di informazioni confidenziali e sensibili. Gestire efficacemente i dati sensibili comporta l'implementazione di politiche, procedure e salvaguardie robuste per proteggere la loro riservatezza, integrità e disponibilità. Ciò include l'identificazione e la classificazione dei dati sensibili in base al livello di sensibilità e all'impatto potenziale in caso di compromissione. Le organizzazioni dovrebbero sempre sviluppare e implementare politiche rigorose, compresi i metodi precedentemente discussi per mantenere al sicuro i dati, come i backup, i ripristini, la crittografia, ecc.

### **Conclusioni**

Per riflettere, il trattamento dei dati personali dovrebbe essere gestito con particolare attenzione, ma dovrebbe seguire le stesse linee guida e leggi del trattamento di qualsiasi altro dato o informazione.

## **L’angolo del Geek**

Attraverso la corretta formazione dei membri del team e l'attuazione di politiche chiare e concise sulla Governance dei Dati conformi alle linee guida e ai framework principali, come il GDPR, è possibile migliorare la sicurezza di un'organizzazione al livello più basilare, semplicemente fornendo informazioni e formazione ai dipendenti e/o ai membri.

Ci sono molti strumenti e risorse disponibili per fornire ai dipendenti, ai volontari o ai membri del gruppo una formazione. Sfortunatamente, le leggi sulla protezione dei dati sono in continua evoluzione e cambiamento, quindi fornire risorse specifiche potrebbe portare a informazioni obsolete. Invece, la maggior parte delle organizzazioni consiglia di fornire una formazione frequente (ad esempio, una volta ogni trimestre) e chiara sulle migliori pratiche di gestione dei dati, nonché di fornire esempi o casi da evitare, discutere incidenti, ecc. Alcuni esempi di conoscenze che non sono influenzate dalle leggi in evoluzione potrebbero essere fattori chiave come:

* Non consentire ai membri del team di accedere a dati sensibili sui loro dispositivi personali.
* Assicurarsi che i membri del team non scambino informazioni sensibili non crittografate su canali esterni.
* Fornire controlli di analisi dei rischi al proprio team su base regolare (semestrale o più) per garantire che tutte le politiche sui dati siano seguite e rispettate.

# **Conclusioni**

In conclusione, la chiave per una Governance dei Dati efficace, così come per la Gestione del Rischio e la Conformità ai framework esistenti, è l'impegno nel fornire ai membri del team la giusta formazione e comprensione di questi concetti.

L'importanza di questi concetti nel gestire un'organizzazione digitalmente sicura, responsabile e affidabile è fondamentale per la sicurezza dei dipendenti, dei membri del team e, nel caso di molte organizzazioni, degli utenti o pazienti.

## **Quiz**

**Qual è lo scopo principale dei framework di governance dei dati?**

a) Per dirci cosa fare e comandarci.

b) Per standardizzare il modo in cui i dati vengono trattati e le relative politiche.

c) Per monitorare come le persone utilizzano i loro sistemi.

d) Per assicurarsi che nessuno sia in grado di vivere offline.

**Il GDPR è rilevante nella sicurezza informatica?**

a) No, è solo menzionato affinché nessuno si lamenti

b) È la principale linea guida per la protezione dei dati in Europa, nonché leader mondiale.

c) È importante ma non quanto la Legge Nazionale

d) Un metodo utilizzato dagli hacker per ottenere accesso a un sistema

**Come dovrebbe preparare un adeguato processo di inserimento (onboarding) un dipendente?**

a) Un dipendente dovrebbe essere pronto a integrarsi senza soluzione di continuità nel team

b) Digli dove si trova il caffè

c) Dovrebbero ricevere una password e un nome utente, tutto il resto è da apprendere

d) Dovrebbero conoscere il nome dell'azienda e la loro posizione

**Dovrebbe essere il dato sensibile trattato con standard diversi?**

a) Dovrebbe essere trattato seguendo gli stessi standard e linee guida, con maggiore attenzione

b) Dovrebbe essere inviato non criptato via email

c) No, è uguale a qualsiasi altro dato

d) Sì

**Qual è il termine per un tipo di attacco informatico in cui un aggressore intercetta la comunicazione tra due parti al fine di rubare informazioni sensibili?**

a) Attacco Man-in-the-Middle (MitM)

b) Attacco Cross-Site Scripting (XSS)

c) Attacco Cross-Site Request Forgery (CSRF)

d) Attacco Ransomware

## **Fonti**

United States Securities and Exchange Commission. (2018). Equifax Inc. Form 8-K: Current report filing (Amended). Retrieved from <https://www.sec.gov/Archives/edgar/data/33185/000119312518154706/d583804dex991.htm>