





CHI SIAMO

La consulenza strategica supporta la pianificazione delle politiche di sicurezza: la protezione dei dati è da considerare un processo.

Concorrono al risultato oltre agli aspetti tecnologici afferenti alla sicurezza informatica, quelli legali, organizzativi e procedurali.

L'approccio sistemico ed integrato, permette di elaborare la soluzione migliore rapportata all'esigenza del Cliente.

Il team di consulenti di DataConSec è composto da personale altamente qualificato, che può vantare una ventennale esperienza nel mondo della sicurezza delle informazioni.

Lo staff è costantemente impegnato in attività di ricerca scientifica in ambito universitario.

MISSION

Il team di DataConSec supporta il cliente nella definizione e attuazione di un progetto generale di Sicurezza e Privacy, come sistema integrato.

Il governo della conformità in ambito ICT si può definire pertanto come il complesso di policy e procedure, attuato e mantenuto dall'organizzazione per garantire nel tempo il soddisfacimento dei requisiti che regolano la gestione corretta delle proprie informazioni. Tale definizione è in linea con il concetto di ISMS (Information Security Management System) come previsto nello standard ISO 27000.

Il valore della consulenza DataConSec è quella di disegnare una strategia personalizzata conforme ai requisiti legali bilanciando la necessità di protezione dei dati e quindi del business.

I NOSTRI SERVIZI



Protezione dei dati



Consulenza di Direzione aziendale



Analisi dei rischi di cyber sicurezza



Cybersecurity



Analisi forense



Whistleblowing

Servizio di adeguamento alla normativa



ConceptLog



AEO

Operatore economico autorizzato



FAD

Portale formazione

PROTEZIONE DEI DATI

- **→ Adeguamento GDPR**
- → Privacy Impact Assessment
- → Data Protection Officer Outsourcing
- **→ Audit Privacy**

DataConSec propone soluzioni complete, servizi dedicati e competenze specialistiche per supportare i Clienti nel percorso di adeguamento al GDPR.

La soluzione di adeguamento più completa riguarda la copertura di tutte le aree chiave e i requisiti previsti dal GDPR che vengono declinate in:

- ▶ Politica per la protezione dei dati personali
- Data Governance
- Misure di accountability
- Trasparenza e diritti per gli interessati



- ▶ Trasferimento dati extra UE
- Analisi di impatto DPIA
- Ruolo di DPO in outsourcing
- ► Risoluzione di casi concreti

La compliance al GDPR è pensata come un vero e proprio **Sistema di gestione** e prevede step progressivi di integrazione con altri modelli organizzativi aziendali al fine di trarre reale valore aggiunto dalle attività svolte.

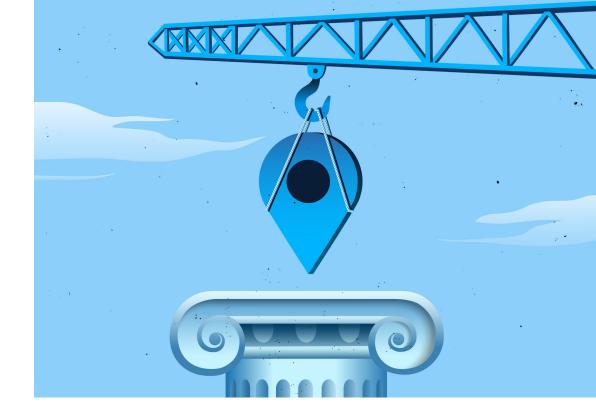
CONSULENZA DI DIREZIONE AZIENDALE

- → Consulenza sistemi di gestione ISO 27001
- \rightarrow Information Risk Management
- \rightarrow 231/01 con focus sui reati informatici

DataConSec può vantare all'interno del suo staff professionisti che si occupano di consulenza di direzione aziendale relativamente alla governance e alla sicurezza delle informazioni.

L'ambito di specializzazione spazia dal Enterprise Risk Management alle attività di Compliance e Audit.

L'esperienza nella revisione dei processi e delle procedure interne ci ha permesso inoltre di accompagnare numerose organizzazioni nella redazione delle IT Policy e durante tutto l'iter di certificazione agli standard internazionali di riferimento (della famiglia ISO si segnalano ad esempio 9001, 20000, 22301, 27001, 38500, 27018, 31000, ecc.).



I nostri consulenti inoltre supportano le aziende nell'adozione dei modelli organizzativi esimenti richiesti dal D.Lgs. n. 231/2001 inerente alla responsabilità amministrativa degli enti e ricoprono un ruolo attivo coadiuvando gli Organismi di Vigilanza in qualità di esperti.

ANALISI DEI RISCHI DI CYBER SICUREZZA

→ Protezione dei dati, del know-how e delle informazioni sensibili per il business

Secondo i dati del report della Polizia postale e delle comunicazioni, pubblicato anche sul Sole 24 Ore, le denunce per attacchi informatici gravi sono aumentate del 45% nel 2022.

Le PMI e gli studi professionali rappresentano il bersaglio principale dei cybercriminali, manifattura e servizi sono i più colpiti dalle richieste di riscatto da parte di criminali informatici, dipendenti infedeli e malintenzionati.

Per far fronte a questo fenomeno, sempre più preoccupante, e non farsi cogliere impreparati è necessario misurare il livello di rischio cyber a cui è esposta la propria organizzazione al fine di proteggere adeguatamente i processi critici e garantire il corretto funzionamento delle attività lavorative.



L'obiettivo di un'analisi del rischio cyber è quello di ottenere una fotografia dello stato di sicurezza del sistema informativo e al termine della verifica produrre un report dettagliato contenente i punti di miglioramento suggeriti.

Il servizio avanzato offerto da DataConSec comprende anche lo svolgimento di specifiche attività tecniche quali:

- ▶ Patch Level Assessment
- **▶** Password Check
- Vulnerability Assessment

CYBER SECURITY

- → Vulnerability assessment
- → Log management
- → Penetration testing
- → Security assessment

Cyber Security

Supportiamo i Clienti nell'implementazione di controlli specifici sugli asset più esposti al rischio sicurezza, definendo i migliori strumenti di governo delle informazioni, che si traducono in maggiore produttività, crescita aziendale e contenimento dei costi.

Cyber Strategy

Supportiamo l'azienda nell'analisi delle criticità relative alla cybersecurity sviluppando programmi di gestione del rischio coerenti con gli obiettivi strategici e il posizionamento dell'azienda stessa.

Cyber Vigilance

Confrontiamo e analizziamo i dati sulle minacce legate alla cybersecurity aziendale per fornire ai responsabili aziendali del settore gli strumenti idonei ad individuare e gestire proattivamente le minacce informatiche, rispondendo tempestivamente agli incidenti informatici.

Cyber Resilience

Attraverso protocolli e tecnologie proattive aiutiamo i Clienti ad adattarsi e rispondere alle minacce informatiche sia interne che esterne, per gestire al meglio la propria attività durante un Data breach o un cyber attacco.

Vulnerability Assessment and Penetration Testing

Svolgiamo attività di Penetration Testing e Vulnerability Assessment sia manuali che automatizzati utilizzando "sonde" preparate ad hoc con diversi moduli a seconda delle esigenze del cliente.

Supporto successivo nella prevenzione di eventi dannosi quali la perdita e distruzione dei dati, interruzione o alterazione del servizio.



ANALISI FORENSE

- → Raccolta prove digitali
- → Analisi, perizie informatico-giuridiche su siti web, pc, smartphone
- ightarrow Recupero dati da dispositivi

La **Digital Forensics** è una disciplina il cui scopo è quello di identificare, acquisire, preservare, analizzare, documentare e presentare le informazioni contenute nei computer, nei dispositivi mobili (cellulari, smartphone, tablet, ecc.) e nei sistemi informativi in generale.

La Digital Forensics evidenzia prove utili per lo svolgimento di attività investigative e che possano essere ritenute valide in un processo giuridico sia esso civile, penale o del lavoro.

Nella Digital Forensics si combinano, integrandosi, competenze giuridiche e tecnico-informatiche.

DataConSec dispone sia di risorse specializzate negli ambiti afferenti alla disciplina in oggetto che di un avanzato laboratorio informatico certificato.

COMPUTER FORENSICS

L'obiettivo che ci si prefigge utilizzando le numerose tecniche di computer forensics è quello di recuperare, analizzare e conservare informazioni sui sistemi di computer per trovare potenziali prove per un processo.

CORPORATE FORENSICS

Le metodologie tipiche della Computer Forensics si applicano al contesto aziendale.

Lo scopo è individuare eventuali attacchi informatici provenienti dall'esterno, scoprire dipendenti infedeli, attività di spionaggio, furto o danneggiamento dei dati, violazione delle policy aziendali.



WHISTLEBLOWING

Il decreto legislativo n° 24/2023, recentemente pubblicato in Gazzetta Ufficiale, prevede che le aziende adottino specifici protocolli volti a agevolare la segnalazione di possibili illeciti.

→ Servizio di adeguamento alla normativa

Il **whistleblowing** è un termine che viene utilizzato per indicare l'atto di segnalare irregolarità o comportamenti illegali all'interno di un'organizzazione.

Una persona che ha conoscenza di attività illecite o non etiche all'interno dell'azienda in cui lavora o con la quale ha a che fare, può decidere di segnalare attraverso opportuni canali tali comportamenti.

Le segnalazioni possono essere effettuate anche in modo anonimo e rappresentano una forma di tutela per la persona che le attua

La legge mira a incentivare la collaborazione dei lavoratori per favorire l'emersione dei fenomeni corruttivi o altri reati all'interno di enti pubblici e privati. L'introduzione di una disciplina ad hoc sul fenomeno del whistleblowing recepisce normative internazionali ed europee volte a rafforzare l'azione di prevenzione e contrasto di questi fenomeni, anche con la previsione di sistemi informatici che consentono ai lavoratori di segnalare in condizioni di sicurezza gli eventuali reati di cui vengono a conoscenza.

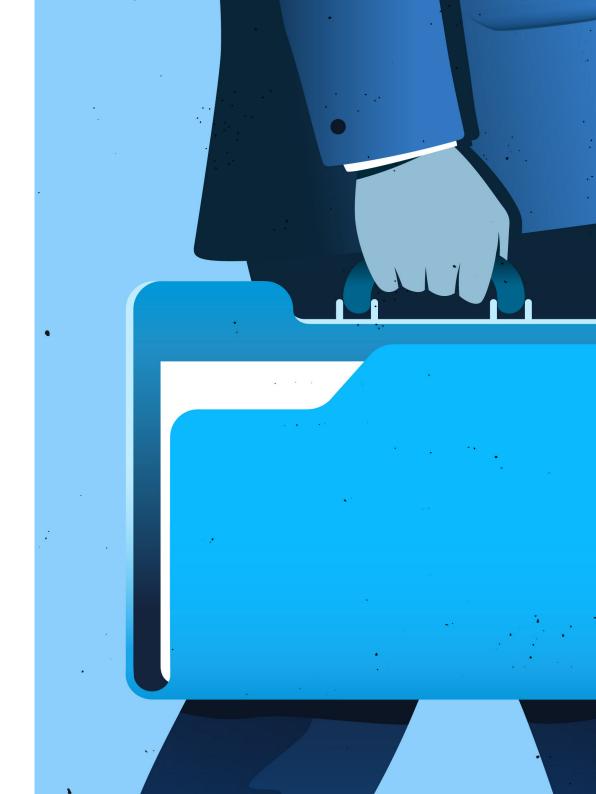
La norma si applicherà:

- ▶ Dal **15 luglio 2023** a tutte le aziende private che hanno impiegato, nell'ultimo anno, una media di lavoratori superiore a **249**.
- ▶ dal **17 dicembre 2023** tutte le aziende private che hanno impiegato, nell'ultimo anno, una media di lavoratori superiore a **50**.

Sono previste sanzioni per le aziende inadempienti: l'ANAC potrà comminare **sanzioni** amministrative pecuniarie di importo variabile dai **10.000 euro** fino ad un massimo di **50.000 euro** in caso mancata implementazione dei canali di segnalazione.

Per la gestione degli adempimenti necessari alla conformità normativa DataConSec offre 3 tipologie di servizi:

- 1. Consulenza tecnologica in merito ai canali informatici sicuri:
- ► Implementazione e configurazione software sia in modalità On-Premise che SaaS;
- ▶ Personalizzazione a seconda del contesto del cliente:
- Manutenzione e supporto;
- ► Formazione.
- 2. Consulenza in merito alla documentazione legale:
- ► Supporto alla direzione e alle funzioni di controllo interno per la definizione di politiche di whistleblowing e procedure interne in linea con il contesto dell'organizzazione;
- Affiancamento alle funzioni interne coinvolte nei processi di whistleblowing per la definizione del contenuto dei moduli di raccolta delle segnalazioni;
- ▶ Supporto legale per gli adempimenti relativi alla protezione dei dati quali per esempio: informative, lettere di autorizzazione e nomine ad hoc, valutazioni di impatto, configurazioni privacy by design e by default;
- ► Formazione.
- **3.** Servizio **"chiavi in mano"** che prevede sia la consulenza tecnologica che quella relativa alla documentazione legale.



CONCEPTLOG SERVIZI GESTITI DI LOG MANAGEMENT

→ Servizio di gestione Log dei profili privilegiati "ConceptLog"

La soluzione di Log Management "ConceptLog" ideato della DataConSec, prevede la raccolta dei log delle utenze amministrative o privilegiate definite all'interno dei sistemi e degli applicativi aziendali.

Il servizio è stato realizzato con l'obiettivo di consentire a tutte le organizzazioni aziendali, di rispondere in maniera semplice, facile e completa all'esigenza di gestire i Log dei profili privilegiati, come imposto dalle raccomandazioni della autorità Garante della Privacy di seguito riportata per completezza di informazione, e aderenti alla normativa vigente in materia di protezione dei dati personali (Regolamento europeo 2016/679 GDPR).

Provvedimento "Amministratori di sistema"
Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008 e modificato in base al provvedimento del 25 giugno 2009).



Il sistema raccoglie un insieme di eventi specifici, conformi ai requisiti normativi e legati ai soli utenti privilegiati (Amministratori di Sistema), indicati dal Cliente ed oggetto del provvedimento.

Il servizio è gestito da DataConSec su infrastruttura cloud collocata in UE e dispone di strumenti di backup opportunamente cifrati al fine di garantire la riservatezza dei dati gestiti dal sistema.

L'archiviazione dei log di accesso degli Amministratori di Sistema (AdS), come da riferimento normativo, prevede un tempo di conservazione non inferiore ai sette mesi.

OPERATORE ECONOMICO AUTORIZZATO

- \rightarrow Esame procedure
- → Pratiche gestionali e documentazione aziendale
- → Audit interno di compliance AEO
- → Redazione analisi dei Rischi
- → Piano Sicurezza documentazione

La consulenza di **DataConSec** prevede l'attivazione di un team di progetto interdisciplinare, del quale faranno parte professionisti di comprovata esperienza e di complementare specializzazione (doganale, organizzazione aziendale e analisi dei rischi, sicurezza fisica, legale, fiscale ed informatica). Il tutto al fine di predisporre la documentazione idonea per la Autorizzazione di status di AEO (questionario di autovalutazione AEO).

L'intero progetto sarà supervisionato, diretto e coordinato dal responsabile di progetto, il quale opererà in accordo con un responsabile designato dall'Organizzazione Cliente.



Per maggiori approfondimenti, visita il sito internet dedicato:

www.consulentiaeo.it

PORTALE FORMAZIONE DATACONSEC ACADEMY

- → Corso sul regolamento GDPR
- → Corso Sicurezza dei Dati Aziendali
- **→ Corso Security Awareness**

DataConSec Academy è la nostra piattaforma e-Learning sulla Cyber Security & Privacy.

Corso privacy GDPR

I dati, le informazioni sono asset aziendali fondamentali, invisibili ma dagli effetti reali, sono un patrimonio che va gestito, valorizzato e difeso.

La privacy, il GDPR, la gestione in sicurezza dei dati aziendali, diventano una necessità indispensabile e da governare in qualsiasi organizzazione.

La formazione è uno strumento indispensabile per un approccio volto a creare una cultura in cui le persone sono parte integrante della strategia di sicurezza aziendale.

Corso sulla Sicurezza delle informazioni aziendali

Il corso presenta in modo chiaro e intuitivo i concetti di base della "Sicurezza delle Informazioni" legata all'uso degli strumenti informatici e delle tecnologie digitali, sia in azienda che a livello personale.

Il corso illustra con semplicità i rischi e le minacce che affrontiamo quotidianamente, fornendo consigli e suggerimenti per poter gestire con consapevolezza e responsabilità le situazioni anomale e gli incidenti di sicurezza.

Corso Security Awareness

Un corso utile a tutti i livelli della struttura Organizzativa aziendale "investire sul fattore umano per promuovere la cultura della cybérsecurity in tutta l'organizzazione".

Gli strumenti informatici presenti nelle strutture operative sono ormai di tipo avanzato, ma l'anello debole resta sempre la persona, che inconsapevolmente, con il suo comportamento, può rendere inefficace qualsiasi corretta procedura di difesa informatica. Non è possibile delegare le misure di sicurezza solamente alla tecnologia, ma il valore della consapevolezza è fondamentale. È per questo che un'efficace protezione dei dati deve necessariamente essere programmata anche attraverso la formazione.



DATA PROTECTION - CONSULTING - SECURITY

DataConSec S.r.l.Business Security & IT Governance

V.le Fratti, 56 - Parma (Italy) Tel. e Fax: +39 0521.771298 e-mail: info@dataconsec.com amministrazione@pec.dataconsec.com www.dataconsec.com

C.F. e P.IVA 02470920345

