

INFORMAZIONI
PERSONALI

Domenico Carnicella

Viale Fratti 56, Parma, Italia

www.dataconsec.com

Sesso M | Nazionalità Italiana

ESPERIENZA
PROFESSIONALE E
COMPETENZE

Compliance & Security manager ICT, Data Protection Officer DPO (EU), Security Manager (tecnologico/legale), laurea magistrale in Giurisprudenza, figura preposta all'individuazione delle soluzioni più idonee per il raggiungimento dei livelli ottimali di sicurezza delle informazioni e della Compliance (tecnico-legale). Garantire la tutela del patrimonio informativo dell'organizzazione, e di assicurare "Business Continuity" intesa come **integrità, disponibilità e riservatezza**. Analizzare i processi di trattamento dati per individuare le procedure più idonee per evitare compromissioni (misure tecnico-organizzative). Effettuare una valutazione dei rischi evidenziando i punti deboli della security aziendale, al fine di raggiungere una ponderazione ed una gestione consapevole del rischio.

Data Protection Officer DPO/RDP (Regolamento privacy EU art. 37): pieni requisiti professionali da Responsabile della protezione dei dati personali, con il compito di informare e consigliare il titolare o il responsabile del trattamento da lui preposto, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento Europeo e dalle altre disposizioni dell'UE o delle normative locali degli Stati membri relative alla protezione dei dati; verificare che la normativa vigente e le policy interne del titolare siano correttamente attuate ed applicate, incluse le attribuzioni delle responsabilità, la sensibilizzazione e la formazione del personale, ed i relativi audit.

Socio fondatore DataConSec Srl www.dataconsec.com

Attestati: <https://www.domenicocarnicella.org/>

Cyber Legal, Policy & Compliance Officer

Consulenza nell'ambito del Risk management informatico-legale e della Compliance per il settore ICT a 360°, Privacy Reg. EU 679/2016 GDPR e "D.lgs. 30 Giugno 2003 n. 196" e Provvedimenti collegati. (rif. Standards **ISO/IEC 29100 - 27701**). Integrazione ed armonizzazione fra i Sistemi di gestione nelle organizzazioni. **Consulente senior sistemi di gestione ISO 27001 (SGSI) ISO 20000 22301 31000 25999 9001, Compliance NIS 2**

- Responsabile della protezione dei dati (RPD)
- Responsabile della tutela della privacy
- Consulente in diritto informatico
- Consulente legale informatico
- Responsabile della governance delle informazioni
- Responsabile della conformità dei dati
- Consulente conformità NIS 2 (ACN)
- Responsabile legale per la sicurezza informatica
- Responsabile IT/ICT Compliance
- Consulente Governance Risk Compliance (GRC).

Ispettore accreditato ISO 27001, di un primario ente di certificazione italiano.

Internal Auditor — ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems. AFNOR Italia febb. 2023

Consulente per l'adeguamento alla direttiva NIS, professionista specializzato nell'aiutare le organizzazioni a conformarsi ai requisiti della direttiva europea NIS 2, relativa alla sicurezza delle reti e dei sistemi informativi. Attività di valutazione della sicurezza attuale, l'identificazione delle aree di miglioramento, l'elaborazione di strategie di adeguamento e il supporto nell'implementazione delle misure necessarie. Accompagna le organizzazioni nel percorso di adeguamento alla direttiva, fornendo competenze tecniche, gestionali e relazionali per garantire la sicurezza dei sistemi

informativi e il rispetto delle normative.

Responsabile della conservazione Agid. Esperto di conservazione digitale per progettazione ed implementazione di requisiti del livello più elevato, in termini di qualità e sicurezza, manuale della conservazione. Competente nell' adottare adeguate misure di protezione dei documenti idonee a garantire la riservatezza, l'autenticità, l'immodificabilità, l'integrità e la fruibilità dei documenti informatici oggetto di conservazione (protocolli accreditamento per i conservatori di cui all'art. 44-bis del CAD agg. 2022)

Organismo di Vigilanza (OdV) e Consulente certificato per l'implementazione di Modelli ex D.I. 231/01 resp. amm.degli enti.

Formazione compliance e governance a 360° sulla consapevolezza delle risorse umane.

Consulente e formatore per Sistema di gestione **Status A.E.O. Dogane** (Authorized Economic Operator).

Maggio 2019– Oggi

Capogruppo comparto ICT (UNICT) consulta informatica UPI Confindustria Parma
Membro **dal 2014** e **Coordinatore Consulta (2019)** settore ICT - **UNICT** - **Vice presidente di SMILE-DIH**. Organizzazione seminari tecnici di approfondimento sul territorio, per informare e formare le aziende associate all'Unione Parmense degli Industriali sulle tematiche di Innovazione e Fabbrica 4.0. Attività di relazione con Confindustrie di altri territori.

Da Gennaio 2012 ad oggi

Sicurezza informatica e Privacy UPI Confindustria PR
Esperto Sicurezza e Privacy di **Unione Parmense Degli Industriali e FIASA PR**.
Referente Privacy e Sicurezza, AEO (dogane), in convenzione dell'Unione Parmense degli Industriali (UPI-GIA, Confindustria):.

FORMAZIONE CENNI

Novembre 2021

Titolo: Le procedure di investigazione finalizzate alla rimozione di contenuti digitali
Criminalità Informatica e Investigazioni Digitali **Università degli studi di Milano UNIMI**

Perfezionamento online in Criminalità Informatica e Investigazioni Digitali, coordinato dal Prof. Giovanni Ziccardi e Pierluigi Perri. Obiettivo del corso: formare esperti in informatica giuridica, in diritto delle nuove tecnologie, in criminalità informatica e investigazioni digitali, con un particolare focus sulle procedure di investigazione finalizzate alla rimozione di contenuti digitali.

Marzo 2021

Titolo: Corso Innovation management – come gestire l'innovazione nell'impresa del futuro

Norme serie Iso 56000 e competenze dell'innovation manager e del chief innovation officer
Autorità emittente CERTIFICATION S.R.L. 18-22-24 FEBBRAIO e 2 MARZO 2021 (16 ore)

Obiettivo del Corso:

Facilitare ed Accelerare l'innovazione: aiutare a generare nuove idee di business, introducendo approcci di lean business, start up, allo sviluppo di nuovi prodotti e servizi.

Potenziare le conoscenze e competenze di Innovation Manager e Chief Innovation Officer

Coltivare la Leadership creativa: facilitare gli imprenditori naturali e gli innovatori nei team interni, fornendo strumenti e strutture che possono diventare catalizzatori per la trasformazione sociale.

Mantenere e sviluppare talento e intraprendenza: sviluppare e mantenere un ambiente di lavoro creativo e innovativo per aumentare la cultura del rischio e della collaborazione in team multidisciplinare e multiculturale.

Maggio Giugno 2019

Titolo: Corso di Perfezionamento in Data Protection e Data Governance
Prepararsi a ispezioni, controlli, verifiche, sanzioni e responsabilità
Settore didattico di Giurisprudenza dell'**Università degli Studi di Milano**
Dipartimento scienze giuridiche "Cesare Beccaria"
Coordinatore: prof. Avv. Pierluigi Perri

Obiettivo del Corso:

Il tema del Corso di Perfezionamento, suddiviso in lezioni teoriche e laboratori pratici, è dedicato all'analisi dei profili di responsabilità, delle modalità ispettive, delle sanzioni, del ruolo essenziale del Data Protection Officer nell'adeguamento e nelle verifiche e a una costante attenzione ai diritti degli interessati. Particolare attenzione inoltre al quadro sanzionatorio negli altri Paesi europei, alla coerenza delle sanzioni irrogate, alla "modularità" dei profili di responsabilità.

- Aprile 2018** **Titolo: Registro dei trattamenti, analisi del rischio. Privacy Impact Assessment (PIA): la valutazione d'impatto sulla protezione dei dati con il Regolamento UE 2016/679 8 ore TÜV Italia Akademie**
- Registro dei trattamenti: strumento indispensabile alla analisi dei rischi
 - Il concetto di rischio nell'ambito della Privacy: le famiglie di rischi
 - Analisi dei rischi e Privacy Impact Assessment (PIA): differenze e punti in comune
 - L'individuazione dei rischi privacy e degli eventi connessi: tecniche e metodologie
 - Approfondimento sulle tipologie di rischi richiamate dal Regolamento Europeo sulla protezione dei dati 2016/679
 - Le misure di mitigazione dei rischi privacy
 - Approfondimento su specifiche aree sensibili (HR, IT, Marketing, ecc.)
 - Definizione e messa in pratica di misure di mitigazione dei rischi
 - La consultazione preliminare
 - Formazione, controllo ed audit sulle misure di mitigazione dei rischi
 - La valenza dinamica della analisi dei rischi e della PIA
 - Documentazione delle analisi dei rischi e della PIA
 - I controlli e gli audit sulla analisi dei rischi e della PIA
 - Esame finale
- Luglio 2014** **Certificazione Auditor/Esperto 231 di Modelli di Organizzazione e Gestione D.Lgs. N. 231/2001 e Membri Organismi di Vigilanza**
- Fornire ai partecipanti gli elementi per una ottimale progettazione ed adozione di un MOG;
 - Erogare l'addestramento specialistico sulle verifiche ispettive tese a valutare la conformità e l'efficacia di un MOG;
 - Fornire elementi di comportamento e migliorare le tecniche di raccolta delle evidenze oggettive e loro valutazione nelle diverse fasi di audit;
 - Presentare i risultati delle verifiche ispettive agli Organismi di Vigilanza e/o alle Direzioni aziendali.
- Fornire gli elementi di formazione necessari per l'accesso al registro AICQ SICEV Per RGVI/Auditor (Schema "RMO 231").
- Marzo 2014** **Certiquality S.r.l: "La nuova ISO/IEC 27001:2013 ed elementi di risk management"**
- Febbraio 2014** **Certiquality S.r.l: Partecipazione corso "Il Risk Management e la norma ISO 31000"**
- Dicembre 2012** **Partecipazione corso "Privacy e tutela dei dati personali alla luce delle recenti novità normative e regolamentari" Paradigma S.r.l**
- Aggiornamento su tutta la Compliance privacy: 40 h in aula, con i maggiori esperti in Italia del settore

Febbraio 2012 **Lead Auditor di sistemi di gestione per la qualità (ISO 9001 e ISO 19011) Certificazione**

Attestato n. 1473

- Stabilire un punto di partenza per l'implementazione di un Sistema di Gestione per la Qualità e un'opportunità per il miglioramento delle prestazioni della qualità;
- Controllare e valutare i progressi nello sviluppo della qualità, stabilendo l'efficacia e l'efficienza del Sistema di Gestione della Qualità attuato;
- Accertare l'adeguatezza del sistema in riferimento allo standard ISO 9001, per la eventuale certificazione (audit di "terza parte" condotto da un Organismo di certificazione accreditato)
- Fornire un controllo interno ufficiale per verificare che i sistemi continuino ad operare e confermino la loro idoneità ed efficacia (audit di prima parte o Verifica Ispettiva Interna condotta da personale interno e indipendente dalle funzioni oggetto di verifica così come previsto dai requisiti della ISO 9001)
- Valutare un fornitore esistente o potenziale relativamente alla sua capacità di fornire merci e/o servizi di qualità adeguata (in questo caso si parla di audit di seconda parte).Principi e terminologia della gestione della business continuity.

Giugno 2011 **Business Continuity Management System Auditor/Lead Auditor Training Course BS 25999:2007 (ISO 22301) Certificazione**

British Standard Institute Licenza N° IT/BCM0402011006

- Garantire la continuità operativa
- gestione della business continuity (BCM da un ampio gruppo di esperti mondali, in rappresentanza dei principali
- Settori industriali e della pubblica amministrazione
- Principi e terminologia della gestione della business continuity.

Novembre 2005 **Certificazione Lead Auditor ISO 27001:2005 (ex BS 7799-2:2002) BSI Italia**

Certificato numero 00301

- Esperto di Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI) secondo la norma ISO/IEC 27001:2005, Lead Auditor (BSI Cert. n° 00301).
- Servizio di consulenza completo in materia di Privacy e Security
- Consulting per le fasi di impostazione implementazione e mantenimento della Certificazione del Sistema di Gestione di Sicurezza delle Informazioni
- expertise , grazie all'expertise maturata da Aditor interno attraverso tutte le fasi del processo richiesto dallo standard ISO:IEC/27001:2005

Laurea in Giurisprudenza (magistrale)

Università degli Studi di Parma. Anno accademico 1992 Pratica professione (Patrocinatore legale)

MATURITA' : Liceo Classico

Competenze tecnico-organizzative e gestionali 360°

- Garantire la conformità e fornire consulenza tecnico-legale e orientamento sulla Sicurezza e la privacy dei dati e standard, leggi e regolamenti sulla protezione dei dati.
- Identificare e documentare le lacune di conformità
- Condurre valutazione dell'impatto sulla privacy e sviluppare, mantenere, comunicare e formare sulle politiche sulla privacy, procedure
- Applicare e sostenere il programma di privacy e protezione dei dati dell'organizzazione
- Garantire che i proprietari dei dati, i titolari, i responsabili del trattamento, gli incaricati del trattamento, i soggetti, interni o i partner e le entità esterne sono informati sui loro diritti di protezione dei dati, obblighi e responsabilità

- Agire come punto di contatto chiave per gestire richieste e reclami relativi ai dati in lavorazione
- Assistere nella progettazione, implementazione, verifica e attività di test di conformità in ordine per garantire la sicurezza informatica e la conformità alla privacy
- Monitorare gli audit e le attività di formazione relative alla protezione dei dati
- Cooperare e condividere informazioni con autorità e gruppi professionali
- Contribuire allo sviluppo della strategia e della politica di sicurezza informatica dell'organizzazione e procedure
- Sviluppare e proporre formazione di sensibilizzazione del personale per raggiungere la conformità e promuovere a cultura della protezione dei dati all'interno dell'organizzazione
- Gestire gli aspetti legali delle responsabilità di sicurezza delle informazioni e le relazioni con terze parti

Competenze chiave

- Comprensione completa della strategia aziendale, dei modelli e dei prodotti e capacità di tenere conto dei requisiti legali, normativi e degli standard
- Eseguire pratiche della vita lavorativa relative alla protezione dei dati e alle questioni di privacy coinvolte l'implementazione dei processi organizzativi, finanziari e della strategia aziendale
- Guidare lo sviluppo di adeguate politiche di sicurezza informatica e privacy e procedure che integrano le esigenze aziendali e i requisiti legali; ulteriore assicurare l'accettazione, la comprensione e l'attuazione e comunicarlo tra le parti coinvolte
- Condurre, monitorare e rivedere le valutazioni dell'impatto sulla privacy utilizzando standard, framework, metodologie e strumenti riconosciuti
- Spiegare e comunicare gli argomenti relativi alla protezione dei dati e alla privacy alle parti interessate e utenti
- Comprendere, mettere in pratica e rispettare i requisiti e gli standard etici
- Comprendere le implicazioni delle modifiche del quadro giuridico per l'organizzazione strategie e politiche di sicurezza informatica e protezione dei dati
- Collaborare con altri membri del team e colleghi