Informazioni personali

Cognome / Nome	**Sferlazza Paolo**
Indirizzo	
Cellulare	
E-mail	
Cittadinanza	
Data di nascita	

Esperienza professionale

Date	Ottobre 2018 – ad oggi
Datore di lavoro	Co-founder of GERICO Security (GEstione RIschi e COntinuità Operativa)
Lavoro o posizione ricoperti	Independent Advisor, Auditor and Trainer
Principali attività e responsabilità	- Attività di progettazione, sviluppo, prevendita ed erogazione di servizi di consulenza in ambito Information Security e IT Governance - Attività consulenziali per l'implementazione e la certificazione di Sistemi di Gestione per: • Sicurezza delle Informazioni (ISO/IEC 27001) • Continuità Operativa (ISO 22301) • Gestione dei Servizi IT (ISO/IEC 20000) • Qualità (ISO 9001) - Gap analysis e attività consulenziali per la conformità allo standard PCI DSS - Audit di parte prima e seconda su sistemi informativi e di terza parte per certificazione PCI DSS - Supporto consulenziale rispetto ai provvedimenti del Garante della Privacy
Date	Maggio 2016 – ad oggi
Datore di lavoro	CSQA Certificazioni (Contractor)
Lavoro o posizione ricoperti	Auditor e Trainer
Principali attività e responsabilità	- Auditor di terza parte sugli schemi ISO/IEC 27001, ISO 22301 e ISO/IEC 20000 - Trainer accreditato People Cert per corsi ITIL Foundation - Trainer per corsi accreditati AICQ – SICEV per Lead Auditor ISO/IEC 27001 e ISO 22301
Date	Ottobre 2018 – ad oggi
Datore di lavoro	Bureau Veritas (Contractor)
Lavoro o posizione ricoperti	Auditor e Trainer
Principali attività e responsabilità	- Auditor di terza parte sugli schemi ISO/IEC 27001, ISO 22301 e ISO/IEC 20000 - Sviluppo ed erogazione dei corsi ISO/IEC 27001 (corso accreditato da CEPAS a novembre 2018) e ISO 22301 - Trainer per corsi accreditati per Lead Auditor ISO/IEC 27001, ISO/IEC 20000 e ISO 22301

Date	Marzo 2010 – Settembre 2018
Datore di lavoro	@Mediaservice.net S.r.l.
Lavoro o posizione ricoperti	Responsabile della Business Unit di Sicurezza delle Informazioni Senior Security Advisor
Principali attività e responsabilità	- Attività di progettazione, sviluppo, prevendita ed erogazione di servizi di consulenza in ambito Information Security e IT Governance - Deputy management presso importante azienda italiana nel coordinamento del team di Information Security e Business Continuity - Attività consulenziali come Project Manager per l'implementazione e la certificazione di Sistemi di Gestione per la Sicurezza delle Informazioni (ISO/IEC 27001) e la Continuità Operativa (ISO 22301) di una infrastruttura critica italiana e di PMI. - Gap analysis e attività consulenziali per la conformità allo standard PCI DSS presso importanti realtà del mercato italiano - Attività di audit per la certificazione di sistemi di pagamento conformi allo standard PCI DSS. - Definizione di policy e procedure, secondo quanto disposto delle normative ISO/IEC 27001, ISO/IEC 20000, ISO 22301 e dallo standard PCI DSS - Responsabile della realizzazione e della gestione del sistema di gestione integrato aziendale ISO 9001 e ISO/IEC 27001 - Sviluppo e implementazione di metodologie di Information Risk Management - Audit di parte prima e seconda su sistemi informativi e di terza parte per certificazione PCI DSS - Studio e verifica delle compliance rispetto ai provvedimenti del Garante della Privacy, in particolare: • Regolamento Europeo sulla Privacy (GDPR) • Dlgs 196/2003 • Amministratori di sistema • Data retention - Supporto professionale ad un Security Manager di un'importante realtà italiana per la gestione dell'IT Governance Aziendale - Definizione di Business Impact Analysis e Business Continuity Plan per PMI - Docenza in ambito Information Security e ITIL - Vulnerability Assessment di reti e di applicazioni web L'attività di consulenza ha permesso di venire a contatto con il management delle più importanti realtà del mercato italiano
Date	2006 - 2009
Lavoro o posizione ricoperti	- Assistente presso la facoltà di scienze MFN
Principali attività e responsabilità	- Assistenza alla didattica nel corso di programmazione e laboratorio - Collaboratore presso la biblioteca dipartimentale - Dipartimento di Informatica (Torino)
Nome e indirizzo del datore di lavoro	Facoltà di scienze MFN
Date	2005 - 2006
Lavoro o posizione ricoperti	Consulente informatico
Principali attività e responsabilità	- Corsi al personale docente per l'utilizzo di sistemi informatici - Gestione e manutenzione di un laboratorio Linux-Windows. - Aggiornamento del sito dell'Istituto e stesura del documento programmatico per la sicurezza (DPS).
Nome e indirizzo del datore di lavoro	Liceo Scientifico Statale Giordano Bruno

Istruzione e formazione

Date	02/10/2015 - 11/10/2015
Nome del corso	Certificazione BCI
Titolo della qualifica rilasciata	Certificazione del Business Continuity Institute (CBCI)
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione	Panta Ray
Date	03/11/2014 - 04/11/2014
Nome del corso	PCI QSA
Titolo della qualifica rilasciata	Payment Card Industry Qualied Security Assessor
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione	PCI SSC
Date	12/02/2014 - 14/02/2014
Nome del corso	Cobit 5
Titolo della qualifica rilasciata	Cobit 5 Foundation
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione	Apmg International
Date	22/01/2014
Nome del corso	La nuova ISO/IEC 27001:2013
Titolo della qualifica rilasciata	Qualifica come Auditor / Lead Auditor sullo schema ISO/IEC 27001:2013
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione	CSQA Certificazioni S.r.l.
Date	06/05/2013 - 08/05/2013
Titolo della qualifica rilasciata	Qualifica di Auditor/Lead Auditor a norma ISO/IEC 22301:12 in merito ai Sistemi di Gestione per la Continuità Operativa, rilasciata dall'ente di accreditamento internazionale RICEC
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione	PDCA S.r.l.
Date	24/10/2012 - 26/07/2012
Nome del corso	Quality Assessor
Principali tematiche/competenza professionali acquisite	Conoscenza e comprensione delle norme UNI CEI EN ISO/IEC serie 17000, UNI CEI ISO/IEC 17025, UNI EN ISO 9001:2008, UNI EN ISO 19011:2011 e delle metodologie e del processo di audit dei Sistemi di Gestione per la Qualità al fine di acquisire la qualifica di LEAD Auditor ISO 9001
Titolo della qualifica	Qualifica di Auditor/Lead Auditor a norma ISO/IEC 9001:2008 rilasciata dall'ente di accreditamento CEPAS
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione	DNV Italia
Date	05/07/2012 - 06/07/2012
Nome del corso	Tecniche per auditing: ISO/IEC 19011:2012
Titolo della qualifica rilasciata	Certificato di superamento del corso riconosciuto da CEPAS
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione	DNV Italia
Date	02/01/2012 - 06/01/2012
Titolo della qualifica rilasciata	OSSTMM Professional Security Tester
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione	ISECOM - Institute for Security and Open Methodologies

Date	26/05/2011 - 11/06/2011
Titolo della qualifica rilasciata	Qualifica di Auditor/Lead Auditor a norma ISO/IEC 27001:05 rilasciata dall'ente di accreditamento internazionale RICEC
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione	Università degli studi di Roma – La Sapienza Master in Governance e audit dei Sistemi Informativi
Date	2007 - 2009
Titolo della qualifica rilasciata	Laurea magistrale in metodologie e sistemi Informatici, con la votazione di 110 su 110. Titolo della tesi :"*Valutazione della sicurezza in sistemi informativi: tools e normative*"
Principali tematiche/competenza professionali acquisite	Il percorso di studi universitari ha fornito una conoscenza completa sugli aspetti principali legati all'ICT. Visto l'interesse personale, sono stati approfonditi molti aspetti legati all'Information security. Una particolare attenzione, durante gli anni accademici, è stata dedicata all'analisi dei più comuni strumenti per lo sviluppo di applicazioni web, quali php, java e J2EE.
Date	2004 - 2007
Titolo della qualifica rilasciata	Laurea triennale in informatica, con la votazione di 104 su 110 Titolo della tesi : "*L'identità nel Web 2.0 : sperimentazione e sviluppo di OpenID*"
Nome e tipo d'organizzazione erogatrice dell'istruzione e formazione	Università degli studi di Torino (Facoltà di Scienze Matematiche e Fisiche - Dipartimento di informatica)

Pubblicazioni e qualifiche

Pubblicazioni

- Monitoraggio dei controlli di security nell'IT – Maggio 2015
- Sistemi di gestione: affinita' e divergenze. E' davvero tutto finalizzato solo ad ottenere un certificato? – Settembre 2014
- Le frodi nella Rete – Il duplice ruolo dell'ICT – Coautore
- PCI Community meeting e PCI DSS 3.0 – Novembre 2013
- PCI DSS: requisiti documentali e attività periodiche – Settembre 2013
- *Dall'audit di processo al penetration test con BackTrack*, Linux Pro – Settembre 2011
- *Dati nell'aria – Tutto ciò che bisogna sapere per craccare una rete wireless*, Linux Pro – Novembre 2011
- *Web App in pericolo* - Linux Pro – Gennaio 2012

Interventi effettuati

- Lo standard ISO 22301 e il processo di certificazione di un Sistema di Gestione di Continuità Operativa - AITI Associazione Industrie Ticinesi (giugno 2018)
- "Come raggiungere la conformità PCI DSS semplificandosi la vita"– Security Summit Maggio 2017 (Roma)
- "Sistemi di Gestione, ne vale davvero la pena – l'esperienza di Snam Rete Gas"– Security Summit Marzo 2015 (Milano)
- "Tanta fatica solo per un bollino...ne vale davvero la pena?" - Security Summit Giugno 2014 (Roma)
- "I sette vizi capitali della PCI DSS" - Security Summit Giugno 2013 (Roma)

Certificazioni e qualifiche	PCI QSA - Qualified Security Assessor (certificate N° 203-599) CRISC - Certified in Risk and Information Systems Control (certificate N° 13108262) CISM - Certified Information Security Manager (certificate N° 1736539) CISA - Certified Information Systems Auditor (certificate N° 13108262) SAFEINFO Auditor (Responsabile dei Gruppi di Verifica - RGVI) (certificate N° 022 AICQ - SICEV) Auditor/Lead auditor ISO/IEC 27001:2005 (certificate N° 0315 /S) Aggiornamento qualifica Auditor/Lead auditor ISO/IEC 27001:2013 CBCI – Certificate Business Continuity Institute Business Continuity Auditor (certificate N° 005 AICQ - SICEV) Auditor/Lead auditor ISO/IEC 22301:2012 OPST – OSSTMM Professional Security Tester COBIT 5 Foundation ITIL v3 Foundation Auditor/Lead auditor ISO/IEC 20000-1:2012 IT Service Management according to ISO/IEC 20000 Auditor/Lead auditor ISO 9001:2015 ISFS – Information Security Based on ISO/IEC 27002 ISMAS - Information Security Management Advanced based on ISO/IEC 27002 Auditor/Lead PDR 43:2 - Requisiti per la protezione e valutazione di conformità dei dati personali in ambito ICT
Trainer	Docente presso il Mater di CyberSecurity e BlockChain presso il COREP (marzo 2019) – Gli standard ISO/IEC 27001 e ISO 22301 Docente qualificato per l'erogazione di corsi Lead Auditor sugli schemi ISO 27001, 22301 e 20000 Trainer qualificato People Cert per l'erogazione di corsi ITIL Foundation Creazione ed erogazione di corsi formativi di: - ITIL Foundation v.3 – corso finalizzato a preparare l'esame di certificazione ITIL Foundation - Information Risk Risk Management - ISO/IEC 27001:2005 e ISO/IEC 27001:2013 - ISO 22301 - ISO 20000 - PCI DSS
Associazioni	UNINFO: - Membro del comitato SC27 per l'ISO/IEC JTC1/SC27 (Gennaio 2013 – Dicembre 2018) - Membro del consiglio direttivo (Gennaio 2013 – Ottobre 2015) Oracle Community for Security: - Membro e contributor dei gruppi di lavoro della Community - Coautore del Libro: "Le frodi nella rete – il duplice ruolo dell'ICT"
Audit	- Attività di audit di prima e seconda secondo parte secondo gli schemi ISO/IEC 27001 e ISO 22301 per i Clienti supportati nei percorsi di certificazione - Attività di audit di terza parte per società di certificazione italiane accreditata da Accredia sugli schemi ISO/IEC 27001, ISO 22301, ISO/IEC 20000 e ISO 9001.

Capacità e competenze personali

Madrelingua(e) **Italiano**

Altra(e) lingua(e)	Comprensione				Parlato				Scritto	
Livello europeo (*)	Ascolto		Lettura		Interazione orale		Produzione orale			
Inglese	B1		B2		B1		B1		B1	

(*) Quadro comune europeo di riferimento per le lingue

Capacità e competenze organizzative

Conoscenza dei principi generali di Project Management, acquisita attraverso lo studio delle più note metodologie (Prince2 e ISIPM) e tramite l'attività lavorativa nella gestione dei progetti come PM.

Esperienza nel campo dell'educazione come coordinatore di centri estivi e campi scuola.

Altre capacità e competenze

Ottime capacità relazionali e di lavoro in gruppo

Patente

B