CURRICULUM VITAE

INFORMAZIONI PERSONALI

Nome	**FOLCHI MAURO**
Anno di Nascita	**1979**
Incarico Attuale	**Responsabile U.O. Strategia Digitale e Cybersecurity**

ESPERIENZA LAVORATIVA

• Date (da – a)	Da agosto 2016 e attualmente in corso
• Datore di lavoro	Equitalia Giustizia S.r.l.
• Tipo di azienda o settore	Società a totale partecipazione pubblica
• Tipo di impiego	Contratto a tempo indeterminato

• Principali mansioni e responsabilità

Da gennaio 2026 e attualmente in corso

Responsabile U.O. Strategia Digitale e Cybersecurity

- Definire le politiche e le linee guida di sicurezza informatica.
- Condurre l'analisi dei rischi IT e coordinare le azioni di mitigazione.
- Presidiare le evoluzioni normative IT e guidare gli adeguamenti necessari.
- Supportare le strutture nella valutazione e trattamento dei rischi di sicurezza.
- Assicurare la data governance del patrimonio informativo aziendale.

U.O. Governance ICT e Business Solution (da luglio 2024 a gennaio 2026)

- Referente Cybersecurity (da febbraio 2025).
- Punto di contatto ACN (da febbraio 2025).
- Supportare la definizione della strategia digitale e dei programmi di transizione digitale.
- Raccogliere i fabbisogni IT contribuendo alla definizione del portafoglio progetti.
- Gestire i rapporti tecnico-operativi con i fornitori IT e presidiare i contratti.
- Collaborare alla predisposizione di analisi funzionali e requisiti tecnici per nuovi sviluppi IT.
- Supportare i progetti IT e i relativi collaudi, interfacciandosi con le strutture utenti.
- Contribuire alla sicurezza informatica e al rispetto delle normative IT.

.

U.O. Governance Demand e Delivery IT (da ottobre 2022 a luglio 2024)

- Gestire i rapporti con il partner tecnologico e con i fornitori IT.
- Presidiare i contratti IT e monitorare avanzamento, qualità e scostamenti dei piani operativi.
- Coordinare progetti IT, inclusa analisi funzionale, definizione requisiti e collaudi.
- Monitorare rischi informatici e assicurare l'adozione delle misure di sicurezza.
- Analizzare evoluzioni normative IT e coordinare gli adeguamenti necessari.
- Curare lo sviluppo delle applicazioni e supportare gli utenti nei test e nei rilasci.
- Contribuire alla gestione documentale e ai modelli di conservazione digitale.

U.O. ICT e Programmazione Operativa (da giugno 2018 a ottobre 2022)

- Rilevare la domanda e contribuire alla definizione del budget IT.
- Gestire il programma di sviluppo informatico per nuovi sistemi e manutenzioni evolutive.
- Condurre progetti IT, dalle analisi funzionali al collaudo delle soluzioni.
- Monitorare rischi informatici, sicurezza e conformità normativa.
- Coordinare gli outsourcer IT e la qualità dei servizi informatici erogati.
- Supportare la formazione utenti in occasione di nuovi rilasci o soluzioni IT.
- Curare la programmazione operativa IT, monitorando piani, avanzamenti e scostamenti.

Funzione Pianificazione e Sistemi Informativi (da agosto 2016 a giugno 2018)

- Raccogliere e analizzare le esigenze IT.
- Contribuire alla pianificazione del budget IT.
- Gestire o supportare i progetti di sviluppo informatico, dalle analisi funzionali al collaudo.
- Monitorare la qualità dei servizi IT erogati, anche in collaborazione con outsourcer.
- Presidiare i rischi informatici e le evoluzioni normative (privacy, sicurezza, standard tecnici).

• Date (da – a)	Da ottobre 2013 a luglio 2016
• Datore di lavoro	Sage S.r.l.
• Tipo di azienda o settore	Settore Sanitario
• Tipo di impiego	Contratto a tempo indeterminato
• Principali mansioni e responsabilità	▪ Supporto metodologico e operativo per la sicurezza informatica. ▪ Gestione delle attività di progettazione e sviluppo IT. ▪ Gestione di abilitazioni/profilazioni del personale. ▪ Amministrazione, gestione e diagnostica apparati rete aziendale (routing & switching). ▪ Amministrazione, gestione e diagnostica firewall. ▪ Amministrazione gestione, configurazione e diagnostica di server e postazioni di lavoro. ▪ Formazione, informazione e addestramento ambito IT. ▪ Gestione delle relazioni con i fornitori esterni e presidio dei relativi contratti.
• Date (da – a)	Da giugno 2009 ad agosto 2012
• Datore di lavoro	Gieffe Servizi S.r.l.
• Tipo di azienda o settore	Settore Commercio
• Tipo di impiego	Contratto a tempo indeterminato
• Principali mansioni e responsabilità	▪ Responsabile SGQ ISO 9001. ▪ Partecipazione ad audit periodici ISO 9001. ▪ Supporto metodologico e operativo per la sicurezza informatica.. ▪ Gestione dell'abilitazione/profilazione del personale. ▪ Amministrazione, gestione e diagnostica apparati rete aziendale (routing & switching). ▪ Amministrazione, gestione e diagnostica firewall. ▪ Amministrazione gestione, configurazione e diagnostica di server e postazioni di lavoro. ▪ Formazione, informazione e addestramento ambito IT. ▪ Gestione delle relazioni con i fornitori IT esterni e presidio dei relativi contratti.
• Date (da – a)	Dal 2007 al 2009
• Datore di lavoro	Villa Serena S.r.l.
• Tipo di azienda o settore	Settore Sanitario
• Tipo di impiego	Contratti di collaborazione
• Principali mansioni e responsabilità	▪ Pianificazione delle verifiche periodiche del Sistema Qualità (SGQ). ▪ Monitoraggio del SGQ. ▪ Organizzazione di gruppi multidisciplinari partecipanti alle verifiche ispettive per il SGQ. ▪ Implementazione di prototipi e applicativi a supporto del sistema informativo. ▪ Elaborazione di rapporti periodici per i Vertici. ▪ Installazione, configurazione e diagnostica della rete aziendale. ▪ Installazione, configurazione e diagnostica server e postazioni di lavoro.

ISTRUZIONE E FORMAZIONE

• Date (da – a)	Aprile 2025
• Nome e tipo di istituto di istruzione o formazione	Google Cloud Cybersecurity Certificate – GOOGLE CLOUD
• Principali materie / abilità professionali oggetto dello studio	Cloud security, IAM, monitoring, firewall, VPN, compliance, uso di Linux, SQL, analisi log e traffico di rete, SIEM, analisi e mitigazione degli attacchi, framework NIST, CIS, SOC, gestione del rischio cloud.
• Qualifica conseguita	Certificato
• Livello nella classificazione nazionale (se pertinente)	
• Date (da – a)	Luglio 2024
• Nome e tipo di istituto di istruzione o formazione	Cisco Certificate in Ethical Hacking – CISCO
• Principali materie / abilità professionali oggetto dello studio	Ricognizione e OSINT, network scanning, enumeration, vulnerability assesment, penetration testing ed exploitation, scripting per l'automazione, analisi del codice e sicurezza applicativa.
• Qualifica conseguita	Certificato
• Livello nella classificazione	

nazionale (se pertinente)	
• Date (da – a)	Gennaio 2024
• Nome e tipo di istituto di istruzione o formazione	Auditor SGSI - Norma ISO/IEC 27001 – WEL
• Principali materie / abilità professionali oggetto dello studio	Norma ISO/IEC 27001:2017, valutazione delle performance, workflow di implementazione del SGSI, tecniche di Audit UNI EN ISO 19011:2018.
• Qualifica conseguita	Attestato di qualifica professionale
• Date (da – a)	Novembre 2023
• Nome e tipo di istituto di istruzione o formazione	Master in Cybersecurity e Data Protection - 24ORE BUSINESS SCHOOL
• Principali materie / abilità professionali oggetto dello studio	Risk Management, gestione dell'incidente informatico, principali tecniche d'attacco nelle aziende, gestione della sicurezza aziendale e misure di protezione, digital forensics, GDPR, Direttiva NIS.
• Qualifica conseguita	Attestato
• Date (da – a)	Novembre 2023
• Nome e tipo di istituto di istruzione o formazione	Certificato IBM Cybersecurity Analyst Professional - IBM SKILLS NETWORK
• Principali materie / abilità professionali oggetto dello studio	Incident response, penetration testing, threat intelligence, vulnerability scanning.
• Qualifica conseguita	Certificato
• Livello nella classificazione nazionale (se pertinente)	
• Date (da – a)	Febbraio 2023
• Nome e tipo di istituto di istruzione o formazione	Certificazione in Cybersecurity (CC) - ISC2 International Information System Security Certification Consortium
• Principali materie / abilità professionali oggetto dello studio	▪ Attesta la capacità di definire e applicare la governance della sicurezza delle informazioni e il framework di gestione dei rischi ▪ Attesta la capacità di assistere la pianificazione strategica nella valutazione e nell'esecuzione operativa di tutte le strategie, politiche e procedure di sicurezza informatica. ▪ Attesta la capacità di stabilire e mantenere un programma completo di cybersicurezza.
• Qualifica conseguita	Certificazione
• Date (da – a)	Aprile 2013
• Nome e tipo di istituto di istruzione o formazione	Certificazione CCNA - CISCO
• Principali materie / abilità professionali oggetto dello studio	▪ Attesta la capacità di comprendere e configurare le basi del networking (OSI/TCP-IP, IPv4/IPv6, subnetting). ▪ Attesta la capacità di configurare e gestire switch e reti LAN (VLAN, trunking, STP, EtherChannel). ▪ Attesta la capacità di configurare routing di base e diagnosticare problemi di connettività. ▪ Attesta la capacità di implementare servizi di rete (DHCP, NAT) e misure di sicurezza (ACL, SSH, port security). ▪ Attesta la conoscenza di concetti di automazione e programmabilità di rete.
• Qualifica conseguita	
• Livello nella classificazione nazionale (se pertinente)	Certificazione
• Date (da – a)	Dal marzo 2005 a ottobre 2006
• Nome e tipo di istituto di istruzione o formazione	Master II Livello in Management e Innovazione Aziende Sanitarie (MIAS) Università "La Sapienza" di Roma

• Principali materie / abilità professionali oggetto dello studio	Acquisizione di conoscenze informatiche, economiche, giuridiche, etiche, manageriali per comprendere e gestire efficacemente risorse e processi organizzativi con particolare riferimento al settore sanitario
• Qualifica conseguita • Livello nella classificazione nazionale (se pertinente)	Diploma di Master II Livello (60 cfu)
• Date (da – a)	Da ottobre 1998 a febbraio 2005
• Nome e tipo di istituto di istruzione o formazione	Laurea vecchio ordinamento Sociologia Politico Istituzionale Università "La Sapienza" di Roma
• Principali materie / abilità professionali oggetto dello studio	Analizzare fenomeni sociali e politici attraverso metodi qualitativi e quantitativi; comprendere il funzionamento delle istituzioni e dei processi decisionali pubblici; interpretare dinamiche di governance, politiche pubbliche e comportamenti collettivi; utilizzare strumenti di statistica e ricerca sociale; gestire informazioni complesse e condurre analisi comparate; applicare competenze di progettazione sociale e policy analysis.
• Qualifica conseguita • Livello nella classificazione nazionale (se pertinente)	Laurea Vecchio Ordinamento
• Date (da – a)	Da settembre 1994 a giugno 1998
• Nome e tipo di istituto di istruzione o formazione	Liceo Scientifico Indirizzo Informatico L.S.S. Benedetto Croce di Roma
• Principali materie / abilità professionali oggetto dello studio	
• Qualifica conseguita • Livello nella classificazione nazionale (se pertinente)	Diploma di Liceo Scientifico
• Date (da – a)	Da luglio 1996 ad agosto 1996
• Nome e tipo di istituto di istruzione o formazione	Intensive English Language Course Emerald Cultural Institute di Dublino
• Principali materie / abilità professionali oggetto dello studio	Corso intensivo di lingua inglese
• Qualifica conseguita • Livello nella classificazione nazionale (se pertinente)	Diploma
CAPACITÀ E COMPETENZE PERSONALI	
MADRELINGUA	Italiano
ALTRE LINGUE	INGLESE
Capacità di lettura	Buono
Capacità di scrittura	Buono
Capacità di espressione orale	Buono
CAPACITÀ E COMPETENZE ORGANIZZATIVE	▪ Coordinamento di soluzioni che integrano sicurezza, innovazione e continuità operativa ▪ Gestione di gruppi eterogenei finalizzata alla collaborazione, chiarezza degli obiettivi e allineamento delle priorità. ▪ Pianificazione strategica capace di adattarsi rapidamente a contesti evolutivi. ▪ Adozione di processi decisionali strutturati e comunicazione orientata all'azione. ▪ Integrazione di tecnologie emergenti all'interno di modelli operativi. ▪ Strutturazione di flussi informativi a supporto di evidenze e metriche verificabili. ▪ Promozione di una cultura della sicurezza radicata nei processi aziendali e nei comportamenti operativi quotidiani.

CAPACITÀ E COMPETENZE TECNICHE	▪ Progettazione, implementazione e supervisione di architetture di sicurezza informatica. ▪ Conduzione di assesment tecnici e di sicurezza. ▪ Gestione della compliance normativa tramite applicazione e mantenimento di framework e standard internazionali. ▪ Definizione di policy tecniche, linee guida e controlli di sicurezza. ▪ Threat intelligence. ▪ Tecniche di ethical hacking. ▪ Analisi delle superfici di attacco e definizione di piani di remediation. ▪ Amministrazione e gestione operativa di apparati di rete, server Windows e Linux e piattaforme cloud. ▪ Conoscenza dei principali sistemi di autenticazione e di gestione delle identità. ▪ Diagnostica avanzata di sistemi, hardware, software e rete.
DATI PERSONALI	Autorizzo il trattamento dei miei dati personali ai densi del decreto legislativo 30 giugno 2003, n.196, recante Codice in materia di protezione dei dati personali