Cyber security
Maggio 2022

CYBER SECURITY & PRIVACY

Quick Start

intellera
consulting

01.

Chi siamo

Chi siamo

I Partner della RTI

Intellera Consulting (*mandataria della RTI)* è una società di consulenza nata dal management buyout della linea di business di PwC Italia **dedicata alla Pubblica Amministrazione e all'Healthcare**; dispone di **network di circa 700 professionisti**, si configura come apripista nella consulenza strategica e direzionale, e propone servizi professionali d'eccellenza a istituzioni, amministrazioni e imprese. Intellera svolge numerosi progetti in ambito cyber security, di diversa natura e complessità, afferenti alle PA Centrali (es: Consip, Ministero dell'Economia e Finanze, Ministero della Salute, INAIL, ecc.), a PA Locali (es: Roma Capitale, Comune di Milano, Regione Lazio, Regione Toscana, Regione Campania, Comune di Venezia, ecc.) e ad altri Enti del settore pubblico (es: AgID, Sogei, Consip, ecc.).

Capgemini è leader mondiale nella Cyber Security ed opera con più di **270.000 persone**, presenti in quasi **50 paesi** in tutto il mondo, con una forte esperienza sui principali mercati internazionale e italiano. La **Cyber Security rappresenta il core business** di Capgemini e viene sviluppata attraverso **un team globale costituito da oltre 4000** risorse con competenze qualificate che offrono un approccio a 360° su piattaforme IT, OT, cloud e IoT. Includiamo un set di servizi gestiti da personale con elevati skill in ambito di Ethical Hacking per fare attività di analisi delle vulnerabilità di servizi e infrastrutture delle aziende clienti.

HSPI SpA è una società di consulenza direzionale nata nel 2003, leader in Italia sulle tematiche di **IT Governance, IT Service Management, Management Consulting,** che conta più di 150 professionisti dislocati sulle tre sedi di Roma, Bologna e Milano in grado di offrire una vasta gamma di servizi professionali grazie ad un modello operativo capace di integrare competenze distintive di Consulenza Direzionale e conoscenze specialistiche in ambito ICT. HSPI ha maturato una notevole esperienza nella PA attraverso l'adozione di metodologie in linea con gli standard internazionali e alla collaborazione e partnership con associazioni internazionali ed enti per lo studio e la diffusione delle migliori pratiche di **IT Governance, IT Security e IT Service Management**

Teleconsys è una **Digital Innovation Company** il cui principale ambito di expertise è supportare le organizzazioni pubbliche e private in tutte le fasi del loro viaggio di trasformazione digitale attraverso l'adozione dei principali **digital enabler** e dell'**open innovation**. Iscritta dal 2019 nella sezione speciale del registro delle imprese in quanto investe più del 3% del VdP in RSI, ha specifiche competenze nella progettazione e realizzazione di soluzioni di Cybersecurity, Data Governance & Protection e Intelligence ed è strutturata su 3 BU (Next Generation Infrastructure & Cybersecurity, Agile Application Development & UX, Intelligent Service & Operation), intersecate da due strutture di innovazione: il **Digital Innovation Experience e l'Innovation & Contamination Lab**.

Chi siamo

La nostra mission

Il gruppo **Cyber Security & Privacy** è costituito da professionisti che hanno acquisito competenze ed esperienze sia **consulenziali** che **tecniche**, nel campo della **governance della sicurezza** e **protezione** degli asset critici. Proponiamo soluzioni modulari, flessibili e resilienti, permettendo ai nostri clienti di usufruire di **una vasta gamma di servizi** che contribuiscono ad incrementare le loro capacità di **identificazione delle minacce informatiche** e di **risposta efficace agli incidenti informatici**.

Benefici per i nostri clienti

Qualità dei servizi

L' alta qualità dei servizi erogati rappresenta un fattore distintivo del nostro team e per particolari tematiche di Cyber Security ingaggiamo esperti esterni per completare il team di lavoro.

Tecnologie all'avanguardia

Il nostro team ha maturato le capacità per l'utilizzo delle principali tecnologie di sicurezza leader nel mercato al fine di massimizzare l'efficacia e l'efficienza delle relative attività progettuali.

Expertise multidisciplinare

Il nostro team ha sviluppato un approccio caratterizzato da competenze specialistiche, tecniche, gestionali e legali, al fine di rispondere efficacemente alle esigenze in ambito Cyber Security e protezione dei dati sempre più complesse.

Settori

Ministeri e Agenzie

(PAC)

02.

I nostri servizi

Lo strumento a disposizione: Servizi di compliance e controllo per la PA

Lotto 2 – PAC

45,6 mln €

1. Security Strategy
2. Vulnerability Assessment
3. Testing del codice statico, dinamico e mobile
4. Supporto analisi e gestione incidenti
5. Penetration Testing
6. Compliance normativa

Servizi di sicurezza da remoto (1/2)

Le Amministrazioni possono aderire ai seguenti Servizi:

L2.S16 - Security Strategy
Supporto nell'individuazione delle linee strategiche in materia di sicurezza ICT, nonché nella definizione e monitoraggio delle azioni strategiche adottate, al fine di realizzare un "progetto di sicurezza" unitario e coerente. Definizione e controllo delle scelte strategiche inerenti il governo della Sicurezza delle informazioni, degli indirizzi organizzativi, tecnologici e dell'approccio da adottare a fronte di nuovi paradigmi architetturali, scenari di attacco e situazioni di rischio consolidate.
L2.S17 - Vulnerability Assessment
Valutazione e identificazione dello stato di esposizione alle vulnerabilità mediante la raccolta di informazioni concernente i servizi erogati, le applicazioni, l'architettura e le componenti tecnologiche. Il servizio è indirizzato principalmente alle Amministrazione che, in fase di definizione della strategia di sicurezza, necessitano di delineare un iniziale valutazione dello stato di sicurezza del sistema informativo e dello stato di esposizione alle vulnerabilità.
L2.S18 - Testing del codice statico
Identificazione delle vulnerabilità software all'interno del codice (sorgente o binario) delle applicazioni nella fase iniziale del ciclo di vita, in modo da poterle eliminare prima della distribuzione. Questa tipologia di test (anche detta "white box testing") deve consentire agli sviluppatori di trovare le vulnerabilità di sicurezza nel codice sorgente durante le prime fasi di sviluppo dell'applicazione garantendo la conformità alle linee guida (ad es. owasp) ed agli standard di codifica senza eseguire effettivamente il codice sottostante.
L2.S19 - Testing del codice dinamico
Il servizio di "Testing del codice - dinamico" consente alle Amministrazioni l'identificazione delle vulnerabilità all'interno delle applicazioni Web in fase di esecuzione e l'analisi dell'esposizione al rischio di attacchi informatici ai sistemi informativi mediante l'utilizzo di tecniche di analisi dinamica. L'approccio adottato dovrà prevedere il "black box testing" o testing funzionale fondato sull'analisi degli output generati dal sistema.

Servizi di sicurezza da remoto (2/2)

Le Amministrazioni possono aderire ai seguenti Servizi:

L2.S20 - Testing del codice mobile

Il servizio di “Testing del codice - mobile” consente alle Amministrazioni di eseguire test mirati alle applicazioni di tipo mobile consentendo la rilevazione delle vulnerabilità di sicurezza che possono essere sfruttate da un attaccante per compromettere i dati delle mobile app, la logica di business o il framework del dispositivo mobile identificando qualsiasi minaccia che mette a rischio l'applicazione e/o l'infrastruttura.

L2.S21 - Supporto all’analisi e gestione degli incidenti

Il servizio “Supporto all’analisi e gestione degli incidenti” consente alle Amministrazioni e agli organismi deputati alle attività di prevenzione, supporto nello svolgimento delle attività di analisi degli incidenti e di divulgazione delle informazioni in caso di emergenza. Il servizio è atto a garantire e supportare le Amministrazioni del rispetto e della corretta esecuzione di tutti i processi di gestione degli incidenti di sicurezza (post-mortem) e di escalation.

L2.S22 - Penetration Testing

Il servizio, condotto su più fasi e mediante l’adozione di adeguati strumenti, si configura nella simulazione di un attacco informatico al sistema da parte di un utente malintenzionato al fine di rilevare la presenza di eventuali falle e vulnerabilità al suo interno. Verranno fornite il maggior numero di informazioni sulle vulnerabilità che hanno permesso l'accesso non autorizzato al sistema con una stima chiara sulle capacità di difesa

L2.S23 - Compliance normativa

Supporto nell’attuazione degli adempimenti del GDPR (Regolamento UE 2016) applicato all’ambito del perimetro IT, al fine di sopperire alle criticità e ai limiti da fronteggiare con riferimento alla protezione dei dati personali. Valutazione dei rischi, registro dei trattamenti, creazione di un modello di privacy compliance, individuazione aree di miglioramento.

Gli step per l'attivazione del Contratto Esecutivo

L'**Amministrazione** trasmette il "Piano dei Fabbisogni" (o "Ordinativo") al Fornitore e contestualmente alla Consip (e/o a terzi dalla stessa indicati)*

Piano dei Fabbisogni

Piano Operativo

Il **Fornitore**, sulla base del Piano dei Fabbisogni, predispone un "Piano Operativo", nel quale formula una proposta tecnico/economica. Il Fornitore invia il Piano all'Amministrazione e per copia conoscenza alla Consip S.p.A. e/o terzi da essa indicati; **entro 15 giorni lavorativi** dall'invio del Piano dei Fabbisogni

L'**Amministrazione**, **entro 30 giorni** dalla ricezione, può approvare il Piano Operativo oppure comunicare la richiesta di eventuali modifiche e/o integrazioni

Approvazione

Integrazioni / Modifiche

Nel caso di integrazioni, il **Fornitore** deve inviare la versione definitiva del Piano Operativo **entro 10 giorni solari** dalla comunicazione di richiesta dell'Amministrazione

Una volta approvato il Piano Operativo, l'**Amministrazione** stipula con il Fornitore il Contratto Esecutivo. Il CE ha una durata massima pari alla durata residua dell'AQ al momento della stipula del CE.

Contratto Esecutivo

Piano di Lavoro Generale

Il **Fornitore** inoltre deve produrre, **entro 10 giorni lavorativi** dalla firma del Contratto Esecutivo, il Piano di lavoro generale, riportante la pianificazione di dettaglio di tutte le attività ed i servizi ricompresi e in conformità con il Contratto Esecutivo

Avvio attività

Grazie.

intellera consulting

Via Gaetano De Castillia, 23
20124 - **Milano** (MI)

Largo Angelo Fochetti, 28
00154 - **Roma** (RM)