Rev. 1.1	Emissione	Data	AGG. 30/09/2023	
Rev. 2.0	Adeguamento descrizione servizi secondo rilievi n. 1 e n. 2 del rapporto audit N° 22 PS 10 MI	Data	AGG. 22/07/2024	
Rev. 2.1	Aggiornamento denominazione servizi saas	Data	AGG. 25/09/2025	
Rev. 2.2	Aggiornamento servizio inrmaONE saas e aggiunta servizi e articoli Zen	Data	AGG. 25/09/2026	

Prog.	Codice	Categoria	Nome del Servizio	Descrizione del Servizio	Orario di Servizio	Ore di Servizio	Eccezioni orario di Servzio	Ore di Supporto	Disponibilità	Tempo presa in carico richiesta	Prezzo del Servizio
1	S-01	Sw Saas	inrima CMDB Saas	INRIMA CMDB è un applicativo Saas che permette la corretta gestione del sistema di gestione della sicurezza delle informazioni attraverso un modulo CMDB, per la gestione avanzata delle configurazioni degli asset rilevanti (fornitori, ditte di manutenzione, dipendenti etc…) ed i beni ICT impiegati per l'erogazione dei servizi interni/esterni (server, client, switch etc…). La gestione prevede la suddivisione degli asset fra più sedi e posizioni, la descrizione delle caratteristiche degli asset, il controllo dei contratti di fornitura, manutenzione, garanzia, licenza associati agli asset e l'inserimento della documentazione relativa agli asset e il collegamento con applicativi di inventory per l'aggiornamento continuo degli asset. Il modulo di risk management permette la valutazione del rischio dell'organizzazione attraverso l'analisi dei controlli di sicurezza adottati dall'azienda, la gestione dinamica del rischio in base alla pianificazione dell'attuazione delle politiche e delle procedure atte ad innalzare il livello di sicurezza delle informazioni. INRIMA One è dotato di un modulo di gestione utenti e ruoli, nonché della gestione dei log degli accessi e delle attività sul database da parte degli utenti.	0-24	24 h	no	24 h	99,00%	1h	Preventivo
2	S-02	Sw Saas	INRIMA GDPR	INRIMA Compliance è lo strumento sviluppato e manutenuto da Go Infoteam per garantire la corretta gestione del sistema di gestione dei dati personali, la gestione del servizio e della sicurezza delle informazioni (GDPR, ISO 27001). INRIMA permette di poter gestire sistemi conformi alle norme indicate e può costituire la base su cui fondare eventuali certificazioni organizzative da parte di enti accreditati, attraverso le seguenti funzionalità disponibili: Profilazione utenti e gruppi, gestione log attività, diario del DPO e gestione messaging su eventi specifici, gestione risorse, ruoli e funzioni aziendali, archiviazione documenti del sistema protezione dati, gestione dei registri delle attività di trattamento di titolari e dei responsabili, generazione di informative, valutazione di impatto sulla protezione dei dati personali DPIA, gestione diritti interessati e registro, gestione Data Breach e registro, registro formazione dei soggetti autorizzati, gestione questionari per audit specifici di sicurezza Analisi dei rischi sugli asset specifici, asset management, change management, incident management, tracciamento scadenza attività e azioni.	0-24	24 h	no	24 h	99,00%	1h	Preventivo
3	S-03	Sw Saas	GO-ELEARNING Saas	La piattaforma Go eLearning permette di gestire ed erogare, in maniera flessibile e facilmente accessibile, corsi di qualsiasi natura attraverso tre diverse modalità di esecuzione: e-learning in modalità completamente online; residenziale, in modalità di svolgimento con presenza fisica in aula ma con registrazione delle presenze sulla piattaforma; mista, in modalità di svolgimento ibrida tra lezioni svolte in aula ed online. La piattaforma, offerta in modalità SaaS, presenta un'architettura evoluta finalizzata a rispondere alle diverse esigenze di formazione attraverso personalizzazioni ed evolutive normative. La fruizione dei corsi nella modalità di erogazione online è basata sul modello SCORM, pertanto i corsi sono organizzati a moduli. Per ciascuno modulo possono essere gestire più lezioni o test, intermedi o finali. Le regole previste dal modello SCORM prevedono di avere la certezza che le lezioni vengano visualizzate in maniera sequenziale ed ordinata dall'allievo (discente). Ciascun corso può essere strutturato da uno o più moduli, allo stesso modo ciascun modulo può essere composto a sua volta da una o più lezioni e test. I test possono essere sottoposti anche durante l'esecuzione del corso, fra una lezione e quella successiva, in modo da garantire una verifica delle capacità acquisite prima del test successivo o finale.	0-24	24 h	no	24 h	99,00%	1h	Preventivo
4	S-04	Sw Saas	Cloud Mobile Saas	Cloud Mobile è lo strumento software sviluppo e mantenuto da Go Infoteam per la gestione dei negozi di telefonia. La piattaforma, offerta in modalità SaaS, presenta un'architettura modulare finalizzata a rispondere alle diverse esigenze di gestione attraverso personalizzazioni ed evolutive commerciali. Grazie ai listini (articoli e servizi) dei gestori sempre aggiornati, sarà facile attraverso le vendite con Cloud Mobile, tenere sotto controllo lo stato delle attivazioni, il compenso canvass, avere in automatico l'allineamento della rendicontazione, nonché delle scorte. Cloud Mobile è il software particolarmente adatto sia per chi apre un nuovo negozio di telefonia che per gestire una rete di negozi già strutturata. Altro punto di forza di Cloud Mobile è la centralità del codice IMEI per il compimento di tutte le operazioni, il che permette una gestione del post-vendita ottimizzata e accentrata sulla sicurezza del cliente e del venditore. Si assicura così tracciabilità, sicurezza, capacità di gestire il parco clienti con uno storico di tutte le movimentazioni, in qualsivoglia momento. Cloud Mobile permette la gestione clienti, dall'emissione di fidelity card per fidelizzare i clienti, inviare promozioni e offerte, ricontattarli grazie a tutte le informazioni a disposizione.	0-24	24 h	no	24 h	99,00%	1h	Preventivo
5	S-06	Sw Saas	inrimaONE Saas - Piano Base	inrimaONE - Piano Base la configurazine iniziale di una piattaforma modulare GRC, erogata in modalità Saas, progettata per supportare le organizzazioni nella gestione integrata della compliance normativa, cybersecurity, governance e resilienza operativa, costituita da una serie di moduli integrati e garantisce la copertura del framework di Cyber Security offrendo un'esperienza intuitiva anche per utenti non specializzati. Il Piano Base è costituito dai moduli Compliance, Document Hub e Asset Management. - Compliance permette di monitorare lo stato di un processo in modo semplice e immediato con l'uso di check-list, di allegare evidenze e di gestire il piano di adeguamento. Il modulo - Document Hub permette la gestione centralizzata in unico repository per tutti i docuemnti ed allegati alle check-list, divisi in categorie e permette una ricerca semplificata per recupero documenti in caso di audit. - Asset Management permette la gestione avanzata delle configurazioni degli asset rilevanti (fornitori, ditte di manutenzione, dipendenti etc…) ed i beni ICT impiegati per l'erogazione dei servizi interni/esterni (server, client, switch etc…) e comprende anche il modulo di gestione utenti e ruoli, nonché della gestione dei log e audit degli accessi.	0-24	24 h	no	24 h	99,00%	1h	Preventivo

Rev. 1.1	Emissione	Data	AGG. 30/09/2023
Rev. 2.0	Adeguamento descrizione servizi secondo rilievi n. 1 e n. 2 del rapporto audit N° 22 PS 10 MI	Data	AGG. 22/07/2024
Rev. 2.1	Aggiornamento denominazione servizi saas	Data	AGG. 25/09/2025
Rev. 2.2	Aggiornamento servizio inrmaONE saas e aggiunta servizi e articoli Zen	Data	AGG. 25/09/2026

6	S-07	Sw Saas	inrimaONE Saas - Piano Avanzato	inrimaONE - Piano Avanzato è la configurazione completa una piattaforma modulare GRC, erogata in modalità Saas, progettata per supportare le organizzazioni nella gestione integrata della compliance normativa, cybersecurity, governance e resilienza operativa, costituita da una serie di moduli integrati e garantisce la copertura del framework di Cyber Security offrendo un'esperienza intuitiva anche per utenti non specializzati. Il Piano Avanzato aggiunge al Piano Base i seguenti moduli Vulnerability Management, Change Management, Incident Management, Disaster Recovery, Insights. - Vulnerability Management permette di registrare le vulnerabilità rilevati sui sistemi dell'organizzazione e di monitorarne le evoluzioni di risoluzione. - Change Management permette la gestione dei cambiamenti secondo i più diffusi framework e schemi di certificazione, seguendo un workflow approvativo semplice e intuitivo e con il supporto dell'intelligenza artificiale se richiesta dall'operatore. - Incident Management permette la registrazione degli incidenti rilevati da segnalazioni interne e/o da sistemi di rilevazione minacce e gestirne l'evoluzione di risoluzione. - Disaster Recovery permette di censire le procedure per la gestione della continuità operativa di cui si dota l'azienda al fine di conultarli rapidamente in caso di necessità. - Insight mostra i dati provenieti dai vari moduli di inrima ONE e di organizzare le metriche in modo personalizzato, consente analisi e viste immediate, permettendo quindi di avere in una dashboard preconfigurata lo stato di conformità sempre aggiornato.	0-24	24 h	no	24 h	99,00%	1h	Preventivo
7	P-01	Sicurezza	Servizio di Vulnerability assessment	Il servizio consiste nella scansione di vulnerabilità condotta su diverse tipologie di sistemi IT/OT presenti in rete presso l'infrastruttura del Cliente (server, apparati di rete, stampanti etc…). Obiettivo del test, il quale può essere condotto dall'esterno della rete (su ip pubblici) e o dall'interno della stessa (su ip privati), in modalità autenticata o meno, è quello di verificare la presenza o meno - con un certo grado di confidenza - di vulnerabilità note nei sistemi, devices e software utilizzati dal Cliente per supportare l'erogazione dei propri servizi interni/esterni. La scansione è eseguita attraverso un apposito strumento software - c.d. scanner - in grado di interrogare i sistemi (espressamente indicati ed autorizzati dal Cliente) tramite apposite richieste inviate per testarne la sicurezza e, attraverso le risposte ricevute, verificare se dalle stesse è possibile rilevare la presenza di una o più delle vulnerabilità rese note in appositi bollettini di sicurezza e database pubblici (c.d. CVE - Common Vulnerabilities and Exposures). Le vulnerabilità note eventualmente rilevate sono accompagnate da una descrizione delle stesse, da un indice di criticità che permette di determinarne la gravità e priorità di risoluzione o mitigazione, nonchè dalla raccomandazione delle necessarie azioni di remediation. Le fasi del servizio si articolano nelle seguenti: - Definizione delle regole di ingaggio: tramite riunione con il Cliente, definizione del perimetro autorizzato di test, richiesta/ricezione di tutte le informazioni necessarie alla conduzione del test (indirizzi ip, descrizione di sistemi particolarmente critici o tecnologie prevalenti, credenziali per l'accesso ai sistemi da scansionare, utenza vpn per l'accesso remoto, tempistiche) e definizione delle tempistiche di inizio e fine del test; - Comunicazione di avvio della scansione: invio di apposita comunicazione almeno 30 minuti prima della data ed ora fissata per l'avvio del test; - Scansione: esecuzione della scansione di vulnerabilità e monitoraggio delle relative performance e/o eventuali problematiche; - Comunicazione di termine della scansione: invio di apposita comunicazione, non oltre 30 minuti dopo la fine della scansione; - Analisi dei risultati: analisi - ad opera dei cybersecurity specialists - dei risultati della scansione, in modo da rilevare elementi di interesse, priorità e statistiche generali, con conclusione; - Generazione e conegna della reportistica: predisposizione della reportistica generale e di dettaglio, volta ad illustrare i risultati emersi dalla scansione e le raccomandazioni degli analisti, in particolare sotto il profilo delle maggiori criticità rilevate, delle azioni prioritarie raccomandate e dell'esito generale - positivo o negativo - della scansione; - Presentazione dei risultati: presentazione al Cliente dei report con spiegazione dei punti di analisi principali emersi ed analisi del risultato generale di scansione.	9-18 LUN-VEN	8 h	13-14	9-18 LUN-VEN	80,00%	16 ore lavorative	Preventivo
8	P-02	Sicurezza	Servizio di Web Application Penetration Test - WAPT	Il servizio consiste nel penetration test condotto specificatamente su un applicativo web, al fine di verificare se lo stesso presenta una o più delle vulnerabilità web comunemente note (sql injection, XSS, CSRF etc…) e/o altre problematiche (di configurazione o di logica) che consentirebbero ad un attaccante di bypassare i suoi meccanismi di sicurezza o comunque eseguire azioni dannose sullo stesso, sui suoi dati o sui suoi utenti. Il Web Application Penetration Test viene eseguito in modo sia manuale sia automatizzato, ossia verificando manualmente la presenza o meno di vulnerabilità nell'applicativo ed accompagnando tale analisi con una serie di scansioni di sicurezza automatizzate. Utilizzando entrambe le modalità, viene pertanto eseguito il c.d. Dynamic Application Security Testing (DAST) dell'applicativo, ossia la sua analisi di sicurezza non basata sul contenuto del codice sorgente - sconosciuto al tester - bensì su come l'applicativo concretamente si presenta e risponde ai test eseguiti dinamicamente. I test manuali vengono condotti secondo metodologia OWASP, applicando conseguentemente una ben nota, riconosciuta e standardizzata serie di verifiche dirette ad analizzare compiutamente la sicurezza dell'applicativo e la sua rispondenza alle principali pratiche di sviluppo sicuro. Le fasi del servizio si articolano nelle seguenti: - Definizione delle regole di ingaggio ed analisi dell'oggetto di test: tramite riunione con il Cliente, definizione del perimetro autorizzato di test, richiesta/ricezione di tutte le informazioni necessarie alla conduzione del test (indirizzi ip, URI, funzionalità ed architettura dell'applicativo, credenziali di accesso semplici e privilegiate) e definizione delle tempistiche di inizio e fine del test;	9-18 LUN-VEN	8 h	13-14	9-18 LUN-VEN	80,00%	16 ore lavorative	Preventivo

Rev. 1.1	Emissione	Data	AGG. 30/09/2023	
Rev. 2.0	Adeguamento descrizione servizi secondo rilievi n. 1 e n. 2 del rapporto audit N° 22 PS 10 MI	Data	AGG. 22/07/2024	
Rev. 2.1	Aggiornamento denominazione servizi saas	Data	AGG. 25/09/2025	
Rev. 2.2	Aggiornamento servizio inrmaONE saas e aggiunta servizi e articoli Zen	Data	AGG. 25/09/2026	

9	P-03	Consulenza	Servizio specialisticio in ambito GDPR	Servizio specialistico per l'esecuzione degli adeguamenti normativi previsti dal GDPR (RE 679/2016), D.Lvo 196/2003 e D. Lvo 101/2018, costituito dalle seguenti attività: - Responsabile della protezione dei Dati ai sensi dell'art. 37 e ss del Regolamento UE 2016/679 - Valutazioni che impattano sulle problematiche di gestione della protezione dei dati - Procedure di acquisizione di servizi e di attivazione di eventuali convenzioni conformi alla normativa - Aggiornamento sistematico del registro dei trattamenti di dati personali - Redazione e aggiornamento delle informative e delle eventuali formule di consenso - Redazione delle nomine interne ai soggetti autorizzati - Redazione delle designazioni dei responsabili ex art. 28 GDPR - Procedure di gestione dei data breach e dell'esercizio dei diritti dell'interessato - Redazione valutazione di impatto (DPIA) - Formazione ed aggiornamento del personale Il servizio è erogato nei giorni lavorativi a seguito di richiesta da parte del cliente e prevede l'avvio dell'esecuzione delle attività specifiche del servizio entro 5 gg lavorativi, dall'acquisizione dei parametri necessari allo svolgimento delle attività, con rilascio della documentazione prevista.	9-18 LUN-VEN	8 h	13-14	9-18 LUN-VEN	80,00%	16 ore lavorative	Preventivo
10	P-04	Consulenza	Servizio specialistico in ambito Cyber Security	Servizio specialistico per l'esecuzione degli adeguamenti previsti dalle best practices di Cyber Security (Framework Nazionale per la Cyber Security, ISO 27001, NIST CSF, CIS Controls), costituito dalle seguenti attività: - CyberSecurity Assessment sullo stato di adeguamento della sicurezza ICT rispetto ad un framework di riferimento - Analisi, valutazione e trattamento del rischio - Raccomandazione di azioni di mitigazione del rischio o miglioramento - Valutazione e predisposizione politiche/procedure di sicurezza delle informazioni - Monitoraggio e verifica dello stato della sicurezza e dei cambiamenti - Supporto alle attività di rilevazione ed analisi degli incidenti di sicurezza informatica, incluso il supporto al coordinamento e alla gestione dell'incidente nonchè alla sua notifica al CSIRT Italia. Il servizio è erogato nei giorni lavorativi a seguito di richiesta da parte del cliente e prevede l'avvio dell'esecuzione delle attività specifiche del servizio entro 5 gg lavorativi, dall'acquisizione dei parametri necessari allo svolgimento delle attività, con rilascio della documentazione prevista.	9-18 LUN-VEN	8 h	13-14	9-18 LUN-VEN	80,00%	16 ore lavorative	Preventivo
11	P-05	Assistenza Tecnica	Servizio specialistico per soluzioni prodotti cyber	Il servizio consiste nella realizzazione di tutte le attività prodromiche e conseguenti all'efficace ed efficiente implementazione di soluzioni di Cyber Security presso i Clienti, come ad esempio strumenti di monitoraggio (SIEM, MDR, NAC etc...), di deception, di protezione (EDR, XDR etc...) o di altro tipo. Tali attività sono dirette a garantire che la soluzione di Cyber Security acquistata dal Cliente venga deployata, configurata, amministrata, utilizzata, aggiornata e manutenuta correttamente per lo scopo di sicurezza cui è destinata, fornendo dunque al Cliente il supporto necessario al corretto e adeguato inserimento nella propria infrastruttura ICT del prodotto di sicurezza. Le attività eseguite - a seconda della natura della soluzione - sono le seguenti: - Configurazione ed avviamento - Personalizzazione - Formazione iniziale - Predisposizione reportistica - Gestione ed amministrazione della soluzione - Assistenza nell'utilizzo e troubleshouting - Gestione del rapporto con il supporto del Vendor. Il servizio è erogato nei giorni lavorativi a seguito di richiesta da parte del cliente e prevede l'avvio dell'esecuzione delle attività specifiche del servizio entro 5 gg lavorativi, dall'acquisizione dei parametri necessari allo svolgimento delle attività. Al termine segue comunicazione scritta di conclusione dell'attività richiesta.	9-18 LUN-VEN	8 h	13-14	9-18 LUN-VEN	80,00%	16 ore lavorative	Preventivo
12	A-01	Assistenza Tecnica	Servizio di assistenza tecnica I livello	Il servizio di assistenza tecnica di I livello prevede i seguenti interventi tecnici: - hardware e/o software su pc, - stampanti multifunzioni (locali e di rete) - configurazioni di base su apparati di rete quali switch e router - interventi sistemistici occasionali su indicazione del referente dell'organizzazione.	9-18 LUN-SAB	9 h	no	9-18 LUN-SAB	85,00%	8 ore lavorative	Preventivo

Rev. 1.1	Emissione	Data	AGG. 30/09/2023	
Rev. 2.0	Adeguamento descrizione servizi secondo rilievi n. 1 e n. 2 del rapporto audit N° 22 PS 10 MI	Data	AGG. 22/07/2024	
Rev. 2.1	Aggiornamento denominazione servizi saas	Data	AGG. 25/09/2025	
Rev. 2.2	Aggiornamento servizio inrmaONE saas e aggiunta servizi e articoli Zen	Data	AGG. 25/09/2026	

13	A-02	Assistenza Tecnica	Servizio di assistenza tecnica II livello	Il servizio di assistenza tecnica di II livello prevede interventi tecnici hardware e software su datacenter, apparati attivi e passivi di rete, storage e l'erogazione del ruolo di amministrazione di sistema L'attività prevede i principali compiti di: - monitorare lo stato dei sistemi e assicurare la corretta gestione delle infrastrutture tecnologiche presenti, secondo i profili di sicurezza, concordati con il Committente; - verificare il corretto funzionamento della rete e di tutti gli apparati di rete, gestire e verificare gli accessi con modalità concordate con il Committente; - gestire gli account/credenziali di accesso degli utenti alle postazioni di lavoro personali ed ai servizi di rete intranet ed internet secondo indicazioni del Committente; - verificare la sicurezza e salvaguardia dei dati a seguito della navigazione degli utenti su internet, nei limiti dei prodotti hardware e software forniti dal Committente; - attivare procedure e strategie di back-up e restore dei dati per la sicurezza dei dati; - segnalare al Committente la necessità di adottare eventuali misure di sicurezza ai sensi del RE 679/2016.	9-18 LUN-SAB	9 h	no	9-18 LUN-SAB	85,00%	8 ore lavorative	Preventivo