CERTIFIED
ISO 27001
ISO 27017
ISO 27018
BUREAU VERITAS

CERTIFIED
ISO 9001
ISO 14001
ISO 45001
BUREAU VERITAS

Rif: CDOO-2025-MT-000272-1

Spettabile

Comune di Oleggio Castello

Via dal Pozzo, 2

28040 – Oleggio Castello (Novara)

Alla cortese Attenzione di Mauro Murazzi

P.IVA 00165200031

S. Stefano Ticino, 28 ottobre 2025

Oggetto: Proposta economica per contratto assistenza MSD V3

In riferimento ai colloqui intercorsi, abbiamo il piacere di sottoporre alla Vostra cortese attenzione la nostra migliore proposta economica per l'assistenza informatica proattiva di Vostro interesse.

Restiamo a Vostra completa disposizione per qualsiasi ulteriore informazione e/o chiarimento dovesse occorrervi.

In attesa di un Vostro cortese riscontro, cogliamo l'occasione per porgere i nostri più cordiali saluti.

Manuel Tosatti
manuel.tosatti@cdesign-group.com

Computer Design s.r.l.
Via Piave, 46
20010 S. Stefano Ticino (MI)
Tel. +39 02 97 48 21
Fax +39 02 97 48 222
P. Iva 11980150152

Sommario

1. Le Nostre Certificazioni ISO 4
2. IT Managed Service 5
2.1. Service Desk 5
2.2. Tipologia delle richieste 6
2.3. Gestione Ticket 6
2.3.1. Proattività 7
2.3.2. Extra Contratto 7
2.3.3. Schema gestione chiamata 8
2.4. SLA – Service Level Agreement 9
2.5. Disponibilità del servizio 9
2.6. Modello organizzativo dei servizi 10
2.7. Servizio di contact center 10
3. Startup e presa in carico 11
4. Governo del contratto - Opzionale 12
4.1. Modello Organizzativo 12
4.2. Processi di Governance 14
4.3. Gestione delle Penali 14
4.4. Gestione dei Problemi 14
4.5. Comunicazioni 15
4.6. Procedura di Escalation 15
4.7. Audit 15
5. Servizi di monitoraggio – Opzionale 17
6. Vulnerability Assessment - Opzionale 18
6.1. Fase di analisi (Assessment): 19
6.2. Fase di consolidamento (Remediation): 19
6.3. Ciclo di valutazione delle vulnerabilità e loro consolidamento: 20
6.4. Vulnerability Assessment – Prima Elaborazione 21
6.5. Vulnerability Assessment –Elaborazioni Successive 21
7. Patch Management - Opzionale 22
7.1. Contesto di riferimento 22
7.2. Modalità operative 23
7.3. Oggetto Del Servizio 24
7.4. Attività non incluse nel servizio di patching 24
8. Analisi CyberSecurity Posture - Opzionale 26
9. IT Managed Service – tipologie di contratto 28
9.1. Remote Service Desk – RSD 28
9.2. Managed Service Desk - MSD 28
9.3. C-Sec 29
9.4. DR - HERO 30
9.4.1. SLA – Attivazione in Caso di Emergenza 30
9.5. MDR Hero 31
9.5.1. SLA – Attivazione in Caso di Emergenza 33
9.5.2. Esclusioni dal contratto 33
10. Servizi Aggiuntivi 34
10.1. Utenti VIP 34
10.2. Presidio OnSite 34
10.3. Sabato Mattina 34
10.4. Reperibilità H24 34

10.5. Servizio Premium – Attività extra 34
10.6. Test Backup 35
11. Corrispettivo Economico 36
11.1. Soluzione Proposta – Contratto MSD 36
12. Esclusioni 37
13. Tariffe servizi 38
13.1. Attività OnSite 38
13.2. Listino di riferimento 38
13.3. Richieste di Assistenza in "emergenza" 39
13.3.1. Clienti con servizio di reperibilità 39
14. Condizioni di Fornitura 40
14.1. Attivazione Servizio 40
14.2. Durata del Contratto 40
14.3. Dati e Programmi 40
14.4. Condizioni di Fatturazione E Pagamento 40
14.5. Metodo di calcolo – MSP (Managed Services Provider) 41
15. Condizioni Commerciali di Fornitura 42
16. Accettazione 43
17. Condizioni generali di fornitura 44

1. Le Nostre Certificazioni ISO

La nostra azienda è certificata secondo i più alti standard internazionali. Le certificazioni ISO che abbiamo ottenuto testimoniano il nostro impegno per la qualità, la sostenibilità, la sicurezza sul lavoro e la protezione delle informazioni, anche in ambienti cloud. Questi riconoscimenti rafforzano la fiducia dei nostri clienti e partner, garantendo processi affidabili, sicuri e trasparenti.

CERTIFIED ISO 27001	**ISO 27001 – Sicurezza delle Informazioni** La ISO 27001 certifica che proteggiamo le informazioni aziendali e dei clienti con sistemi di gestione della sicurezza informatica avanzati. **Vantaggi per il cliente:** Protezione dei dati sensibili, Riduzione dei rischi informatici, Conformità alle normative sulla privacy
CERTIFIED ISO 27017	**ISO 27017 – Sicurezza nel Cloud** Estensione della ISO 27001, la ISO 27017 fornisce linee guida specifiche per la sicurezza delle informazioni nei servizi cloud, sia per i fornitori che per i clienti. **Vantaggi per il cliente:** Maggiore sicurezza nei servizi cloud, Controlli specifici per ambienti virtualizzati, Fiducia nei servizi digitali
CERTIFIED ISO 27018	**ISO 27018 – Privacy nel Cloud** La ISO 27018 è uno standard internazionale focalizzato sulla protezione dei dati personali nei servizi cloud pubblici, in conformità con le normative sulla privacy. **Vantaggi per il cliente:** Protezione dei dati personali nel cloud, Conformità al GDPR e ad altre normative |Maggiore trasparenza e controllo
CERTIFIED ISO 9001	**ISO 9001 – Qualità** La ISO 9001 certifica il nostro sistema di gestione per la qualità. Garantiamo processi efficienti, orientati al miglioramento continuo e alla soddisfazione del cliente. **Vantaggi per il cliente:** Servizi/prodotti affidabili, Controllo qualità rigoroso, Miglioramento continuo
CERTIFIED ISO 14001	**ISO 14001 – Ambiente** Con la ISO 14001, gestiamo in modo responsabile l'impatto ambientale delle nostre attività, promuovendo la sostenibilità e il rispetto delle normative ambientali. **Vantaggi per il cliente:** Collaborazione con un'azienda eco-consapevole, Riduzione dell'impatto ambientale, Conformità normativa
CERTIFIED ISO 45001	**ISO 45001 – Salute e Sicurezza sul Lavoro** La ISO 45001 attesta il nostro impegno per la salute e la sicurezza dei lavoratori, attraverso la prevenzione dei rischi e la promozione del benessere sul luogo di lavoro. **Vantaggi per il cliente:** Continuità operativa, Ambiente di lavoro sicuro, Immagine aziendale solida

Le nostre certificazioni ISO rappresentano un impegno concreto verso l'eccellenza, la sicurezza e la sostenibilità. Scegliere noi significa affidarsi a un partner certificato, competente e responsabile.

2. IT Managed Service

Con il termine **IT Managed Service** identifichiamo una famiglia di servizi che hanno l'obiettivo di gestire, manutenere e rendere più sicure le infrastrutture IT dei clienti. Il fulcro di questa famiglia di servizi è il **Service Desk** di Computer Design S.r.L. (di seguito CD), gruppo di professionisti specializzati nella gestione delle infrastrutture IT dei clienti.

2.1. Service Desk

Il nostro modello di Service Desk è stato pensato in modo scalabile per dare possibilità al cliente di scegliere la formula più congeniale alle sue esigenze, arrivando fino ad una copertura 24x7 con diversi Service Level Agreement. Il Service Desk di CD è composto da un team con elevate competenze sulle tecnologie, organizzato in turni e predisposto ad integrarsi nel flusso operativo del cliente.

Grazie a queste caratteristiche possiamo proporre al cliente un servizio che si adatta alle diverse esigenze con Service Level Agreement definiti e misurabili.

Il team del Service Desk e composto da tecnici, la maggior parte dei quali in possesso di certificazioni tecniche dei diversi brand-vendor. Le figure si differenziano per seniority crescente sia dal punto di vista di gestione delle problematiche (Customer support) sia dal punto di vista tecnico (Technical Support). Il gruppo del service desk fa riferimento al Team Leder del Service Desk. Il Team Leader del service Desk riporta al CTO che la responsabilità ultima per il corretto funzionamento del TEAM di Service Desk.
IL CTO gestisce e coordina anche il TEAM di Specialisti di CD, professionisti con le massime competenze in ambito IT.

Nel dettaglio la struttura di Service Desk è così organizzata:

A. **Key User CLIENTE**
   E' necessario che il cliente nomini un referente principale (**KEY USER**) che sarà l'unica figura professionale autorizzata ad aprire il Ticket al nostro service desk
B. **SPOC - Single Point Of Contact**
   Tutte le richieste arrivano a SPoC (Single Point of Contact). Il gruppo dedicato al servizio SPoC riceve tutte le richieste dei clienti e dai servizi di Monitoring; le organizza e le inoltra al Technical Service.
C. **TSC - Technical Support Center (service desk reattivo di 1°, 2° e 3° livello)**
   Il TSC opera in stretta connessione con i servizi di SPoC e Monitoring e si occupa di svolgere le attività remote orientate alla risoluzione dei problemi tecnici, fornendo un Service Desk finalizzato al ripristino del servizio nel minor tempo possibile per limitare gli impatti sull'operatività del Cliente. Il TSC è inoltre responsabile dell'escalation al Service Desk proattivo SSC per l'approfondimento e l'indagine delle problematiche più complesse dopo che il servizio è stato ripristinato. Il Service Desk è inoltre responsabile dell'escalation al SPECIALIST SUPPORT CENTER (SSC) per l'approfondimento e l'indagine delle problematiche più complesse dopo che il servizio è stato ripristinato.
   Nel dettaglio le attività TSC sono così sintetizzabili:
   a. Analizzare e sviluppare le Incident, Service o Change Request (Ticket) indirizzate dallo SPoC (interno o esterno in caso di fornitore esterno) sulla base delle procedure di Incident Management concordate con il cliente.
   b. Effettuare remotamente le attività di diagnosi e di ripristino del servizio secondo lo SLA concordato con il cliente.
   c. In caso di necessità inoltrare le attività di Root Cause Analysis verso il Service Desk proattivo di 2° livello (SSC) e verificarne l'operato fino alla risoluzione del problema tenendo costantemente aggiornato lo SPoC.

   Il Team TSC viene così declinato:

a. **TSC 1° Livello – (area Pc e Stampanti)** – Si occupa dell'analisi e risoluzione dei Ticket che hanno come oggetto problematiche su Personal Computer e Stampanti. Qual ora la problematica non venga risolta viene effettuata un'escalation al personale di II Livello (area infrastruttura).
b. **TSC 2° Livello – (area Infrastruttura)** – Si occupa dell'analisi e risoluzione dei ticket che hanno come oggetto problemi sull'infrastruttura.
Qual ora la problematica non venga risolta viene effettuata l'escalation al personale di III Livello
c. **TSC 3° Livello –** Personale Specialistico con preparazione specifica su tecnologia e/o prodotto, preposto alla risoluzione di problemi complessi e di ticket non risolte con l'assistenza di livello I e II.

D. SSC – Specialist Support Center

Lo **Specialist Support Center**, opera in stretta connessione con il servizio TSC e si occupa delle attività di investigazione e risoluzione da remoto di problematiche particolarmente complesse e dell'implementazione di eventuali Change Request sui sistemi del Cliente.

Il Team è costituito da figure professionali di elevata competenza in grado di risolvere i problemi più critici e di offrire consulenza a valore evidenziando possibili aree di miglioramento dell'infrastruttura o adeguamenti. Sono le stesse figure con elevato skill tecnologico che vengono impiegate nell'area di delivery dei progetti. Il team, opera in stretta connessione con il servizio TSC e si occupa delle attività di investigazione e risoluzione da remoto di problematiche ad alto impatto e dell'implementazione di eventuali Change sui sistemi del Cliente e di offrire consulenza a valore evidenziando aree di miglioramento (Performance&Tuning), provisioning dell'infrastruttura (CapacityPlan) e stato di salute degli ambienti (HealthCheck).

Nel dettaglio le principali attività di pertinenza dello Specialist Support Center saranno le seguenti:

a. Problem Investigation (definizione delle Root Cause Analysis) di prodotto finalizzate sia al ripristino del servizio che alla fix della problematica,
b. Tuning and performance on-demand dei sistemi,
c. Advanced Infrastructure Analysis con considerazioni finalizzate all'evoluzione della performance e della stabilità dei servizi,
d. Problem Management: analisi e lavoro congiunto con il Cliente nel caso di problematiche ricorrenti ad alto impatto.

2.2. Tipologia delle richieste

Di seguito riportiamo la tipologia con la relativa classificazione dei ticket (richieste) gestite dal servizio di Service Desk. La classificazione si basa sugli standard ITIL:

- **INCIDENT**: Secondo quanto definito da ITIL, un INCIDENT è un'interruzione non pianificata di un servizio o una riduzione della qualità di un servizio. **Le richieste classificate come INCIDENT sono soggette agli SLA** contrattuali:
- **REQUEST**: ITIL definisce SERVICE REQUEST come una "richiesta formale da parte di un utente, ad esempio una richiesta di informazioni o consigli; per reimpostare una password; o per installare una workstation per un nuovo utente". **Le richieste classificate come REQUEST NON sono soggette agli SLA** contrattuali;

2.3. Gestione Ticket

Di seguito riportiamo le modalità di gestione delle richieste di assistenza:

a) Apertura della chiamata di assistenza attraverso e-mail o telefono da parte dei soli Key Users del cliente.
b) Presa in carico dei ticket da parte di SPoC con invio di email al Key User interessato in base agli SLA previsti e a seconda del tipo di contratto.
c) Apertura Ticket di assistenza.

d) Al singolo Ticket verrà attribuito un parametro di criticità secondo la tabella che definisce gli SLA; Tale parametro è definito dal Service Desk in base alla severità del problema e viene classificata come INCIDENT o REQUEST
e) Analisi della problematica oggetto del ticket da parte degli specialisti di CD in considerazione dell'ambito richiesto e risoluzione dello stesso.
f) E' ad insindacabile giudizio di CD individuare ed assegnare risorse tecniche adeguate alla risoluzione del problema.
g) Nel caso non sia possibile la risoluzione per cause non dipendenti da Computer Design verrà fatta escalation verso AM e Area Delivery per attività extra contratto e contestualmente verrà chiusa la chiamata.
h) Chiusura del ticket con invio mail al Key User interessato.

2.3.1. Proattività

A fronte dell'adozione dei nostri servizi di supporto di tipo proattivo, le segnalazioni al sistema di ticketing possono pervenire in automatico dal sistema di monitoring oppure dalle console di gestione in possesso del cliente, opportunamente configurate. Tali segnalazioni vengono trattate secondo la seguente metodologia:

a. Alla segnalazione di anomalia viene aperto un Ticket di assistenza.
b. A fronte di tale ticket il nostro servizio tecnico effettua l'analisi e se l'anomalia lo consente provvede a risolverla definitivamente ed a chiudere il ticket.
c. Se l'anomalia richiede una attività dipendente del cliente il Service Desk provvederà a comunicare tali esigenze al cliente e nel contempo mette in "PAUSA" il sensore dello strumento di monitoring o della console.
d. Se è il Cliente ad assumersi la responsabilità di NON effettuare interventi risolutivi, il servizio di Service Desk provvederà a concordare col Cliente due opzioni:
    1. Mettere in "PAUSA" il sensore, in attesa della successiva risoluzione dell'anomalia;
    2. Cancellare il sensore. In questo caso non sarà più possibile tenere sotto controllo il parametro o il dispositivo.

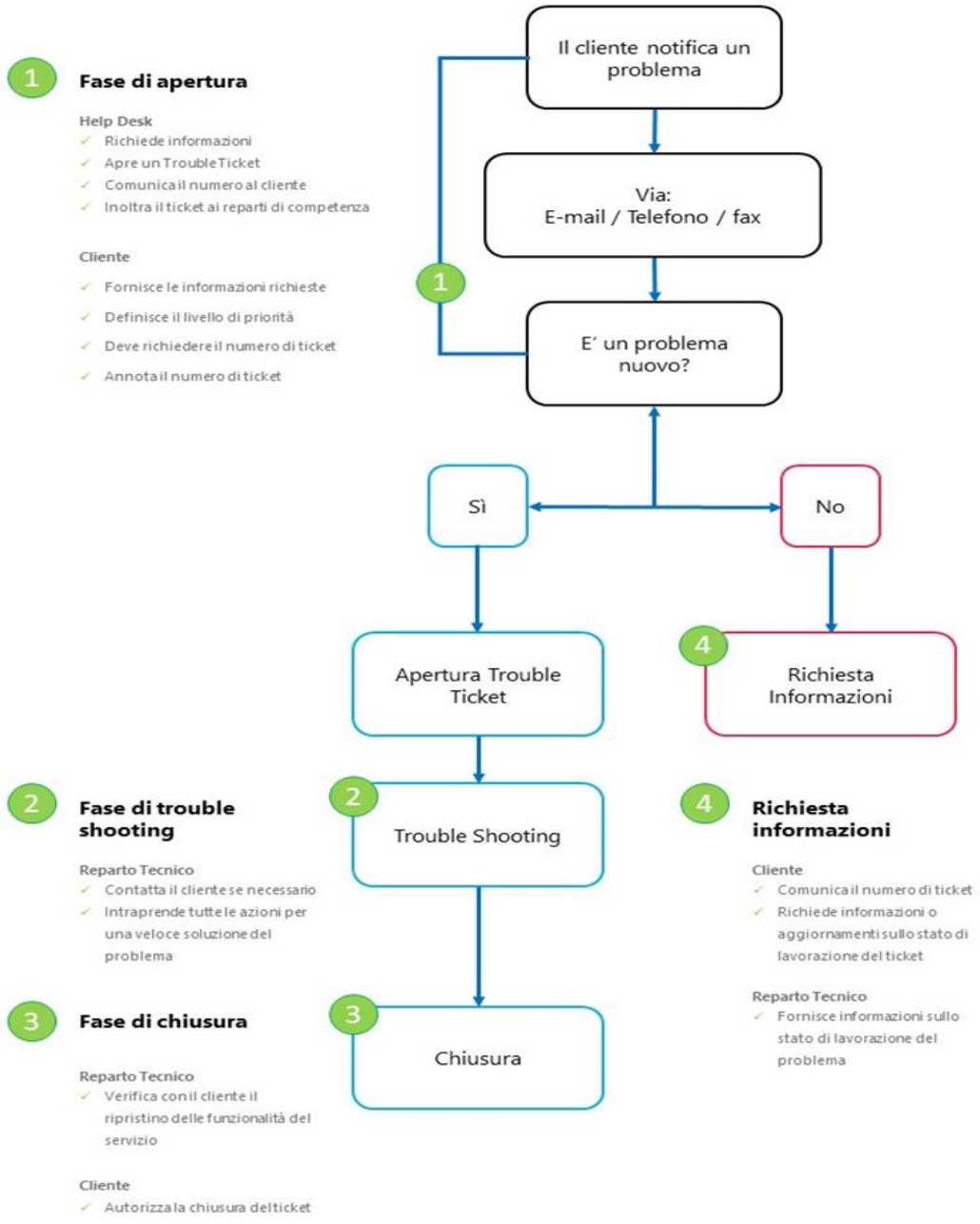
2.3.2. Extra Contratto

Nel caso in cui l'analisi/risoluzione della problematica oggetto della singola richiesta di assistenza non fosse compresa nei servizi di cui al presente contratto, Service Desk provvederà ad effettuare un'escalation verso AM e Area Delivery che valuteranno insieme al cliente eventuali interventi di CHANGE sulla infrastruttura del cliente stesso. Tali processi sono fuori perimetro rispetto al contratto Managed IT.

Tutte le attività eseguite saranno fatturate a consumo con modalità tempo e materiali, secondo le tariffe di cui al Paragrafo "Tariffe Servizi".

2.3.3. Schema gestione chiamata

Di seguito lo schema a blocchi della Gestione della chiamata.



2.4. SLA – Service Level Agreement

Di seguito riportiamo gli SLA attivabili per la gestione delle richieste di tipo INCIDENT:

SLA			Tempo Di Presa In Carico	Tempo Di Presa In Carico	Tempo Di Presa In Carico	Indici Sla
Criticità	**Impatto**	**Descrizione**	**Platinum**	**Gold**	**Silver**	**% presa in carico del problema**
Priorità 1 (Alta)	Bloccante	Fondamentale per il business e per il processo. Sistema di produzione bloccato (una funzionalità del sistema, vitale per il business, è preclusa. Non è possibile proseguire l'attività con altre funzioni o modalità operative)	2 Ore	4 ore	8 ore	80% Dei ticket entro il tempo previsto
						90% entro il tempo previsto + 2 ore
						100% entro il tempo previsto + 4 Ore
Priorità 2 (Media)	Non Bloccante (Grave)	Fondamentale per il processo ma non per il business. Problema semi-bloccante (alcune funzionalità sono precluse, la maggior parte del business è supportata)	4 ore	8 ore	16 ore	80% Dei ticket entro il tempo previsto
						90% entro il tempo previsto + 4 ore
						100% entro il tempo previsto + 8 Ore
Priorità 3 (Bassa)	Non Bloccante (Non Grave)	Non bloccante né per il business né per il processo. Problema generico (problema su di una specifica funzione che non preclude la normale operatività del sistema)	8 ore	16 ore	40 ore	80% Dei ticket entro il tempo previsto
						90% entro il tempo previsto + 8 ore
						100% entro il tempo previsto + 16 Ore

2.5. Disponibilità del servizio

Il servizio di assistenza è attivo nei seguenti periodi:

Periodo (Giorno/Ore)	22.00 – 05.59	06.00 – 8.59	09.00 – 17.59	18.00 - 21.59
Lunedì - Venerdì	H24	H24	BASE	H24
Sabato, Domenica e Festività	H24			

2.6. Modello organizzativo dei servizi

Con lo scopo di fornire il miglior servizio possibile abbiamo identificato questi ruoli all'interno della nostra organizzazione:

AM - Account Manager
Stato Avanzamento Lavori. Rappresenta il punto di escalation per il Cliente ed interviene su tematiche che necessitino di una revisione contrattuale del servizio e. Identifica il punto d'incontro tra esigenze tecniche ed economiche per le eventuali estensioni e modifiche del servizio
ATR – Account Technical Referral
È il responsabile ultimo di qualsiasi progetto proposto e rilasciato, e viene sempre consultato in caso di problematiche tecniche che dovessero emergere su progetti in corso o già conclusi. Pianifica ed effettua incontri periodici con il Cliente per verificare e discutere gli aspetti qualitativi dei servizi.
Partecipa a SAL periodiche, redige e presenta al Cliente i rapporti periodici sull' andamento dei servizi e fornisce eventuali chiarimenti sul contenuto. E' una figura che appartiene all'area tecnica di delivery e lavora a stretto contatto con l'account Manager. In dettaglio prevede:

- Gestione tecnica del cliente
- E' il referente per qualsiasi problema di carattere tecnico e operativo sul cliente
- E' il responsabile delle soluzioni tecniche proposte al cliente
- A ogni cliente viene assegnato un ATR (e solo uno)
- Lavora in sinergia con il AM di riferimento del cliente

2.7. Servizio di contact center

Il gruppo di Service Desk si fa carico di contattare e coordinare eventuali altri fornitori del cliente coinvolti in una problematica degli apparati e/o infrastruttura secondo le condizioni definite dal cliente con il fornitore.

L'attivazione di questo tipo di servizio è subordinata alla fornitura da parte del cliente di tutte le informazioni necessarie per contattare gli altri fornitori. Le informazioni dovranno esserci comunicate durante la fase di presa in carico dell'infrastruttura.

3. Startup e presa in carico

Si tratta di una attività fondamentale che verrà erogata presso il cliente dal nostro personale tecnico prima dell'avvio della fase a regime del servizio.
L'attività di Startup & presa in carico del Servizio ha come finalità la raccolta di tutte le informazioni necessarie per la piena comprensione dell'infrastruttura informatica del cliente quali:

- Architettura del sistema nel suo complesso;
- Informazioni di dettaglio su tutti gli apparati Hardware;
- Informazioni sulle configurazioni SW;
- Elenco analitico di tutti i servizi informatici operativi sui sistemi quali, a titolo esemplificativo, Mail, Web, Data Base, File Server, ecc.;
- Informazioni relative agli aspetti organizzativi e procedurali del cliente che siano rilevanti ai fini dell'assistenza sistemistica;
- Verifica dei prerequisiti per il collegamento da Remoto. Definizione delle modalità di accesso e rilascio delle relative credenziali di amministratore;
  Qualora, per policy aziendale non sia possibile rilasciare le credenziali di accesso le stesse (eventualmente temporanee) dovranno essere fornite per ottenere l'assistenza in caso di apertura di un ticket (e disabilitate dopo la chiusura del ticket) Ovviamente in questo caso non sara possibile effettuare assistenza di tipo Proattivo
  L'accesso remoto verrà reso operativo solo nel caso in cui il Cliente dovesse rilasciare per iscritto specifica autorizzazione in tal senso;
- Predisposizione dell'infrastruttura necessaria per consentire l'accesso remoto al sistema informativo del Cliente;
- Installazione (se previsto dal contratto) dei sensori sulle varie apparecchiature oggetto del contratto e che saranno oggetto della gestione Proattiva (se previsto dal contratto).

Nel corso della fase di Startup & presa in carico del Servizio verranno altresì valutati e concordati con i referenti tecnici i livelli di soglia a livello di ogni apparato sotto contratto che verrà successivamente configurato nel software di monitoraggio.
A tale proposito vi evidenziamo che e' possibile cambiare e/o ampliare i sensori e le relative soglie nel corso della durata del contratto mediante una comunicazione scritta
Le risultanze della fase di Startup & presa in carico del Servizio verranno inserite in un apposito documento che verrà sottoposto alla approvazione del cliente e costituirà il punto di riferimento per la configurazione, l'avviamento e l'erogazione dei vari servizi.

Il documento che verrà predisposto in fase iniziale con lo Start-Up e mantenuto nel tempo sulla base delle modifiche della infrastruttura del cliente conterrà le seguenti informazioni:

- Riferimenti del cliente (con l'indicazione delle persone che possono richiedere assistenza)
- Elenco degli apparati oggetto dell'assistenza con l'indicazione di:
  - Configurazioni Hw
  - Configurazioni Sw
- Elenco dei servizi oggetto dell'assistenza
- Sensori applicati e soglie di allarme
- Credenziali di accesso per i sistemi

4. Governo del contratto - Opzionale

In questo capitolo è definito il governo del Contratto in termini di comitati, ruoli, responsabilità ed attività che dovranno essere poste in essere per consentire un fattivo ed efficace espletamento dei Servizi previsti dal contratto.

Gli obiettivi sono i seguenti:

- indirizzare e verificare il complessivo e costante allineamento de cliente e di Computer Design sugli obiettivi strategici, contrattuali, operativi e sulla qualità dei Servizi;
- indirizzare l'adeguamento dei servizi in funzione dell'evoluzione delle tecnologie e delle esigenze di supporto alle operatività del cliente;
- garantire la conformità delle modalità di erogazione dei Servizi con i termini e le condizioni sottoscritte e definire i meccanismi di risoluzione delle criticità e di gestione dell'escalation;
- individuare le aree di miglioramento e attivare le relative azioni.

4.1. Modello Organizzativo

Il Modello Organizzativo per il Governo del Contratto prevede i seguenti organismi decisionali:

- Steering Committee;
- Operating Committee.

Nelle tabelle che seguono è riportata la descrizione di ciascun organismo di governo, che dovrà essere posto in essere al fine di assicurare il Governo delle attività.

Steering Committee	
Ruolo	Lo Steering Committee ha la funzione di indirizzo strategico e supervisione complessiva del rapporto contrattuale tra le Parti.
Componenti	Il cliente definirà una figura che avrà il ruolo di Responsabile dello Steering Committee. Il responsabile dello steering Committee è anche il responsabile del contratto da parte del cliente. Computer Design nominerà una figura di riferimento (Contract Manager) che, per tutta la durata del Contratto, sarà espressione della più alta capacità decisionale di Computer Design nell'ambito del Contratto e avrà la responsabilità della conduzione e del coordinamento dell'erogazione dei Servizi.

Competenze	È competenza dello Steering Committee:
	• affrontare le tematiche organizzative e strategiche inerenti i Servizi fornendo le linee guida per l'esecuzione ed evoluzione dei Servizi;
	• valutare le opportunità di evoluzione e cambiamento dei Servizi (fermo restando le necessarie approvazioni formali); nello specifico:
	  ○ valutazione delle proposte di modifica da apportare al contratto richieste dalle Parti o che si rendessero opportune ai sensi del contratto, ivi inclusi termini dell'esercizio del diritto da parte del cliente di estendere la durata del contratto;
	  ○ evoluzione / aggiunta / eliminazione di Servizi;
	• valutare e verificare il rispetto dei volumi e dei costi individuati per la determinazione dei corrispettivi (Canone Annuo) in relazione ai cambiamenti del Parco Target e delle coperture contrattuali in termini di garanzia/manutenzione;
	• verificare le eventuali penali;
	• proporre e condividere le evoluzioni applicabili al perimetro dei Servizi;

	• ratificare l'avvio di attività supplementari di Supporto Specialistico richieste dalla Funzione ICT o dalle strutture di Business del cliente; • sui termini contrattuali, esaminare le controversie attinenti alla sua interpretazione, la sua applicazione/esecuzione e le obbligazioni ivi contenute, in particolare quelle non risolte che dovessero insorgere nell'ambito dell'Operating Committee, nonché l'individuazione delle azioni atte alla risoluzione delle controversie.
Frequenza	Lo Steering Committee, presieduto e coordinato dal Responsabile, si riunirà trimestralmente o, in caso di eventi straordinari, su richiesta scritta di una delle Parti non oltre 5 (cinque) giorni dal ricevimento della richiesta. Saranno programmate almeno 4 (quattro) riunioni annuali di cui: • una da tenersi almeno 1 (un) mese prima della fine di ogni anno di erogazione della fornitura, avente ad oggetto la pianificazione delle attività nonché i termini di evoluzione del Parco Target per l'anno successivo; • una da tenersi entro 3 (tre) mesi successivi la chiusura di ogni anno di erogazione dei Servizi rilevante ai fini del pagamento del canone, avente ad oggetto la determinazione del consuntivo economico dell'anno precedente. Alle riunioni dello Steering Committee potranno essere invitati ad intervenire persone il cui contributo sia ritenuto necessario in relazione agli argomenti dell'ordine del giorno.

Operating Committee	
Ruolo	L'Operating Committee è responsabile della gestione ordinaria dei Servizi.
Componenti	L'organismo è composto dai Responsabili dei Servizi identificati del cliente e dai Responsabili Operativi che Computer Design individuerà per ambito di Servizi.
Competenze	È di competenza dell'Operating Committee: • pianificare e controllare le attività operative • supervisionare l'adempimento delle obbligazioni previste nel Contratto tra Computer Design ed il Cliente e, in particolare, della qualità dei Servizi erogati nel rispetto degli SLA analizzandone il loro andamento nel tempo; • quantificare le eventuali penali; • individuare eventuali opportunità di variazioni o integrazioni applicabili al Perimetro dei Servizi da proporre allo Steering Committee; • analizzare le esigenze di acquisto di asset tecnologici; • identificare opportunità di miglioramento sull'utilizzo delle tecnologie in uso durante il periodo contrattuale e sulla loro possibile evoluzione; • svolgere la valutazione di la fattibilità tecnica e relativa formulazione per evoluzioni tecnologiche ed organizzative da proporre allo Steering Committee; • effettuare la pianificazione tecnica per le eventuali attività supplementari di Supporto Specialistico richieste dalla Funzione; • risolvere eventuali controversie nell'ambito dell'ambito dell'applicazione del Contratto ed eventualmente attivare l'escalation allo Steering Committee; • predisporre i report di servizio per lo Steering Committee relativi ad esigenze e problematiche operative; • verificare il rispetto delle politiche per la sicurezza delle informazioni e dei Sistemi Informatici; • promuovere le iniziative per potenziare la protezione e la riservatezza delle informazioni; • revisionare e controllare le eventuali attività relative a qualsivoglia cambiamento tecnologico e/o organizzativo; • assicurare che le comunicazioni fra le Parti siano continuative e sufficienti;

	• attivare i team di lavoro che, a fronte del verificarsi di eventi eccezionali, individuino e indirizzino la soluzione del problema; • approvare le soluzioni ed il delivery.
Frequenza	Il meeting di gestione dei servizi (Stato Avanzamento Lavori - SAL) si riunirà con frequenza almeno mensile o su richiesta. Alle riunioni di gestione dei servizi potranno essere invitati ad intervenire persone il cui contributo sia ritenuto necessario in relazione alla discussione.

4.2. Processi di Governance

Di seguito vengono descritti i principali processi di Governance che regolamentano la gestione dei rapporti fra il cliente e Computer Design.

Gli organismi di Governance gestiranno i seguenti processi principali:

A. Gestione delle penali
B. Gestione dei problemi
C. Comunicazioni
D. Procedura di escalation

Di seguito è descritto ciascun processo in termini di procedure da seguire e coinvolgimento degli organismi di Governance.

4.3. Gestione delle Penali

L'Operating Committee esaminerà, mensilmente in meeting di SAL, i report di misurazione degli SLA, al fine di verificare l'applicazione di penali causate dalle eventuali violazioni dei LdS previsti e ne farà opportuna annotazione in apposito verbale con indicazioni di eventuali disaccordi emersi tra le Parti.

Il Responsabile del Cliente per il Contratto consuntiverà le eventuali penali maturate a carico di Computer Design.

In caso di contestazione delle penali da parte di Computer Design, sarà avviata la procedura di escalation presso lo Steering Committee.

4.4. Gestione dei Problemi

Entrambe le Parti dovranno essere diligenti e cooperare in modo efficace, efficiente e professionale nella risoluzione di conflitti, problemi o dispute che potrebbero sorgere durante lo svolgimento del contratto o dopo la cessazione dello stesso relativamente ad un qualsiasi aspetto del Contratto.

Al sorgere di un qualsiasi problema, che abbia degli effetti sulle prestazioni concordate e/o che rappresenti impedimento alle attività del cliente, Computer Design dovrà:

- informare tempestivamente il Responsabile del Servizio del Cliente;
- identificare nel minor tempo possibile l'inconveniente e le possibili cause;
- apportare nel minor tempo possibile le correzioni necessarie.

4.5. Comunicazioni

Saranno costituiti specifici riferimenti telefonici e di posta elettronica.

Ogni comunicazione tra le Parti che abbia effetti ai fini del Contratto sarà disciplinata da quanto stabilito e concordato in fase di avviamento dei Servizi in termini di strumenti e protocolli trasmissivi.

Resta inteso che le comunicazioni di tipo operativo e informativo che non abbiano effetti ai fini del Contratto potranno essere effettuate anche tramite solo posta elettronica.

4.6. Procedura di Escalation

Le eventuali controversie che dovessero sorgere nel corso dello svolgimento del Contratto in merito all'erogazione del servizio e/o all'interpretazione del Contratto dovranno essere oggetto di un tentativo di soluzione condivisa come segue:

- all'insorgere di una controversia la Parte interessata dovrà comunicare all'Altra l'inconveniente e chiedere l'applicazione della procedura di escalation del problema;
- l'Operating Committee si dovrà riunire al più presto possibile al fine di avviare il processo di analisi della controversia con lo scopo di identificare la soluzione dello stesso.

Qualora non si raggiunga in tempi brevi, ed al massimo entro una settimana, un accordo soddisfacente per entrambe le parti, il problema sarà sottoposto allo Steering Committee che ricercherà la soluzione.

Se anche in questo caso, entro 10 (dieci) giorni lavorativi non si giungesse ad una soluzione del conflitto si dovrà far riferimento a quanto definito dalle condizioni de contratto stesso.

4.7. Audit

Il cliente ha facoltà di organizzare degli Audit (verifiche Ispettive) al fine di verificare il corretto svolgimento di quanto previsto contrattualmente.

Obiettivo del presente paragrafo è descrivere e regolamentare il processo di gestione degli Audit adottato dal Cliente nei confronti di Computer Design.

Inoltre, sempre in ambito audit, qualora il Cliente venga sottoposta a Verifiche Ispettive di Terze Parti, Computer Design potrà essere coinvolta dal Cliente per quanto attiene alle attività di propria competenza e dovrà mettere a disposizione il proprio personale e tutto quanto necessario per il corretto svolgimento della Verifica Ispettiva esterna.

Il criterio di attivazione del processo è costituito dalle esigenze del Cliente di verifica in relazione a quanto previsto contrattualmente nell'ambito dell'esecuzione delle attività di competenza di Computer Design; nella tabella che segue sono riportate le definizioni delle voci più rilevanti nel processo:

Audit	
Rilevazione	Anomalia o non completo soddisfacimento rispetto ai requisiti contrattuali e normativi
Azione Correttiva	Azione identificata per correggere quanto evidenziato a seguito di una Rilevazione.

Di seguito sono descritte le attività che costituiscono il processo di Audit:

A. **Predisposizione piano delle Verifiche Ispettive e comunicazione a Computer Design.** Il Cliente può prevedere delle visite ispettive. In caso di verifiche ispettive il cliente deve dare comunicazione a Computer Design almeno 30 gg prima identificando le eventuali competenze di supporto necessarie all'effettuazione delle Verifiche Ispettive.
B. **Esecuzione delle Verifiche Ispettive**. Il Cliente provvederà ad organizzare la Verifica Ispettiva, definire il Gruppo di Auditor, che può essere composto da strutture interne o da fornitori specializzati (che saranno identificati secondo necessità tra fornitori di comprovata esperienza in ambito audit), predisporrà eventuali check list di supporto e si accorderà preventivamente con Computer Design in merito alle modalità e alla data di svolgimento delle Verifiche Ispettive. Il Gruppo di Auditor effettuerà le Verifiche Ispettive sulla base di quanto concordato. Computer Design durante le Verifiche Ispettive dovrà rendere disponibile quanto necessario. Si specifica inoltre che:

    a. le verifiche che debbano coinvolgere le sedi di Computer Design saranno organizzate in maniera tale da non costituire impedimento ad attività estranee all'oggetto del contratto;
    b. in ogni caso, l'Audit garantirà la riservatezza delle informazioni aventi carattere industriale e commerciale di Computer Design.

A. **Redazione e invio del verbale a Computer Design**. A conclusione delle Verifiche Ispettive il cliente redigerà il verbale di verifica, annotando le eventuali rilevazioni riscontrate, e lo invierà per condivisione a Computer Design e per conoscenza ai comitati identificati nel Modello Organizzativo.
B. **Definizione delle azioni correttive e invio al Cliente**. Sulla base delle eventuali rilevazioni emerse e condivise, Computer Design dovrà individuare e definire le azioni correttive opportune, le responsabilità e le tempistiche di esecuzione delle stesse e provvedere a trasmetterle al Cliente per verifica ed accettazione. Il Cliente, qualora Computer Design non rispetti i tempi concordati per la definizione e l'invio delle azioni correttive, si riserverà di valutare eventuali azioni nei confronti della stessa.
C. **Accettazione delle azioni correttive e comunicazione a Computer Design**. A fronte delle azioni correttive definite, il Cliente verificherà la coerenza tra le rilevazioni evidenziate e gli interventi proposti a Computer Design, risolvendo eventuali problematiche e/o richiedendo i chiarimenti necessari. Il Cliente, nel caso di valutazione positiva delle azioni ed i tempi proposti da Computer Design, ne comunicherà l'accettazione.
D. **Implementazione delle azioni correttive**. A fronte delle azioni accettate dal Cliente, Computer Design dovrà implementare le attività con le modalità concordate e nei tempi prestabiliti.
E. **Verifica e chiusura delle azioni correttive**. Il Cliente, in base alle tempistiche d'implementazione delle azioni definite, verificherà gli stati di avanzamento e l'efficacia delle stesse. Computer Design dovrà comunicare al Cliente la chiusura delle attività implementative; Il Cliente, quindi, qualora le azioni correttive adottate da Computer Design abbiano eliminato non solo gli effetti, ma anche le cause che hanno portato al manifestarsi delle rilevazioni, dovrà formalizzare la chiusura delle rilevazioni tramite apposito verbale. Il Cliente, qualora Computer Design non rispetti i tempi concordati per le implementazioni delle azioni correttive, si riserverà di valutare eventuali azioni nei confronti dello stesso.
F. **Invio verbale di chiusura a Computer Design**. Verificata positivamente l'efficacia delle azioni e redatto il verbale di chiusura delle stesse, il Cliente notificherà la chiusura a Computer Design.

5. Servizi di monitoraggio – Opzionale

Il Team Service Desk è in grado di controllare e gestire da remoto in tempo reale l'intera infrastruttura del Cliente per mezzo di una propria soluzione di monitoraggio automatico basato su tecnologia PRTG (AerMonitor).

Il servizio (se previsto da contratto) prevede la fornitura di una piattaforma CLOUD per il monitoraggio delle infrastrutture IT. La piattaforma è in grado di monitorare la maggior parte degli apparati collegati alla rete del cliente (server, client, switch, router, ecc.) e fornire la reportistica periodica degli eventi rilevati. Il monitoraggio automatico prevede il controllo del corretto funzionamento dell'infrastruttura IT del cliente su base H24, con l'eventuale segnalazione di un malfunzionamento verso il servizio di SPoc/TSC, in base alle regole d'ingaggio definite con il cliente.

La piattaforma è messa a disposizione dei clienti all'interno del servizio stesso (Managed IT service). La definizione delle soglie di attenzione sarà concordata congiuntamente in fase di Startup & presa in carico del Servizio, mentre l'implementazione sul sistema di monitoraggio sarà effettuata dal personale tecnico di CD in fase di avviamento del servizio.

A fronte dell'adozione dei nostri servizi di supporto (Managed IT service) saranno abilitati una serie di sensori (contrattualmente stabiliti) che hanno il compito di segnalare tempestivamente al nostro SPoC le anomalie che emergono. Verrà installato un PROBE (piccolo agente software) che avrà il compito di raccogliere tutte le segnalazioni provenienti dai sensori locali ed inviarle al sistema di monitoring in CLOUD (console). La modalità di installazione del Probe sarà concordata con il cliente in fase di Startup & presa in carico del Servizio.

La rilevazione di un'anomalia potrà dare seguito all'intervento di assistenza sistemistica, qualora la stessa rientra nel perimetro dell'offerta. Nel caso l'alert evidenzi una criticità non coperta dal servizio di assistenza proposta, la segnalazione sarà inoltrata al Cliente affinché lo stesso venga informato tempestivamente e possa dare corso a idonee azioni correttive. Il cliente in ogni casa avrà accesso alla console per potere verificare direttamente lo stato dei sensori.

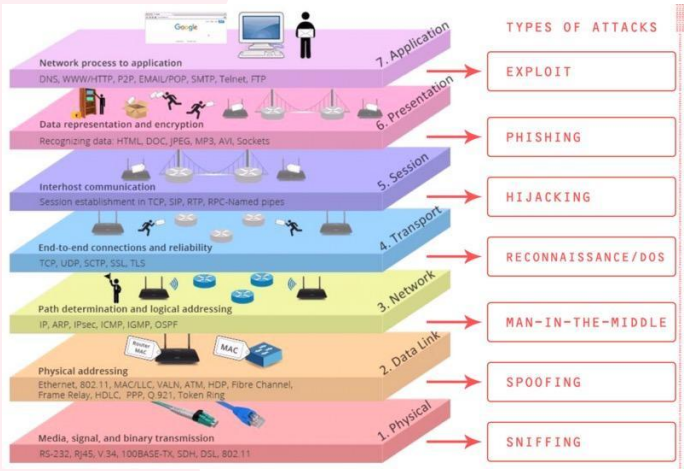
Il servizio di monitoraggio di base prevede l'installazione di Agent sia sui server che sui personal computer oggetto dell'assistenza. In caso di necessità particolari del cliente è possibile prevedere una configurazione specifica dei sensori. In questo abbiamo bisogno di avere una visione dettagliata delle esigenze del cliente, in modo tale da poter quantificare correttamente l'effort e la relativa quotazione. Il dettaglio puntuale del Servizio sarà comunque definito all'interno del servizio di presa in carico che verrà redatto tra le parti in fase di Startup & presa in carico del Servizio.
Configurazione standard dei sensori del sistema di monitoraggio:

- Per i Server è previsto il monitor dei seguenti parametri
  - Accesso / Spento
  - Hardware /Software Inventory
  - Parametri Vitali per il server
  - Qual ora si decida monitorare/gestire ulteriori parametri, gli stessi dovranno essere prestabiliti e concordati.
- Per i Personal Computer è previsto il monitor dei seguenti parametri
  - Hardware /Software Inventory
  - Qual ora si decida monitorare/gestire ulteriori parametri, gli stessi dovranno essere prestabiliti e concordati.
- Per le apparecchiature di Rete è previsto il monitor dei seguenti parametri
  - Accesso / Spento
  - Raggiungibilità
  - SNMP (se attivo e disponibile)
  - Qual ora si decida monitorare/gestire ulteriori parametri, gli stessi dovranno essere prestabiliti e concordati.

6. Vulnerability Assessment - Opzionale

In linea generale si definisce **vulnerabilità** la caratteristica di un componente di un qualsiasi sistema di presentare assenti, ridotte o compromesse misure di sicurezza contro attacchi, usi impropri o dannosi; il componente vulnerabile rappresenta un punto debole del sistema perché consente a un eventuale aggressore di compiere azioni di danneggiamento parziale o totale. La **valutazione delle vulnerabilità** (o ***Vulnerability Assessment***) è il processo di identificazione, quantificazione e classificazione delle gravità delle vulnerabilità presenti in un qualsiasi sistema focalizzandosi sia sul rischio per il singolo componente che su quello che viene indotto al resto del sistema circostante.

Nell'ambito delle tecnologie ICT, il ***Vulnerability Assessment*** (**VA**) è in particolare il processo di valutazione delle vulnerabilità e dei relativi rischi di sfruttamento presenti nelle reti di computer, sistemi, hardware, applicazioni e altri enti dell'infrastruttura ICT ad ogni livello fisico e logico poiché, come è noto, ogni strato della pila ISO/OSI è suscettibile di essere attaccato mediante tecniche specifiche. Il **VA** è da considerarsi un'attività fondamentale nell'esercizio di una rete informatica sia alla luce delle normative di conformità richieste alle organizzazioni che, ancor prima, nello svolgimento efficiente delle operazioni aziendali.



Il cuore di un **VA** è un'**analisi automatizzabile** che assegna un livello di rischio a ciascuna vulnerabilità in base a precisi standard come il CVSS (*Common Vulnerability Scoring System*), facilmente interpretabile perché la formula su cui è basata la valutazione fornisce per ogni ente analizzato un risultato oggettivo da 0 a 10 dove il valore 10 indica il massimo rischio: a questa analisi possono anche essere correlati in modo personalizzato parametri di priorità, urgenza e impatto che indicano la dipendenza delle funzioni aziendali dalle risorse affette per permettere di concentrarsi dapprima su quelle vulnerabilità che, se sfruttate, potrebbero creare il maggior numero di problemi per l'organizzazione.

Questa è una parte importante della gestione delle vulnerabilità perché, essendo limitati il tempo e le risorse a disposizione del team di sicurezza ICT, nello svolgimento delle operazioni di consolidamento che costituiscono il ***Remediation Plan*** **(RP)** il team stesso dovrà concentrarsi sulle risorse che potrebbero subire il maggior disservizio con i maggiori danni indotti e allo stesso tempo scegliere consapevolmente di accettare la continuità dei rischi minori differendone la risoluzione.

Riassumendo e focalizzando i punti fondamentali, la valutazione delle vulnerabilità e il piano di consolidamento garantiscono a un'organizzazione i seguenti vantaggi:

- Identificazione tempestiva e coerente dei rischi e delle minacce;
- Pianificazione ed esecuzione di azioni correttive con la adeguata priorità;
- Protezione dei sistemi da accessi non autorizzati e da compromissioni dei dati;
- Ottemperanza alle esigenze di conformità sia in generale che per settori specifici (ad esempio GDPR, HIPAA e PCI DSS).

Verrà prodotta la seguente documentazione:

- Output integrale dello strumento di scansione con le note per una corretta interpretazione;
- Presentazione riassuntiva dei risultati ottenuti dall'analisi delle vulnerabilità con evidenza degli stati di crisi;
- Proposta Tecnico/economica per la mitigazione puntuale delle vulnerabilità evidenziate nel report

- Proposta Tecnico/economica per un contratto di patching e update gestito. Questo servizio permette di avere costantemente aggiornata la proposta infrastruttura con le patch e le vulnerabilità riconosciute. Ad ogni ciclo di aggiornamento sarà eseguita una VA per certificare lo stato dell'infrastruttura.

6.1. Fase di analisi (Assessment):

Tra le metodologie per l'esecuzione delle valutazioni di vulnerabilità la più efficace in termini di tempo e costi è l'analisi tramite un software di scansione automatica corredato di un database di vulnerabilità note: esso viene configurato per analizzare in modo completo ogni ente dell'infrastruttura in esame, eseguendo diversi tipi di scansioni con o senza credenziali note, dall'interno della rete e/o dall'esterno. Il software garantisce un'elevata efficacia grazie a un frequente aggiornamento del proprio database, riduce al minimo l'evidenza di falsi positivi e falsi negativi nei rilevamenti e fornisce risultati sia fruibili senza post-processo in termini di valore CVSS che eventualmente integrabili con altre fonti dati e/o considerazioni soggettive per analisi ulteriormente personalizzate.

6.2. Fase di consolidamento (Remediation):

L'attività di VA deve essere completata con l'esecuzione delle operazioni di consolidamento delle vulnerabilità scoperte che dipende dalla natura di ciascuna risorsa vulnerabile: ad esempio firmware di un hardware, sistema operativo di un computer, topologia della rete ecc. e in linea generale deve interessare i seguenti punti:

a. **Connettività Internet** – Anche assumendo che il firewall perimetrale sia di tecnologia recente e ben configurato, è noto che attraverso di esso vengono esposti dei servizi ben definiti (ad esempio web server di front-end, mail transfer agent, server VPN ecc.) ma la cui invulnerabilità a connessioni dannose deve essere verificata. D'altra parte l'esposizione di altri servizi effettuata da personale non competente per risolvere un'esigenza di connettività senza tenere conto della sicurezza (esempio: porta RDP aperta verso l'esterno) mette a grave rischio la rete aziendale, quindi occorre verificare dall'esterno e sanare queste configurazioni.
b. **Accessibilità fisica degli apparati e dei cablaggi** – La protezione contro gli accessi non autorizzati agli apparati e ai cablaggi è un'attività logistica che persegue la segregazione ordinata degli apparati di rete in locali ad accesso riservato ed eventualmente controllato, protetti contro eventi dannosi (es. allagamenti, incendi), la collocazione dei cablaggi in canalizzazioni specifiche ed eventualmente la rimozione fisica o logica delle permutazioni sui punti rete cablati ma non utilizzati.
c. **Accessibilità logica dei punti rete cablati e della rete wireless** - Gli aspetti di accessibilità wired e wireless evidenziano la necessità di adottare un sistema di Network Access Control (NAC) per garantire che un endpoint non preventivamente autorizzato possa essere connesso alla rete aziendale. Questo è tanto più importante nel caso della rete wireless il cui segnale può essere captato anche all'esterno delle mura aziendali, ma anche per i punti rete fisici a cui potrebbero essere connessi device BYOD o di personale esterno all'azienda (es. consulenti, fornitori, ecc…).
d. **Aggiornamento dei software di base e applicativi di tutti i computer -** A causa del numero di computer presenti in azienda e del loro stato di manutenzione informatica è ben noto che l'operazione principale di consolidamento delle vulnerabilità è un efficace periodico patching. Essa non può essere demandata al singolo operatore ma deve essere gestita in modo organico tramite un apposito software che eventualmente permetta di soddisfare ulteriori necessità del team ICT, come l'inventario delle risorse hardware e software, l'accesso remoto per teleassistenza, la distribuzione di sistemi operativi e di applicazioni, la riconfigurazione automatica.
e. **Aggiornamento dei firmware degli apparti legacy** – le operazioni vengono svolte in genere mediante strumenti proprietari del singolo vendor oppure tramite strumenti di Operation Management orizzontali dotati di un ampio database di apparati gestibili.
f. **Corretta configurazione dei servizi pubblicati dai computer e in particolare dai server –** i servizi segnalati come vulnerabili dallo strumento di scansione non per problemi software ma perché non si sono adottate delle

misure minime di sicurezza devono essere riconfigurati secondo le best practices suggerite dallo strumento di analisi.

6.3. Ciclo di valutazione delle vulnerabilità e loro consolidamento:

Come avviene per tutti i processi di miglioramento della qualità, l'attività di analisi delle vulnerabilità e della loro successiva risoluzione deve essere effettuata ciclicamente essendo in continua evoluzione tecnologica sia l'infrastruttura informatica che le possibili tecniche di attacco, in quanto ogni risorsa è suscettibile di presentare vulnerabilità non prevedibili a priori. Si configura pertanto la seguente serie di azioni:

1. **Identificare tutte le risorse informatiche della rete** – Attraverso un'intervista verranno identificati gli intervalli di IP da analizzare e ottenuto l'inventario delle risorse hardware, possibilmente organizzato in uno schema fisico e logico della rete. L'inventario permette un controllo incrociato con le risorse rilevate dallo strumento di scansione in modo da accertarsi che tutte le risorse siano state analizzate e che non ce ne siano di inaccessibili.
2. **Scoprire le vulnerabilità e le minacce potenziali a cui le risorse sono soggette** – Questa operazione altamente ed efficientemente automatizzabile viene eseguita come già detto mediante specifici software di analisi che provvedono ad interrogare gli intervalli di IP segnalati, identificare le risorse con porte in ascolto, accedere alle medesime sia attraverso credenziali fornite a priori e/o tramite tentativi di hacking (effettuando quindi anche un Penetration Test) e identificare i servizi accessibili, le versioni e le loro vulnerabilità tramite interrogazione del proprio database, continuamente aggiornato. Il software di analisi crea una esaustiva reportistica su numero, livello, gravità delle vulnerabilità segnalando mediante una graduatoria di valori CVSS quelle più frequenti e/o pericolose.
3. **Analizzare e sintetizzare i risultati ottenuti per la loro comprensione immediata** - La reportistica ottenuta automaticamente dal software può essere filtrata al grado di dettaglio desiderato per essere sottoposta alle gerarchie aziendali: in questa fase si vuole evidenziare agli Executive una macro-analisi del grado di vulnerabilità e di compromissione dell'infrastruttura.
4. **Assegnare a ogni risorsa un peso proporzionale all'impatto causato dalla sua indisponibilità** – è possibile in seguito assegnare soggettivamente a ogni risorsa un peso proporzionale all'impatto sulla produttività aziendale dovuto alla indisponibilità della stessa, che permette di meglio definire la criticità ai fini del business delle risorse censite. Il peso è tanto maggiore quanto la risorsa gestisce attività legate al core business aziendale piuttosto che ad attività collaterali e di supporto, quanto la risorsa sia un single point of failure o sia ridondata, quanto dalla disponibilità di questa risorsa ne dipendano altre.
5. **Valutare la probabilità che le vulnerabilità possano essere sfruttate** - Si analizzano le vulnerabilità a partire dalle più frequenti e/o pericolose e, in base alla loro sfruttabilità da parte di un exploit in funzione della posizione della risorsa in rete, si affina il risultato del software di analisi per determinare la probabilità di attacco reale alla risorsa. Il software di analisi infatti non è a conoscenza del fatto, ad esempio, che una vulnerabilità grave scoperta in una risorsa appartenente a un intervallo di IP "blindato" possa non essere sfruttabile perché la risorsa affetta non è accessibile da altri intervalli di IP e questa informazione è quindi funzione della topologia della rete e del suo grado di accessibilità.
6. **Definire una matrice di rischio delle risorse basata su probabilità e impatto delle minacce -** Si incrociano i dati ottenuti in tutte le fasi precedenti sulle occorrenze delle vulnerabilità, sul loro grado di pericolosità e sull'impatto che un disservizio sulle risorse affette avrebbe sull'attività aziendale per generare una matrice di rischio che evidenzia la priorità delle risorse a cui applicare le operazioni di consolidamento.

MATRICE DELLA VALUTAZIONE DEL RISCHIO					
Altamente probabile 5	5	10	15	20	25
Molto probabile 4	4	8	12	16	20
Probabile 3	3	6	9	12	15
Poco probabile 2	2	4	6	8	10
Improbabile 1	1	2	3	4	5
Probabilità / *Impatto*	Marginale 1	Minore 2	Soglia 3	Serio 4	Superiore 5

NOTA: Esempio di matrice, righe e colonne possono essere aumentate/diminuite in funzione del grado di dettaglio con cui i sw tipizzano le vulnerabilità. La matrice dovrebbe essere tridimensionale (Frequenza, Probabilità, Impatto) ma Frequenza+Probabilità è un parametro già generato dal sw di scansione al punto 2 mentre l'impatto è un fattore discrezionale secondo il punto 4.

7. **Proporre una raccomandazione tecnico/economica per la mitigazione del rischio** – In base alla graduatoria della gravità delle vulnerabilità è possibile definire gli interventi da effettuare e, grazie ai dettagli crescenti degli output del software di analisi, valutare l'entità delle azioni correttive (riconfigurazioni di servizi, aggiornamenti di firmware, installazione di patch, modifica della topologia della rete ecc…), il tempo necessario all'esecuzione e la sua quantificazione economica.
8. **Applicare le azioni correttive** – Si procede nel piano di applicazione delle misure correttive determinate secondo le priorità e le tempistiche definite, vengono rilasciati periodicamente al cliente gli stati di avanzamento dell'attività e vengono valutati di volta in volta gli eventuali vincoli non prevedibili che verranno risolti in corso d'opera.
9. **Validare la soluzione mediante una nuova analisi delle vulnerabilità** - Al termine delle operazioni di consolidamento delle risorse si esegue una nuova analisi delle vulnerabilità per dimostrare la diminuita esposizione delle risorse a possibili attacchi e il miglioramento della qualità generale dell'infrastruttura ICT.
10. **Stabilire la data di esecuzione di un nuovo ciclo** – La ciclicità del processo descritto è palese essendo lo stato dell'infrastruttura ICT non statico ma in continua evoluzione tenendo conto dell'introduzione in rete di nuove risorse hardware e software non precedentemente analizzate, della scoperta di nuove vulnerabilità nei software già presenti e dell'introduzione di altre vulnerabilità per installazione di nuovi software, del grado di aggiornamento tecnologico delle risorse, dell'obsolescenza delle risorse mantenute in esercizio anche oltre la data di fine supporto. Il ciclo verrà ripetuto a distanza di un tempo congruo; possibili intervalli sono: trimestre, semestre, anno in funzione dell'ampiezza dell'infrastruttura da monitorare e della sua evoluzione.

6.4. Vulnerability Assessment – Prima Elaborazione

Per poter implementare correttamente tale processo di controllo e' necessaria una prima fase di elaborazione per identificare e sistemare tutte le situazioni critiche e partire da una situazione infrastrutturale stabile.

6.5. Vulnerability Assessment –Elaborazioni Successive

Dopo esecuzione e sistemazione di quanto evidenziato nella prima ELABORAZIONE e' possibile schedulare periodicamente (Normalmente ogni mese dopo l'applicazione di patch) l'elaborazione di tale servizio così da ottenere un report che evidenzi lo stato dell'infrastruttura aggiornato.

7. Patch Management - Opzionale

Applicare le patch è una esigenza di tutte le organizzazioni: questo, tuttavia, è un processo che rischia di creare non pochi problemi, se non gestito adeguatamente. E' indispensabile predisporre processi e procedure corrette al fine di assicurare un aggiornamento ottimale del sistema garantendo la sicurezza delle informazioni e la loro disponibilità.

Oltre a ciò, è importante evidenziare che l'aggiornamento dei sistemi essendo una attività complessa dove non può essere garantita in nessun caso la correttezza e coerenza dell'aggiornamento nell'ambiente software presente nel sistema aggiornato. Tutto questo è quasi impossibile da realizzare se non con l'aiuto di uno strumento software in grado di gestire tutti gli step operativi del processo di patching: verifica patch disponibili, approvazione patch, deploy, reportistica.

Per agevolare i nostri clienti nella gestione di uno dei processi più complessi ma fondamentale per il mantenimento di un livello minimo di sicurezza, abbiamo predisposto il servizio di Patch Management come estensione del contratto di Management IT. In dettaglio il servizio è cosi strutturato:

- Verifica e/o fornitura di una soluzione SW per analisi e gestione delle patch installabili sull'infrastruttura del cliente;
- Creazione di policy per l'installazione automatica delle patch per i sistemi previsi;
- Predisposizione mensile del report con le patch/aggiornamenti installabili in base alla tipologia dei sistemi (Critici, Non Critici, Client, Switch, Firewall, ecc.).

7.1. Contesto di riferimento

Il processo di patching è un processo molto critico e bisogna mettere particolare attenzione su diversi aspetti sia tecnici che organizzativi. In dettaglio si evidenza che:

- **Impatto**: l'installazione di patch o aggiornamenti hanno impatti diretti o indiretti su sistemi afferenti a diversi domini aziendali, per ognuno dei quali è necessario considerare diversi ruoli:
  - Chi autorizza gli interventi
  - Chi può realizzare l'intervento ottimizzando le risorse impiegate
  - Chi deve essere informato degli interventi
  - Chi verifica che il sistema aggiornato sia perfettamente funzionante

- **Rischi**: i sistemi affetti da vulnerabilità possono essere protetti da altri sistemi di sicurezza e quindi non esporre il Cliente a effettivi rischi, questa indicazione permette di impostare le corrette priorità per la fase di aggiornamento e messa in sicurezza dei sistemi.
- **Processo**: è necessario prevedere tutte quelle procedure che in caso di problemi consente di "ripristinare" una situazione corretta e coerente (RollBack).

L'attività di Patching e' sostanzialmente composta da diverse fasi distinte e consecutive:

A. **Salvataggio Ambiente** – e' cura del cliente mettere in atto tutte quelle procedure che in caso di problemi consente di "ripristinare" una situazione corretta e coerente (se viene espressamente richiesto il backup o soluzione equivalente come lo snapshot potrà essere effettuato direttamente da Computer Design prima dell'inizio dell'attività di Patching)
B. **Patching** – Applicazione delle modifiche/patch concordate
C. **Test CD** - Riavvio dei sistemi e Test di base effettuati dal personale CD
D. **Test Cliente** - Al completamento della fase di aggiornamento il cliente deve necessariamente effettuare tutti i test che ritiene indispensabili (applicativi e non).

E. **Rilascio dei sistemi** – Il sistema aggiornato verrà rilasciato e considerata chiusa la fase di aggiornamento solo dopo che il sistema ha superato tutti i test (CD e/o Cliente).
F. **Roll Back** - In caso di non superamento dei test o su specifica indicazione del cliente verrà effettuata la fase di Roll-Back del sistema all'ultimo backup disponibile. L'esito dell'attività di aggiornamento sarà riportato su apposito verbale ci chiusura attività.
G. **Vulnerability Assessment** – Al completamento della fase di Patching, nel caso in cui il cliente abbiamo sottoscritto questo servizio, verrà effettuata una attività di Vulnerability Assessment dei sistemi e redazione del relativo Report.

7.2. Modalità operative

Per riuscire a strutturare un processo di patching dei sistemi è necessario mappare puntualmente i servizi applicativi con i server che sono necessari per l'erogazione del servizio stesso, attribuendo una classificazione in base alla criticità del servizio e alla tipologia di gestione del patching che si vuole gestire. Senza questa mappatura diventa impossibile verificare l'impatto di un aggiornamento e l'eventuale disservizio richiesto.

Rientrano nella classificazione tutti gli apparati che possono essere soggetti ad attività di patching, a titolo esemplificativo e non esaustivo: Switch, Router, Access Point, FireWall, server e client. Di seguito riportiamo la classificazione minima consigliata:

A. **Sistemi Critici** si intendono: asset o dispositivi ad alto fattore di rischio con bassa latenza ed alto livello di impatto sul business. Ogni disservizio, per attività di aggiornamento di questi sistemi DEVE essere preventivamente accettata e concordata dal Cliente. Attività di aggiornamento tipicamente al di fuori del normale orario di lavoro;
B. **Sistemi Non Critici** si intendono: asset o dispositivi a medio-basso fattore di rischio con alta latenza e medio-basso livello di impatto sul business. Ogni disservizio, per attività di aggiornamento di questi sistemi ha un impatto trascurabile sugli utenti. Attività di aggiornamento fattibile in orario di lavoro;
C. **Postazioni di Lavoro** si intendono tutti gli apparati che possono essere inseriti nella procedura di aggiornamento automatico.
D. **Out** si intendono i sistemi che sono fuori dal processo di aggiornamento. Ad esempio, sistemi fuori supporto, dove il produttore non rilascia più aggiornamenti.

Lista Patch: Per i sistemi che non rientrano nella policy di gestione automatica delle patch verrà predisposta la lista delle patch installabili. Per quei sistemi in cui sono presenti applicazioni specifiche il personale di CD (o il cliente) si preoccuperà di verificare con il produttore (o chi si occupa della manutenzione dell'applicativo) la possibile installazione delle patch. Il report sarà integrato con analisi puntuale delle matrici di compatibilità. Alla fine di questo processo, la lista sarà verificata insieme al cliente per la validazione di quelle effettivamente da installare e quando effettuare l'aggiornamento dei sistemi (stima dei disservizi, finestre temporali per gli aggiornamenti, ecc.).

Il servizio di monitoraggio e controllo di Computer Design verifica costantemente la pubblicazione delle informazioni relativamente alla scoperta alle vulnerabilità ZERO DAY e ne dà visibilità ai clienti. Questo tipo di segnalazioni saranno incluse nei report con la lista delle patch installabili.

Per i sistemi sui saranno installate le patch il cliente deve garantire la disponibilità del proprio personale per effettuare i test applicativi alla fine della fase di aggiornamento. Oppure deve fornire a Computer Design gli script di test per verificare il corretto funzionamento dei sistemi dal punto di vista dei servizi utenti. In caso di esito negativo dei test il personale coinvolto nella fase di test effettuerà un rollback dei sistemi alla situazione precedente all'aggiornamento.

Per il corretto equilibrio tra esigenze di sicurezza e attività di aggiornamento consigliamo un aggiornamento di questa tipologia di sistemi almeno ogni 3 mesi.

7.3. Oggetto Del Servizio

Il presente contratto ha come obiettivo la fornitura di un servizio di patch management.

La fase iniziale del contratto sarà dedicata al setup dello strumento di gestione (componente di back end e il client su tutti i sistemi gestiti) e alla creazione della policy di aggiornamento dei sistemi (sistema di approvazione delle patch, periodicità degli aggiornamenti, censimento sistemi critici e non, ecc.). In questa fase sarà predisposta anche tutta la parte di documentale e procedurale per garantire il governo del processo di aggiornamento. Questa attività sarà svolta dal personale di Computer Design con affiancamento del personale del cliente.

Per questo tipo di attività Computer Design metterà a disposizione del cliente profili professioni adeguati in base alle tecnologie su cui si andrà ad operare. In ogni caso saranno utilizzati profili Senior e Technical Specialist.

Il contratto include i seguenti servizi:

- Fornitura in modalità MSP, per la durata del contratto stesso, di uno **TOOL** per la gestione del parco installato e la gestione del processo di patching [1)].
- **Postazioni di Lavoro**: Per questa tipologia di sistemi viene impostata la regola dell'aggiornamento in automatico allo spegnimento. In questo modo abbiamo i sistemi sempre aggiornati limitando al minimo il disservizio.
- **Sistemi Critici e Non critici**: In queste categorie, oltre ai Sistemi operativi di server Virtuali o Fisici rientrano apparati come Firewall, switch, stampanti. Firmware dei server fisici e storage, ecc.
- **Report Mensile**: dettaglio delle attività svolte nel mese ed elenco delle patch installabili (che non rientrano nelle casistiche incluse nel contratto) sui sistemi nel perimetro contrattuale.
- **Vulnerability Assessment**: nel caso in cui il cliente abbiamo sottoscritto questo servizio, verrà preparato un report mensile, ed inviato al cliente, di analisi delle vulnerabilità dei sistemi (Critici e Non-Critici) in base al livello di aggiornamento del sistema stesso: per ogni sistema vengono analizzate le patch mancanti e le vulnerabilità scoperte

Il servizio prevede la gestione delle patch e degli aggiornamenti degli applicativi e dei sistemi di cui il produttore mette a disposizione pubblicamente gli aggiornamenti e di cui esiste una documentazione pubblica. **L'installazione delle patch è fattibile solo per quei sistemi per i quali il cliente possiede un contratto assistenza con il produttore che dia diritto all'aggiornamento software e/o firmware.**

[1)] Se il cliente dispone di una piattaforma equivalente sarà valutato, in fase di startup del servizio, il possibile utilizzo ed eventualmente se la piattaforma possiede tutte le funzionalità necessarie al mantenimento degli SLA e della qualità del servizio come previsto dal contratto

7.4. Attività non incluse nel servizio di patching

Sono considerati non inclusi nel presente contratto i seguenti servizi/attività:

- Aggiornamento dei sistemi, che non rientrano nella procedura automatica di installazione. Per aggiornamento si intende installazione della/delle patch e gli eventuali riavvi necessari per l'applicazione delle modifiche.
- Aggiornamento dei sistemi **esclusi** dal perimetro descritto nel punto precedente.
- Aggiornamento upgrade/update del **firmware** interno Server e Client, stampanti, docking station, ecc.
- Le eventuali attività **ONSITE** non sono incluse nel presente servizio.

- Tutte le altre casistiche, comprese le vulnerabilità di tipo ZERO DAY, sono da intendersi escluse dal presente contratto e saranno valutate singolarmente di volta in volta con il cliente. Il servizio di monitoraggio e controllo di Computer Design verifica costantemente la pubblicazione delle informazioni relativamente alla scoperta alle vulnerabilità ZERO DAY e ne dà visibilità ai clienti.

Gli eventuali interventi relativi ai punti sopra elencati, saranno considerate attività extra.

8. Analisi CyberSecurity Posture - Opzionale

Il NIST (National Institute of Standards and Technology) definisce la cybercecurity posture come "l'insieme di dati che riguardano lo stato della sicurezza di una rete aziendale, la capacità di organizzarne le difese e l'efficienza nel rispondere ad eventuali attacchi".

Questo servizio è pensato per innalzare il livello di sicurezza delle infrastrutture IT dei clienti avendo una visione complessiva dell'efficienza dei sistemi per la sicurezza. Solo una visione globale e strutturata aiuta a comprendere dove possono essere presenti eventuali falle e, di conseguenza, permette di intervenire con misure adeguate. La nostra visione prevede una fase preliminare per SETUP di base per aumentare livello di Scurezza e un mantenimento continuo dello stato di sicurezza dell'Infrastruttura.

Questo tipo di approccio proattivo alla scurezza è coerente con quanto previsto dal GDPR. Il cliente deve possedere nella propria infrastruttura tutti gli strumenti che consentono di realizzare quanto previsto dalla normativa GDPR, questo servizio prevede la gestione dei suddetti strumenti in modo da adempiere a quanto previsto dalla normativa. Gli strumenti potranno essere scelti dal cliente rispetto al budget del Titolare del trattamento dei dati ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware.

Molte delle attività previste per l'adeguamento GDPR implicano la presenza di procedure operative interne del cliente (dismissione degli account, dismissione dei PC, test restore, ecc.) e/o documenti di sistema come il documento programmatico sulla sicurezza e/o il Privacy Impact Assessment (PIA). In caso sia necessario possiamo aiutare il cliente nella preparazione di tutte le procedure necessarie, mappare e classificare gli archivi dei dati (per identificare particolari categorie di dati personali). Durante la fase di assesment inziale saranno verificata la presenza e le qualità delle procedure, in caso di necessità sarà preparata una proposta economica per la predisposizione e/o adeguamento delle procedure.

Si ricorda che per una corretta implementazione delle norme a tutela del trattamento dei dati come previsto dal GDPR, nell'infrastruttura del cliente devono essere presenti diversi strumenti. Se gli strumenti sono presenti il servizio C-SEC include la loro gestione e manutenzione. In particolare, gli strumenti sono:

- sistema di autenticazione (ad esempio Active Directory);
- sistema Antivirus;
- Sistema di Backup;
- Sistema SIEM per la gestione dei log degli accessi e loro storicizzazione.

In particolare, questi sono gli aspetti normativi gestiti dal servizio C-SEC:

- **Encryption dispositivi**
  - Verifica che il sistema di encryption (p.es Bitlocker per Windows) dei supporti sia operativo su tutti i sistemi in modo coerente con la procedura operativa presente dal cliente.
- **Password Policy**
  - La normativa prevede una gestione del sistema di autenticazione (gestione dei Codici indentificativi e Parole chiavi per accedere ai sistemi). Per gestione si intende monitorare costantemente i codici presenti e la loro assegnazione ai collaboratori. Questo processo serve a verificare la "qualità" delle credenziali di acceso e verificare puntualmente a chi sono assegnati.
    Nel report mensile è presente elenco degli account presenti nel sistema con tutti i dati descritti in precedenza (ad esempio: qualità della password, account senza scadenza, password appartenente a databreach conosciuti, data ultimo accesso, ecc.). Su segnalazione del cliente, CD provvederà a dismettere gli account non più necessari.

- **Controllo Antivirus**
  - Verifica che il sistema antivirus presente nell'infrastruttura del cliente sia attivo e funzionante. Verifica del corretto aggiornamento del prodotto e verifica dell'applicazione in modo corretto delle policy previste e che il prodotto antivirus sia installato su tutti i sistemi in modo coerente con le politiche presenti nell'infrastruttura del cliente.
    Nel report mensile saranno indicate eventuali criticità come, ad esempio, elenco dei sistemi dove non è presente il sw antivirus con relative indicazioni.
- **Controllo sistema di Backup**
  - Verifica che il sistema di backup presente nell'infrastruttura del cliente sia attivo e funzionante. Verifica del corretto aggiornamento del prodotto e verifica dell'applicazione in modo corretto delle policy previste, in particolare che non siano presenti errori durante l'esecuzione dei backup e che tutti i sistemi rientrino nella policy di backup in modo coerente con quanto previsto dalle procedure interne del cliente. In caso di gestione manuale del repository offline, sarà a cura del cliente provvedere a scollegare eventuali dispositivi e alla loro conservazione sicura, preferibilmente offsite rispetto alla posizione dei dati.
    Nel report mensile saranno indicate eventuali criticità come, ad esempio, elenco dei sistemi dove non è presente il backup o altre criticità legate al salvataggio dei dati.
  - Test di ripristino: per verificare la qualità dei backup, il servizio prevede di eseguire un test di restore ogni 12 mesi. Per poter eseguire il test è necessario che il cliente disponga della dotazione tecnica per poter eseguire il test di restore in sicurezza.
- **Dismissione supporti**
  - Nelle verifiche mensili sarà predisposto un elenco dei supporti che dovranno essere alienati (PC, Server o altri apparati che sono stati de commissionati). Elenco servirà al personale del cliente per verificare la corretta cancellazione dei dati prima dell'alienazione.
- **Sistema di alert**
  - Il servizio prevede il controllo (durante gli orari e i giorni previsti come disponibilità del servizio), delle console dei prodotti software inerenti la sicurezza (SIEM, antivirus, etc) presenti nell'infrastruttura del cliente per verificare eventuali problemi di sicurezza. Nel caso di evidenza, sarà avvisato il referente del cliente. Il presente servizio non prevede attività di contenimento dell'eventuale attacco e/o ripristino dei dati e/o dei sistemi in caso di perdita causa attacco.
- **Gestione Asset**
  - Il contratto prevede l'installazione su tutti i PC e server di uno strumento per la gestione degli apparati. Lo strumento prevede, tra le altre funzionalità, la gestione dell'hardware e software inventory e la gestione degli aggiornamenti. La funzionalità di inventory è fondamentale per verificare la compliance per il rispetto del diritto d'autore per le licenze software. Il report degli asset è disponile su richiesta da parte del cliente.
- **Gestione dei LOG**
  - Verifica mensile del sistema SIEM per la gestione e storicizzane dei LOG di accesso. Verifica del corretto aggiornamento del prodotto e verifica dell'applicazione in modo corretto delle policy previste per la storicizzazione dei LOG e la segnalazione delle criticità. Nel report mensile saranno indicate eventuali criticità evidenziate dallo strumento.
- Hardening dei sistemi server secondo best practice internazionali.
- Policy sui Firewall: Implementazione policy secondo best practice internazionali

9. IT Managed Service – tipologie di contratto

Nel presente capitolo vengono descritti le varie tipologie di contratto e o moduli attivabili per ogni tipologia.

9.1. Remote Service Desk – RSD

Questa tipologia di contratto ha per obiettivo la presa in carico delle segnalazioni aperte dal cliente in modalità reattiva sugli asset consolidati durante la fase di Startup & presa in carico del Servizio (vedi paragrafo specifico) ed è finalizzato al ripristino del servizio nel minor tempo possibile.

I servizi inclusi prevedono:

- Servizio di Contact Center;
- Interventi sistemistici per gli ambienti (HW/SW) consolidati durante la fase di Startup & presa in carico del Servizio, necessari al ripristino dei sistemi per incident e problemi segnalati dal Cliente:
- Valutazione delle richieste di intervento sul parco software/hardware avanzate da Cliente attraverso il servizio di presa in carico delle richieste;
- Request la cui analisi e realizzazione richiedono un tempo inferiore a 15 minuti.

Tutti gli interventi di assistenza sistemistica saranno tracciati sul sistema di ticketing.

Si intendono comunque attività effettuate da Remoto.

9.2. Managed Service Desk - MSD

Questa tipologia di contratto ha per obiettivo la presa in carico delle segnalazioni provenienti dai sistemi di monitoring e di alerting in modalità proattiva sugli asset consolidati durante la fase di Startup & presa in carico del Servizio (vedi paragrafo specifico) ed è finalizzato al ripristino del servizio nel minor tempo possibile.

Questa tipologia di contratto prevede tutti i servizi previsti per il contratto **Managed Service Desk – RSD** con l'aggiunta di questi servizi:

- Governo del contratto: vedi Paragrafo "Governo del contratto";
- Servizio di Monitoring; vedi Paragrafo "Monitoring";
- Gestione delle richieste provenienti dal sistema di monitoring e dalle console di gestione del cliente;
- Verifica della problematica finalizzate sia al ripristino del servizio che alla fix della problematica.
- Gestione degli Alert generati dal Sistema di monitoring che superano e soglie definite con il Cliente ed implementate nel sistema di monitoring;
- Verifica del corretto funzionamento dei servizi mediante esame delle segnalazioni pervenute via E-Mail dalle console dei servizi di backup, Antivirus, storage, ecc. (qual ora attivo).

Tutti gli interventi di assistenza. Saranno tracciati sul sistema di ticketing e saranno evidenziati in un report mensile fornito al cliente.

Si intendono comunque attività effettuate da Remoto.

9.3. C-Sec

Questa tipologia di contratto ha per obiettivo la messa in sicurezza dell'infrastruttura del cliente e la creazione di un sistema di controllo e di miglioramento continuo. I servizi inclusi nel presente contratto sono:

- **Patch Management**: vedi Paragrafo "**Aggiornamento sistemi - Patch Management**"
- **Vulnerability assessment** vedi Paragrafo "**Vulnerability Assessment**", con frequenza mensile
- Analisi CyberSecurity Posture: vedi paragrafo "Analisi CyberSecurity Posture";
- Governo del contratto: vedi Paragrafo "Governo del contratto";
- **Report mensile** - Status dell'infrastruttura IT. Nel report saranno raccolti tutti i dati come descritto nei punti precedenti con l'aggiunta dele seguenti informazioni:
    - Eventuali criticità rilevate nell'infrastruttura dal report precedente o eventuali criticità/indicazioni che sono rimaste aperte
    - Attività svolte dal report precedente
    - Interventi consigliati per migliore lo stato complessivo dell'infrastruttura
    - Attività di formazione consigliate per il personale operativo
    - Elenco apparati de-commissionati
    - Analisi qualitativa sullo stato dell'infrastruttura

Si intendono comunque attività effettuate da Remoto.

9.4. DR - HERO

Questa tipologia di contratto prevede la fornitura di un servizio di supporto e presidio, erogato in **modalità H24**. Obiettivo del servizio è l'attivazione del sito secondario di DR a seguito di una richiesta di Emergenza da parte del cliente.

Il Fornitore metterà a disposizione del Cliente un servizio di allerta pronto a recepire la richiesta di attivazione del processo di DR. Il servizio di allerta, una volta autenticato il Cliente, attiverà il processo di DR secondo tempi e modi concordati. Il Cliente condividerà con il Computer Design l'elenco del personale autorizzato a chiedere l'accensione del sito di DR e le modalità di autenticazione. Al completamento del processo CD comunicherà al cliente la disponibilità del sito di DR.

Saranno applicate le procedure operative previste dal manuale di continuità operativa predisposte dal cliente.

Il fornitore assicura l'assistenza operativa ed il presidio a supporto del personale del Cliente, che è comunque responsabile della conduzione in esercizio dei sistemi.

Eventuali anomalie emerse durante le fasi di allineamento del sito di DR, verranno gestite come Incident. In caso di Incident si informerà il Cliente per concordare l'apertura di un Ticket di progetto Out-Of-Scope rispetto al presente contratto. I Report generati conterranno i dettagli degli interventi effettuati e quelli non risolti.

Non viene gestito nelle presenti procedure l'eventuale intervento del Cliente teso ad interrompere il processo di attivazione del sito secondario di DR a seguito di una richiesta di Emergenza. Tale evento verrà gestito e preso in carico a fronte di specifica richiesta del cliente, generando imponderabili situazioni non preventivabili.

Questo contratto prevede solo una attivazione (**UNO**) del sito di DR: ulteriori attivazioni saranno erogate secondo gli accordi economici stabiliti tra Cliente e Computer Design.

9.4.1. SLA – Attivazione in Caso di Emergenza

A seguito di quanto sopra indicato la nostra proposta l'attivazione del sito secondario di DR prevede i seguenti tempi e modalità di intervento:

- Tutte le attività di attivazione del sito secondario in caso di dichiarazione di emergenza da parte del cliente verranno effettuate secondo questa regola di ingaggio: inizio procedure di attivazione **entro 24 ore solari** all'apertura della richiesta dello stato di emergenza.
- Le attività verranno effettuate in modalità H24/365 (**Lun/Dom 0.01/24.00**), senza nessun giorno dell'anno escluso.

9.5. MDR Hero

Questa tipologia di contratto ha come obiettivo la fornitura di un servizio Co-Managed MDR Support; è una estensione del servizio **MDR Complete di Sophos**, pensato per "completare" ed estendere il servizio verso il cliente, in grado di parlare la stessa lingua del cliente. Il Service Desk di Computer Design diventa l'interfaccia unica verso il cliente con l'obiettivo di far percepire un Team unico: Security Operation, Threat Labs, AI scientist e CD-Service Desk.

Collaboriamo a quattro mani, con il Team MDR per la gestione della risposta agli incidenti. Il NOC di Computer Design, grazie alla conoscenza dell'infrastruttura del cliente, può fornire al Team MDR tutte le informazioni per potersi "muovere" in modo efficace ed efficiente ottimizzando ulteriormente i tempi di riposta e di efficacia in caso di incident di sicurezza. In particolare, il Team di CD, in caso di incidente, interagisce direttamente con il TEAM Sophos con copertura H24, garantendo la pronta riposta ed attivazione delle contromisure. Il cliente viene continuamente aggiornato sull'evoluzione ma non è convolto nella fase di attivazione (Rapid Response).

La subscription MDR Complete prevede 2 opzioni di Modalità di risposta alle minacce: **Collabora** e **Authorize**. Il servizio MDR Hero è applicabile solo con la scelta della modalità **Authorize**.

Il servizio **MDR Hero** ha per obiettivo la presa in carico delle segnalazioni aperte dal Team MDR di Sophos, in modalità **reattiva** (Remote Service Desk) sugli asset consolidati durante la fase di Startup & presa in carico del Servizio (vedi paragrafo specifico) ed è finalizzato ad eseguire le indicazioni predisposte dal Team MDR. Il team di Computer Design è il primary contact del servizio MDR.

Le attività incluse prevedono:

AZIONI	DESCRIZIONE
Change Configurations	Modifica delle configurazioni per gestire e contenere la minaccia. Può includere la regolazione delle policy di sicurezza di EDR/MTR, abilitazione MDR su dispositivi non protetti e modifica delle esclusioni.
Isolate Hosts	Sfruttare la funzionalità di host isolato di Sophos Central, per limitare l'esposizione degli asset compromessi.
Block Files	Blocca i file tramite SHA256 in modo da evitare l'attivazione dei contenuti dannosi.
Run Scan	Avvio della scansione dei sistemi
Block websites/IPs/CIDR	Blocco di uno specifico sito WEB o IP Address grazie al WEB Control
Block Application	Blocco di una specifica applicazione grazie all'Application Control
Live Terminal	Se altre azioni di risposta non sono efficaci, uso di Live Terminal per accesso diretto all'host.

Tutti gli interventi di assistenza sistemistica saranno tracciati sul sistema di ticketing e saranno evidenziati in un report mensile fornito al cliente.

Questo servizio può essere attivato solo per i clienti che hanno un contratto attivo per il servizio MDR di Sophos. Può essere associato al servizio C-SEC per avere una gestione a 360° per gli ambiti di Cyber Security.

I servizi inclusi prevedono:

- Verrà fornito un numero di telefono specifico per contattare il SOC di Computer Design. Canale telefonico diretto durante gli incidenti attivi.
- Interventi sistemistici per gli ambienti (HW/SW) consolidati durante la fase di Startup & presa in carico del Servizio, necessari al contenimento della minaccia a seguito degli incident e problemi segnalati dal Team MDR.
- Valutazione delle richieste di intervento sul parco software/hardware avanzate dal Team MDR di Sophos attraverso il servizio di presa in carico delle comunicazioni del Team MDR.
- Change Request la cui analisi e realizzazione richiedono un tempo inferiore a 15 minuti.
- Meeting mensile di aggiornamento sulle ultime minacce e sulle attività svolte dal Team Unico MDR e CD.

DESCRIZIONE DEL SERVIZIO				
Sophos MDR	**CD**	**Macro Attività**	**MDR Hero**	**Note**
✓		Visibilità globale sulle minacce grazie alla telemetria di +556.000 clienti	✓	
✓		Threat-hunting proattivo e non solo monitoraggio reattivo	✓	
✓		Security Operation Center	✓	
	✓	Network Operation Center	✓	
	✓	Gestione IT e Incident response completa sull'ambiente del cliente	✓	
	✓	Utilizzo della stessa lingua del cliente	✓	
✓		Copertura globale del servizio per clienti multi-sede	✓	
✓		Team unico in grado di rispondere alle minacce	✓	**Sophos**: Security Operation, Threat Labs, AI scientist e Automation **CD**: SOC, NOC
✓		Livelli target di servizio: 2 min detection 30 min response	✓	
✓	✓	Integrazione dei dati dei vari strumenti di security	✓	
✓	✓	Copertura del servizio H24	✓	
	✓	Interventi on-site		Attività **non inclusa** nel contratto ma erogabile in accordo con il cliente.
	✓	Conoscenza dell'infrastruttura del cliente: Layout, fisica, strumenti di accesso	✓	
	✓	Possibilità di attivare contratti verso terzi	✓	
	✓	Interventi atti al ripristino a seguito di un incident.		Attività **non inclusa** nel contratto ma erogabile in accordo con il cliente.
✗	✗	Revisione continua delle impostazioni di Sicurezza, patching dei sistemi aggiornamento delle policy secondo best practice internazionali, VA e PT	✗	Attività **non incluse** nel contratto ma erogabile tramite l servizio MSD C-SEC

9.5.1. SLA – Attivazione in Caso di Emergenza

A seguito di quanto sopra indicato riportiamo i tempi e modalità di intervento previsti per questa tipologia di contratto:

- Servizio di Contact Center. Il servizio di Contact Center verso altri fornitori, incluso nel servizio, viene "esteso" e adattato alla copertura **H24**. In ogni caso le regole di ingaggio degli altri fornitore dipendono dalle condizioni definite dal cliente con il fornitore stesso
- SLA di intervento: **PLATINUM**
- Copertura del servizio **H24**:

9.5.2. Esclusioni dal contratto

Il servizio NON include attività On-Site e attività di ripristino in caso di attacchi. Nel caso in cui fossero necessarie queste tipologie di attività, sarà applicato lo SLA Platinum del servizio, ma saranno fatturate a consuntivo in base a quanto specificato nel capitolo: Tariffe servizi.

10. Servizi Aggiuntivi

10.1. Utenti VIP

E' possibile attivare un servizio "UTENTI VIP". I ticket al service desk relative ad una serie di Utenti Specifici, indicati dal cliente in fase di configurazione del servizio, verranno automaticamente definiti come problematiche con criticità di tipo "Priorità 1 (Alta)".

10.2. Presidio OnSite

E' possibile attivare un servizio di presidio on-site. Il servizio prevede la presenza di uno o più tecnici specializzati, per l'assistenza specialistica, presso la sede del cliente secondo un calendario definito.

Il servizio di PRESIDIO ON-SITE è un servizio aggiuntivo rispetto a quanto previsto dal servizio IT Managed Service. I tecnici, durante le giornate di presidio, svolgeranno attività definite e concordate con il cliente.

La fornitura delle prestazioni dei servizi di presidio on-site sarà fornita secondo il Livello di Servizio prescelto e secondo modalità e condizioni concordate.

10.3. Sabato Mattina

E' possibile attivare un servizio (per i clienti che hanno un piano BASE) che consenta di ottenere assistenza il sabato mattina (ore 9.00/13.00). Verrà fornito un numero di telefono specifico a cui il nostro tecnico sara reperibile. In questo caso l'assistenza che verrà fornita e del tipo Best Effort e non gestito sulla base degli SLA previsti con il cliente,

10.4. Reperibilità H24

E' possibile attivare un servizio (per i clienti che hanno un piano BASE) che consenta di ottenere assistenza nei periodi non coperti dal piano BASE. Verrà fornito un numero di telefono specifico a cui il nostro tecnico sarà reperibile. In questo caso l'assistenza che verrà fornita e del tipo Best Effort e non gestito sulla base degli SLA previsti con il cliente. Le attività erogate saranno fatturate a consuntivo in base a quanto specificato nel capitolo: **Tariffe servizi**.

10.5. Servizio Premium – Attività extra

Servizio il premium prevede un numero di Giornate, prepagate, di assistenza che il cliente potrà utilizzare per tutte quelle attività che non sono comprese nel perimetro del presente contratto.

Gli interventi potranno essere effettuati dal lunedì al venerdì, escluso i giorni di festività infrasettimanali del calendario italiano ed altre eventuali giornate che verranno comunicate entro il 20/12 dell'anno precedente a quello cui si riferiscono. La pianificazione degli interventi verrà concordata di volta in volta con il cliente mediante l'apertura di un ticket a cui seguirà conferma formale da parte del cliente.

Eventuali estensioni del servizio in giorni non previsti dovranno essere concordate tra le parti e non sono inclusi nei corrispettivi di cui al presente contratto bensì saranno fatturati sulla base della tariffa specificata nelle condizioni di fornitura del presente contratto.

La giornata lavorativa e': dalle ore 9:00 alle ore 18:00 con un'ora di pausa pranzo.

Al fine del calcolo della consuntivazione mensile delle attività svolte si farà riferimento ai Rapportini di Intervento. Le giornate saranno conteggiate secondo quanto specificato nel capitolo **Tariffe e Servizi**.

Le giornate non utilizzate, nel periodo di validità del presente contratto, potranno essere riportate come giornate da utilizzare nel rinnovo del contrato.

10.6. Test Backup

Oltre al servizio di verifica del corretto funzionamento del servizio di backup mediante esame delle segnalazioni pervenute via E-Mail dal sistema di Backup (qual ora attivo) è possibile attivare un servizio di test **LITE** sui backup.

Tale test consente di controllare periodicamente che una porzione di 1 backup sia integro ed aggiornato.

Sono previsti 3 Test all'anno. Tale servizio e così strutturato:

- In accordo con il cliente verrà stabilito:
  - Il giorno in cui verrà effettuata la prova di Test (esempio l'ultimo venerdì del mese)
  - La porzione del backup da estrarre (esempio: Il file/cartella xxx del Backup zzz) - La porzione estratta non potrà superare il 10% del totale del backup
  - Test formali da effettuare da parte di CD (Esempio: ultima data di modifica del file = Mese in cui si effettua il test)
- Le risorse necessarie per il ripristino del backup e' messo a disposizione dal cliente
- Inizio Attività di ripristino
  - Nella data concordata e durante l'orario lavorativo (**Lun/Ven 8.00/19.00**), con esclusione delle giornate di festività previste dal calendario italiano.
- Comunicazione da parte di CD al cliente del completamento dell'attività di ripristino e correttezza del test formale eseguito
- Test da parte dei Key User (attività di competenza del Cliente) del backup ripristinato. Entro 5 Giorni
- Chiusura della richiesta di test del Backup.
  - In caso di Esito positivo verrà predisposto un verbale di chiusura ed eventualmente si procederà alla cancellazione dell'ambiente di test
  - In caso di Esito negativo del Test. Cliente e Computer Design si adopereranno per effettuare le opportune analisi tecniche ed eventuali risoluzioni per procedere ad una ripetizione del test. Tali attività saranno gestite mediante un approccio a progetto.
  - Computer Design svolgerà ogni attività necessaria per risolvere i problemi evidenziati. Qualora fosse evidente, che l'esito è negativo a causa di sistemi e/o competenze al di fuori della propria sfera di competenze, Computer Design concorderà col Cliente le fasi di ingaggio con i vari referenti per risolvere il problema.
  - Nota Bene: In mancanza di comunicazione da parte del cliente dell'esito dei loro test si assume che il test sia positivo.

11. Corrispettivo Economico

Per quanto sopra descritto la nostra proposta è così sintetizzabile:

11.1. Soluzione Proposta – Contratto MSD

Voce	Q.Ta'	Prezzo Unit.	Prezzo Tot.
Managed Service Desk/Silver/Base Ticket Anno = 20/anno - Durata 3 anni	1,00	4.995,00 €	4.995,00 €

Prezzo a Voi riservato	**4.995,00 €**

Infine, come riportato anche nelle condizioni di fatturazione vi evidenziamo che

Il corrispettivo del contratto (vedi prospetto sopra) verrà fatturato secondo le seguenti regole:

- **Canone**: In una soluzione anticipata

12. Esclusioni

Rimangono esclusi tutti i servizi non previsti nel documento di Attivazione dei Servizio.

A tale proposito abbiamo predisposto un elenco esemplificativo ma non esaustivo delle attività non previste ma che possono essere effettuate e consuntivate a tempo e materiali.

- Difetti causati da utilizzo e/o installazione non compatibili con le istruzioni operative descritte nel manuale del prodotto;
- Hardening dei sistemi
- Diagnosi ed eliminazione di difetti e danni dovuti a:
  - Difetti su cavi e connettori esterni all'apparecchiatura
  - Danni provocati da eventi atmosferici (es.: acqua, incendi, fulmini ecc.)
  - Possibili influenze ambientali (es.: campi magnetici, anomalie elettriche, ecc.)
- Supporto sull'implementazione, installazione e formazione di prodotti software
- Upgrades o major release dei sistemi operativi o applicativi
- Riparazioni hardware del materiale
- Gestione e risoluzione dei malfunzionamenti causati da interventi impropri di personale del Cliente o di terze parti.
- La manutenzione dell'HW (gestita tramite garanzia del Vendor o fornitori terzi).
- Gli interventi per problemi che possono essere risolti solo dai produttori delle tecnologie coinvolte.
- Installazione di Patch software o aggiornamento firmware (se non previsti contrattualmente).
- Change Request la cui analisi e realizzazione richiedono un tempo superiore a 15 minuti.
- Formazione del personale.
- I servizi si intendono erogati da remoto, le eventuali attività ONSITE non sono incluse nel presente servizio.

13. Tariffe servizi

13.1. Attività OnSite

Nel caso in cui il soddisfacimento della richiesta del Cliente non fosse risolvibile con la sola assistenza come sopra descritta ma si rendesse necessario l'intervento presso la sede del Cliente le Parti concordano che essi saranno regolati come segue:

- Segnalazione da parte di CD del fatto che la problematica oggetto della richiesta non potrà essere risolta senza intervenire presso la sede del Cliente.
- Preventivazione dei costi per gli interventi necessari.
- Invio del preventivo a mezzo e-mail al Key User che ha richiesto assistenza.
- Esecuzione degli interventi solo nel caso in cui vi sia accettazione a mezzo e-mail da parte del Key User che ha richiesto assistenza per conto del Cliente.
- Chiusura della chiamata con invio mail al Key User interessato.
- Tutte le attività eseguite saranno fatturate a consumo con modalità tempo e materiali, secondo le tariffe di cui nel capitolo **Tariffe e Servizi** paragrafo **Listino di riferimento**. (eventuali spese di viaggio, vitto e alloggio verranno conteggiate a pie di lista) se eccede quanto contrattualmente già previsto.
- Il tempo di intervento è entro le 8 ore lavorative dalla conferma del Cliente.
- Per tempo di intervento on-site si intende il tempo intercorrente tra la conferma formale del cliente (e-mail) al servizio clienti e l'arrivo del tecnico CD all'ingresso della sede del cliente oggetto dell'intervento.

Per **orario lavorativo** si intende (Lun/Ven 8.00/19.00), con esclusione delle giornate di festività previste dal calendario italiano.

13.2. Listino di riferimento

Eventuali attività non incluse nel contratto di Managed IT saranno fatturate secondo il seguente listino:

Figura	Tipologia	Tariffa Oraria Listino	Tariffa Oraria Riservata
Assistenza & Micro Attività - Indipendente dalla Figura Professionale	On Site	90,00 €	75,00 €
Assistenza & Micro Attività - Indipendente dalla Figura Professionale	Remoto	75,00 €	65,00 €

Le tariffe si intendono per ora consuntivata in orario standard.

Al fine del calcolo per la consuntivazione mensile delle attività svolte si farà riferimento ai Rapportini di Intervento. Le giornate saranno conteggiate con il seguente metodo:

Attività Remoto

Tra 0 e 0,25 ore = fatturazione 0 FTE

Dalle 0,25 = Fatturazione ore effettive – con minimo fatturabile di 2 ore e arrotondamento all'ora superiore

Attività OnSIte

Fatturazione minima 0,5 FTE

Per impegno tra 4 ore e 8 ore = fatturazione 1 FTE

Oltre le 8 Ore - Fatturazione ore effettive – con maggiorazione tariffe "fuori orario standard"

FTE = Full Time Equivalent -> Giornata lavorativa

Eventuali attività non incluse nel contratto di Managed IT effettuate in orario non lavorativo saranno fatturate applicando una maggiorazione, alle tariffe di riferimento, secondo il seguente schema.

Periodo (Giorno/Ore)	22.00 – 05.59	06.00 – 8.59	09.00 – 17.59	18.00 - 21.59
Lunedì - Venerdì	100%	50%	Non Applicabile	50%
Sabato, Domenica e Festività	100%			

13.3. Richieste di Assistenza in "emergenza"

Per richieste di intervento, da parte del cliente, con la caratteristica di "**urgenza**", e con SLA **"il più presto possibile"** (Best Effort), al di fuori del periodo di disponibilità del servizio contrattualizzato nel contratto **Managed IT,** verrà applicato un importo per l'attivazione della richiesta in aggiunta alle ore impiegate per la gestione della richiesta.

La fatturazione dell'attivazione del servizio avverrà secondo il seguente schema:

Periodo (Giorno/Ore)	22.00 – 05.59	06.00 – 8.59	09.00 – 17.59	18.00 - 21.59
Lunedì - Venerdì	2.000,00 €	1.500,00 €	Inclusa nel contratto	1.500,00 €
Sabato, Domenica e Festività	2.000,00 €			

Per la consuntivazione e valorizzazione delle ore, fare riferimento al capitolo **Tariffe e Servizi** paragrafo **Listino di riferimento** e le relative maggiorazioni per attività fuori orario di lavoro.

13.3.1. Clienti con servizio di reperibilità

Per i clienti con il servizio di reperibilità saranno consuntivate solo le ore impiegate per la gestione della richiesta. Per la valorizzazione delle ore, fare riferimento al capitolo **Tariffe e Servizi** paragrafo **Listino di riferimento** e le relative maggiorazioni per attività fuori orario di lavoro.

14. Condizioni di Fornitura

14.1. Attivazione Servizio

Entro 30 Giorni dalla firma del presente contratto verrà effettuata la fase di Startup & presa in carico del Servizio. Durante questa fase sarà predisposta tutta la documentazione a completamento del contratto.

A seguito di tale approvazione da parte del cliente verrà inviato una comunicazione che formalizza l'attivazione dei servizi di supporto con i riferimenti tecnico/commerciali oltre al flusso di apertura Dei ticket

14.2. Durata del Contratto

Il presente contratto ha durata di 12 mesi a partire dalla attivazione del contratto. Dopo i primi 12 mesi è previsto un rinnovo tacito. Per le condizioni di operatività del rinnovo tacito si veda l'art. 20.2 delle condizioni generali di contratto che vengono altresì sottoscritte dal cliente.

14.3. Dati e Programmi

La perdita di dati e/o programmi, anche se causata da interventi di assistenza o riparazione, non è coperta dal servizio di manutenzione offerto nè può dar luogo a richieste di danni o rimborsi e attività avendo il Cliente cura di tenere quotidianamente una copia di backup aggiornata di dati e programmi.

14.4. Condizioni di Fatturazione E Pagamento

IVA:	Tutti i prezzi sopra esposti si intendono IVA esclusa.
Validità offerta:	30 giorni data offerta (salvo scadenza promozione o esaurimento scorte).
Fatturazione:	Il corrispettivo del contratto verrà fatturato secondo le seguenti regole: • **Una Tantum**: Alla attivazione del contratto • **Canone Annuale**: Annualmente in una soluzione anticipata • **Canone Mensile (Server, Network, Client, Mobile e Stampanti)**: Il corrispettivo verrà fatturato ogni mese verificando esattamente quante apparecchiature sono gestite e inventariate
Modalità di pagamento:	Vostra solita.
Attivazione	30 giorni dall'esecuzione della presa in carico (Assessement Iniziale)
Accettazione dell'ordine:	L'accettazione dell'ordine è subordinata all'approvazione del fido da parte della Direzione Amministrativa di CD. Allo stesso modo gli ordini dei clienti non in regola con i pagamenti, rimarranno inevasi sino alla definizione della posizione contabile.

Rimborsi Spese:	Nel caso in cui un collaboratore di CD dovesse svolgere delle attività al di fuori dalle sedi previste, le spese vive sopportate nell'interesse o su richiesta del cliente, quali in particolare note e fatture pagate a terzi per il cliente, spese di trasferta, spese di soggiorno, pernottamento e vitto fuori domicilio e le spese per l'uso dei servizi pubblici (posta, telefono, ecc.) verranno rimborsate dalla Cliente in modalità a piè di lista, dietro presentazione di una nota spese dettagliata e dei relativi giustificativi. Per le trasferte in auto, autorizzate dal Cliente, il rimborso previsto è di € 0,5 al chilometro. In questo caso non è necessario alcun giustificativo.

14.5. Metodo di calcolo – MSP (Managed Services Provider)

Per quanto riguarda i servizi MSP la durata viene indicata come **Periodo** del servizio e può essere **Mensile o Annuale**. Per periodo si intende la durata minima per quale il cliente si impegna alla sottoscrizione di quel servizio.

Mensile: Nel caso di periodo mensile il conteggio avviene a fine mese in base ai consumi effettivi del mese in corso (ogni servizio ha la sua modalità di conteggio dei consumi mensili). Si potrà procedere ad un aumento/diminuzione delle licenze mese per mese sulla base di specifiche richieste da parte del cliente e/o esigenze e/o attivazioni/disattivazioni eventualmente effettuate direttamente nella consolle del prodotto da parte del cliente. **Le eventuali attivazioni aggiuntive verranno conteggiate, in mancanza di un accordo scritto, ai prezzi di listino in vigore al momento dell'attivazione**

Ogni mese il prezzo potrà variare in funzione del listino di riferimento dei produttori del software previsto per il servizio. In base al conteggio e al listino di riferimento sarà fatturato mensilmente il corrispettivo del servizio.

Annuale: All'interno di questo periodo non posso essere fatte variazioni in diminuzione delle quantità, ma solo nuove sottoscrizioni. Alla scadenza del periodo, durante la fase di rinnovo, sarà possibile diminuire le quantità per il nuovo periodo di sottoscrizione. All'interno del periodo il prezzo del servizio è bloccato e non soggetto a revisione. La fatturazione solitamente è anticipata per il periodo (annuale o multipli di essa).

Licenze Microsoft 365 non mensili: Per le licenze Microsoft con periodo annuale o multipli di annualità, in caso di aggiunta di licenze e' possibile venga calcolato il rateo del costo della nuova licenza: dalla data di attivazione della nuova licenza alla data effettiva di scadenza della licenza già attiva. Le date fanno riferimento a quanto riportato dal portale Microsoft. In questo modo le licenze avranno un'unica data di fine periodo.

Per **attivazione del servizio** si intende la creazione e attivazione dello "spazio/licenze" a Voi dedicate, nella o nelle console di riferimento dedicate all'erogazione del servizio oggetto della presente proposta e sulla base della configurazione sopra riportata.

15. Condizioni Commerciali di Fornitura

Iva	Tutti i prezzi sopra esposti si intendono IVA esclusa.
Consegna:	30 giorni dalla conferma dell'ordine, salvo disponibilità dei produttori
Fatturazione:	Materiale: Alla consegna Attività: Alla chiusura della stessa/Consuntivo Mensile
Modalità di pagamento:	Ricevuta Bancaria 30 gg Data Fattura Fine Mese se non diversamente concordato
Spese di trasporto (ove applicabili):	25,00 € + IVA fino a 100 Kg. Il costo si intende per le consegne a livello strada. Le consegne particolari (al piano, a specifici orari, etc.) dovranno essere preventivamente concordate e possono dare origine ad un sovraprezzo.
Validità offerta:	Le condizioni indicate nella presente proposta, hanno validità 30 giorni dalla data della presente (salvo scadenza promozione o esaurimento scorte).
Accettazione dell'ordine:	L'accettazione dell'ordine è subordinata all'approvazione del fido da parte della Direzione Amministrativa di Computer Design. Allo stesso modo gli ordini dei clienti non in regola con i pagamenti, rimarranno inevasi sino alla definizione della posizione contabile.
Chiusura attività:	Alla chiusura dell'attività (esecuzione servizi professionali) verrà sottoscritto relativo rapporto di intervento o verbale di collaudo.
Garanzia Post Vendita per le installazioni:	Tutte le installazioni di Computer Design sono coperte da garanzia di conformità per 15 giorni dopo la chiusura dell'attività. Tale garanzia copre le problematiche di installazione e configurazione direttamente collegate all'attività oggetto dell'offerta; non è prevista da questa garanzia l'assistenza sulle componenti hardware o software. Al termine di tale periodo ogni intervento sarà da considerarsi a parte. Contattateci per ulteriori informazioni sui contratti di assistenza post-vendita di Computer Design.
Servizi di Assistenza	Le attività eseguite da CD (in Remoto e/o On-Site) con modalità tempo e materiali saranno valorizzate a consuntivo sulla base delle tariffe concordate Al fine del calcolo della consuntivazione mensile delle attività svolte si farà riferimento ai Rapportini di Intervento. Le attività saranno conteggiate con il seguente metodo: **Attività Remoto** - **Tra 0 e 0,25 ore =** fatturazione 0 FTE - **Dalle 0,25 =** Fatturazione ore effettive – con minimo fatturabile di 2 ore e arrotondamento all'ora superiore **Attività On-Site** - Fatturazione minima 0,5 FTE - Per impegno tra 4 ore e 8 ore = fatturazione 1 FTE - Oltre le 8 Ore - Fatturazione ore effettive – con maggiorazione tariffe "fuori orario standard" FTE = Full Time Equivalent -> Giornata lavorativa
Assistenza Extra:	Eventuali attività extra non previste nella presente Offerta sono Escluse. E dovranno essere oggetto di specifici accordi formali.
Interventi in giorni festivi:	Eventuali attività che verrebbero effettuate in orario non lavorativo saranno consuntivate calcolando il tempo effettivo e fatturate applicando una maggiorazione secondo il seguente schema:
Rimborsi spese:	Nel caso in cui un collaboratore di CD dovesse svolgere delle attività al di fuori dalle sedi previste, le spese vive sopportate nell'interesse o su richiesta del cliente, quali in particolare note e fatture pagate a terzi per il cliente, spese di trasferta, spese di soggiorno, pernottamento e vitto fuori domicilio e le spese per l'uso dei servizi pubblici (posta, telefono, ecc.) verranno rimborsate dalla Cliente in modalità a piè di lista, dietro presentazione di una nota spese dettagliata e dei relativi giustificativi. Per le trasferte in auto, autorizzate dal Cliente, il rimborso previsto è di € 0,5 al chilometro. In questo caso non è necessario alcun giustificativo.

Periodo (Giorno/Ore)	22.00 – 05.59	06.00 - 8.59	09.00 - 17.59	18.00 - 21.59
Lunedì - Venerdì	100%	50%	0%	50%
Sabato Domenica e Festività	100%			

16. Accettazione

Con la firma d'ordine alla presente proposta tecnico economica, il cliente accetta e conferma le "Condizioni generali di fornitura".

PER ACCETTAZIONE	
Computer Design S.r.l.	Cliente (Timbro e firma autorizzata) _____
Nome e Cognome **Manuel Tosatti**	Nome e Cognome, funzione
	N.B.: Firmare tutte le pagine contrassegnate dalla freccia Rossa

Data

_____

17. Condizioni generali di fornitura

1. Oggetto

1.1. Le presenti Condizioni Generali ("***CGC***") sono parte integrante del contratto commerciale tra Computer Design S.r.l. ("Computer Design" e/o "la Società") ed il Cliente ("Il Cliente") avente per oggetto la fornitura e/o la rivendita ("distribuzione") di servizi informatici ("***i Servizi***"), comprendenti servizi in modalità Cloud e/o Saas "software-as-a-service" ("*Servizi Cloud*"), la manutenzione, l'assistenza tecnica, la consulenza informatica, la messa a disposizione di uno spazio hosting, l'attività di disaster recovery ed ogni altra prestazione di servizi di natura informatica ("*gli altri Servizi*") nonché la concessione di licenza e/o sviluppo di software ("***il Software***") ovvero la fornitura di beni hardware ("***i Beni***"), il tutto secondo quanto indicato nell'Offerta commerciale, negli eventuali Addendum, ordini o altri documenti contrattuali.
I Servizi, il Software e i Beni sono definiti collettivamente in prosieguo, quali la "***Fornitura***".

1.2. Il contratto è rivolto esclusivamente ad Aziende, a Studi professionali e comunque ai possessori di Partita Iva che lo utilizzano per lo svolgimento della propria attività e che hanno sede in Italia o all'estero.

1.3. Il contratto si intenderà perfezionato al momento dell'accettazione da parte del Cliente dell'Offerta emessa da Computer Design. Tale accettazione potrà essere formalizzata mediante la restituzione di una copia dell'Offerta sottoscritta per accettazione dal legale rappresentante del Cliente o da chi ha il potere di firma, incluse le CGC. La restituzione da parte del Cliente del documento, proveniente dai numeri di fax o di indirizzo @mail del Cliente stesso, fa presumere che la sua sottoscrizione sia stata posta da soggetto munito dei necessari poteri rappresentativi.

1.4. La copia dell'Offerta restituita con modifiche apportate dal Cliente dovrà intendersi nuova proposta ex art. 1326, ultimo comma cod. civ. e come tale non sarà vincolante per Computer Design a meno di sua espressa accettazione.

1.5. Nessuna deroga alle presenti Condizioni Generali sarà valida e vincolante se non espressamente concordata per iscritto dai legali rappresentanti delle parti. Resta espressamente esclusa l'applicabilità di qualunque altra configurazione di "condizioni generali "predisposta dal Cliente.

2. Oggetto e limiti Fornitura

2.1. Computer Design garantisce al Cliente che fornirà i Servizi secondo diligenza e professionalità, nel rispetto delle disposizioni contrattuali, costituendo la propria prestazione una obbligazione di mezzi e non di risultato.

2.2. La Fornitura viene scelta dal Cliente sulla base delle informazioni dallo stesso reperite sul mercato; pertanto il Cliente si dichiara compiutamente informato in relazione al campo ed ai limiti delle sue applicazioni, nonché dell'input richiesto e dell'output ottenibile. Le informazioni tecniche sui Servizi, Licenze e/o Beni di terzi eventualmente inserite nelle Offerte, sono ricavate dalle informazioni pubblicate dalle relative case produttrici.

2.3. In caso di attivazione dei Servizi, la Società non fornisce garanzie sulla qualità delle comunicazioni in merito a perdite o a ritardi delle connessioni o a qualsiasi altra imperfezione e non assume alcuna responsabilità al riguardo. In particolare, è noto alle parti che l'utilizzo del Protocollo IP per il trasporto dei dati risente degli stessi fenomeni che si possono riscontrare sulla rete Internet, a seconda delle fasce orarie, della qualità e della velocità della propria connessione alla rete, il tutto salva l'applicazione e nei relativi limiti degli SLA – Service Level Agreement concordati con il Cliente.

2.4. Durante la validità del contratto il Cliente può aderire alla manutenzione annuale pagando il relativo compenso concordato; in ogni caso, ogni modifica richiesta dal Cliente o consulenza inerente ai Servizi che non sia prevista dalla manutenzione sarà fatturata alle condizioni indicate in Offerta; sono, in particolare, escluse dal contratto, dove non diversamente esplicitato, lo studio e la verifica di modifiche relative all'integrazione e configurazione di eventuali servizi aggiuntivi.

3. Termini e consegne

3.1. I termini di consegna per la realizzazione dei Servizi, lo sviluppo del Software e/o la fornitura dei Beni, eventualmente riportati sulla conferma d'ordine e/o nell'offerta, hanno carattere puramente indicativo, costituiscono cioè una semplice previsione dei tempi necessari alla consegna e come tali sono rispettati nel limite del possibile con esclusione di ogni possibile pretesa risarcitoria a favore del Cliente per eventuali ritardi.

3.2. Tutte le vendite si intendono franco stabilimento di produzione o franco magazzino di Computer Design e i Beni viaggiano ad esclusivo rischio del Cliente. Ai sensi dell'art. 1510 cod. civ. Computer Design si libera dall'obbligo della consegna dei Beni rimettendoli al vettore o allo spedizioniere per il trasporto.

4. Corrispettivi, pagamenti e sospensione

4.1. Tutti i corrispettivi pattuiti dovranno considerarsi al netto di IVA.
Computer Design emetterà fattura a fronte dell'esecuzione di ciascuna Fornitura. Il Cliente dovrà effettuare il pagamento secondo le modalità e i tempi previsti nella conferma d'ordine e/o offerta. Qualsiasi altra condizione di pagamento dovrà essere approvata per iscritto dalla Società.

4.2. Nel caso di mancato pagamento entro i termini stabiliti e senza pregiudizio di ogni altro suo diritto, Computer Design si riserva il diritto di sospendere la Fornitura ai sensi dell'art. 1460 cod. civ., previa comunicazione al Cliente, mediante indirizzo di posta elettronica certificata (pec) o raccomandata a.r., con un preavviso minimo di 5 (cinque) giorni lavorativi. Il Cliente acconsente sin da ora a tale sospensione, impegnandosi a porre in essere ogni idonea disposizione organizzativa della propria struttura in grado di evitare che dalla interruzione della Fornitura e/o dei Servizi possa derivare pregiudizio alla propria attività, pur sempre consapevole che, ove anche ciò si verificasse, sarebbe comunque a suo carico, non potendo rivolgere alcuna pretesa nei confronti di Computer Design. In ogni caso di ritardo nei pagamenti da parte del Cliente, sia che sia stata predisposta la sospensione della Fornitura ovvero anche in assenza di sospensione, ogni termine di consegna o altro eventuale termine previsto nel contratto a carico della Società sarà prorogato in corrispondenza ed in automatico.

4.3. In ogni caso, Computer Design ha facoltà di emettere la fatturazione decorsi 10 giorni dall'avvenuto rilascio del consuntivo dei lavori, in caso di intervenuta prestazione di attività di assistenza e/o manutenzione tecnica.

5. Fornitura – i Servizi e il Software

5.1. Computer Design conserva tutti i diritti sui concetti, le idee, il Know-how o le tecniche relative ai Servizi.

5.2. Computer Design concede al Cliente una licenza d'uso, non esclusiva e non trasferibile, del software concesso in licenza al Cliente ovvero realizzato e/o sviluppato per conto del Cliente, del quale la Società o la sua diretta licenziante è legittima titolare, e ciò per l'erogazione dei Servizi specificati nell'Offerta commerciale dietro corrispettivo, attribuendogli la facoltà d'uso del software medesimo nei limiti ivi indicati. La licenza d'uso non concede alcun diritto sul codice sorgente originale. Tutte le tecniche, gli algoritmi e i procedimenti contenuti nel software e nella relativa documentazione sono informazioni protette dal diritto d'autore e sono di proprietà del legittimo titolare, quale licenziante della Società ovvero della Società stessa; pertanto, non possono essere usati in alcun modo dal Cliente per scopi diversi da quelli consentiti dalla legge e/o dal contratto. Il Cliente si impegna quindi a non modificare, duplicare, distribuire, riprodurre, cedere a terzi a qualsiasi titolo, in qualsiasi modo e a mezzo di qualsiasi server, terminale o postazione, ogni applicativo di cui ai Servizi. La distribuzione a scopo di lucro, la pubblicazione a scopo di lucro, la modificazione, l'elaborazione in qualunque forma e modo, la decompilazione (reverse engeneering), il mirroring, fraiming, posting o qualsiasi altro mezzo di riproduzione analogo e, in genere, la memorizzazione digitale del software deve considerarsi abusiva e sarà perseguita a norma delle vigenti leggi.

5.3. Il contratto può prevedere l'installazione di applicazioni software o componenti hardware di cui il Cliente detiene le relative licenze d'uso. In tal caso, è di esclusiva responsabilità del Cliente la verifica e l'adeguamento delle licenze d'uso per poterlo utilizzare con la tipologia di servizio prevista contrattualmente.

5.4. In caso di servizi Cloud, essi verranno erogati presso l'IDC di STACK Infrastructure situato a Siziano (PV).

5.5. Il Cliente concede alla Società un account amministrativo ai propri sistemi da mantenere attivo durante tutto il corso del rapporto.

5.6. Nel caso di sviluppo software da parte della Società in ambiente open source il codice sorgente verrà rilasciato al Cliente nei limiti e nei termini di cui alle licenze utilizzate e, in ogni caso, all'avvenuto pagamento del saldo dovuto dal Cliente.

5.7. In caso di sviluppo software, l'oggetto del contratto -salvo diversi accordi tra le parti- non si estende a "compliance" fiscali e legali (ad es. verifiche su conformità legge privacy ex Reg. Ue n. 2016/679 e D.lgs. n. 231/03 sul contenuto del sito web predisposto a favore del Cliente) collegate al Servizio.

6. Audit – Servizi e licenze

6.1. La Società ha il diritto di verificare la conformità del Cliente, quale licenziatario, rispetto alle licenze rilasciate in base agli ordini e/o altri documenti contrattuali.
Al tal fine, il Cliente si impegna a:
(i) Registrazioni: conservare e, su richiesta della Società, fornire documentazione sufficiente a certificare la conformità in base alle opzioni di licenza applicabili per il software concesso in licenza, che possa includere, ma non sia limitata a, numeri di serie, chiavi di licenza, log, localizzazione, modello (inclusa quantità e tipo di processore) e numero di serie di tutte le macchine sulle quali è installato o consultabile il software concesso in licenza o dalle quali è possibile accedere al software concesso in licenza, i nominativi di coloro (numero di utenti) che accedono o sono autorizzati ad accedere al software concesso in licenza, alle metriche, ai report, alle copie del software concesso in licenza (per prodotto e versione) e ai diagrammi di architettura di rete in quanto riguardanti la licenza, lo sfruttamento dei prodotti concessi in licenza e l'attività di supporto e manutenzione ad essa associati;
(ii) Questionario: entro sette (7) giorni dalla richiesta della Società, il Cliente, quale licenziatario, fornirà un questionario compilato accompagnato da una dichiarazione scritta che attesti l'accuratezza delle informazioni fornite;
(iii) Accesso: fornire ai rappresentanti e/o delegati della Società la possibilità di installare nei propri sistemi plugin atti a monitorare il corretto funzionamento dei sistemi e la corrispondenza contrattuale delle licenze installate nonché a fornire l'assistenza necessaria e l'accesso alla documentazione e ai computer ai fini dell'ispezione e del controllo dei computer e della relativa documentazione, durante il normale orario di lavoro del Cliente, per verificarne la conformità alle licenze, prestando piena collaborazione nello svolgimento di tale verifica.
(iv) Non conformità: nel caso in cui la verifica riveli che l'uso delle licenze è nei limiti del 10% in più rispetto ai diritti acquisiti, i costi supplementari per le licenze saranno fatturati direttamente al Cliente ai prezzi correnti di listino. Nel caso in cui l'utilizzo registrato è almeno pari o superiore al 10% rispetto ai diritti acquisiti, i costi supplementari per le licenze saranno aumentati (per il periodo in cui è perdurato l'inadempimento) del 50% rispetto ai prezzi di listino. Inoltre, nel caso in cui il Cliente stia utilizzando una funzione od opzione per la quale non ha acquisito i diritti, la Società sarà autorizzata a fatturare i costi supplementari per le licenze al prezzo di listino corrente. Il Cliente dovrà pagare quanto dovuto entro trenta (30) giorni dalla data della relativa fattura. Nel caso in cui la Società non applichi uno dei rimedi di cui sopra, la Società stessa potrà risolvere il contratto, ai sensi e per gli effetti dell'art. 1456 cod. civ.

6.2. Il Cliente sia in fase precontrattuale che nel corso del rapporto ha la facoltà di richiedere alla Società copia della documentazione e/o dei riferimenti tecnici e/o delle certificazioni esistenti attestanti la presenza dei requisiti di sicurezza della infrastruttura Cloud oggetto del rapporto tra le parti, il tutto a tutela della sicurezza delle informazioni ivi contenute, consentendo -altresì- al Cliente la conduzioni di Audit, a propria cura e spese, al fine della verifica della corrispondenza di tali informazioni allo stato di fatto della relativa infrastruttura oggetto del rapporto.

7. Collaudo – sviluppo software

7.1. Entro 10 giorni a decorrere dalla data della definitiva consegna, il Cliente procederà al collaudo del software realizzato, personalmente, con l'assistenza della Società ovvero tramite terzi appositamente incaricati.

7.2. La Società è tenuta a prestare al Cliente, a propria cure e spese, l'assistenza tecnica necessaria e a mettere a disposizione dello stesso le attrezzature eventualmente occorrenti alle operazioni di collaudo.

7.3. È in ogni caso facoltà della Società intervenire al collaudo, anche attraverso propri rappresentanti. Nel caso in cui la Società partecipi al collaudo, essa è tenuta a sottoscrivere i documenti di collaudo che verranno sottoscritti dai collaudatori (verbali, certificati, ecc.).
7.4. Ove, per cause ad esso non imputabili, il Cliente non possa provvedere al collaudo nel termine di cui al precedente comma 7.1, il Cliente ha facoltà di stabilire un'altra data, restando inteso che tale rinvio -in tale circostanza- non costituirà accettazione dell'opera ovvero collaudo tacito. Se invece il Cliente non intende dar corso al collaudo, ovvero alla suindicata richiesta di rinvio dello stesso, decorsi 10 giorni dalla consegna dell'opera, la stessa dovrà intendersi definitivamente approvata.
7.5. In caso di esito negativo del collaudo, la Società dovrà provvedere, a propria cura e spese, entro il termine che le verrà comunicato dal Cliente, alla eliminazione dei difetti e/o delle carenze riscontrate. Dopo la comunicazione, da parte della Società, dell'avvenuta eliminazione dei difetti e/o delle carenze, il Cliente procederà ad un nuovo collaudo nei termini e con le modalità di cui ai commi precedenti.
7.6. In caso di esito positivo del collaudo, comprovato dalla non contestazione di alcun vizio entro 10 giorni dalla consegna o dalla comunicazione dell'avvenuta eliminazione dei difetti e/o delle carenze, l'opera si considererà definitivamente accettata e collaudata.
7.7. Si richiamano le eventuali indicazioni specifiche e/o integrative in materia di accettazione del software, eventuali attività di "baby sitting" e di manutenzione, di cui all'offerta commerciale.

8. Riserva di proprietà

8.1. Le vendite a pagamento dilazionato, con o senza rilascio di effetti cambiari, sono sempre effettuate con riserva di proprietà a favore di Computer Design fino al saldo integrale del pagamento. Il Cliente non può vendere né costituire in pegno, o trasferire la merce, fino a totale estinzione del debito.

9. Obblighi e responsabilità – Servizi (Cloud, Saas e hosting)

9.1. Fermo restando ogni altro obbligo posto dalla legge e/o da altre previsioni del contratto, il Cliente si impegna per tutta la durata del contratto a:
a) utilizzare i Servizi in conformità alle disposizioni di legge in materia di tutela civile e penale, alle regole della netiquette, dei programmi, dei sistemi informatici, delle comunicazioni informatiche e telematiche;
b) utilizzare i Servizi esclusivamente in relazione all'ambito della propria attività e a non compiere alcun atto diretto a consentire a terzi l'utilizzo dei Servizi;
c) utilizzare i Servizio che gli sono stati espressamente assegnato e nei limiti di banda, CPU (Central Processing Unit) e spazio su disco che sono stati eventualmente assegnati;
d) astenersi dal trasmettere, divulgare, distribuire, inviare o altrimenti mettere in circolazione, tramite i Servizi, informazioni, dati e/o materiali osceni, diffamatori, illegali, altrimenti lesivi, turbativi, o in violazione di diritti di terzi, anche sotto il profilo della violazione della normativa sul trattamento dei dati personali;
e) non utilizzare i Servizi per atti contro la morale e l'ordine pubblico o con lo scopo di recare molestia alla quiete pubblica e privata, di recare offesa o danno diretto e/o indiretto a chiunque, e di violare i contenuti della corrispondenza altrui, ovvero di ledere i diritti di proprietà intellettuale e industriale di terzi;
f) a mantenere, in ogni ipotesi in cui, a norma di contratto, il Cliente viene a collegarsi direttamente al data center di Computer Design, o ad ogni altra struttura di Computer Design, i propri sistemi in efficienza per evitare la propagazione di virus o altre manomissioni ai sistemi di Computer Design, essendo in ogni caso il Cliente responsabile per ogni danno eventualmente determinato da tali atti.
9.2. Il Cliente, quale unico ed esclusivo amministratore dei Servizi, dichiara inoltre: a) di essere esclusivo responsabile dello smarrimento o della divulgazione delle credenziali di accesso nonché della gestione degli accessi al suo account, impegnandosi ad informare tempestivamente CD di qualsiasi uso non autorizzato del proprio account o di qualsiasi violazione alla sicurezza riscontrata; b) di essere in regola con le licenze del software autonomamente inseriti ed utilizzati nell'Infrastruttura virtuale.
Il Cliente si impegna a manlevare e tenere indenne la Società (nonché i suoi rappresentanti, dipendenti o collaboratori) da tutte le perdite, i danni, responsabilità, costi, oneri e spese, ivi comprese le eventuali spese legali, che dovessero essere subite o sostenute dal medesimo, quale conseguenza di qualsiasi inadempimento da parte del Cliente agli obblighi e garanzie previste nel presente contratto anche in ipotesi di azione promossa da terzi a qualunque titolo e, in ogni caso, per le violazioni di cui ai paragrafi che precedono (art. 9.1/9.2).

10. Accesso, reso e/o conservazione dati in Cloud

10.1. Durante la sospensione dei Servizi di cui all'art. 4.2, il Cliente non potrà avere accesso a dati e/o informazioni e/o contenuti dal medesimo immessi e/o trattati nell'Infrastruttura virtuale.
10.2. In caso di recesso anticipato del contratto ovvero in ogni altra ipotesi di cessazione del contratto per ogni ragione e/o causa, il Cliente potrà, in alternativa tra loro:
a) avere libero accesso ai dati ai fini del download nel proprio sistema informatico, nei 10 gg. successivi alla data di cessazione del contratto, ovvero:
b) affidare alla Società il back up dei dati risiedenti sul server in uso al Cliente (anche eventualmente oggetto di comodato e/o noleggio da parte di Computer Design), alle condizioni economiche concordate tra le parti e previa nomina della Società, da parte del Cliente, quale responsabile esterno al trattamento dei dati oggetto di tale memorizzazione esterna.
Decorsi 30 giorni dalla cessazione del contratto, il Cliente autorizza CD, anche ai sensi dell'art. 28 co. 3 lett. g) ex GDPR, a provvedere alla cancellazione dei dati del Cliente stesso dalle proprie strutture informatiche.
Il Cliente prende atto che, dopo la cessazione del Servizio Cloud, la Società potrà non essere autorizzata da parte del proprietario del software licenziante (ad es.: Microsoft) a concedere in uso il relativo software al Cliente per il recupero dei dati su infrastruttura (Virtual Machine) del Cliente stesso.

11. Garanzie, esoneri e limiti di responsabilità

11.1. Rivendita di beni/servizi di terzi: L'acquisto dei Beni e/o Servizi dalla Società, la quale agisca quale rivenditrice, comporta l'accettazione integrale delle condizioni di garanzia fornite dal produttore, che possono essere indipendenti dal volere o della possibilità di controllo e/o intervento, della stessa Computer Design. Il Cliente, pertanto, è consapevole che la merce acquistata sarà garantita dal produttore e alle condizioni dallo stesso previste, ed accetta, quindi, rimossa ogni riserva, tutte le modalità di prestazione della garanzia del produttore, anche se non specificata in Offerta e/o in Ordine. La Società non assume nessuna responsabilità sul corretto funzionamento e sulle prestazioni promesse dai produttori dell'hardware ovvero del software di base utilizzato per creare gli ambienti operativi e gestionali (ad es.: sistemi operativi, software per data base, software per le reti, posta elettronica, packages di varia natura - ERP...), applicazioni sviluppate in casa dal Cliente o da terzi per conto del Cliente con esclusione di quelli sviluppati dalla Società. In ogni caso, Computer Design declina in ogni caso qualunque responsabilità per danni o perdite, diretti o indiretti, derivanti dai Beni – dei quali è mero rivenditore – o dall'uso degli stessi e dalle prestazioni di Servizi in rivendita – dei quali è mero intermediario – quali proposti nelle offerte in forma scritta o elettronica, anche per ritardata o mancata consegna del prodotto, né per la corrispondenza della merce alle specifiche eventualmente specificate nell'offerta.
11.2. Beni e/o Servizi di Computer Design: In caso di fornitura di Servizi informatici da Computer Design al Cliente, la Società garantisce al Cliente che fornirà i Servizi secondo diligenza e professionalità, nel rispetto delle disposizioni contrattuali, costituendo la propria prestazione una obbligazione di mezzi e non di risultato. In caso di fornitura/vendita di Beni (hardware), Computer Design garantisce che i suoi prodotti sono privi di vizi e/o difetti per il periodo di 12 mesi dalla consegna, salvo diversi accordi tra le parti. Tale garanzia è limitata ai vizi di funzionamento del prodotto evidenziatisi in condizioni di normale utilizzo e manutenzione.
11.3. La garanzia per la vendita di Beni comporta unicamente, a discrezione di Computer Design, la sostituzione e/o la riparazione dei Beni o relativi componenti ad essa restituiti nel suo magazzino sito in Santo Stefano Ticino (MI) – via Piave n. 46 dal Cliente a proprie spese, per i quali i difetti siano stati riconosciuti da Computer Design.
11.4. Le garanzie e i rimedi previsti dai precedenti paragrafi sono condizionati al corretto immagazzinamento, installazione, funzionamento e manutenzione dei prodotti ("i Beni") in conformità alle istruzioni d'uso fornite al Cliente, e ciò anche in relazione ai Servizi resi, la cui responsabilità e onere per il corretto utilizzo dei Servizi e/o del software, il corretto caricamento dei dati iniziali ed il corretto uso nel tempo è -e resta esclusivamente- del Cliente, il quale dovrà osservare, nell'uso degli stessi, le norme operative indicate dal Cliente, essendo -altrimenti- esclusa ogni garanzia al riguardo. Pertanto gli obblighi di Computer Design in relazione alla garanzia non sono validi in tutti i casi di: malfunzionamento del software o delle configurazioni hardware imputabili al Cliente, programmi informativi non utilizzati dal Cliente conformemente alle istruzioni ricevute dalla Società, modifica da parte del Cliente del suo ambiente informativo, reti, server e workstation incluse, ad insaputa della Società o comunque rilascio da parte del Cliente di indicazioni errate o incomplete, così come in ogni ipotesi di trascuratezza, negligenza o imperizia d'uso ovvero utilizzo da parte del Cliente diverso da quello per cui il prodotto e/o servizio è stato progettato e/o dimensionato.
11.5. Con particolare riferimento alla concessione di licenza di software e/o alla fornitura di Servizi informatici, la Società non potrà in alcun modo essere ritenuta responsabile per disservizi e/o danni causati dall'uso del software e/o dei Servizi oggetto del presente contratto in caso di: - manomissioni o interventi che compromettano il corretto funzionamento del software effettuati da personale del Cliente o da terzi non autorizzati dalla Società; - errata utilizzazione del software da parte del Cliente o di operatori o di terzi utilizzatori autorizzati; - non regolare funzionamento di hardware o software utilizzati dal Cliente, la cui manutenzione non è eseguita direttamente dalla Società; - interruzione totale o parziale del servizio di accesso locale o di terminazione della chiamata fornito da operatore di telecomunicazione e/o della rete internet; - inosservanze, inadempimenti e violazioni di legge imputabili al Cliente, quali, a mero titolo esemplificativo, ma non esaustivo, violazioni della D.Lgs. 9 aprile 2008, n. 81 o della normativa Privacy vigente.
11.6. Resta peraltro inteso che eventuali modifiche apportate direttamente dal Cliente al software e/o ai Servizi comporteranno la immediata cessazione di ogni garanzia.
11.7. In ogni caso, Computer Design, salvo quanto disposto dall'art. 1229 cod. civ, non assume alcuna responsabilità, per qualsiasi danno possa derivare dalla fornitura a favore del Cliente, sia diretto che indiretto senza esclusione alcuna.
11.8. Ove dovesse essere accertata in giudizio con sentenza passata in giudicato, una responsabilità della Società in merito alle attività di Sua competenza, le parti convengono sin da ora di limitare tale responsabilità ai soli danni diretti e che, in ogni caso, il limite massimo dell'importo dell'eventuale risarcimento dei danni dovuto, per qualsiasi ragione, dalla Società al Cliente, sarà pari al 50% delle somme già ricevute dal medesimo a fronte delle attività svolte. E' espressamente escluso il risarcimento al Cliente di qualsiasi danno ulteriore sofferto.

12. Risoluzione anticipata e penali

12.1. Salvo ed impregiudicato ogni altro suo diritto, Computer Design potrà risolvere il Contratto previa diffida ad adempiere ai sensi dell'art. 1454 c.c. in caso di inadempimento del Cliente di una qualunque delle obbligazioni previste a suo carico dal Contratto.
12.2. In ogni caso di risoluzione del contratto per fatto e colpa del Cliente, così come in ipotesi di recesso anticipato del contratto da parte del Cliente, le rate e gli anticipi riscossi da Computer Design rimarranno acquisiti a titolo di canone d'uso o di indennità/penali, salvo il maggior danno.
12.3. In particolare, ogni caso di risoluzione del contratto per fatto e colpa del Cliente, così come in ipotesi di recesso anticipato del contratto da parte del Cliente, il Cliente stesso è tenuto a pagare immediatamente, a titolo di penale, i canoni di manutenzione/assistenza tecnica rimanenti dal momento della comunicazione di risoluzione fino al termine del Contratto.

13. Decadenza

13.1. Qualunque azione giudiziale derivante dalla vendita dei beni o dall'attività di manutenzione e/o assistenza tecnica dovrà essere iniziata entro il termine di decadenza di un anno dal verificarsi del fatto che ha dato origine alla relativa pretesa.

14. Riservatezza e trattamento dati personali

14.1. Il Cliente e Computer Design si impegnano a garantire che tutte le informazioni relative a procedure che le parti avranno occasione di scambiarsi in corso d'opera saranno considerate riservate; analoga riservatezza verrà richiesta a tutto il personale sia dipendente che ausiliario, che collaborerà alla realizzazione delle procedure e dei programmi
14.2. Nel corso dello svolgimento di tutte le attività connesse all'esecuzione del presente contratto, ciascuna delle parti potrà trovarsi nella condizione di dover trattare dati personali riferibili a dipendenti e/o collaboratori dell'altra parte, motivo per il quale ciascuna di esse s'impegna sin d'ora a procedere al trattamento di tali dati personali in conformità alle disposizioni di cui al Regolamento Europeo 679/2016 in materia di protezione dei dati personali, nonché tutte le norme di legge di volta in volta applicabili.

14.3. Le parti s'impegnano a condurre le attività di trattamento di dati personali sulla base dei principi di correttezza, liceità, trasparenza e tutela della riservatezza dei soggetti interessati e per il solo ed esclusivo fine di perseguire le finalità di cui al presente contratto nonché degli eventuali obblighi di legge allo stesso connessi. I dati personali raccolti nell'ambito del presente contratto saranno trattati da ciascuna delle parti limitatamente al periodo di tempo necessario al perseguimento delle finalità di cui sopra. Nel caso in cui tali dati costituiscano contatti professionali (da intendersi per tali tutti i contatti di professionisti e/o soggetti che agiscono nella loro qualifica professionale), potranno essere trattati sin quando ciascuna delle parti lo ritenga utile al fine di dar corso ad una possibile prosecuzione della collaborazione professionale.
14.4. A tal proposito, ciascuna delle parti si impegna a render accessibili detti dati solo ai propri dipendenti e/o collaboratori che, in ragione della propria funzione e/o attività, hanno la necessita di trattare gli stessi, per il fine di cui sopra. Le parti dichiarano espressamente di aver debitamente informato e di informare i propri dipendenti e/o collaboratori man mano che diverrà necessario.
14.5. Qualora, nell'ambito di svolgimento delle prestazioni di cui al presente contratto, ciascuna delle parti si trovi nella condizione di affidare in parte e/o in toto attività di trattamento di dati personali di propria titolarità e/o per i quali sia stata nominata responsabile del trattamento da altro titolare, entrambe s'impegnano a sottoscrivere un separato accordo scritto volto a formalizzare la nomina a responsabile e/o sub-responsabile del trattamento della parte affidataria al fine di procedere ad una corretta gestione delle attività di trattamento di dati personali cosi come previsto dall'articolo 28 Regolamento Europeo EU 679/2016.
14.6. La sottoscrizione di tale accordo, qualora sussistano le esigenze di cui sopra, è condizione necessaria ed imprescindibile per l'affidamento di attività di trattamento di dati personali.
14.7. In caso di nomina di cui agli artt. 14.6/14.6 che precedono, su richiesta del titolare, il responsabile nominato: (i) fornirà tutte le informazioni necessarie a dimostrare il proprio adempimento agli obblighi in materia di protezione dei dati personali previsti nella nomina e dalla normativa privacy, comprensivi alla verifica delle misure di sicurezza idonee adottate dal titolare; (ii) riconosce altresì al titolare, e agli incaricati di questo, il diritto di accedere ai locali di sua pertinenza dove hanno svolgimento le operazioni di trattamento o dove sono custoditi i dati personali e/o la documentazione relativa alla relativa nomina. Al fine dell'esercizio di tali diritti, la richiesta di accesso al responsabile verrà posta con almeno 7 (sette) giorni di preavviso, con l'indicazione della data ed il nominativo delle persone chiamate ad effettuare le operazioni di verifica; le predette verifiche saranno espletate nei normali orari di ufficio senza arrecare pregiudizio all'attività lavorativa de titolare.
14.8. La visione completa dell'informativa privacy di Computer Design, comprensiva dell'esercizio dei diritti dell'interessato, è accessibile al sito www.cdesign-group.com – sezione Informativa Privacy Clienti.
14.9. La Società, in caso di Servizi Cloud, non fornirà a terzi i dati personali ivi contenuti e/o ogni altra informazione riferita al Cliente, se non previo espresso consenso del Cliente stesso, fatta eccezione per provvedimenti delle forse dell'ordine e/a di altra pubblica autorità competente, in forza di atti vincolanti per la Società e prevalenti su ogni altra normativa in materia di riservatezza tra le parti.

15. Referenze

15.1. La Società autorizza il Cliente a comunicare, anche all'interno del proprio sito internet o di altre comunicazioni telematiche, che il medesimo è un suo fornitore e il Cliente autorizza la Società a dichiarare che il Cliente stesso è un suo cliente (anche indicando, eventualmente, i Servizi da lui acquistati, eventuali case history a ciò associati, ragione sociale e/o logo del Cliente).

16. Subappalto

16.1. La Società potrà subappaltare, in tutto od in parte, le attività di cui al Contratto, restando comunque responsabile nei confronti del Cliente.

17. Forza Maggiore

17.1. La Società non sarà responsabile nei confronti del Cliente per qualsiasi inadempimento o ritardo nell'adempimento delle obbligazioni nascenti dal contratto dovuti a cause di forza maggiore od eventi comunque al di fuori del proprio controllo, inclusi, ma non solo, incendi, terremoti, epidemie, alluvioni, tumulti, sommosse, scioperi anche aziendali, serrate, ritardi nei trasporti, morte od infortuni dei dipendenti od incaricati della Società, problemi nella fornitura elettrica e nelle comunicazioni, divieti e proibizioni disposti dalle autorità.

18. Divieto di sollecitazione personale

18.1. Il Cliente, per la durata del contratto e per il periodo di un anno dalla sua scadenza si impegna a non assumere o ad offrire assunzione (con qualsiasi forma di collaborazione, saltuaria o continuativa) dipendenti e/o collaboratori o subfornitori anche professionisti aventi in essere un rapporto con Computer Design che svolgano, abbiano svolto o siano ad altro titolo coinvolti nelle attività, anche nell'ipotesi in cui l'offerta provenga dal dipendente o dal collaboratore di Computer Design. Il Cliente assume i presenti obblighi anche per conto delle società dallo stesso controllate o allo stesso collegate.
18.2. In caso di violazione della clausola dei punti del presente capitolo mediante l'effettivo inizio anche occasionale di una collaborazione di lavoro con le persone indicate al punto 18.1, il Cliente si impegna al pagamento, a favore della Società, di una penale pari al importo mensile lordo della retribuzione o stipendio percepita da tali soggetti che verrà calcolato per il periodo di un anno (importo lordo mensile x 12 mesi), salvo i maggiori danni nelle ipotesi di concorrenza sleale.

19. Legge applicabile e foro competente

19.1. Le condizioni generali e gli altri documenti contrattuali saranno disciplinati dalle leggi della Repubblica Italiana ed il Foro di Milano avrà esclusiva competenza per qualsiasi controversia ad essi connessa.

20. Durata, rinnovo e cessazione

20.1. I Servizi sono previsti nella durata indicata nella conferma d'ordine e/o offerta.
20.2. Nel caso in cui il Cliente abbia attivato un contratto di durata periodica o continuativa della Fornitura, esso -alla sua scadenza naturale- verrà tacitamente rinnovato, per il periodo di 12 mesi, e così di volta in volta per le successive scadenze e ciò ove una delle parti non abbia provveduto a comunicare la propria disdetta mediante comunicazione scritta da inviarsi - mediante lettera raccomandata a.r. o email pec certificata - almeno 60 giorni prima della sua scadenza, originaria o rinnovata.
20.3. Alla cessazione del contratto per qualsiasi motivo o causa, così come in caso di mancato rinnovo dello stesso, ogni Servizio in corso verrà disattivato, rimanendo onere del Cliente scaricare i propri dati, eventualmente risiedenti presso la struttura informatica di Computer Design con le modalità di cui all'art. 10 che precede; prima di tale evento comunque il Cliente - a condizione che sia in regola con il pagamento dei corrispettivi dovuti fino a quel momento - ha la facoltà di richiedere successivamente l'estratto di tutti i dati memorizzati in esecuzione al Servizio. In caso di mancata richiesta dei dati entro il termine di 30 giorni dalla cessazione per qualsiasi motivo del Servizio, la Società provvederà alla rimozione e cancellazione definitiva di tutti i dati in possesso presso il server dedicato.

21. Sicurezza e appalto di servizi

21.1. Per le attività svolte nei luoghi di lavoro del Cliente, quest'ultimo si impegna ad adottare le misure necessarie per la tutela della sicurezza e della salute nei luoghi di lavoro secondo la normativa tempo per tempo vigente nonché, a tale fine, ad informare la Società riguardo: (i) le specifiche norme di sicurezza del lavoro in uso presso le proprie sedi; (ii) le policies e, in particolare, quelle relative alla sicurezza, alla normativa Privacy e alla riservatezza in uso presso la propria organizzazione. Le Parti si impegnano in ogni caso a rispettare scrupolosamente le normative di sicurezza previste presso le sedi e ad apportare qualsiasi modifica e/o integrazione dovesse risultare opportuna al DUVRI anche nel corso del rapporto contrattuale.

22. Adozione Modello 231

22.1 Il Cliente dichiara di essere a conoscenza della politica aziendale adottata da Computer Design S.r.l. la quale ha adottato un Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001, dei principi etici e delle norme di condotta enunciati nel Codice Etico, pubblicato sul sito internet aziendale (https://www.cdesign-group.com/) e, in caso di disattesa e di violazione delle stesse, della conseguente applicazione delle sanzioni previste dal Sistema Disciplinare.
22.2 Il Cliente si impegna, pertanto, a tenere un comportamento in linea con il Codice Etico e con le norme di condotta in esso enunciate e a mantenere una condotta tale da non esporre Computer Design S.r.l. al rischio dell'applicazione delle sanzioni previste dal suddetto Decreto Legislativo e dalle norme da esso richiamate anche in materia di salute e sicurezza sul lavoro.
22.3 L'inosservanza di tale impegno da parte del Cliente costituirà grave inadempimento contrattuale e legittimerà Computer Design S.r.l. a risolvere il presente contratto con effetto immediato, ai sensi e per gli effetti di cui all'art. 1456 c.c., fermo restando il risarcimento dei danni.

23. Clausole finali

23.1. Il contratto esaurisce la disciplina dei diritti e degli obblighi del Cliente e del fornitore per quanto riguarda l'oggetto del contratto stesso.
23.2. E' da intendersi annullata e privata di effetto ogni eventuale precedente e diversa pattuizione scritta e/o orale fra le parti riguardate l'oggetto del contratto.
23.3. Eventuali tolleranze, anche reiterate e prolungate, a violazioni e inottemperanza a clausole del presente contratto non costituiranno precedente e non potranno menomare la validità ed efficacia sia delle clausole non osservate sia di tutte le restanti.
23.4. Ove il presente contratto stabilisca esoneri e/o limitazioni di responsabilità a favore di Computer Design, le stesse avranno effetto per le ipotesi di colpa lieve, ad esclusione di dolo o colpa grave.
23.5. Ogni modificazione delle condizioni e dei termini del contratto richiede forma scritta a pena di nullità.
23.6. Le condizioni particolari sottoscritte dalle parti con separata scrittura prevalgono, in caso di contrasto o incompatibilità, con le presenti condizioni generali.
23.7. L'accettazione delle presenti Condizioni Generali si intende valida ed efficace con la sottoscrizione delle medesime anche da parte del solo Cliente.

Data_____

_____
Timbro e firma del Cliente
(il legale rappresentante)

Agli effetti degli artt. 1341 e 1342 del codice civile, il cliente dichiara di approvare specificatamente le disposizioni dei seguenti articoli specificati nelle "Condizioni Generali di Contratto": **2.3** (Oggetto e limiti Fornitura); **3** (Termini e consegne); **4.2** (Sospensione Fornitura); **6 (iv)** (penale – Audit non conformità); **7.4/7.6** (Collaudo – accettazione); **8** (Riserva di proprietà); **9.2** (manleva); **10.1** (accesso dati e sospensione servizi); **10.**2 (accesso e cancellazione dati); **11** (esoneri e limiti di responsabilità); **12** (Risoluzione anticipata e penali); **13** (Decadenza convenzionale); **16** (Subappalto – autorizzazione); **17** (Forza maggiore); **18** (divieto sollecitazione personale); **19** (foro esclusivo); **20.2** (rinnovo tacito); **22.3** (Modello 231 – violazione e risoluzione di diritto); **23.4 (**esoneri e/o limitazioni di responsabilità); **23.5** (forma scritta).

Data_____

_____
Timbro e firma del Cliente
(il legale rappresentante)