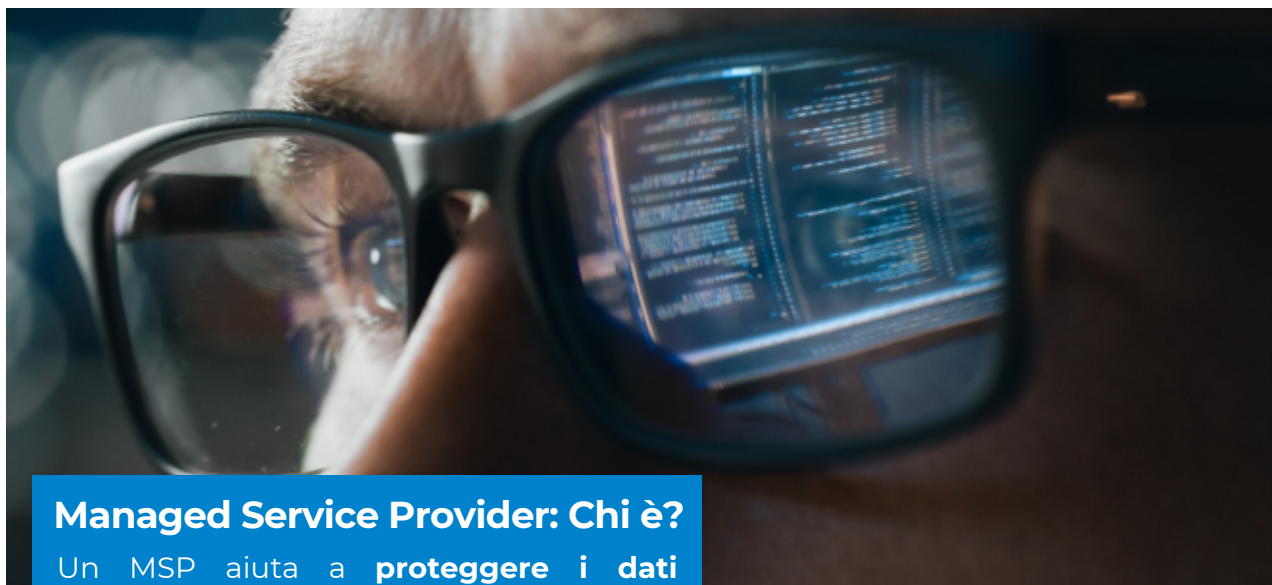


CORE UP MAGAZINE

**SPECIAL EDITION - MSP: L'ANGELO CUSTODE
CHE MONITORA IL TUO AMBIENTE IT****Managed Service Provider: Chi è?**

Un MSP aiuta a **proteggere i dati sensibili** e il know-how aziendale con il monitoraggio costante dell'ambiente IT, la manutenzione e la gestione proattiva. In caso di attacchi o disastri IT l'azienda riparte nel minor tempo possibile, riducendo quindi i tempi di fermo e le perdite economico-finanziarie.

Offre servizi altamente specializzati su base contrattuale, spesso con un **canone** mensile/annuale, permettendo al cliente di **esternalizzare le complessità tecnologiche** e concentrarsi sul proprio core business.

• Dati sensibili al sicuro: imprenditori liberi di concentrarsi sul fatturato

Quando hai un **partner IT** con funzione di MSP puoi contare su un'infrastruttura IT efficiente e sicura mentre ti dedichi al tuo lavoro.

In caso di incidente IT dovuto a un attacco hacker o a un errore umano, un MSP ti aiuta a contenere i **danni** e le **perdite** perché ti permette di ripartire nel minor tempo possibile, scongiurando i tanto temuti **down-time**.

Inoltre, se scegli un MSP che fornisce anche hardware e software, avrai un parco macchine IT sempre aggiornato e performante.

• I vantaggi per le aziende che scelgono un MSP:

- Continuità operativa** e riduzione dei tempi di fermo
- Assistenza telefonica e da remoto illimitata
- Rete IT più sicura e sempre aggiornata**
- Unico referente IT: risparmio di tempo/denaro
- Consulenza IT altamente qualificata
- Zero sorprese di spesa:** comodo contratto con canoni periodici fissi
- Rinnovo parco macchine con comoda **formula noleggio**



CORE UP MAGAZINE

QUANTO COSTA UN UFFICIO FERMO A CAUSA DI UN INCIDENTE IT?



Facciamo un esempio: Un ufficio di dieci persone senza un partner **MSP** è completamente fermo ormai da due ore a causa di un **problema sull'infrastruttura IT**. L'azienda ha contattato l'assistenza tradizionale, ma il tecnico non si libererà prima di tre ore perché è da un altro cliente. Avere delle risorse inattive costa due volte all'imprenditore perché, oltre al costo del lavoro stesso, si aggiunge la mancata produttività.

DIFFERENZA TRA ASSISTENZA TRADIZIONALE E MSP

BREAK-FIX: Si tratta della classica "chiamata" attraverso la quale il **fornitore dei servizi IT** di un'azienda viene allertato rispetto a una situazione critica che si è palesata. Il fornitore viene attivato quando il guasto o il problema sta già mettendo in difficoltà l'azienda.

APPROCCIO PROATTIVO MSP: È un approccio che tende a **prevenire** e a limitare il pericolo di fermi aziendali grazie al **monitoraggio 24/7 della rete IT**. La **gestione proattiva** permette di valutare e intervenire in tempi brevi con costi prevedibili.

Cosa sarebbe successo se l'azienda avesse avuto un partner tecnologico MSP? Grazie al monitoraggio proattivo dell'ambiente IT aziendale e alle migliori competenze IT necessarie in quel momento, Core Up sarebbe potuta intervenire preventivamente (in molti casi) e da remoto. Ciò significa notevole diminuzione dei tempi morti, i cosiddetti down-time, e quindi riduzione dei costi generati dai fermi aziendali.

IL MANCATO FATTURATO E ALTRI COSTI

Se consideriamo i **costi di inattività** in ottica di mancato fatturato, pensiamo a quando un'azienda subisce un down-time con fermo lavoro, ad esempio, di tre giorni*. Oltre ai mancati guadagni è bene ricordare che andrebbero considerati altri costi, come:

- costo del **personale** inattivo
- costi per il **ripristino** dell'infrastruttura IT, il recupero dei dati e la bonifica dei sistemi
- costi legati al **danno** reputazionale (perdita del valore del brand)
- **penali** contrattuali per ritardi nelle forniture
- **sanzioni** GDPR / NIS2

**In caso di incidente IT il tempo per il ripristino dei sistemi e la ripresa delle attività è mediamente di 20 giorni lavorativi (fonte Clusit).*

CORE UP MAGAZINE

**LA STRATEGIA PER AUMENTARE LA CYBERSECURITY
IN AZIENDA? IL DISASTER RECOVERY**

Un piano di Disaster Recovery ha come obiettivo principale quello di sviluppare, testare e documentare un **iter ben strutturato** e facilmente comprensibile che permetta di **recuperare** l'operatività il più rapidamente ed efficacemente possibile dopo un disastro IT imprevisto o a causa di un'emergenza che interrompe i sistemi informativi, le piattaforme tecnologiche critiche, l'infrastruttura di telecomunicazioni e, conseguentemente, le operazioni aziendali.

Un Disaster Recovery ha due parametri chiave:

**RTO
Recovery Time Objective**

Attraverso il calcolo del Recovery Time Objective (RTO), puoi determinare il tempo massimo entro il quale la tua azienda deve recuperare l'operatività dopo un incidente. Determinando i costi e i rischi provocati dall'inattività della tua impresa, è possibile calcolare l'RTO ideale, riuscendo così a definire la strategia di backup migliore per te.

**RPO
Recovery Point Objective**

Per ridurre al minimo l'impatto di un attacco IT, è fondamentale avere un **backup*** quanto più recente possibile. Dovrai decidere ogni quanto effettuare dei backup immutabili. L'RPO indica il tempo che intercorre tra i punti di ripristino (backup). Per definire l'RPO, dovrai domandarti qual è la soglia accettabile di perdita dei dati, che ti permetta di ripartire senza subire conseguenze gravi.

***Approfondimento: I Backup Immutabili**

I backup immutabili sono copie di backup dei dati che non possono essere modificate, eliminate, crittografate o alterate in alcun modo da niente e nessuno.

Quando sono utili? In particolare quando si devono ripristinare i dati persi o danneggiati a seguito di un disastro IT o di un attacco hacker. Ma sono importanti anche per le aziende che, per conformità a requisiti normativi, devono conservare più copie dei dati.

Come funzionano? I dati immutabili sono coperti da una protezione WORM, che sta per "write once, read many".

Perché usarli? Visto il costante aumento degli attacchi ransomware, nei quali gli hacker criptano i dati e chiedono un riscatto per sbloccarli, avere un backup immutabile salva i dati dalle azioni criminali così le aziende sono pronte a ripartire nel minor tempo possibile.

CORE UP MAGAZINE

PERCHÈ PER MOLTE AZIENDE L'ADOZIONE DI UNA STRATEGIA CYBER È PERCEPITA COME UNA DECISIONE TROPPO IMPEGNATIVA?

Esistono delle barriere (concrete e psicologiche) che rallentano o impediscono lo sviluppo di una strategia cyber aziendale. Parliamo di freni e paure che portano spesso le aziende a dire **"sono cosciente dei rischi e del problema, ma non so da che parte cominciare"**.

Ecco un elenco di ostacoli che danno vita ai dubbi che frenano l'adozione di una strategia di cybersecurity:

- Spesso, laddove mancano figure specifiche in azienda, diventa difficile definire il **budget** necessario e le azioni specifiche da compiere per aumentare la resilienza informatica.
- Le conformità ai requisiti delle nuove normative (come ad esempio **NIS2**) sono spesso percepite come una fatica e non come un'opportunità per migliorare la sicurezza IT.

- La carenza di personale interno o di figure specializzate che possano dedicarsi alla **cybersecurity** in azienda spaventa chi pensa di doversi occupare di questioni troppo tecniche.
- Il timore di non riuscire a stare al passo con la continua evoluzione delle **minacce cyber** porta a sconforto e conseguente inazione.
- La mancanza di tempo per la formazione specifica delle risorse interne (**cybersecurity awareness**) genera stress e paure nel team, che si trova impreparato ad affrontare i pericoli del web.
- La paura che i **processi aziendali** diventino meno fluidi dovendo sottostare a controlli ulteriori è un freno che porta a rimandare l'adozione di una strategia IT.

**LA SPINTA VERSO LA MATURITÀ INFORMATICA: NIS2 E SUPPLY CHAIN**

Le aziende in perimetro NIS2 devono adeguarsi alle prescrizioni previste. **Ma non solo loro:** NIS2 riguarda anche (indirettamente) fornitori e subappaltatori.

Quindi, se un fornitore presenta lacune di IT security che influenzano la catena di approvvigionamento, l'azienda direttamente soggetta a NIS2 valuterà l'attenzione che i fornitori riservano alla sicurezza informatica così da preservare la propria resilienza operativa.

CORE UP MAGAZINE

**CARA AZIENDA, CHI È IL PEGGIOR NEMICO DEL TUO IT MANAGER?
NO, NON È UN HACKER, È LO STRESS!**

Uno dei rischi che impatta sulle aziende è lo stress che coinvolge i professionisti IT, i sistemisti e gli IT Manager e che porta spesso al temuto **burnout**. Lavorare sottopressione cercando di far fronte alle decine di task giornaliere in ambito IT e CYBERSECURITY in azienda non è mai piacevole né produttivo.

L'azienda può trovarsi esposta ai rischi legati, ad esempio, al mancato aggiornamento dei software o all'assenza di formazione del personale nel riconoscere e-mail malevole perché, diciamolo, un responsabile IT da solo non ha il tempo e le risorse di controllare ogni aspetto della cyber security.

La **soluzione** a questa situazione critica esiste: si chiama **IT COGESTITO** ed è il nostro strumento per dare una mano (concretamente) agli IT Manager nelle aziende.

HAI MAI SENTITO PARLARE DELL'IT-COGESTITO?**IT COGESTITO (CO-MANAGED IT)**

La **soluzione che riduce il rischio** e migliora la sicurezza informatica è un partner IT esterno che dia una mano al reparto IT nell'attivare tutte quelle strategie cyber che tengono al sicuro l'azienda, i suoi dati, il fatturato e la produzione.

**CO-MANAGED IT: non è outsourcing,
è partnership**

Non sostituisce il **reparto IT interno**, bensì lo rafforza e lo **supporta**, liberandolo dalle attività ripetitive. Un MSP (Managed Service Provider) non ruba il posto all'IT interno: gli permette di diventare più forte e di dedicarsi a progetti di digitalizzazione.

IT COGESTITO: LIBERA, NON SOSTITUISCE**UN IT MANAGER INTERNO NON DEVE
LAVORARE SOTTOPRESSIONE**

L'IT interno ha competenze verticali, conosce meglio di chiunque altro le dinamiche IT e i processi dell'azienda, MA:

- Non è **onnipresente** (va in ferie, si ammala, ...)
- Non può essere **onnisciente** (non può essere esperto di qualsiasi ambito IT)
- Non può disporre degli stessi strumenti di **monitoraggio evoluto** che mette a disposizione un MSP esterno (costi troppo elevanti per un singolo reparto IT)

**"SPERIAMO CHE NON CI SUCCEDA NULLA"
NON È UNA STRATEGIA**

Cosa fa un **MSP** esterno che collabora in modalità di IT COGESTITO?

- Monitora l'infrastruttura con strumenti avanzati
- Attiva procedure già pronte in caso di disastri IT
- Riduce al minimo i tempi di ripristino (RTO) e i dati persi (RPO)

I nostri servizi per le aziende

Noleggio operativo di stampanti, pc e hardware per l'ufficio

Nessuna gestione dei cespiti, assistenza on site e da remoto compresa, parco IT sempre aggiornato, rifornimento automatico dei toner (per le stampanti), referente unico per tutte le macchine dell'ufficio, costi di noleggio deducibili.



Novità Soluzioni di Stampa:
da oggi puoi scegliere anche
il noleggio BREVE con
durata **da 12 a 36 mesi!**

Proponiamo sia un servizio di MSP completo sia un servizio di **IT COGESTITO**, inteso come supporto per alcune delle tante attività che un reparto IT interno svolge quotidianamente.



MSP: Managed Service Provider

Un MSP aiuta a proteggere dai cybercriminali i dati sensibili e il know-how aziendale con il monitoraggio 24/7 dell'ambiente IT, la manutenzione e la gestione proattiva. In caso di attacchi o disastri IT l'azienda riparte nel minor tempo possibile, riducendo i tempi di fermo e le perdite economico-finanziarie.

IT Consulting e Progettazione Infrastruttura IT

Una consulenza IT ben fatta e proficua parte sempre da un metodo di lavoro chiaro. Core Up ascolta le necessità dell'azienda, analizza la situazione e propone i servizi e le soluzioni che migliorano davvero l'operatività e la sicurezza dell'ambiente IT.



Le fasi della **consulenza**:
Primo incontro,
Assessment, Progetto,
On Boarding, Report.

Le **potenzialità** dei nostri monitor interattivi:
Vetro antiriflesso, Risoluzione 4k,
Touch ad alta precisione,
Riassunto automatico a fine riunione, e altro ancora.



Monitor interattivi per meeting room

Gestione smart dei meeting: grazie alla nostra soluzione collaborativa ottimizzi e rendi più produttive le riunioni e la formazione del personale. Vuoi provare con mano le funzionalità dei nostri monitor? Scrivici per fissare una prova: segreteria@coreup.it

Telefonia e connettività

Core Up è partner di Vallcom, azienda con un'esperienza di oltre 40 anni nel settore delle telecomunicazioni e dell'IP-Networking: PBX (Private Branch Exchange), fornitura e installazione dei terminali, la migliore connettività sul mercato.



Vantaggi:
Interlocutore unico
Offerta costante di servizi
Qualità e trasparenza

*I nostri **SPECIAL**: le soluzioni per aumentare la sicurezza cyber e proteggere il tuo lavoro*

Abbiamo creato dei pacchetti di servizi altamente specializzati per valutare e verificare la **maturità informatica** della tua azienda e il **livello di cybersecurity** per migliorarlo. Qui proponiamo tre servizi che, contattandoci allo 030.4194040 o scrivendo a info@coreup.it possiamo preventivare a un **costo speciale** nei mesi di **gennaio e febbraio 2026**:

VULNERABILITY ASSESSMENT

Analisi di sicurezza che identifica le potenziali vulnerabilità dei sistemi e dell'infrastruttura informatica di un'azienda. Diventa così possibile valutare attraverso quali canali l'azienda potrebbe essere attaccata e il danno che potrebbe subire e, di conseguenza, pensare a soluzioni che aumentino il livello di impenetrabilità.

PENETRATION TEST

Attacco informatico simulato e controllato, condotto da un MSP per identificare (e quindi poi correggere) le vulnerabilità dei sistemi, delle reti o delle applicazioni aziendali. Si ottiene così una visione realistica del grado di sicurezza di un'azienda, si scoprono i punti deboli di un'infrastruttura IT e si testano le misure di sicurezza per correggere le vulnerabilità prima che possano essere sfruttate dai cybercriminali.

IT CONSULTING

I risultati ottenuti dai due test precedenti vanno interpretati da un MSP esperto, che fornirà una consulenza IT su misura sulla base delle reali necessità del cliente, tenendo conto delle normative vigenti (ad esempio NIS2).

Progettiamo soluzioni concrete che migliorano l'operatività, l'efficienza e la sicurezza della tua infrastruttura IT e monitoriamo le attività svolte attivandoci in ottica propositiva.

Chi siamo

Core Up lavora per far sì che le aziende siano libere di dedicarsi alla propria attività senza preoccuparsi della **gestione**, del funzionamento e della sicurezza degli **hardware** dell'ufficio, dei software e dell'**infrastruttura IT** aziendale.

Proponiamo servizi di **monitoraggio costante e proattivo** e di manutenzione e aggiornamento dell'ambiente IT per prevenire e ridurre i **rischi cyber**. Inoltre, offriamo il noleggio operativo delle macchine per l'ufficio, la migliore connettività e telefonia per le aziende e una consulenza IT altamente personalizzata.



Soluzioni IT per la continuità
e la sicurezza del tuo business

Diamo i numeri

500 clienti

24/7 monitoraggio
dell'ambiente IT

700 stampanti e
multifunzioni a noleggio

30 anni di esperienza



Perché scegliere Core Up?

- Professionalità ed esperienza
- Reperibilità e tempi di intervento certi
- Costi sotto controllo con comodi canoni periodici personalizzabili
- Produttività aziendale ottimizzata
- Parco IT sempre aggiornato

Seguici su LinkedIn



Questo magazine è stato
lasciato da: _____