GUIDA ALLA SOPRAVVIVENZA

SE LAVORI COME IT MANAGER, SISTEMISTA

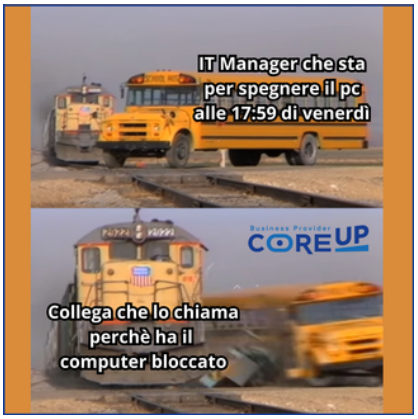
O TECNICO INFORMATICO IN AZIENDA

Cosa troverai all'interno:

- Una panoramica sui rischi di stress e burnout legati alla tua professione
- Info e vantaggi dell'**IT COGESTITO**
- Un UTILISSIMO e CONCRETO esempio di dialogo tra un IT Manager e la Dirigenza per convincere il tuo capo ad attivare un supporto IT cogestito che ti aiuti davvero

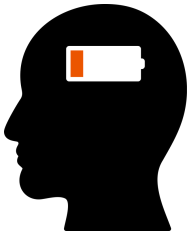
Business Provider
COREUP

Caro IT Manager, Sistemista o Tecnico Informatico, se ti riconosci in questi meme,
su con la vita e leggi questa guida: **NON SEI SOLO, CORE UP TI AIUTA!**



Per altri meme
guarda qui:

Stress e Burnout: i nemici della tua professionalità



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 **CYBER SECURITY** 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.

Come funziona l'IT COGESTITO?

Per cominciare prendiamo in carico tutte le azioni ricorsive e necessarie in modo che le risorse interne si concentrino su altro (richieste dei colleghi, studio e sviluppo di nuove soluzioni, etc).
Poi possiamo affiancare i reparti IT con tutte le nostre competenze e gli strumenti di MSP per monitorare e manutenere l'infrastruttura IT.

Quindi: **Grazie all'IT COGESTITO un Managed Service Provider come Core Up supporta strategicamente il tuo team IT interno.** Ecco come:
- Gestendo tutte quelle attività (ricorsive) che richiedono troppo tempo al dipartimento interno (gestione antivirus, aggiornamenti di sistema, gestione firewall, adeguamenti normative NIS2)
- Contribuendo in modo significativo ad aumentare la sicurezza IT grazie al monitoraggio proattivo 24/7 dell'infrastruttura IT
- Aumentando le competenze specifiche del dipartimento IT interno grazie all'esperienza, a figure altamente specializzate e ai servizi di consulenza IT su misura.

“Il mio capo ha detto che non abbiamo budget per la cybersecurity!”

Vogliamo aiutarti ancor prima di diventare il tuo **partner tecnologico di fiducia**: ecco una serie di **risposte e argomentazioni** che puoi riferire al tuo titolare per convincerlo ad **investire nel reparto IT** (evitandoti stress, burnout e liste infinite di task da completare).

Ricorda: se l’azienda per cui lavori subisce una perdita di dati, un attacco hacker o un fermo lavoro potrebbero chiederti come mai non sono state prese tutte le misure necessarie per evitarlo o limitare i danni. Previeni: parla con il tuo titolare, esponi perplessità e rischi, porta esempi e commenta dati certi sui costi che un incidente IT può generare.

IT MANAGER

“Sono qui per proporre di investire nel reparto IT esternalizzando alcuni servizi in modalità co-gestita, cosicché un partner IT esterno mi dia un supporto tecnico per migliorare la sicurezza informatica in azienda”

CEO

“Quest’anno abbiamo già speso tutto il budget destinato al reparto IT, mi dispiace!”

Capisco che il **budget** sia una questione rilevante, ma vorrei farLe una domanda: **Quanto costerebbe, invece, un ufficio fermo per ore o giorni a causa di un attacco hacker o di un collega che clicca su un’e-mail con dentro un virus?**”

“Non saprei! Lei lo sa?”

“Prendiamo un’azienda che fattura € 1.000.000,00 in un anno. Consideriamo una giornata lavorativa di 8 ore per 300 giorni all’anno. Organizziamo questi numeri in una formula: 1.000.000 : (8 ore al giorno x 300 giorni lavorativi x 60 minuti/ora) = € 6,94/minuto
Che moltiplicati per 60 minuti fa € 416 all’ora (quindi, € 3.328,00 al giorno).
I costi di inattività considerati in questa formula sono in ottica di “MANCATO FATTURATO” rispetto a quello annuale: pensi se questa azienda subisse un downtime con fermo di lavoro per tre giorni! Oltre al mancato fatturato è bene ricordare che andrebbero sommati anche altri costi, come il costo del personale inattivo, i costi per il ripristino dell'infrastruttura IT e i costi legati al danno reputazionale”.

IT MANAGER

THE BOSS

“Ok, ma di sicuro non falliremo per un incidente IT suvvia…”

“Certo che un **attacco hacker** può anche far **fallire** un’azienda! Vuole un esempio? Estate 2025: in Germania fallisce un’azienda da 70 milioni di euro e 170 dipendenti a causa di un attacco hacker subito nel 2023. Einhaus Group, azienda di riparazioni e assicurazioni per gli smartphone, ha subito un attacco a marzo 2023 che ha causato, nell’immediato, il blocco delle operazioni e una richiesta di riscatto di 200.000 Bitcoin, e nel lungo periodo il **fallimento**.

Ad un certo punto le perdite legate al down time hanno superato l’importo del riscatto richiesto: l’azienda ha quindi deciso di pagare MA ORMAI il **danno economico**, sommato a quello reputazionale, ha creato una **caduta irreversibile**.

Se un disastro del genere può colpire una grande azienda che fatturava 70 milioni di euro, pensiamo a quale impatto un attacco hacker o un incidente IT potrebbe avere su aziende più piccole, con risorse più limitate.
È per questo che diventa fondamentale e strategico ragionare sul valore della prevenzione, del controllo e del monitoraggio dell’ambiente IT della propria azienda: proteggere i dati sensibili di clienti, dipendenti e fornitori, così come il know-how aziendale, significa investire nel futuro e nella longevità della propria azienda”.

“Ma noi siamo una piccola azienda, mica una multinazionale! Non siamo un bersaglio interessante per gli hacker!“

IT MANAGER **THE BOSS**

Secondo il Clusit (Associazione italiana per la sicurezza informatica) in Italia le **piccole aziende** sono diventate uno dei **bersagli preferiti dai cybercriminali**. Ecco le ragioni:

1.Le piccole imprese sono più vulnerabili e più facili da attaccare perché solitamente non investono o non hanno budget da dedicare alla sicurezza informatica.

2.Gli hacker utilizzano software automatizzati che scandagliano la rete alla ricerca di falle e vulnerabilità, indipendentemente dalla grandezza dell'azienda

3.Gli hacker sono organizzati in società che sferrano diversi attacchi contemporaneamente in tutto il mondo. Questo porta a una dilatazione notevole del campo di azione.

4.Molto spesso le piccole imprese che vengono attaccate collaborano con aziende molto più grandi; quindi, diventano un punto di accesso indiretto per gli hacker".

"A noi non accadrà mai nulla perché abbiamo l'IT Manager più bravo del mondo!" (affermazione seguita da buffetto affettuoso sulla guancia)

"Beh, grazie del complimento ma ho letto il Future of Cyber Survey 2025 di Deloitte (azienda specializzata in Risk Management) e ci ho trovato una frase interessante: ***"Gli investimenti in cybersecurity possono ottimizzare, preservare e generare valore per l'intera organizzazione".***

Eh già, perché gli investimenti in ambito cyber aiutano a prevenire costi e danni reputazionali a seguito di un incidente IT / attacco hacker e servono a garantire ai propri clienti e fornitori una strategia per la protezione dei dati e dei processi diventando un vantaggio competitivo sul mercato".

"La verità è che sembra che le cose non siano importanti finché non ti capita qualcosa o finché non diventano obbligatorie..."

IT MANAGER **THE BOSS**

“Mi permetto di sottolineare che in realtà una certa obbligatorietà c’è già: ha presente la **NIS2**? Quella **direttiva europea** che implementa i controlli di sicurezza, introducendo un innovativo scenario di vigilanza per ridurre i rischi e prevenire i danni informatici…”

“Questa la so! La interrompo subito: la nostra azienda non rientra in nessuna categoria di obbligatorietà, quindi siamo a posto!”

“Verissimo, ma alcuni dei nostri maggiori clienti saranno direttamente interessati da questa direttiva e noi, rientrando nella sua **catena di approvvigionamento**, siamo tenuti a garantire alti standard di sicurezza informatica.
Se non lo facciamo potremmo rischiare di essere rimpiazzati da un altro fornitore, che a differenza nostra, ha già deciso di investire nel **potenziamento del reparto IT**. È anche una questione di immagine: se ci presentiamo come azienda sicura risultiamo più affidabili, non crede?”

“Ok, mi ha convinto! DA DOVE COMINCIAMO?”

“Che ne dice di incontrare Core Up, l’azienda che potrebbe diventare il nostro partner tecnologico per l’IT COGESTITO? Così si renderà conto anche Lei di tutto quello che possono fare per noi. Che poi, gliela butto lì, oltre alla **cybersecurity**, si occupano di **consulenza e progettazione dell’ambiente IT** e di **noleggio operativo di stampanti**, multifunzioni, pc, server e software.
Non voleva mica sostituire i vecchi pc? Sicuramente un unico partner che segua tutta la tecnologia in ufficio sarebbe comodo, utile e vantaggioso economicamente…“

RECAP IT COGESTITO: I CONCETTI CHIAVE

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 didigitalizzazione.

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 e dorme come tutti)
- Non può essere onnisciente (non può essere eserto 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 il tempi di ripristino (RTO) e i dati persi (RPO)

Cosa ti separa dal supporto IT proattivo in modalità cogestita che aumenta la sicurezza e alleggerisce il tuo lavoro?

Una chiacchierata con la dirigenza
(usa lo schema di dialogo che abbiamo scritto)

Una telefonata allo 030.4194040 per un appuntamento conoscitivo e di approfondimento

030.4194040

info@coreup.it

segreteria@coreup.it

www.coreup.it

Core Up Srl

Via Bruno Buozzi 1/A

25125 Brescia

Seguici su LinkedIn: