IT•NEWS

N. 7 MAG./GIU. 2022

L'indispensabile road-book

per rendere sempre più digitale e competitiva la tua impresa

IN QUESTO NUMERO

L'EDITORIALE

A cura di **Alessio Angioli**

Alfabetizzazione Digitale

Perché è importante lo sviluppo di competenze e formazione

Il digitale risiede al centro della nostra società. Negli anni passati poteva rappresentare un optional, mentre oggi è parte integrante e ineliminabile della nostra quotidianità. I dati annuali raccolti negli indici DESI come altri studi, mostrano che l'alfabetizzazione digitale nel nostro paese è ancora troppo scarsa: le abitudini del singolo faticano a seguire i continui cambiamenti e nuove strade digital. Ed è così che il processo di costruzione di nuove abilità e professionalità non decolla.

Le opportunità della digitalizzazione rappresentano lo strumento di cambiamento dei processi, dei ruoli, dei servizi ai clienti. In sostanza fanno parte delle nuove strategie aziendali e la formazione è indispensabile per l'innovazione dei modelli organizzativi. Il posizionamento di un'impresa sul mercato dipende dalla comprensione dell'imprenditore nel vedere che la crescita delle persone sono il suo principale strumento di sviluppo.

Lo sviluppo tecnologico delle imprese finalmente è a portata di mano.

Saranno estesi fino a tutto il 2023 gli incentivi e le agevolazioni Industria e Formazione 4.0.

Approfitta dei corsi di formazione 4.0 e ottieni il bonus per credito d'imposta. Maggiori info sul sito del MISE

L'agevolazione vuole incoraggiare le imprese ad investire sulla formazione del personale sulle materie aventi riguardati la digitalizzazione.

Il Credito d'imposta, pari al 50% delle spese sostenute dalle aziende per la formazione del personale dipendente finalizzata all'acquisizione o al consolidamento delle competenze per la trasformazione tecnologica e digitale 4.0 (articolo 1, comma 210 e seguenti, legge 160/2019), resta applicabile fino alle spese sostenute nel periodo d'imposta in corso al 31 dicembre 2022.

INTERVENTI AMMISSIBILI

Il bonus può essere utilizzato per la formazione sulle tecnologie previste dal Piano Nazionale Industria 4.0 sui temi:

- **Big data e analisi dei dati;**
- **Cloud e fog computing;**
- **Cyber security;**
- **Sistemi cyber-fisici;**
- **Prototipazione rapida;**
- **Sistemi di visualizzazione e realtà aumentata;**
- **Robotica avanzata e collaborativa;**
- **Interfaccia uomo macchina;**
- **Manifattura additiva;**
- **Internet delle cose e delle macchine;**
- **Integrazione digitale dei processi aziendali.**

LE ATTIVITÀ FORMATIVE DOVRANNO RIGUARDARE I SEGUENTI AMBITI:

- **Vendita e marketing;**
- **Informatica e tecniche;**
- **Tecnologie di produzione.**

AGEVOLAZIONI

- **Credito di imposta del 50% delle spese sostenute per le Piccole Imprese con un MAX di 300.000 € annui**
- **Credito di imposta del 40% delle spese sostenute per le Medie Imprese con un MAX di 250.000 € annui**
- **Credito di imposta del 30% delle spese sostenute per le Grandi Imprese con un MAX di 250.000 € annui**
- **Credito di imposta del 60% delle spese sostenute nel caso in cui i destinatari delle attività di formazione ammissibili rientrino nelle categorie dei lavoratori dipendenti svantaggiati o molto svantaggiati**

SPESE AMMISSIBILI

Le spese ammissibili al credito di imposta formazione 4.0 sono:

- **-le spese di personale relative ai formatori per le ore di partecipazione alla formazione;**
- **-i costi di esercizio relativi a formatori e partecipanti alla formazione direttamente connessi al progetto di formazione, quali le spese di viaggio, i materiali e le forniture con attinenza diretta al progetto, l'ammortamento degli strumenti e delle attrezzature per la quota da riferire al loro uso esclusivo per il progetto di formazione;**
- **-i costi dei servizi di consulenza connessi al progetto di formazione;**
- **-le spese di personale relative ai partecipanti alla formazione e le spese generali indirette (spese amministrative, locazione, spese generali) per le ore durante le quali i partecipanti hanno seguito la formazione.**

I·TEAM

Dal 18 maggio riapre il bando della Camera di Commercio di Firenze, concedendo voucher digitali alle micro, piccole e medie imprese di qualsiasi settore che risiedono sul territorio fiorentino.

VALORE DEL VOUCHER

Fino a 6.000 euro nella misura del 50% dell'importo complessivo delle spese ammesse ed effettivamente sostenute, oltre la premialità di cui all'art. 4 del disciplinare, relativo al rating di legalità. L'investimento minimo richiesto è di euro 3.000.

Conoscere i fondamenti di internet e del digitale è basilare come fattore di crescita personale, ma anche nei rapporti sociali, nelle interazioni con le amministrazioni pubbliche e come elemento di base per svolgere qualunque attività lavorativa. Ridurre il gap della "digital divide culturale" è l'obiettivo del programma che troviamo all'interno del PNRR, e la formazione ha un ruolo centrale perché questa fa parte della nostra esistenza e come tale deve essere pianificata e gestita, soprattutto dalle aziende. Per questo avete bisogno della forza dell'I-Team, professionisti di estrazione diversa con competenze complementari e un'elevata specializzazione in comparti specifici. Diamo risposte uniche e subito operative per le vostre richieste.

L'APPROFONDIMENTO DEL MESE

POSSIBILI RISCHI CYBER derivanti dalla situazione Ucraina e nuove misure di protezione delle infrastrutture digitali nazionali

(ovvero "LA CYBERSICUREZZA SPIEGATA A MIA NONNA")

A cura di
Federico Melucci

Il conflitto ucraino-russo, purtroppo, ci coinvolge pesantemente per quanto riguarda la guerra cibernetica in atto.

Gli attacchi informatici, in Italia, sono in forte e continuo aumento in particolar modo da un mese prima del conflitto sul campo.

Anche se non gestiamo, nel nostro sistema, dati che possano essere ritenuti importanti, non siamo esenti da attacchi informatici che ci possono creare danni importanti.

Gli attacchi hacker sono in continua ricerca di sistemi poco protetti indipendentemente dai dati gestiti dagli stessi.

Un sistema poco protetto è un ottimo "ponte" per sferrare attacchi a siti istituzionali e commerciali, bersagli sensibili come obiettivi cyber-bellici.

La conseguenza naturale ad un attacco sferrato da un ignaro sistema informatico non protetto è che tale sistema risulta correo dell'attacco sferrato ad obiettivi sensibili e soggetto a visite (inaspettate e poco gradite) della polizia postale o di altro organismo di indagine.

Il sistema informatico poco protetto che gestisce invece dati importanti per l'azienda è soggetto, oltre a ciò sopra descritto, anche alle richieste di riscatto di un attacco ransomware, con cui i gruppi di hacker in guerra tra loro si autofinanziano.

- L'Agenzia per la cybersicurezza nazionale (https://www.acn.gov.it/) e il CSIRT (https://www.csirt.gov.it/) sono due organismi istituiti per decreto legge a tutela degli interessi nazionali per la Cybersicurezza.

  Il CSIRT, in particolare, ha dettato le linee guida per alzare il livello di attenzione a protezione dei possibili rischi causati dalla situazione in Ucraina in tema di sicurezza informatica.
  (Trovate il link a queste misure direttamente dalla home page del loro sito, oppure al seguente indirizzo: https://www.csirt.gov.it/contenuti/misure-di-protezione-delle-infrastrutture-digitali-nazionali-dai-possibili-rischi-cyber-derivanti-dalla-situazione-ucraina-bl01-220214-csirt-ita)

Di seguito sintetizziamo e spieghiamo in parole semplici le azioni che sono raccomandate.

MISURE ORGANIZZATIVE/ PROCEDURALI:

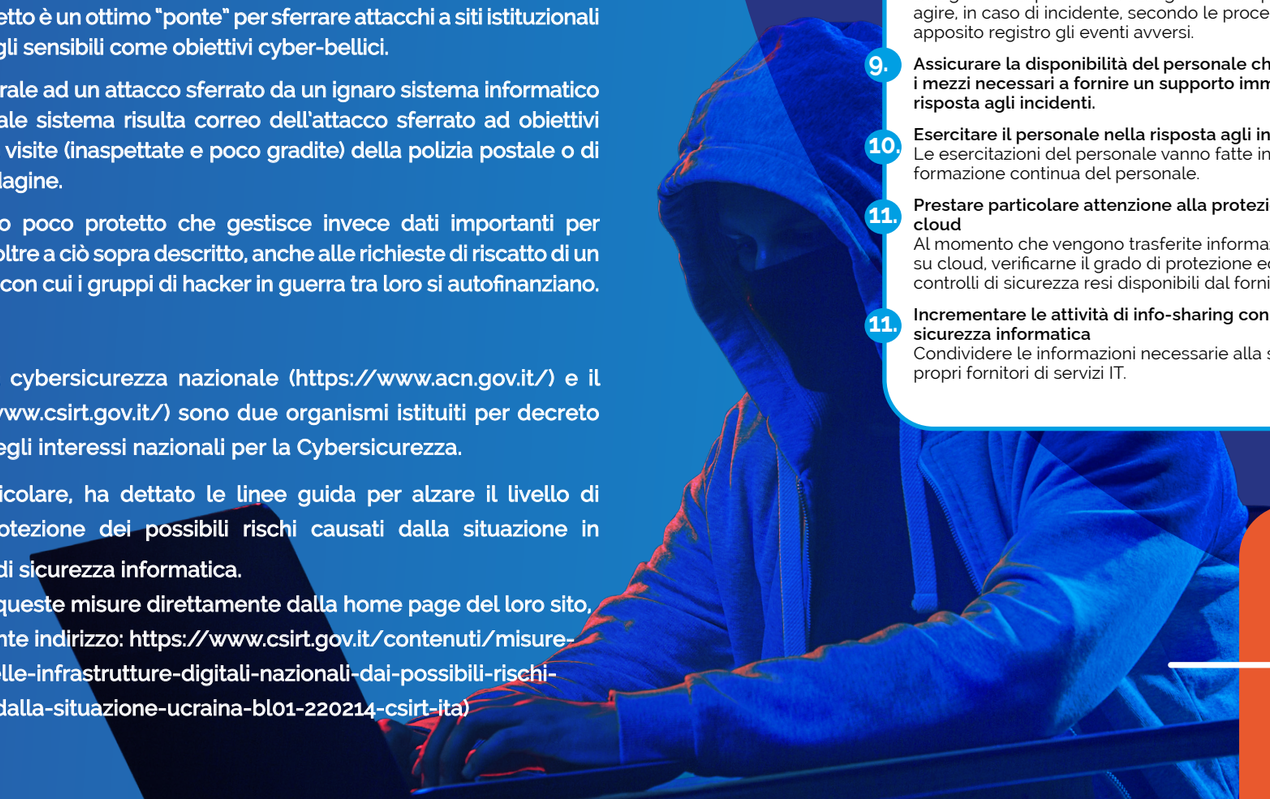
1. **Verifica della consistenza e disponibilità offline dei backup necessari**
   Implementare, oltre che ad un sistema di copie di backup in locale, anche un sistema di copie in cloud dei dati più importanti
2. **Identificazione dei flussi informativi**
   Identificare, anche tramite procedure documentate, come e dove vanno le informazioni aziendali. L'attenzione deve essere posta sia alle informazioni digitali che a quelle cartacee.
3. **Implementazione di una zona DMZ**
   La zona DMZ (Demilitarized Zone) è quella "zona cuscinetto" messa a protezione della rete interna che impedisce un accesso diretto da Internet verso programmi e servizi aziendali.

   La DMZ viene implementata proprio per far sì che un eventuale attacco da esterno limiti la propria azione alla stessa e non penetri all'interno. Se l'azienda opera con commercio elettronico B2B o B2C è opportuno che il sito e-commerce e i dati relativi siano ospitati in una zona DMZ.
4. **Applicazione del principio di privilegio minimo**
   Evitare di dare agli utenti permessi di accesso alle informazioni superiori a quelle necessarie. Specialmente quando questi utenti hanno la possibilità di accesso da remoto.
5. **Incremento delle attività di monitoraggio e logging**
   Monitorare, anche attraverso l'ausilio di software e/o servizi specifici, chi, quando e come ha effettuato un accesso al sistema informativo e le operazioni che ha effettuato dopo tale accesso.
6. **Aggiornamento dei piani di gestione degli incidenti cyber**
   Aggiornare il Piano di Continuità e Resilienza con le procedure di attenuazione del rischio e il registro degli eventi riguardanti gli incidenti informatici.
7. **Creazione, aggiornamento, mantenimento di un piano di continuità operativa e resilienza**
   Attivare ed aggiornare il registro degli eventi in caso di perdita di accesso o di controllo in ambiente informatico e/o operativo.
8. **Designazione di un team di risposta alle crisi**
   Designare i responsabili e assegnare i compiti per chi dovrà agire, in caso di incidente, secondo le procedure scrivendo su apposito registro gli eventi avversi.
9. **Assicurare la disponibilità del personale chiave, identificare i mezzi necessari a fornire un supporto immediato per la risposta agli incidenti.**
10. **Esercitare il personale nella risposta agli incidenti informatici**
    Le esercitazioni del personale vanno fatte in ambito della formazione continua del personale.
11. **Prestare particolare attenzione alla protezione degli ambienti cloud**
    Al momento che vengono trasferite informazioni importanti su cloud, verificarne il grado di protezione ed utilizzare tutti i controlli di sicurezza resi disponibili dal fornitore di servizi cloud.
11. **Incrementare le attività di info-sharing con le strutture di sicurezza informatica**
    Condividere le informazioni necessarie alla sicurezza IT con i propri fornitori di servizi IT.

MISURE TECNICHE:

1. **Dare priorità alle attività di patching dei sistemi internet-facing**
   Aggiornare e tenere aggiornati i sistemi e i programmi che si collegano, anche saltuariamente, ad Internet.
2. **Verifica delle interconnessioni tra la rete IT e le reti OT**
   La Tecnologia dell'Informazione (IT) controlla i dati; la Tecnologia Operativa (OT) controlla le apparecchiature. Se in passato le due tecnologie non avevano contatti, con l'avvento della " Internet Of Things" (IoT o, tradotto, Internet delle Cose) questi contatti sono frequenti (ad esempio il controllo del riscaldamento da smartphone, il controllo delle telecamere di sorveglianza ecc.) e sono "cavalli di Troia" molto apprezzati dagli hacker per entrare nella rete aziendale e prenderne il controllo.

   È necessario verificare l'integrità e la sicurezza delle interconnessioni tra queste due reti.
3. **Monitoraggio degli account di servizio e degli account amministrativi**
   Tutti gli account devono essere monitorati negli accessi al sistema e alle procedure.
4. **Monitoraggio dei Domain Controller**
   Monitoraggio del server di dominio, cioè il server che permette di accedere ai dati dell'utente da qualunque pc della rete.
5. **Ricerca di processi e/o esecuzione di programmi da linea di comando che potrebbero indicare il dump di credenziali**
   Ricerca di processi e/o programmi in grado di poter intercettare e copiare le credenziali di accesso al sistema.
6. **Monitoraggio dell'installazione di software di trasferimento**
   Verificare se nella rete sono installati (senza motivo) software di trasferimento (come ad esempio FileZilla) o di archiviazione su cloud (ad esempio Rclone).
7. **Monitoraggio del traffico di rete analizzando picchi anomali nella connettività di rete in uscita**
   Controllare o far controllare regolarmente dal proprio fornitore di servizi IT il traffico rete in uscita e in ingresso dai dispositivi di collegamento tra rete interna ed esterna (firewall e router).
8. **Dare priorità alle analisi a seguito di individuazione di codice malevolo**
   Se viene trovato software malevolo nel sistema informatico, non procrastinare l'analisi del perché è nel sistema e la messa in sicurezza del sistema stesso.
9. **Assicurarsi che tutti gli accessi remoti richiedano l'autenticazione a più fattori (MFA)**
   Tutti gli accessi da esterno devono richiedere non solo la password ma anche un altro fattore di autenticazione, ad es. il codice tramite SMS.



La Pantarei Informatica Srl offre un Servizio di Analisi dei rischi ai propri clienti al fine di attuare le misure di sicurezza consigliate dagli organi preposti.

PRENOTALO SUBITO!

A cura di
Marco Melucci

WHATSAPP BUSINESS

L'APP di messaggistica rientra nella classifica degli strumenti di comunicazione più utilizzati

Nell'ormai lontano 2014, Zuckerberg aveva intuito le potenzialità di WhatsApp: infatti, già nel 2018, sviluppa la versione Business, progettata specificamente per le PMI.

E i numeri lo dimostrano:

- 2 miliardi di utenti attivi al mese di cui 33 milioni di Italiani
- 60 miliardi di messaggi scambiati al giorno
- un tasso di coinvolgimento del 98% nei messaggi letti e il 90% di messaggi letti in 3 secondi dalla ricezione

Uno degli Asset più importanti da mettere a budget per la vita della propria azienda è avere un **sofisticato sistema di protezione**.

Non è un caso che i servizi di sicurezza informatica abbiano oggi un ruolo decisivo. Una delle azioni fondamentali da seguire per ridurre al minimo il rischio di attacchi informatici e non farsi cogliere impreparati è la **dotazione di antivirus di alto livello come Eset Endpoint Security.**

La tua azienda deve essere dove è il tuo cliente, e il tuo cliente è dentro WhatsApp. That's it.

WhatsApp Business permette l'invio di messaggistica istantanea, semplice e diretta, consentendo di automatizzare e organizzare l'interazione con i propri clienti, al fine di agevolare le **strategie di marketing One to One**. Comunicare in tempo reale con i clienti su una piattaforma che ritengono perfettamente, certificata e di cui hanno totale fiducia, incrementa e conferma il posizionamento del brand identity e il profitto. Anche i **messaggi di risposta automatica** sono una funzione molto apprezzata, perché consentono di gestire le operazioni di assistenza clienti in momenti specifici della giornata se lo preferite, oppure in caso di momentanea assenza.

La funzione Integrazione del catalogo consente di creare, integrare e sfogliare i cataloghi dei prodotti.

Da poco sono attive le Reactions, molto utili perché rendono un feedback immeditato.

Le news 2022 che incrementeranno il tuo business.

Finalmente sono in arrivo nuove funzioni che porteranno maggiori benefici alle aziende che utilizzano WhatsApp Business:

- **Inserimento immagine di copertina nei profili business.** Questa nuova possibilità è un grande vantaggio a livello di marketing aziendale. Se prima avevamo una sola immagine per raccontare l'azienda, d'ora in avanti avete più chance. Per esempio, se è in corso una promozione, sarà possibile metterla in evidenza. L'infografica della copertina non risulta invadente come l'invio diretto di messaggi.
- **Attivazione della Community.** L'amministratore potrà raggruppare i gruppi in uno spazio semplice da gestire. È una funzione ottimale per dividere i diversi reparti in gruppi, raggruppandoli nelle community. Oro colato per dare informazioni di tipo generale che interessano tutti o solo a specifici gruppi.
- **Funzione Sondaggi.** Strettamente legata alle chat di gruppo, ogni utente "del gruppo" potrà creare sondaggi, a cui gli altri potranno votare in un click, e a fine sondaggio tutti potranno verificare il risultato, Con questa nuova funzione saranno ridotte le troppe notifiche dei gruppi e risultati sempre sotto controllo diventando un valido strumento a livello organizzativo aziendale.
- **Gestione Ordini.** L'aspetto logistico è fondamentale per la corretta gestione degli ordini: così avrete in un unico posto le comande della merce da preparare per il ritiro o la consegna. Per il momento, la funzione "Carrello" permette agli utenti di raggruppare più articoli in un solo ordine, ma è necessario comunque dividere le chat per stato dell'ordine con Etichette come "da evadere", "in preparazione" e "consegnati".

A breve si potranno **mostrare in chat i propri prodotti caricati su Facebook e Instagram Shop,** rafforzando il legame tra le tre applicazioni.

Altra novità riguarda la **funzione che notifica quando un prodotto, per esempio, torna disponibile**.
Un avvertimento immediato e gradito dall'utente.

Per **WhatAspp Pay** c'è ancora da aspettare ma l'opportunità di effettuare pagamenti direttamente dalla piattaforma potrebbe diventare concreta addirittura a fine 2022.

WhatsApp Business è un'altra opportunità offerta dal digital per promuovere la tua attività, comunicare con i tuoi clienti e acquisirne di nuovi, rimanendo sulla cresta dell'onda e tenendo testa ai competitor agguerriti.

A cura di
Paolo Vannini

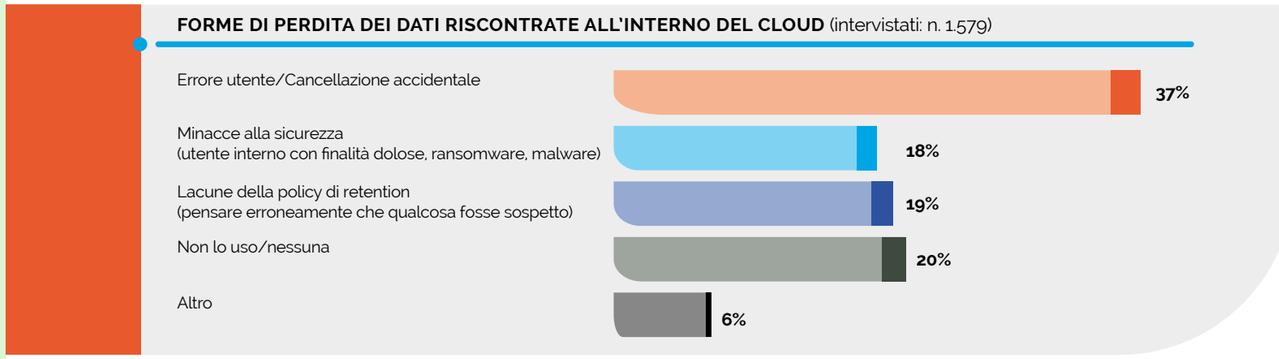
SOLUZIONI BACKUP MICROSOFT 365

La scelta intelligente che evita la perdita dei tuoi dati nel cloud

La protezione dei dati e il loro recupero sono un argomento delicato su cui ci si può facilmente confondere e, di conseguenza, possono crearsi delle situazioni spiacevoli di vulnerabilità. Microsoft 365 è una piattaforma SaaS robusta ed estremamente funzionale che risponde perfettamente alle esigenze di molte organizzazioni. Offre l'Availability e l'Uptime delle applicazioni per garantire la produttività degli utenti. Molte aziende sono fortemente convinte che Microsoft 365 ed altre applicazioni similari siano dotate di un sistema di salvataggio mediante il quale in caso di perdita del dato o del documento, esso possa essere recuperato in qualsiasi momento e in qualsiasi luogo. Ed è così, **ma solo se hanno implementato una soluzione di backup in grado di offrire accesso completo ai dati di Microsoft 365 e il loro completo controllo.**

Il dubbio si colloca tra la responsabilità mal identificata di Microsoft e l'effettiva responsabilità dell'utente di garantire la protezione e la retention a lungo termine dei dati di Microsoft 365. Microsoft si occupa dell'infrastruttura e fornisce la georidondanza che spesso viene confusa con il backup, per cui la responsabilità dei dati rimane a carico del cliente.

Una dettagliata analisi ha rivelato che il 76% delle organizzazioni intervistate non possiedono sistemi di backup ; ovvero, 6 su 10 ne sono sprovviste, mettendo a rischio i loro dati nel cloud. I file e le cartelle cancellati nel cloud di Microsoft 365 sono mantenuti per un tempo di 140 giorni; dopo, il dato viene perso definitivamente.
Quando ci rendiamo conto di questa mancanza, ormai è troppo tardi e i dati preziosi sono ormai persi.



Alcuni dei motivi per cui il **backup di Microsoft 365** è fondamentale e rientra in questa stima a fianco, ma ci sono altri fattori come:

- **Requisiti legali e di conformità**
- **Gestione di distribuzioni e migrazioni di e-mail ibride a Microsoft 365**
- **Minacce esterne alla sicurezza**

Con le giuste soluzioni di backup, se elimini accidentalmente o intenzionalmente le e-mail o dei documenti prima di implementare un blocco per motivi legali, sarai comunque in grado di ripristinarli per assicurarti di adempiere ai tuoi obblighi legali. Inoltre, eseguire il backup con regolarità garantisce che una copia separata dei dati sia priva di infezioni e facilmente recuperabile. I backup possono essere utili anche in scenari a breve termine.

Ad esempio, se un dipendente dice qualcosa di inappropriato in una conversazione di Teams, ma poi elimina il messaggio, avere un backup renderebbe quelle chat recuperabili e disponibili per la revisione delle risorse umane.

- La protezione mediante il backup è essenziale per il successo della tua attività. L'I-TEAM propone le migliori soluzioni e tecnologie di backup e di protezione avanzata anche in caso di sofisticato attacco malware. Finalmente la tua impresa può dormire sonni tranquilli, ma solo se ti rivolgi ad I-TEAM, proponiamo le migliori soluzioni di ripristino dei dati, evitando interruzioni dell'attività e garantendo la continuità operativa.

I·TEAM

Cinque società che si sono unite per dare forma a un grande progetto:
aiutare le imprese a crescere nella digitalizzazione
e nella rivoluzione digitale, per avere performance
sempre più efficaci ed efficienti, all'altezza dei grandi cambiamenti
dell'economia e della società contemporanea.

Allyou.srl

ego communication

GlobalNet
Servizi di Telecomunicazioni per la tua Azienda

OMEGA SISTEMI
Soluzioni Informatiche Professionali

NETWORK PRIVACY

PANTAREI INFORMATICA
La tecnologia resa semplice

WWW.I-TEAM.TECH

Via Benedetto Dei 64 · 50127 FIRENZE · Numero Verde 800-199760 · info@i-team.tech