smeup

WEBINAR

Proteggi i tuoi dati aziendali con strategie moderne

Backup, *crittografia* e *conformità normativa* per la sicurezza dei tuoi sistemi.

13 MARZO
2025

EDU TIPS
CYBERSECURITY

EDU TIPS | smeup

Sicurezza informatica, il percorso formativo per rafforzare la tua sicurezza aziendale.

Le minacce digitali sono in continua evoluzione e affrontarle con consapevolezza è fondamentale.

Smeup ti invita a seguire un **percorso formativo gratuito** composto da **10 webinar di 30 minuti** , pensati per guidarti con soluzioni pratiche e strategie concrete nella **sicurezza aziendale** .

EDU TIPS Cybersecurity

10 webinar TIPS - 30 minuti al mese
su tematiche specifiche di Cybersecurity

DATA	DESCRIZIONE
28/1	Mese 1: **Sicurezza dell'infrastruttura**
13/2	Mese 2: **Cyber Security Awareness**
13/3	**Mese 3: Data Protection**
10/4	Mese 4: **Identità e accesso**
13/5	Mese 5: **Cloud security**
12/6	Mese 6: **Incident response**
8/7	Mese 7: **Sicurezza delle applicazioni**
11/9	Mese 8: **Analisi delle minacce e vulnerability assessment**
10/10	Mese 9: **Sicurezza delle reti industriali (OT)**
11/11	Mese 10: **Sicurezza in ambito A.I.**

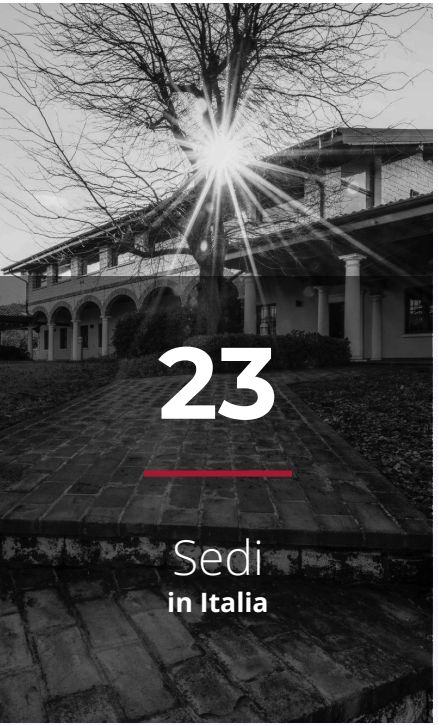
👉 **SCOPRI DI PIÙ**

COMPANY OVERVIEW

smeup in breve.

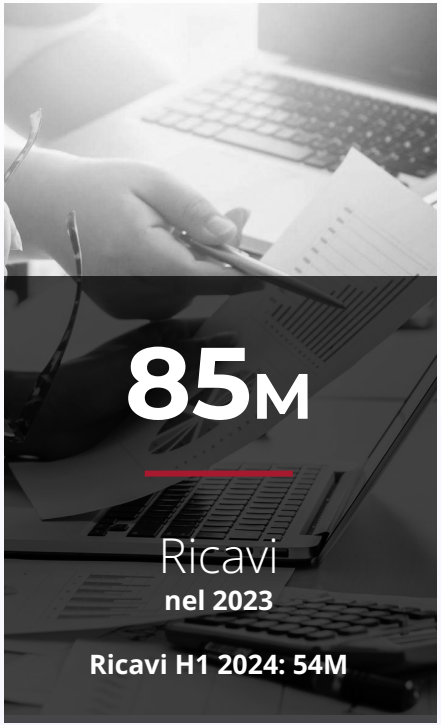
COMPANY **OVERVIEW**

smeup in Numeri.



23

Sedi
in Italia



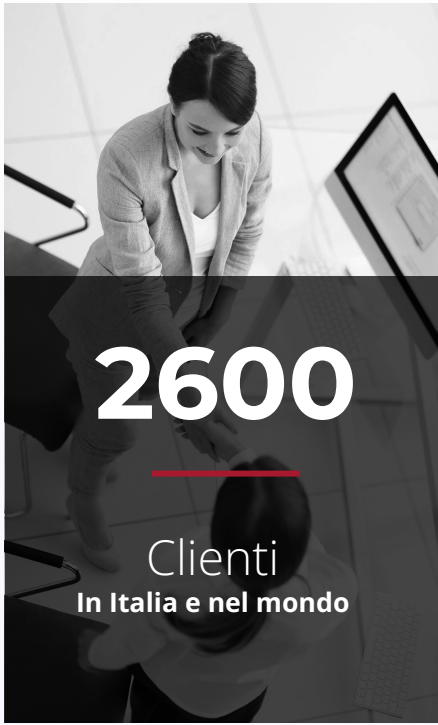
85M

Ricavi
nel 2023

Ricavi H1 2024: 54M

610

Collaboratori
nelle nostre aziende



2600

Clienti
In Italia e nel mondo

BUSINESS SECTOR

BUSINESS SOFTWARE APPLICATION

Soluzioni **Software** per **PMI** e **grandi industrie.**

Ogni azienda è unica. smeup lo sa!
Usare la digitalizzazione per sviluppare il business e generare valore, ***insieme***.

- **e** GESTIONALI ERP
- **b** BUSINESS ANALYTICS
- **d** DOCUMENTALE
- **w** WEB & MOBILE APPLICATION
- **f** IOT E INTEGRAZIONE INDUSTRIALE
- **l** LOGISTICA E TRASPORTI

BUSINESS SECTOR

INFRASTRUCTURE, CLOUD & SECURITY

Soluzioni per **Architetture IT** e **servizi gestiti.**

Innovazione e **sicurezza** per rispondere ai bisogni delle aziende.

- i INFRASTRUTTURA
- c CLOUD
- cs CYBER SECURITY
- ps IBM POWER SYSTEMS

EDU TIPS

WEBINAR
SPECIALE TEMA EDU TIPS

GIANPIERO CIOLA

Product Manager @smeup ICS

smeup.com

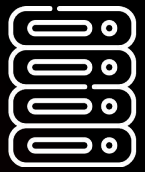
smeup

DATA **PROTECTION**

Dove risiedono i nostri dati?

I nostri dati risiedono nei server cloud, nei data center aziendali
e nei dispositivi di produzione.

EDGE



CORE

CLOUD

Prendere coscienza del nuovo perimetro di competenza!

DATA **PROTECTION**

Le principali minacce alla Data Protection.

La protezione dei dati è fondamentale per garantire la sicurezza delle informazioni aziendali e personali. Le principali minacce alla Data Protection, se non affrontate correttamente, possono compromettere la privacy e la continuità operativa.

Le minacce alla Data Protection sono sempre più sofisticate e variegate. È essenziale adottare strategie di protezione adeguate per prevenire danni significativi e garantire la sicurezza a lungo termine.

- **Attacchi ransomware**: cifratura dei dati e richiesta di riscatto.
- **Errori umani:** cancellazione accidentale, configurazioni errate.
- **Guasti hardware e disastri naturali:** perdita di dati per malfunzionamenti imprevisti.
- **Furto di dati e accessi non autorizzati:** problemi di sicurezza interna ed esterna.

DATA **PROTECTION**

Cosa si intende per Data Protection?

La capacità di poter ripristinare sempre e ovunque i tuoi dati qualsiasi cosa accada.

REPOSITORY

Ambiente dedicato e specifico, progettato per essere affidabile.

ARCHITETTURA

Procedure e funzionalità flessibili ed efficaci per garantire tempi di ripartenza certi e adeguati.

TECNOLOGIA

Supervisionare l'intero processo continuo di protezione dei dati e certificarne la qualità.

Proteggere i dati significa garantirne il ripristino.

DATA **PROTECTION**

Come si realizza la Data Protection?

La capacità di poter ripristinare sempre e ovunque i tuoi dati qualsiasi cosa accada.

3

Il numero di COPIE distinte dei dati di produzione.

2

Le differenti TECNOLOGIE di salvataggio delle copie di sicurezza.

1

Il numero minimo di COPIE di sicurezza offline.

Un backup sicuro deve essere ridondante, diversificato e sempre accessibile per garantire ripristini rapidi e certi.

DATA **PROTECTION**

Esempio pratico di strategia 3-2-1.

Immaginiamo che un'azienda gestisca dati critici relativi ai clienti e alla produzione.
Ecco come può applicare la regola 3-2-1:

3 COPIE DEI DATI

Originale: database principale sul server aziendale.

Backup locale: copia di sicurezza su Appliance dedicate.

Backup esterno: copia aggiuntiva salvata in un data center remoto.

2 TECNOLOGIE DIVERSE

Il backup locale viene salvato su **dischi fisici**.

Il backup remoto viene archiviato su **cloud criptato**.

1 COPIA OFFLINE

Una copia crittografata viene salvata su **supporti immutabili**, custoditi in un luogo sicuro e disconnesso logicamente da internet per evitare attacchi ransomware.

In caso di ransomware, il backup offline permette di ripristinare i dati senza pagare il riscatto.

DATA **PROTECTION**

Compliance e sicurezza: confronto tra GDPR e NIS2.

GDPR	NIS2
Protezione dei dati personali	Nuovi obblighi di sicurezza per le aziende critiche
Diritto alla portabilità	Gestione del rischio
Obbligo di notifica delle violazioni	Risposta agli incidenti

COME ADEGUARSI?

1. Avere un piano documentato
2. Adottare misure di sicurezza adeguate
3. Formare il personale

DATA **PROTECTION**

Best practice per una Data Protection efficace.

Per garantire una protezione efficace, è fondamentale adottare pratiche quotidiane che riducano i rischi e migliorino la gestione delle informazioni sensibili, mantenendo un alto livello di sicurezza e prevenendo vulnerabilità nel lungo periodo.

Adottare queste best practice non solo rafforza la sicurezza dei dati, ma garantisce anche la conformità alle normative vigenti. Implementare soluzioni proattive è essenziale per prevenire incidenti e minimizzare i danni in caso di violazioni.

- **Automatizzare i backup** per ridurre il rischio di errore umano.
- **Classificare i dati** per proteggere al meglio quelli più sensibili.
- **Aggiornare costantemente le policy di sicurezza.**
- **Utilizzare strumenti di monitoraggio** per individuare anomalie nei dati.


EDU TIPS
Q&A

Thank you!

GIANPIERO **CIOLA**

Product Manager @smeup ICS

gianpiero.ciola@smeup.com

EDU TIPS CYBERSECURITY