ASSOLOMBARDA

Con il patrocinio del Comune di Cassano d'Adda

Unipol

Affrontare il cyber risk: scenari normative e soluzioni per le imprese

8 luglio 2026 – ore 17:30

Casa Berva, Via Giuseppe Verdi, 26

Cassano d'Adda MI

Con il patrocinio del Comune di Cassano d'Adda

ASSOLOMBARDA

Unipol

FABIO COLOMBO

Sindaco di Cassano d'Adda

Affrontare il cyber risk: scenari normative e soluzioni per le imprese

08 luglio 2026

Con il patrocinio del Comune di Cassano d'Adda

ASSOLOMBARDA

Unipol

NICOLA FRACASSI

Presidente Zona Adda Martesana Assolombarda

Affrontare il cyber risk: scenari normative e soluzioni per le imprese

08 luglio 2026

Con il patrocinio del Comune di Cassano d'Adda

ASSOLOMBARDA

Unipol

ANDREA MONTIN

Area Credito e Finanza Assolombarda

Affrontare il cyber risk: scenari normative e soluzioni per le imprese

08 luglio 2026

ASSOLOMBARDA

Approcciare il rischio cyber: dall'identificazione alla gestione

Andrea Montin - Area Credito e Finanza

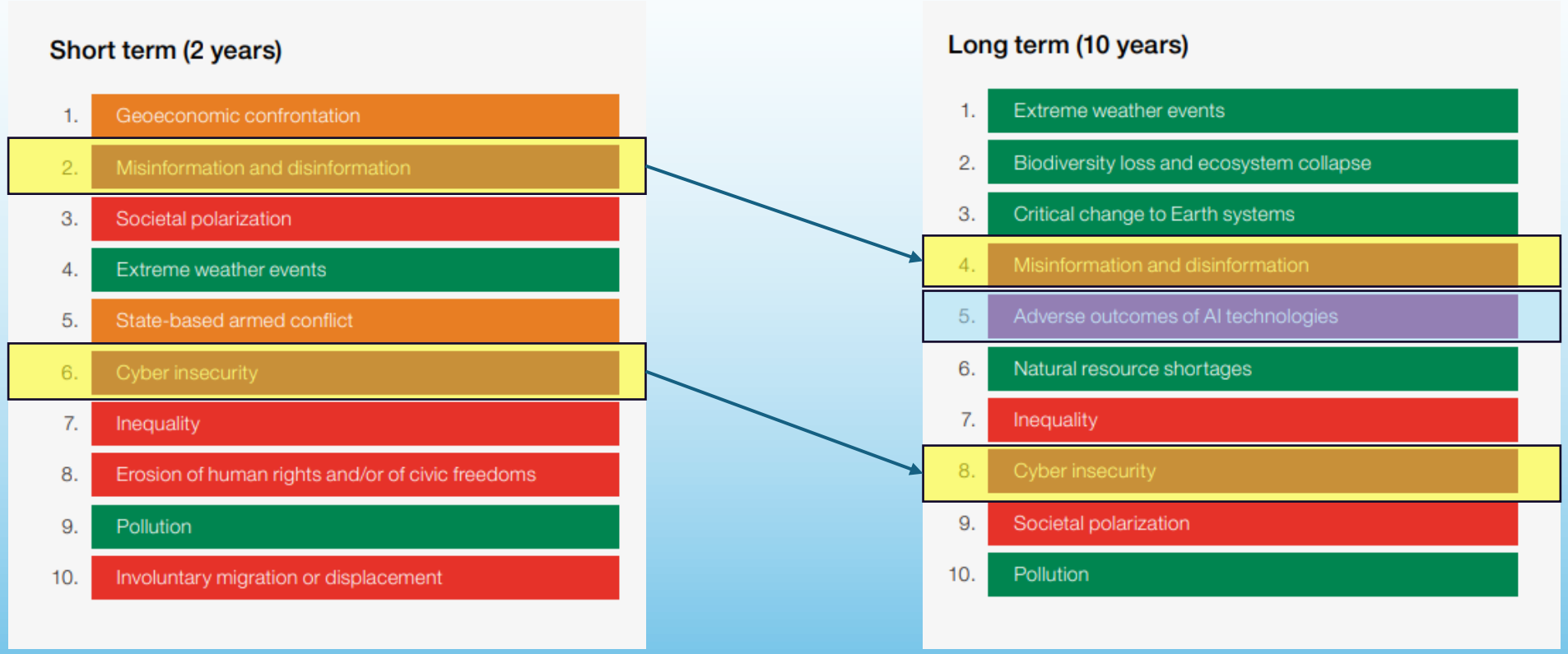
08.07.2026

Agenda

1. La percezione e i numeri del rischio cyber
2. Che cos'è il rischio cyber
3. Come identificare e valutare il rischio
4. La gestione del rischio: dall'inerente al residuo

1. La percezione e i numeri del rischio cyber

I rischi tecnologici sono tra le priorità dei prossimi anni, secondo il Global Risk Report 2026 del World Economic Forum



Cyber insecurity e disinformazione sono tra i rischi più rilevanti nel breve periodo

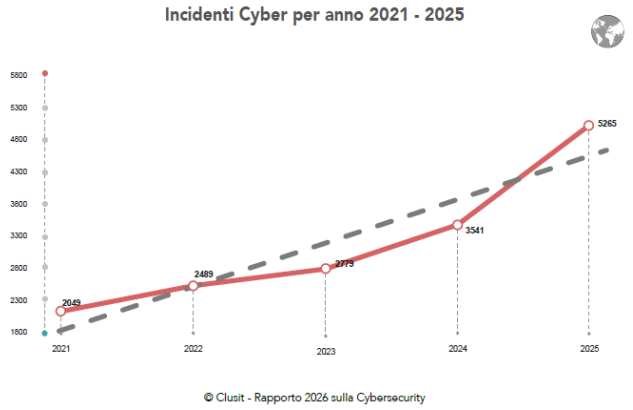
AI, disinformazione e cyber insecurity confermano la centralità dei rischi tecnologici nel lungo periodo

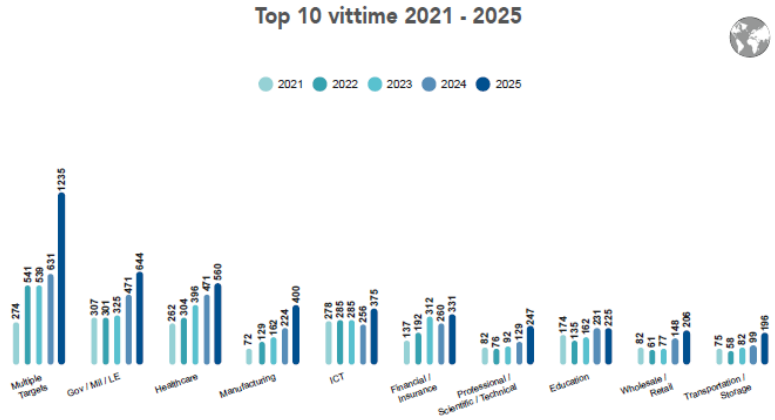
ASSOLOMBARDA

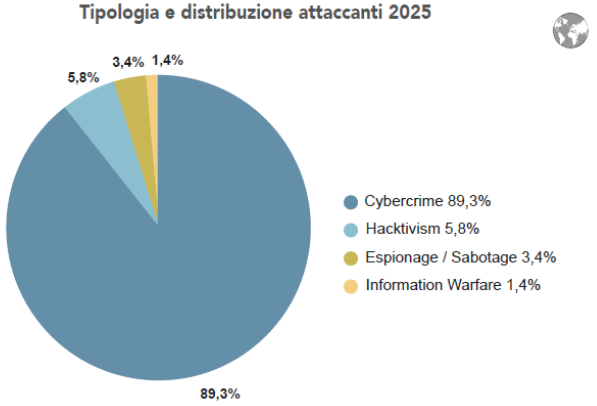
1. La percezione e i numeri del rischio cyber

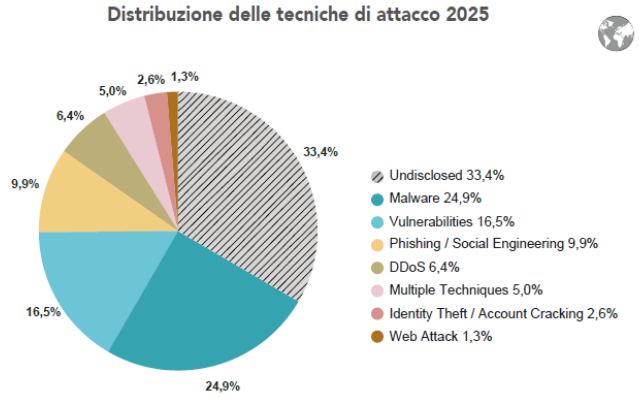
RAPPORTO CLUSIT 03.2026

1. Incidenti cyber per anno 2021–2025
Gli incidenti cyber mostrano un trend di crescita costante, con un’accelerazione significativa nel 2025
2. Top 10 vittime 2021–2025
Gli attacchi colpiscono settori molto diversi, confermando che il rischio cyber riguarda l’intero sistema economico
3. Tipologia e distribuzione attaccanti 2025
Il cybercrime rappresenta la principale matrice degli attacchi, confermando la natura sempre più industrializzata del fenomeno
4. Distribuzione delle tecniche di attacco 2025
Le tecniche di attacco sono diversificate: malware, vulnerabilità e phishing restano tra i principali vettori di compromissione









Il cyber risk e i suoi fattori di rischio

*Il rischio cyber è l'effetto dell'incertezza su o all'interno delle tecnologie e dei sistemi informativi; riguarda in particolare la possibile perdita di **riservatezza**, **integrità** o **disponibilità** di dati, informazioni e sistemi, con potenziali impatti negativi su operatività, asset, reputazione e continuità aziendale*

	Fattori di rischio
Riservatezza – Confidentiality (C) Garantire la riservatezza (privacy) dei dati creati, custoditi, trasmessi e diffusi evitandone l'accesso a utenti non autorizzati	• Accessi non autorizzati • Errore umano • Ingegneria sociale
Integrità - Integrity (I) Garantire la protezione del dato da qualsiasi tentativo di manomissione dello stesso, prevenendo alterazione o cancellazione non autorizzata	• Accessi non autorizzati • Errore umano
Disponibilità – Availability (A) Garantire la continuità alla fruizione e all'accesso di dati e servizi, impedendo interruzioni nell'erogazione di servizi hardware e software	• Attacchi DoS o DDos • Attacchi Ransomware • Errore Umano

2. Che cos'è il rischio cyber

Dalle minacce...

Malware / Ransomware *Blocco dei sistemi, cifratura dei dati e richiesta di riscatto*	**Phishing/social engineering** *Manipolazione delle persone per ottenere accessi, dati o pagamenti non autorizzati*	**DDoS** *Interruzioni o degrado dei servizi digitali*
Vulnerabilità *Sfruttamento delle falle tecniche e sistemi non aggiornati*	**Web attack** *Attacchi combinati sui siti web, applicazioni e infrastrutture*	**Account cracking** *Compromissioni di account e utilizzo illecito di identità*

... agli impatti aziendali

Operatività *Interruzione e rallentamenti nei processi critici*	**Finanza** *Costi diretti e indiretti, perdita di ricavi e penali*	**Compliance e legale** *Violazioni normative, sanzioni e contenziosi*
Reputazionale *Perdita di fiducia dei clienti, partner e fornitori*	**Supply chain** *Effetti sui fornitori e sulla continuità del servizio*	...

Identificare il rischio

Per identificare il rischio bisogna conoscere e comprendere il perimetro aziendale e gli elementi da proteggere

Il contesto

Organizzazione, sedi, business unit, processi...

Gli asset critici

Hardware, software, reti, sistemi...

I dati rilevanti

Dati personali, commerciali, finanziari...

Vulnerabilità

Sistemi non aggiornati, configurazioni...

Non si può proteggere quello che non è stato prima identificato, classificato e collegato ai processi aziendali

Valutare e prioritizzare il rischio

Ogni rischio, incluso quello cyber, deve essere misurato in termini di probabilità e impatto per capire la reale esposizione e decidere le priorità di intervento

Probabilità

Verosimiglianza che l'evento si realizzi

- *Dipendenza da sistemi informatici per la gestione dati*
- *Livello di utilizzo dello smartworking*
- *Attacchi cyber subiti negli ultimi anni*
- ....

×

Impatto

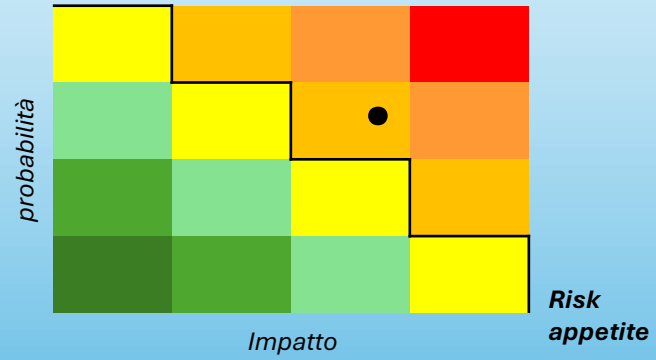
Effetti sull'operatività, ricavi, compliance...

- *Possibile blocco dell'operatività aziendale*
- *Danno economico diretto in caso di interruzione*
- *Conseguenze sulla reputazione aziendale*
- ....

=

Severity inerente

Gravità del rischio, senza strumenti di trattamento



*Se il rischio cyber supera la **propensione al rischio dell'azienda**, quest'ultima dovrà mettere in atto delle azioni di prevenzione e protezione per far si che il rischio venga a stabilizzarsi in una **zona accettabile***

Gestire il rischio cyber: un approccio continuativo

0. GOVERNACE

Contesto organizzativo

Strategia di gestione dei rischi

Ruoli, responsabilità e compiti

Policy aziendale

Supervisione

Gestione del rischio nella catena di fornitura

1. IDENTIFICARE

Gestione degli asset

Valutazione del rischio

Miglioramento

2. PROTEGGERE

Gestione delle identità, e controllo degli accessi

Consapevolezza e formazione

Sicurezza dei dati, delle piattaforme

Resilienza infrastruttura

3. RILEVARE

Monitoraggio continuo

Analisi degli eventi avversi

4. RISPONDERE

Gestione e analisi degli incidenti

Segnalazione e comunicazione della risposta

Mitigazione degli incidenti

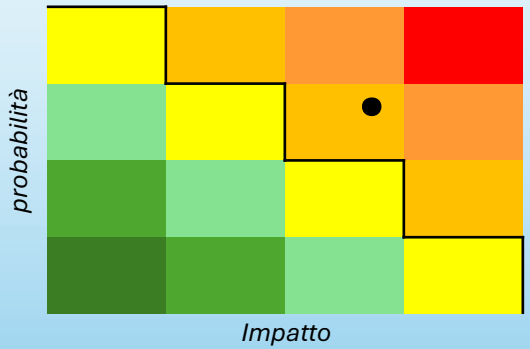
5. RIPRISTINARE

Esecuzione del piano di ripristino dagli incidenti

Comunicazione sul ripristino dagli incidenti

Dal controllo operativo alla protezione finanziaria

Severity inerente



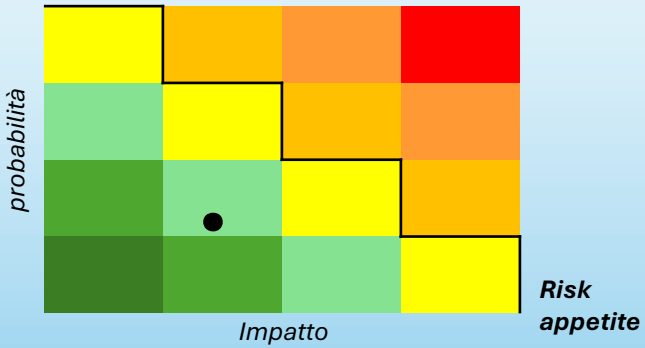
Efficacia dei controlli

Azioni di prevenzione e protezione

+

Trasferimento assicurativo

Severity residua



Il rischio cyber non si elimina: si riduce con i controlli e si trasferisce la quota assicurabile al mercato assicurativo

ASSOLOMBARDA

Grazie per l'attenzione!

andrea.montin@assolombarda.it

Con il patrocinio del Comune di Cassano d'Adda

ASSOLOMBARDA

Unipol

MIRIAM IERACI

Area Industria Energia e Innovazione Assolombarda

Affrontare il cyber risk: scenari normative e soluzioni per le imprese

08 luglio 2026

Con il patrocinio del Comune di Cassano d'Adda

ASSOLOMBARDA

Unipol

MICHELE CARLI

Responsabile Cyber Risk – Unipol Assicurazioni

Affrontare il cyber risk: scenari normative e soluzioni per le imprese

08 luglio 2026

Il Ruolo dell'Assicuratore nella Gestione del Rischio

Bologna, Aprile 2026

CYBER SELF ASSESSMENT

COPERTURA CYBER

FOCUS INCIDENT RESPONSE

BITSIGHT

Dalla valutazione del rischio informatico alle strategie di mitigazione e supporto operativo

Questionario cyber come strumento di self-assessment

Il cliente è guidato nella **compilazione di un questionario** che consente di mappare il proprio livello di **rischio in ambito cyber**. Questo processo di autovalutazione permette di ottenere una fotografia consapevole del **profilo di rischio informatico**, evidenziando esposizioni, lacune organizzative e criticità tecnologiche.

Risultati e gestione attiva del rischio

I risultati del **self-assessment** non si limitano a una valutazione statica, ma rappresentano un punto di partenza per intraprendere un percorso di rafforzamento delle misure di sicurezza. Il cliente può così definire **priorità di intervento e best practice** e migliorare progressivamente la propria **resilienza agli attacchi informatici.**

Sistemi di supporto e leva finanziaria

Opportunità per investimenti in cyber security:

- **8 centri di competenza nazionali** (esempio: Start 4.0, Cyber 4.0)
- **incentivi pubblici dedicati**
- **strumenti di finanza agevolata**

Copertura Cyber

DANNI DA RCT

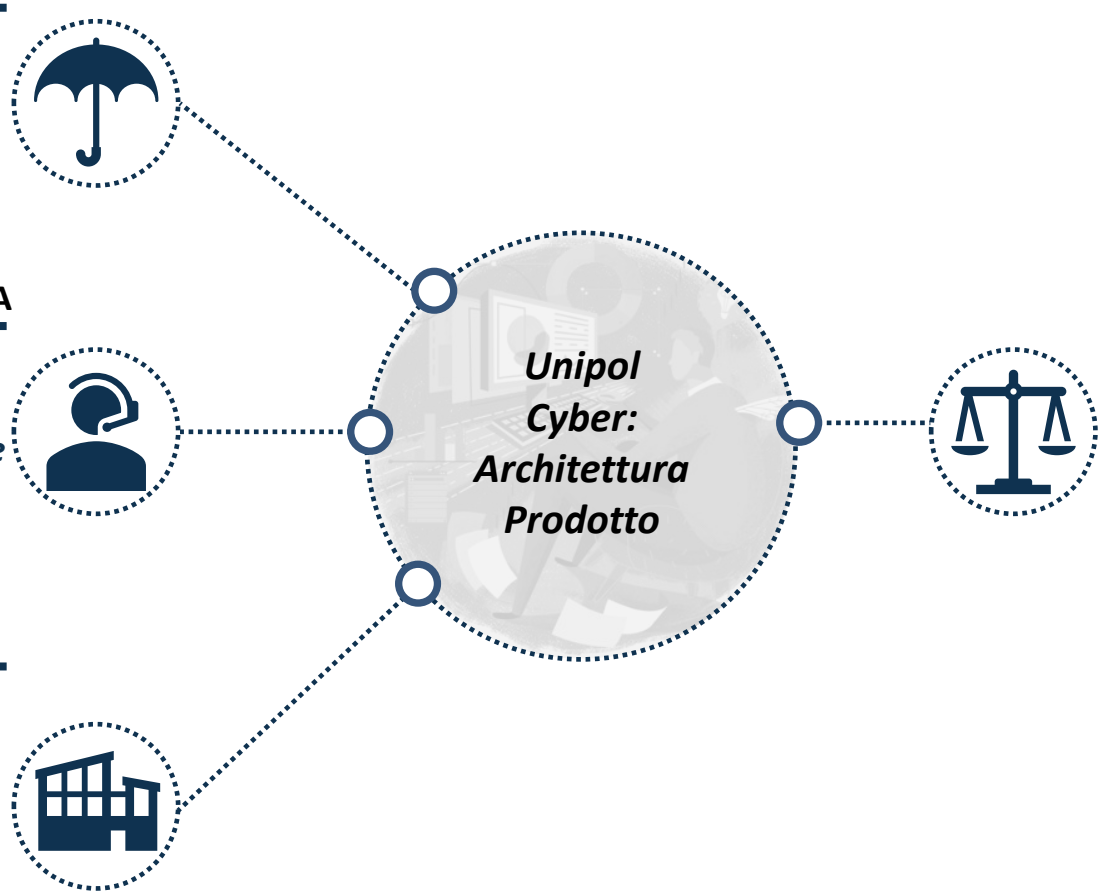
Danni arrecati a terzi a seguito di trasmissione di **Malware**; Danni patrimoniali arrecati a terzi a seguito di **interruzione di attività**.

PRONTA RIPRESA

In caso di sinistro il Cliente può decidere di avvalersi dei servizi offerti dal ***Cyber Incident Response Team*** per **limitare** o **evitare** l'aggravamento del danno

DANNI ALL'ORGANIZZAZIONE

Costi di **rilevazione e investigazione**, Costi di **notifica**, Costi di **istruttoria**, Monitoraggio del **credito** e dell'identità, **Onorari di consulenti e esperti**, Perdita di **immagine**, Ricostruzione Dati e Archivi, **Estorsione informatica**



TUTELA LEGALE

Supporto per la gestione attiva e passiva.

DANNI SUBITI:

- Spese di costituzione di parte civile nel procedimento penale;
- Spese per la rimozione/riduzione di contenuti lesivi della reputazione pubblicati online.

DELITTI:

- Delitti colposi e contravvenzioni
- Delitti dolosi

ALTRE COPERTURE:

- Vertenze contrattuali;
- Tutela privacy;
- Ripristino onorabilità creditizia;
- Ricorso all'Arbitro bancario finanziario (ABF)

Focus Pronta Ripresa: Incident Response

In caso di sinistro il Cliente può decidere di avvalersi dei servizi offerti dal ***Cyber Incident Response Team*** per **limitare** o **evitare** l'aggravamento del danno.

- **ANALISI FORENSE**
- **ANALISI IT**
- **ISTRUTTORIA**
- **GESTIONE DELLE PERDITE**
- **INDAGINI INTERNE**
- **ESTORSIONE INFORMATICA**
- **PROTEZIONE DEI DATI**
- **PUBBLICHE RELAZIONI**

Collaborazione con

Crawford®

Numero verde:
800184645
Call Center
UnipolAssistante attivo h24
rivolgendosi
all'intermediario presso il
quale il contratto è stato
stipulato

Previsto **sconto commericale** del **20%** per gli associati di **Assolombarda**

ASSOLOMBARDA

Con il patrocinio del Comune di Cassano d'Adda

ASSOLOMBARDA

Grazie per l'attenzione!

Contatti:
zone@assolombarda.it