# Cyber-rischi

## Che cos'è un cyber-rischio ?

Il termine cyber-rischio raggruppa l'insieme dei rischi e dei pericoli legati all'uso delle tecnologie digitali che possono compromettere la riservatezza, l'integrità, l'autenticità o la disponibilità dei dati e degli strumenti di produzione.

Nessuna azienda è immune a questi rischi, indipendentemente dalle dimensioni, dalla natura della sua attività o del suo settore (commercio, servizi, sanità, finanza, industria, ecc.). Basta un incidente per mettere in pericolo tutta l'attività di un'azienda.

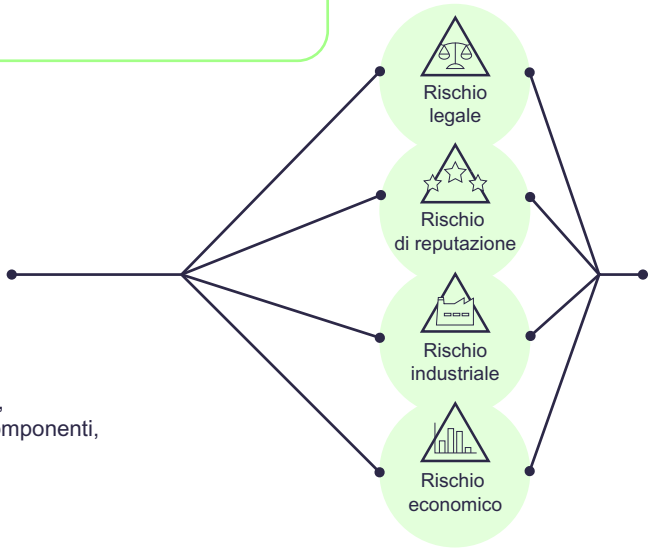
Siate vigili : prendete le decisioni giuste e applicate le buone pratiche.

## Pericoli legati ai cyber-rischi

Compromettendo la sicurezza di dati, siano essi sensibili o meno, i cyber-rischi possono avere pesanti conseguenze come perdite finanziarie, interruzione delle attività commerciali, disturbo dell'attività, rischi di sicurezza, arresto della produzione o danni alla reputazione.

**Rischi interni**
Negligenza, cattivo uso dei sistemi informatici o dei dati, errore umano, dolo, mancanza di formazione, ecc.

**Rischi esterni**
Attacco informatico, incidenti all'infrastruttura come danni delle acque e incendi, carenza energetica, carenza di componenti, incendio presso un partner, evoluzione delle normative, ecc.




**Prevenzione e riduzione dei rischi**
Diversi provvedimenti permettono di ridurre i cyber-rischi: attuare politiche di sicurezza, formare i dipendenti, implementare procedure di soccorso e di recupero.

***« Nel mondo interconnesso in cui viviamo oggi, le minacce cibernetiche sono una realtà inevitabile. Occorre adottare tassativamente tutte le misure necessarie per proteggere al meglio l'azienda, le collaboratrici e i collaboratori. »***

Dimitri Konstantas, Professore e Direttore *dell'Information Science Institute* dell'Università di Ginevra

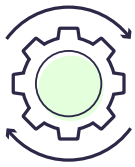


REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX
h e g Haute école de gestion Genève
UNIVERSITÉ DE GENÈVE

Per saperne di più

# Come comportarsi

## Proteggete i vostri file e i vostri apparecchi

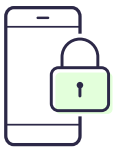


Tenete aggiornati i software e i sistemi implementando gli aggiornamenti automatici delle applicazioni, dei browser web, dei sistemi operativi, degli apparecchi e delle attrezzature.

Proteggete l'accesso agli apparecchi (computer, tablet, smartphone, ecc.) con una password forte generata da voi o da un servizio di gestione delle password e non lasciateli senza sorveglianza nei luoghi pubblici. Siate prudenti quando usate le reti Wi-Fi pubbliche.

Imponete l'autenticazione a più fattori per accedere alla vostra rete aziendale (SMS, e-mail, applicazione di autenticazione, ecc.).

Salvate i file importanti offline, su disco fisso esterno o nel cloud per poter accedervi anche in caso di perdita, guasto o furto del dispositivo. Assicuratevi anche di archiviare i fascicoli cartacei in modo sicuro.



Usate una chiave crittografica per proteggere le informazioni sensibili e critiche presenti sugli apparecchi della vostra azienda, come i computer portatili, i tablet, gli smartphone, i dischi fissi amovibili e le chiavette USB, e impiegate soluzioni di archiviazione su cloud.

Utilizzate software e/o sistemi di protezione (antivirus, firewall, sistema di rilevamento e prevenzione delle intrusioni (IDS/ IPS), ecc.).

**La sicurezza della vostra azienda è fondamentale!**
Chiedete assistenza ai specialisti.

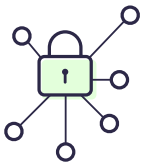
# Come comportarsi

## Proteggete la vostra rete

Attivate il firewall per controllare e filtrare il traffico di rete autorizzando o bloccando alcuni tipi di comunicazioni e contenuti in funzione di regole predefinite.

Proteggete il router cambiando il nome e la password predefinito e disattivando la gestione da remoto. Ricordate di cambiare regolarmente la password.

Assicuratevi che la rete wireless offra una crittografia WPA2 o WPA3 e che sia attiva la protezione delle informazioni che passano sulla rete contro l'accesso da parte di persone non autorizzate.



Definite delle liste restrittive di apparecchi autorizzati ad accedere alla rete dell'azienda.

Cambiate il nome predefinito della rete Wi-Fi in modo da non poter essere identificati. Per maggior discrezione, potete nasconderla.

## Fate della sicurezza una cultura aziendale

Create una cultura della sicurezza formando regolarmente i vostri team e informandoli dei nuovi rischi e delle nuove vulnerabilità.

Create un Piano di continuità operativa (PCO) che illustrerà il modo in cui salvate i dati e mantenete l'azienda in attività in caso di incidente, attacco o danni. Mettete questo piano per iscritto, comunicatelo a tutte le persone interessate dell'azienda e testatelo regolarmente.

# Preparare una strategia

## Come ridurre i cyber-rischi in azienda ?

Indipendentemente dalle dimensioni, ogni azienda dovrebbe seguire queste **5 tappe**.

## 1 Identificare

- Stilate un elenco di tutte le apparecchiature, applicazioni e servizi usati dall'azienda : computer, smartphone, tablet, ma anche periferiche come stampanti o qualsiasi altro oggetto o macchina collegato alla rete o a Internet.
- Create e condividete una politica di cybersicurezza per l'azienda che tenga conto :
  - dei ruoli, delle responsabilità e degli accessi di ogni collaboratrice e collaboratore, e di eventuali terzi - persona o azienda - che potrebbero accedere a informazioni sensibili,
  - della procedura da seguire per proteggersi dagli attacchi e limitare i danni, in caso di attacco.

## 2 Proteggere

- Controllate chi può accedere alla rete dell'azienda e chi può usare i computer e gli altri apparecchi (collaboratrici, collaboratori, clienti, partner, fornitori).
- Usate e configurate dei software di sicurezza per proteggere i dati.
- Crittografate i dati sensibili e conservate le chiavi di crittografia in un luogo sicuro e separato.
- Definite un piano per salvare i dati con regolarità e in modo automatico (vedi pagine 15-16).
- Aggiornate regolarmente o automatizzate gli aggiornamenti di tutti i software.
- Formate regolarmente tutte le persone che usano le vostre apparecchiature. Aiutate le collaboratrici e i collaboratori a comprendere le poste in gioco e i rischi per loro stessi e per l'azienda.

## 3 Rilevare

- Istituite una sorveglianza attiva delle apparecchiature per rilevare eventuali accessi non autorizzati da parte di persone, periferiche (come chiavette USB) e software.
- Sorvegliate le connessioni non autorizzate alla vostra rete.
- Investigate eventuali attività sospette sulla vostra rete o i vostri sistemi.

# Preparare una strategia

## 4 Rispondere

Stilate un Piano di continuità operativa (PCO) in modo tale che, in caso di interruzione di servizio e/o attacco, siate in grado di:

- identificare e contenere l'attacco,
- segnalare l'attacco alle autorità competenti,
- avvertire i clienti, i team e i partner i cui dati potrebbero essere stati esposti,
- garantire la continuità delle attività,
- riassorbire le vulnerabilità e ristabilire l'attività,
- aggiornare la vostra politica di gestione dei cyber-rischi,
- anticipare eventuali scenari imprevisti (come un disastro naturale) che potrebbero danneggiare i vostri dati.

**Testate e aggiornate regolarmente il vostro PCO**

## 5 Ripristinare

Dopo un attacco:

- identificate, catalogate e analizzate i danni causati (apparecchiature danneggiate, perdita di dati, accessi compromessi, ecc.),
- mettete in sicurezza e ripulite l'ambiente di lavoro e le apparecchiature che sono state colpite,
- riparate e ripristinate le apparecchiature e le parti della rete che sono state danneggiate,
- tenete informati i team, i clienti e i partner su come stanno proseguendo le procedure di ripristino.

**Per aiutarvi a preparare una strategia di protezione contro i cyber-rischi e metterla in pratica, fatevi assistere da un'azienda specializzata.**

### Lo sapevate?

In caso di cyber-attacco, la durata media per il ripristino completo del funzionamento dell'azienda è di 22 giorni.

Per saperne di più consultate il sito Internet dell' **Ufficio federale della cybersicurezza (UFCS)** della Confederazione.

# Sicurezza fisica delle risorse digitali

## La prevenzione dei cyber-rischi inizia dalla sicurezza fisica

Alcune lacune nella sicurezza fisica possono esporre dei dati sensibili.

Esempio:

- un computer o un telefono cellulare non protetti dimenticati sul treno,
- documenti d'archivio depositati in un punto di raccolta dei rifiuti, accessibili a tutte e tutti,
- file e hardware informatico rubati durante un furto.

### Responsabilità digitale delle aziende

Sensibilizzare le collaboratrici e i collaboratori alla responsabilità digitale è essenziale perché spesso sono l'anello più vulnerabile di fronte alle cyber-minacce e le loro azioni possono avere un impatto diretto sulla sicurezza e sulla reputazione dell'azienda.

*Consultate la guida sulla responsabilità digitale delle aziende*

## Come proteggere le apparecchiature e i fascicoli fisici

- Archiviate in modo sicuro i fascicoli cartacei e le apparecchiature elettroniche contenenti informazioni sensibili in un armadio o in un locale chiuso a chiave, a prova di incendio (rivolgetevi ad aziende specializzate).
- Limitate l'accesso ad archivi, fascicoli o apparecchiature alle persone autorizzate e conservate una traccia di tutti questi accessi.
- Distruggete in modo sicuro i fascicoli e i dati obsoleti. Usate un distruggidocumenti o rivolgetevi ad un'azienda specializzata nella distruzione sicura per eliminare i documenti cartacei o i supporti di dati. Non accontentatevi di gettarli via o di riciclarli.
- Ricordate regolarmente ai team di bloccare la postazione di lavoro quando si assentano e di non lasciare senza sorveglianza documenti sensibili, chiavette USB, dischi fissi, telefoni cellulari, ecc.
- Chiedete ai team di proteggere gli smartphone secondo le buone pratiche vigenti, se ne fanno un uso professionale.

# Sicurezza fisica delle risorse digitali

## La prevenzione dei cyber-rischi inizia dalla sicurezza fisica

La perdita, il furto o l'uso errato di un apparecchio possono avere conseguenze gravi.

Proteggete i dati contenuti in questi apparecchi applicando le seguenti buone pratiche.

- Usate password forti : una password robusta e lunga (almeno 12 caratteri), complessa e unica (contiene caratteri speciali come !?@#%, lettere maiuscole e minuscole e cifre).
- Assicuratevi che queste password siano generate e salvate in modo sicuro, usando un gestore di password.
- Definite una password diversa per ogni account o applicazione.
- Differenziate le password private da quelle professionali.
- Non comunicate mai a nessuno le vostre password.
- Cambiate regolarmente le password.
- Bloccate i vostri apparecchi usando dei codici.
- Imponete l'autentificazione a più fattori (MFA) per accedere alla rete dell'azienda e ai vari strumenti (es. : password monouso e/o doppia autentificazione).
- Disattivate il bluetooth degli apparecchi quando non ne avete bisogno.
- Limitate i tentativi di connessione a 5 al massimo per proteggervi dalle intrusioni.
- Crittografate i dispositivi mobili contenenti informazioni sensibili. Crittografate anche gli scambi interni o esterni contenenti informazioni sensibili.
- Depositate le chiavi crittografiche in un luogo sicuro e distinto dalle vostre infrastrutture.
- Prima di rivendere o donare vecchi computer, dispositivi mobili, stampanti o altre apparecchiature elettroniche, usate un software di distruzione dei dati o rivolgetevi a un'azienda specializzata.
- Non limitatevi a cancellare semplicemente i dati.
- Informate regolarmente i team sui cyber-rischi e formateli mettendo a loro disposizione il materiale adeguato e la possibilità di seguire una formazione continua.
- Incoraggiate l'adozione di buone pratiche in materia di sicurezza, sia in ufficio che a casa.
- Diffondete il vostro Piano di continuità operativa (PCO). Ogni membro del team deve sapere chi contattare e conoscere le tappe da seguire se un dispositivo o un fascicolo viene perso o rubato.

# Proteggere gli accessi da remoto

**I vostri team e partner devono seguire standard di sicurezza elevati quando accedono da remoto alla vostra rete, che si tratti di apparecchiature aziendali o personali.**

## Proteggere le apparecchiature in caso di accesso da remoto

- Proteggete il router : cambiate sistematicamente i parametri predefiniti (nome e password) e tenete aggiornato il software.
- Crittografate i dati che transitano sulle reti o che si trovano sugli apparecchi che si collegano alla vostra rete remota.
- Configurate le regolazioni degli smartphone, dei tablet e dei computer portatili : cambiate le regolazioni predefinite per impedire le connessioni automatiche alle reti wireless.
- Tenete aggiornati i software anti-virus e programmate degli aggiornamenti automatici su tutti gli apparecchi che possono collegarsi a distanza alla vostra rete (computer e dispositivi mobili inclusi).

### Telelavoro

Quando siete all'esterno dell'azienda, rispettate le regole fissate dalla vostra azienda riguardo l'uso degli strumenti informatici e di sicurezza. Applicate anche le buone pratiche di cybersicurezza a casa vostra e quando siete in trasferta.

## Fornire ai team e ai partner degli strumenti che permettano di mantenere un livello elevato di sicurezza

- Assicuratevi che qualsiasi accesso da un luogo esterno passi attraverso un router che applichi gli standard migliori in materia di crittografia delle comunicazioni wireless (come WPA2 o WPA3).
- Usate una VPN aziendale per permettere ai team di accedere da remoto alla rete, in modo da crittografare il traffico tra gli apparecchi e la rete Internet.
- Usate l'autenticazione a più fattori (MFA) e scegliete password robuste.
- Assicuratevi che la rete Wi-Fi per gli ospiti sia separata dalla rete aziendale e fornite codici di connessione unici per gli ospiti.
- Includete delle clausole di sicurezza in tutti i contratti con i partner che dovranno collegarsi alla rete dell'azienda.

# Web hosting

## Desiderate creare un sito Internet o aggiornarlo ?

Se non avete le competenze necessarie per creare un sito Internet, rivolgetevi ad uno specialista di creazione e hosting di siti Internet. Esistono numerose opzioni di web hosting che occorrerà studiare in funzione delle vostre esigenze. Quando paragonerete i vari servizi, la sicurezza dovrà essere la vostra preoccupazione principale.

### Le domande da porre al vostro futuro hosting provider

- ☐ Il sito è protetto da un protocollo TLS ? Il protocollo è incluso nel contratto di hosting ?
- ☐ Vorrei usare il mio nome di dominio per i miei indirizzi e-mail professionali : potete implementare un meccanismo di sicurezza, come SPF, DKIM o DMARC ?
- ☐ Chi è responsabile degli aggiornamenti di sicurezza e della manutenzione del mio sito Internet e con che frequenza vengono eseguiti ?
- ☐ Una volta che il sito Internet est online, chi avrà i diritti di amministrazione e pubblicazione ?
- ☐ Verrà attuata un'autenticazione a più fattori per le persone che avranno i diritti di amministrazione e pubblicazione del sito Internet ?

## Proteggete il vostro sito Internet usando TLS

TLS è un protocollo di sicurezza ideato per fornire comunicazioni protette su una rete informatica. Viene usato per crittografare i dati trasmessi sulla rete, garantendo la riservatezza e l'integrità delle informazioni scambiate tra due sistemi. Quando il protocollo TLS è attivo correttamente sul vostro sito Internet, l'URL inizierà con https ://.

## Autentificate i vostri indirizzi e-mail

Potete configurare gli indirizzi e-mail dell'azienda in modo che utilizzino il nome di dominio del vostro sito Internet (ad esempio : lamiasocietà.ch / nome@lamiasocietà.ch). Per essere sicuri che nessun truffatore possa inviare delle e-mail a vostro nome usurpando il nome di dominio della vostra organizzazione, dovete certificare l'autenticità delle e-mail. Per fare questo, potete appoggiarvi a meccanismi o norme di verifica come Sender Policy Framework (SPF), Domaine Keys Identified Mail (DKIM) o Domain-based Message Authentification, Reporting & Conformance (DMARC).

## Eseguite la manutenzione del vostro sito internet

È necessario chiarire sin dall'inizio chi è responsabile della manutenzione del sito Internet, che potrà essere eseguita internamente o da un fornitore esterno, in base alle competenze che possedete. Assicuratevi di eseguire l'aggiornamento regolare dei componenti del sito Internet e della sicurezza.

# Assicurazioni e aspetti legali

## Gestire un cyber-incidente e rimettere la propria azienda in funzione è costoso e complesso

In Svizzera esistono offerte di cyber-assicurazioni destinate alle PMI che possono comprendere assistenza tecnica, protezione contro le perdite finanziarie, copertura della responsabilità civile e assistenza legale.

Sottoscrivere un'assicurazione non esclude la possibilità di un cyber-incidente e non vi protegge da esso.

**Check-list prima di sottoscrivere una cyber-assicurazione**

- ☐ Il sito è protetto da un protocollo TLS? Il protocollo è incluso nel contratto di hosting?
- ☐ Fare uno studio delle attività dell'azienda per redigere un inventario dei rischi a cui essa è più esposta in funzione del livello di impatto.
- ☐ Stabilire la portata della copertura di cui l'azienda ha bisogno.
- ☐ Valutare le diverse opzioni di assicurazione e scegliere quella che risponde meglio alle esigenze dell'azienda in base alle sue attività.
- ☐ Informarsi sulle coperture e sulle esclusioni di ogni polizza.
- ☐ Informarsi sui rischi coperti dall'assicurazione, in particolare perdita di dati, richieste di dati personali, violazioni di dati e spese legali e professionali generate dalle violazioni di terzi.
- ☐ Assicurarsi che la polizza assicurativa copra davvero i rischi a cui l'azienda potrebbe essere esposta e che il risarcimento corrisponda al livello di rischio assicurato.

Per aiutarvi a valutare i rischi, consultate la piattaforma dell'**Observatoire du Numérique**

## Quadro normativo

In Svizzera, la gestione dei cyber-rischi rientra nel quadro normativo disciplinato dalla Legge sulla sicurezza delle informazioni (LSI) e dalla Legge sulla protezione dei dati (LPD).

I quadri normativi variano a seconda delle regioni e del tipo di attività delle aziende. È indispensabile informarsi sulle normative vigenti nei paesi in cui l'azienda è attiva per essere in regola con le leggi vigenti.

Per maggiori informazioni consultate la guida **Réglementations relatives à la protection des données dans le monde**.

**Lo sapevate?**

Secondo l'articolo 19 della Legge federale sulla protezione dei dati (LPD), siete tenuti ad informare le persone quando raccogliete i dati che le riguardano.

# Il phishing

## Come funziona ?

### Ricevete un messaggio e-mail o un messaggio di testo

Sembra provenire da una persona o da un'azienda che conoscete, che vi chiede di rispondere per e-mail o cliccando su un link per fornirle dei dettagli sulla vostra identità, la vostra password oppure informazioni sensibili sull'azienda.

### Sembra vero

È facile falsificare dei logo e creare falsi indirizzi e-mail. In generale, i truffatori usano nomi di azienda famigliari oppure si fanno passare per persone che conoscete.

### È urgente

Il mittente vi spinge ad agire rapidamente o con urgenza, lasciando pensare che ci saranno conseguenze negative se non agite.

### Cosa succede dopo

Se cliccate su un link, gli hacker possono identificare che avete interagito con il messaggio e proseguire la richiesta allo scopo di sottrarvi informazioni o spingervi ad eseguire delle azioni, come ad esempio versare del denaro.

### Se ricevete un messaggio che vi sembra sospetto

- **Verificate l'indirizzo del mittente**
- **Verificate le URL passandoci sopra con il mouse prima di cliccarci sopra**
- **Non rispondete al messaggio**
- **Non rivelate mai la vostra identità**
- **Non comunicate mai delle coordinate bancarie**
- **Non versate mai del denaro**
- **Non aprite gli allegati**

*Segnalate i messaggi fraudolenti sulla piattaforma dell'Ufficio federale della cybersicurezza (UFCS) : https ://www.ncsc.admin.ch/*

### Segnalatelo !

Se avete ricevuto un'e-mail di phishing o scoperto un sito di phishing, segnalatelo sul sito **https ://antiphishing.ch**

### Mettete alla prova i vostri team !

Fate regolarmente dei test interni per valutare la consapevolezza e la comprensione delle collaboratrici e dei collaboratori nei confronti dei cyber-rischi e delle poste in gioco per l'azienda, ad esempio attraverso una campagna di falso phishing.

# Casi pratici

## Basta un clic…

Quando una persona clicca su un link fraudolento che permette di installare un ransomware, tutta la rete dell'azienda si blocca e i dati vengono presi in ostaggio. Gli hacker chiedono un riscatto, sotto forma di bonifico bancario o di criptovaluta, per sbloccare l'accesso ai dati.

Nel frattempo, l'attività dell'azienda è bloccata. I dati necessari al suo funzionamento, le informazioni sensibili sulla clientela, i team e le attività commerciali si ritrovano nelle mani degli hacker.

**Quasi l'80% dei cyber-incidenti è dovuto a un errore umano interno all'azienda o è legato ai suoi partner.**

**L'ufficio federale della cybersicurezza (UFCS)** raccomanda di fare sempre una denuncia penale. Contattate la polizia cantonale. Potete trovare il posto di polizia competente più vicino a voi sul sito **Suisse e-Police**.

## I virus informatici: come funzionano?

Ci sono diversi modi per impiantare dei malware in un sistema.

- Tramite e-mail fraudolente contenenti dei link o degli allegati che mettono in pericolo i dati e la rete. Queste e-mail di phishing (vedi pagina precedente) sono all'origine della maggior parte degli attacchi con richiesta di riscatto (o ransomware).
- Visitando dei siti Internet infetti, scansionando un QR Code o cliccando su link che scaricano automaticamente un malware sul computer o sullo smartphone.
- Collegando alla rete o ai computer una periferica o un computer esterno all'azienda (chiavetta USB, disco fisso, smartphone ecc.).
- Eseguendo delle applicazioni non verificate o non approvate.
- Autorizzando l'apertura di link esterni o il lancio di macro durante l'accesso a documenti che vi vengono trasmessi da una persona esterna all'organizzazione.

### Cosa fare in caso di richiesta di riscatto?

L' **UFCS** sconsiglia di pagare un riscatto, perché non avete nessuna garanzia che i dati vi saranno restituiti. Inoltre, cedere al ricatto contribuisce a finanziare le attività criminali e incoraggia i criminali a proseguire le loro attività o a ricominciarle.

# Prevenire gli attacchi e le loro conseguenze

## Preparare un piano di continuità operativa (PCo)

Questo piano vi permetterà di mantenere l'azienda in funzione in caso di cyber-attacco o di cyber-incidente. Mettete questo piano per iscritto, comunicatelo internamente e testatelo regolarmente.

## Sensibilizzare i vostri team all'ingegneria sociale

Formate e informate i vostri team sulle diverse tecniche di manipolazione usate per spingere una persona a trasmettere essa stessa delle informazioni, che siano sensibili o no. Possono essere dati personali o informazioni riservate che permettono di accedere alla rete informatica di un'organizzazione. Le tecniche usate consistono nello sfruttare il fattore umano, ad esempio rubando l'identità o il ruolo di una persona o di un'organizzazione.

## Prima di cliccare su un link poco sicuro…

- Verificate che il nome di dominio esista veramente e che corrisponda a ciò che desiderate consultare.
- Verificate che il sito sia protetto: l'URL deve iniziare per https (la « s » di « https » indica che le informazioni sono crittografate), e controllate che il certificato non sia scaduto o non valido (il lucchetto a fianco dell'URL non deve essere sbarrato).
- Assicuratevi di rivolgervi a una persona o a un'organizzazione reale e degna di fiducia e che non stiate per scaricare un malware o per condividere i vostri accessi con un truffatore.
- In caso di dubbio, parlatene con qualcuno. Ciò vi aiuterà a stabilire se la richiesta è reale o se è un tentativo di phishing.
- Se il dubbio rimane, telefonate direttamente al fornitore interessato o alla persona che dovrebbe avervi mandato l'e-mail. Diffidate del numero riportato nel messaggio e usate invece la vostra rubrica.

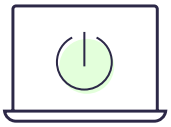
**Siate proattivi !**

**Lo sapevate ?**

In caso di cyber-attacco, la durata media per il ripristino completo del funzionamento di un'azienda è di 22 giorni.

# Come procedere in caso di attacco

## 1 Limitate i danni



- Isolate le reti interne (Wi-Fi e LAN) ed esterne (WAN / Internet).
- Identificate il computer o gli apparecchi infetti e spegneteli. Se non riuscite a identificarli rapidamente, eseguite queste operazioni per tutto il parco informatico.
- Modificate tutte le password.
- Eseguite o fate eseguire un controllo di tutti gli apparecchi (computer e server) per assicurarsi che non siano infetti.

## 2 Date l'allarme

- Seguite le procedure previste dall'azienda per avvertire il vostro responsabile o il fornitore IT.
- Avvisate i colleghi e condividete la vostra esperienza in caso di phishing, perché questi tentativi riguardano spesso più di una persona all'interno di una stessa azienda.

## 3 Segnalate la frode

- Se dei dati o delle informazioni personali sono stati compromessi, avvertite le persone interessate.
- Segnalate i messaggi fraudolenti sulla piattaforma dell'**Ufficio federale della cybersicurezza (UFCS)**.
- In caso di reato, presentate una denuncia alla polizia.

## 4 Comunicate

- Tenete informati i collaboratori, le collaboratrici, i partner e i clienti.

**Fate riferimento alla legge federale sulla sicurezza dell'informazione (LSI)**
All'articolo 74b sono elencate le autorità e le organizzazioni soggette all'obbligo di segnalare un cyber-attacco. Si tratta di numerose aziende in vari settori.

# Proposta di strategia di salvataggio dei dati

**Il salvataggio, o backup, consiste nel copiare su un supporto e/o in uno spazio esterno le informazioni necessarie per il buon funzionamento dell'azienda e a metterle in sicurezza per potervi accedere in caso di cyber-incidente. Senza questo tipo di salvataggio, è impossibile ripristinare i dati dell'azienda.**

## Istituzione di un piano di salvataggio

1

### Mappate i dati

- Fate un inventario di tutti i dati che possedete.
- Valutate la criticità dei dati per l'attività dell'azienda.
- Organizzate e suddividete questi dati in categorie.
- Definite la posizione dei dati : recensite gli apparecchi che li utilizzano e le posizioni in cui sono archiviati.
- Catalogate le persone e i sistemi che hanno accesso a questi dati.

2

### Gerarchizzate i dati

Classificate i dati per livello di importanza. Per fare questo, ponetevi queste domande :

- Quali sono i file e le informazioni indispensabili per il funzionamento globale dell'organizzazione e per ciascun degli uffici o dei dipartimenti ? (Esempio : contabilità, contatti, schede clienti, agende, rissorse umane, documenti strategici e commerciali, ecc.).
- Quali sono i dati e i documenti indispensabili e non recuperabili in caso di perdita, furto o distruzione dell'hardware ?

3

### Definite le posizioni di salvataggio

Per una buona strategia di salvataggio e un ripristino rapido dei dati dell'azienda, salvate i vostri dati in 3 posizioni diverse :

- archiviazione con salvataggio all'interno dell'organizzazione (es. : server di backup),
- archiviazione offline su disco fisso, all'interno dell'organizzazione e accessibile rapidamente (es. : locale protetto),
- archiviazione su disco depositato all'esterno dell'organizzazione (es. : cassaforte in banca).

Per maggior sicurezza e autonomia, potete eseguire un salvataggio ulteriore su un NAS (mini-server di file), una SAN (soluzione di salvataggio adattata alle medie e grandi imprese), un cloud o un data center.

In caso di archiviazione su cloud, fate attenzione al luogo in cui si trovano i server che ospitano i dati, agli obblighi legali dell'azienda in materia di hosting dei dati e alle leggi applicabili dei vari paesi. Si raccomanda di privilegiare l'uso di un cloud che archivi ed elabori i dati sul territorio nazionale.

# Proposta di strategia di salvataggio dei dati

## 4 Organizzate un calendario di salvataggio

È importante salvare regolarmente i dati. Stabilite una frequenza adatta alle attività della vostra organizzazione.

Ad esempio, potete scegliere un salvataggio quotidiano, integrato da salvataggi settimanali e mensili. Controllate e testate regolarmente gli archivi di salvataggio e i processi di ripristino.

Questo calendario vi permetterà di ripristinare i dati facilmente e rapidamente in caso di incidente, con una perdita minima, ovvero inesistente.

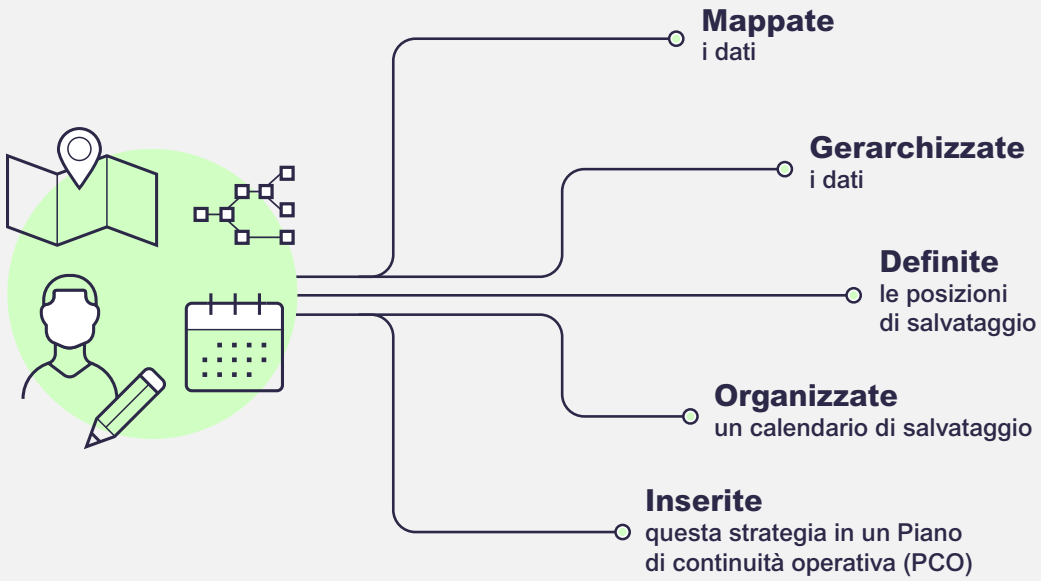
## 5 Inserite questa strategia in un piano di continuità operativa (PCO)

Nel PCO è descritto il modo in cui si può mantenere la continuità delle attività per ridurre al minimo le interruzioni e i problemi (vedi pag. 5).

Vi è anche descritta la procedura da seguire per proteggere e ripristinare i dati in caso di incidente informatico.

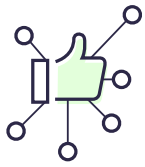
La strategia di salvataggio è quindi una parte essenziale, poiché determina il modo in cui il servizio informatico può essere rimesso in funzione per rilanciare le attività dell'azienda.

## Piano di salvataggio



# In breve

## Pratiche errate



- Credere che la cybersicurezza sia unicamente un problema informatico.
- Adottare una nuova tecnologia e nuove pratiche digitali senza un'analisi preliminare dei rischi e delle opportunità.
- Sottostimare il rischio di impatto o la probabilità di un cyber-incidente.
- Trascurare l'importanza di un piano di continuità operativa e di una strategia di salvataggio dei dati.
- Raccogliere ed elaborare più informazioni del necessario.

## Pratiche corrette per proteggere gli apparecchi, la rete e i dati

- Mantenete i software aggiornati.
- Proteggete il router Wi-Fi con una crittografia WPA2 o WPA3.
- Salvate regolarmente i dati.
- Esigete password forti e uniche per tutte le apparecchiature o gli accessi.
- Attivate un'autenticazione a più fattori.

## pratiche corrette per proteggere il personale, l'azienda, le clienti, i clienti e i partner

- Stabilite una politica in cui l'accesso alle risorse è limitato per impostazione predefinita ed è autorizzato soltanto alle persone interessate.
- Limitate la presenza di informazioni pubblicate sul sito aziendale. Evitate qualsiasi informazione che permetta di identificare le persone e il loro ruolo all'interno dell'azienda, per prevenire furti di identità o manovre di ingegneria sociale.
- Formate i team mettendo a loro disposizione del materiale adeguato e la possibilità di seguire una formazione continua interna o esterna.

**La sicurezza della vostra azienda è fondamentale!**
Chiedete assistenza ai specialisti.