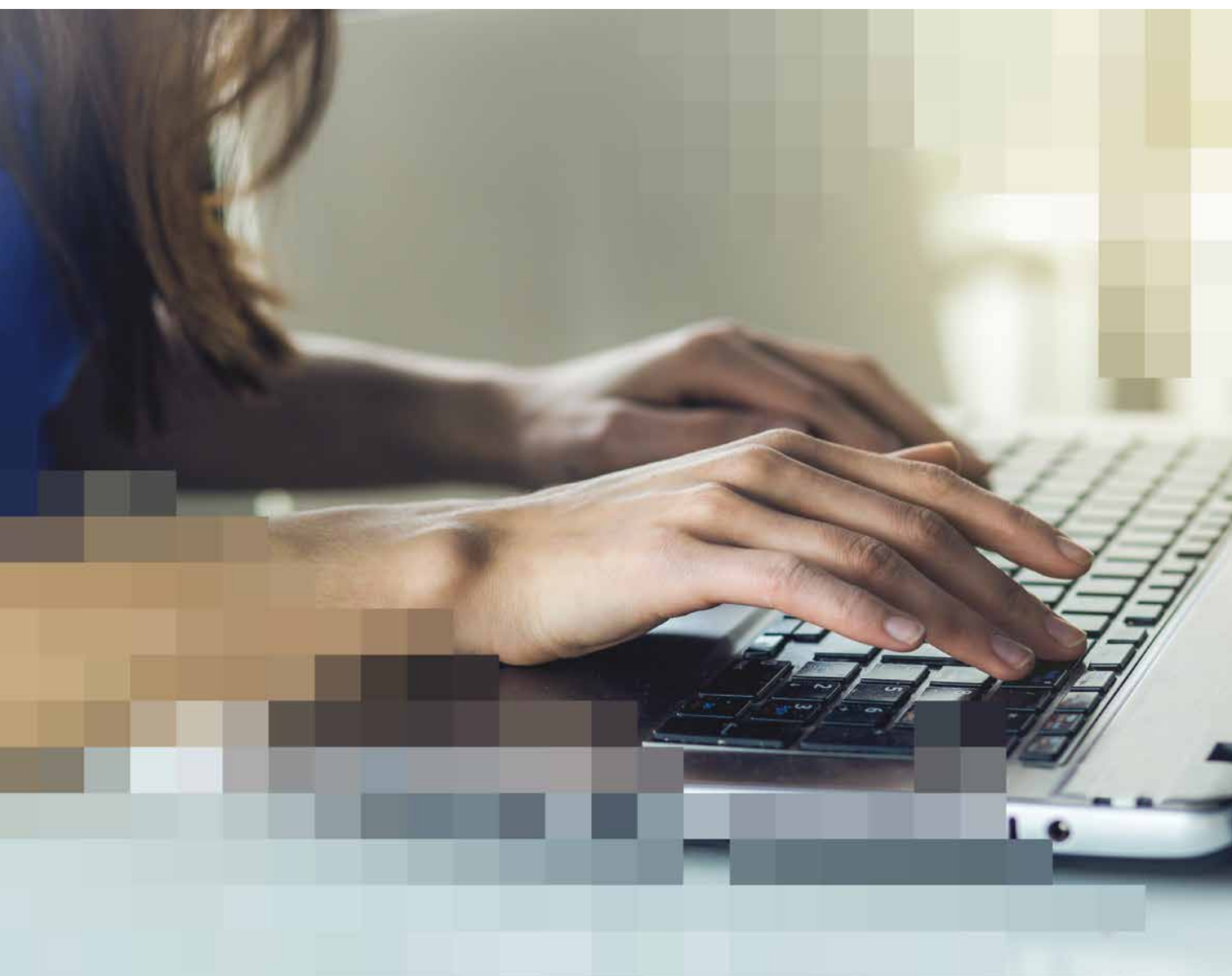


# Prevenzione della criminalità informatica

## Guida per i comuni



# Indice

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Cosa c'entra il cybercrime con il vostro comune</b> .....                    | <b>3</b>  |
| <b>2</b> | <b>Come i criminali possono danneggiare il vostro comune</b> .....              | <b>4</b>  |
| 2.1      | Metodi utilizzati dai truffatori .....  | 4         |
| 2.2      | Varianti di estorsione e furto .....  | 5         |
| <b>3</b> | <b>Come potete proteggere il vostro comune</b> .....                            | <b>7</b>  |
| 3.1      | Misure organizzative di protezione .....  | 7         |
| 3.2      | Misure tecniche di protezione .....   | 10        |
| <b>4</b> | <b>Cosa considerare quando si esternalizzano i servizi TIC</b> .....            | <b>11</b> |
| <b>5</b> | <b>Cosa si deve fare in caso di danni</b> .....                                 | <b>13</b> |
| <b>6</b> | <b>Come potete contribuire all'identificazione degli autori del reato</b> ..... | <b>14</b> |
| 6.1      | Non siate timidi nel segnalare .....  | 14        |
| 6.2      | Segnalare immediatamente gli incidenti .....                                    | 14        |

## Checklist

- > Consigli per i quadri comunali per proteggersi dagli attacchi informatici
- > Consigli per i collaboratori comunali per prevenire i reati informatici
- > Quanto è ben protetta il vostro comune dagli attacchi informatici?
- > Standard e linee guida raccomandate nel settore delle TIC

# 1 Cosa c'entra il cybercrime con il vostro comune

Maggiore vicinanza ai cittadini, migliore promozione turistica e commerciale, crossmedialità, servizi veloci: la digitalizzazione offre ai comuni molte nuove opportunità. Allo stesso tempo, richiede nuovi processi e comporta una maggiore dipendenza dal funzionamento delle tecnologie dell'informazione e della comunicazione (TIC) e dai relativi fornitori di servizi. I criminali sfruttano queste reti e dipendenze.

Nel suo rapporto sulla situazione 2019<sup>1</sup>, il Servizio delle attività informative della Confederazione afferma che anche la pubblica amministrazione è bersaglio di attacchi informatici. Dall'amministrazione comunale alla fornitura di energia elettrica, tutti possono essere colpiti. Ad esempio, il sito web può andare offline, ma anche l'intera rete può essere colpita. Oltre alle perdite finanziarie, in alcuni casi le informazioni riservate finiscono nelle mani sbagliate, con gravi conseguenze: perdita di dati, guasti al sistema, richieste di risarcimento per violazione dei dati o danni alla reputazione sono solo alcuni esempi.

## Gli attacchi informatici possono distruggere in modo permanente la fiducia della popolazione nell'amministrazione.

Con questo materiale informativo forniamo ai Comuni di piccole e medie dimensioni raccomandazioni specifiche per la protezione dalla criminalità informatica e mostriamo come reagire dopo un attacco. Ciò contribuisce anche all'attuazione delle misure della "Strategia nazionale per la protezione della Svizzera contro i rischi informatici (NCS) 2018-2022", che mira a proteggere la Svizzera in ambito informatico come compito congiunto di tutti i livelli di governo e di altri partner<sup>2</sup>.

Vi invitiamo inoltre a segnalare gli incidenti rilevanti alla polizia. Solo attraverso la cooperazione tra le autorità di polizia e le persone coinvolte, infatti, è possibile identificare e condannare i colpevoli e combattere a lungo termine la criminalità informatica.

---

<sup>1</sup> Nachrichtendienst des Bundes (2019). Sicherheit Schweiz 2019. Lagebericht des Nachrichtendienstes des Bundes. [www.vbs.admin.ch](http://www.vbs.admin.ch)

<sup>2</sup> Bundesrat (2018). Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022, [www.isb.admin.ch/isb/de/home/themen/cyber\\_risiken\\_ncs.html](http://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs.html)

## 2 Come i criminali possono danneggiare il vostro comune

I criminali informatici ricattano e derubano i comuni minacciando di pubblicare dati sensibili o di paralizzare i servizi, in particolare nel settore della sicurezza delle forniture.

### 2.1 Metodi utilizzati dai truffatori

Gli autori utilizzano l'inganno per convincere la persona presa di mira a compiere un'azione contro la sua volontà. Nella maggior parte dei casi, l'obiettivo è quello di invogliare la persona ad aprire un allegato e-mail, a cliccare su un link, a inserire dati personali come le password o a effettuare un pagamento.

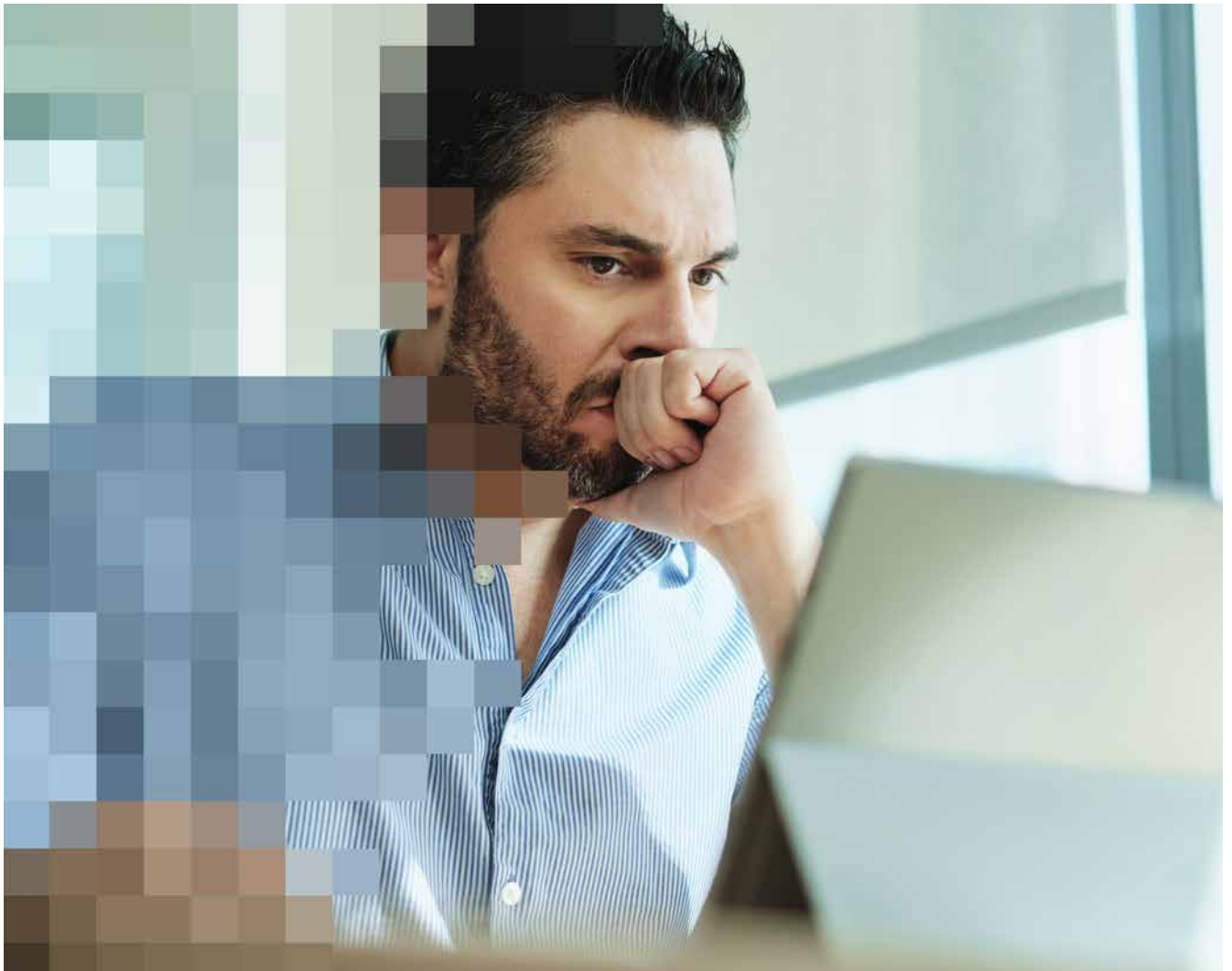
Un metodo comune è il cosiddetto social engineering. Spesso gli autori si informano in anticipo sulla struttura amministrativa, organizzativa o aziendale. Ciò avviene attraverso informazioni accessibili al pubblico, ad esempio sul sito web dell'amministrazione comunale o sui social network. Quindi si sceglie una persona bersaglio e la si mette di fronte a uno scenario su misura per lei. Ad esempio, gli autori cercano di ottenere nomi utente e password fingendo al telefono di essere un dipendente di un'azienda di software. Fingendo di avere problemi informatici gravi e fingendo di conoscere l'azienda, la persona presa di mira viene fatta sentire insicura finché non rivela le informazioni desiderate. A volte i criminali usano anche nomi di unità amministrative, come le autorità fiscali o i fornitori di energia, nelle loro e-mail o telefonate.

#### Tipi di manipolazioni

|                     |  |
|---------------------|--|
| Gerarchia           | Gli autori sfruttano la struttura organizzativa gerarchica e creano una certa pressione ad agire. Di solito fingono un'identità e chiedono ai dipendenti di rivelare informazioni sensibili o di trasferire denaro a nome di un superiore. |
| Pressione di tempo  | La persona presa di mira è indotta a credere di dover agire sotto pressione.   |
| Avività / Curiosità | Alla persona presa di mira viene promesso un premio o una sorpresa se si apre il file o si clicca sul link.  |
| Paura / Rabbia      | Ci sono minacce di conseguenze se la richiesta non viene soddisfatta, o se vengono fatte dichiarazioni palesemente false che si suppone vengano chiarite cliccando su un link maligno.   |
| Prendere a bordo    | L'argomento presentato fa leva sull'emotività del destinatario. La persona presa di mira dovrebbe, ad esempio, essere coinvolta per eliminare le lamentele.  |

## 2.2 Varianti di estorsione e furto

I criminali accedono alla rete del Comune attraverso dati di accesso rubati, malware o sistemi scarsamente protetti. Se i criminali trovano dati preziosi, li criptano o minacciano di pubblicarli o cancellarli a meno che non venga pagato un riscatto. A volte i dati vengono anche copiati e venduti a terzi o vengono attivati pagamenti nell'e-banking.



## Procedure frequenti

|                                    |   |
|------------------------------------|---|
| Ransomware                         | Il malware viene inviato su larga scala, ad esempio tramite e-mail. Le vittime individuate con questo metodo vengono poi spiate in modo mirato e vengono raccolte informazioni. Se gli autori hanno successo, prendono il controllo e iniziano a criptare i dati. I dati possono anche essere rubati. I ricattatori chiedono un riscatto per la decodifica dei dati (inglese ransom).   |
| Troiani in E-Banking               | Oltre al ricatto, i criminali informatici si concentrano anche sulla manipolazione degli ordini di pagamento. A questo scopo utilizzano i trojan per l'e-banking. I trojan di e-banking sono programmi che consentono agli aggressori di accedere al conto e-banking della vittima. I trojan vengono spesso inviati per e-mail (ad esempio, camuffati da fattura o domanda di lavoro).  |
| Phishing                           | Le potenziali vittime vengono informate tramite e-mail, sito web, telefonia Internet o SMS che alcuni dati di accesso non sono più sicuri o aggiornati. Allo stesso tempo, viene chiesto loro di modificarli utilizzando il link fornito, che conduce a un sito Web falso. Se la persona contattata si collega al sito web, gli autori ottengono i dati di accesso, ad esempio i dati della carta di credito o le password della posta elettronica o di un altro account.   |
| DDoS<br>(attacchi di sovraccarico) | DDoS è l'acronimo di Distributed Denial of Services. In questo tipo di attacco, i servizi, ad esempio il sito web, il servizio di posta elettronica o il sistema telefonico digitale, vengono sovraccaricati da un gran numero di richieste. Di conseguenza, i sistemi si interrompono e l'amministrazione o l'azienda non può più svolgere il proprio compito. Per interrompere l'attacco viene pagato un riscatto. A volte i criminali utilizzano gli attacchi DDoS anche per distrarre dall'effettivo "attacco digitale" con i dati di accesso precedentemente rubati. |
| Remote Access<br>(accesso remoto)  | Remote Access è utilizzato per accedere a un computer o a una rete dall'esterno, ad esempio quando si lavora da casa o per la manutenzione remota da parte del personale di supporto. I criminali utilizzano questo accesso remoto anche per accedere alle reti amministrative e aziendali, ad esempio attraverso tentativi di phishing o attacchi a password, componenti di rete non protetti o non aggiornati.  |

# 3 Come potete proteggere il vostro comune

Per proteggersi dagli attacchi informatici sono necessarie diverse misure tecniche e organizzative. Alcune possono essere implementate dai quadri comunali stessi, altre devono essere discusse con i responsabili TIC interni o esterni. Una sintesi delle misure di protezione qui elencate è disponibile come lista di controllo alla fine di questo documento.

## 3.1 Misure organizzative di protezione

### > **Definire le responsabilità**

Designare le persone della vostra amministrazione che sono responsabili dell'adempimento dei rispettivi compiti in relazione alla sicurezza dei sistemi TIC. Chiarite anche i ruoli e le responsabilità in materia di organizzazione delle emergenze e delle crisi e le relative competenze.

Le interfacce con i partner devono essere identificate in anticipo e i processi devono essere armonizzati. Chiarite con il vostro responsabile TIC di quali incidenti di sicurezza dovete essere informati. Questo vale sia per gli incidenti che riguardano la vostra infrastruttura sia per quelli del fornitore di servizi TIC.

### > **Registrare l'ambiente TIC**

Documentate la vostra infrastruttura TIC in un elenco di inventario il più dettagliato possibile. Solo se conoscete la vostra infrastruttura TIC, i servizi, i computer, gli utenti, ecc. saprete cosa dovete proteggere e monitorare.

### > **Prendere precauzioni**

Una buona strategia contro i cyberattacchi inizia prima dell'incidente vero e proprio: processi e percorsi di escalation ben studiati sono essenziali per mantenere il controllo.

Definite quali file di log (file di log degli eventi) salvare e per quanto tempo.

È meglio farlo in una posizione centrale. I dati di log completi aiutano a riconoscere l'origine di un attacco, a ottenere informazioni sui sistemi infetti nella propria rete e ad adottare contromisure adeguate. Data la loro importanza, gli aspetti di protezione dei dati dei file di log non devono assolutamente essere trascurati. Chiarite le questioni relative ai file di log e al rilevamento degli attacchi con il vostro responsabile TIC.

### **Strategia preventiva in caso di emergenza**

- > Concetto di comunicazione e di crisi adattato alle dimensioni del comune e coordinato con il fornitore di servizi.
- > Elenchi di contatti (unità interne ed esterne, fornitori di servizi).
- > Considerazioni sulla perdita totale del panorama TIC (sostituzione, ripresa dell'attività, perdita di dati, ecc.)
  - > sui mezzi di comunicazione da utilizzare se i sistemi TIC non sono più disponibili.
- > Scenari di emergenza TIC, esercitazioni e verifica della vulnerabilità dell'infrastruttura TIC.

> **Regolamentate il trattamento delle informazioni e dei dati sensibili**

Tenete un inventario dei dati e delle informazioni e definite gli elementi particolarmente sensibili. Create un concetto di protezione per questi elementi. Per le norme cantonali e comunali in materia di protezione dei dati, consultate i siti web del vostro cantone e della vostra associazione comunale (si veda anche il capitolo 4: "Ottenere assistenza").

Pensate bene a quali informazioni divulgare sul vostro sito web o sui social media, poiché queste informazioni sono raccolte da criminali. In particolare, la persona responsabile delle transazioni finanziarie dell'amministrazione che ha accesso all'e-banking non dovrebbe essere indicata sul sito web. Le informazioni e i dati riservati non devono mai essere trasmessi attraverso canali impersonali come il telefono o la posta elettronica. Le informazioni riservate devono essere costantemente criptate o inviate per posta a soggetti esterni.

Fate attenzione quando utilizzate i servizi cloud. Questi sono utilizzati da molti programmi. Pensate a quali dati devono essere archiviati localmente e a quali dovrebbero essere archiviati nel cloud. Non memorizzare mai dati sensibili non criptati in un cloud. Prima di utilizzare un servizio cloud, leggete i termini e le condizioni generali (CG) dell'azienda che offre il servizio e prestate attenzione alle norme sulla protezione dei dati. I dati non devono essere ceduti, ad esempio per scopi commerciali. Chiedete all'autorità di controllo della protezione dei dati.

Un aiuto per la protezione dei dati e un elenco delle autorità di controllo competenti sono disponibili sul sito web della Conferenza dei Commissari svizzeri per la protezione dei dati, [privatim](http://privatim.ch), [www.privatim.ch](http://www.privatim.ch)

> **Utilizzate password sicure**

Definite regole vincolanti per le password e applicatele in modo coerente con i dipendenti. La lunghezza minima di una password deve essere di dodici caratteri e la password deve essere composta da lettere maiuscole e minuscole, numeri e caratteri speciali.

Idealmente, dovrebbe essere generata in modo casuale e non contenere informazioni personali, come il nome o la data di nascita. L'autenticazione a due fattori offre un'ulteriore protezione.

Evitate di usare la stessa password più volte! Se è difficile ricordare diverse password, è consigliabile utilizzare un gestore di password.

Se si seguono queste regole, la modifica ciclica delle password non è obbligatoria. Tuttavia, le password devono essere cambiate al più tardi quando potrebbero essere conosciute da terzi o quando i dipendenti non lavorano più per il Comune.

> **Sensibilizzate i dipendenti e i membri della milizia<sup>3</sup>**

I quadri del comune hanno il dovere di proteggersi dagli attacchi informatici. Ciò include anche la sensibilizzazione dei dipendenti. Gli impiegati comunali hanno molte responsabilità all'interno dell'amministrazione comunale e sempre più spesso devono prendere decisioni su questioni relative alle TIC.

Si raccomanda che gli impiegati comunali ricevano una formazione speciale in questo settore e che in generale investano in corsi di sensibilizzazione alla sicurezza per i dipendenti e i membri di milizia. Organizzatela insieme ad altri comuni o alle organizzazioni comunali cantonali.

Ciò può contribuire a ridurre gli sforzi e i costi. Le informazioni per i dipendenti sono contenute nella lista di controllo "Consigli per i dipendenti comunali per prevenire la criminalità informatica".

---

3 Politici, esterni, ecc.

> **Fate attenzione alle e-mail**

Il malware elettronico arriva spesso sul vostro computer attraverso allegati di posta elettronica camuffati da presunte fatture o domande di lavoro. Bloccate la ricezione di allegati e-mail pericolosi. Un elenco dettagliato e aggiornato di tali allegati pericolosi è disponibile sul sito web di GovCERT<sup>4</sup>. Assicuratevi che non sia possibile eseguire macro in documenti Office di origine non sicura. Discutetene con il vostro responsabile TIC.

Definite i canali di comunicazione per i dipendenti per la segnalazione di incidenti sospetti (e-mail, computer, telefonate, ecc.) e, se possibile, attivate una funzione per la segnalazione di e-mail dubbie.

Comunicare con attenzione anche con i cittadini. Inviare le e-mail solo in formato testo e utilizzare con parsimonia gli allegati. Evitate i documenti Office con macro e utilizzate invece i documenti PDF. Non divulgate i link e non collegatevi a siti web che richiedono nomi utente, password o altri dati. La maggior parte delle e-mail fraudolente sono indirizzate in modo impersonale; scrivete ai cittadini usando il loro

## Se conoscete i vostri gateway, potete tenerli chiusi ai criminali informatici.

> **Protegete il vostro conto bancario online**

Utilizzate un computer separato per i pagamenti, sul quale non navigate in Internet o non ricevete e-mail. Parlate con il vostro responsabile TIC della possibilità di effettuare i pagamenti online in un'area separata dal resto delle vostre applicazioni (sandboxing) o in un sistema virtualizzato dedicato e appositamente protetto.

Chiarite tutti i processi relativi alle transazioni di pagamento. Questi devono essere rispettati dai dipendenti in ogni caso, ad esempio con il principio del doppio controllo e/o della firma collettiva: in questo caso, i pagamenti devono essere firmati anche da un altro utente dell'e-banking prima di essere avviati. Questo vale in particolare se più dipendenti sono autorizzati a effettuare pagamenti. Parlate con la vostra banca delle possibili misure di sicurezza.

---

4 [www.govcert.ch/downloads/blocked-filetypes.txt](http://www.govcert.ch/downloads/blocked-filetypes.txt)

## 3.2 Misure tecniche di protezione

### > **Backup dei dati**

Definite un processo che regoli i backup regolari dei dati e rispettate con coerenza. Pensate a quanti giorni di perdita di dati potete sopportare e conservate una copia aggiuntiva del vostro backup separatamente (offline) e fuori sede. Voi e il vostro sostituto dovrete esercitarvi di tanto in tanto a importare i backup, in modo da avere familiarità con il processo in caso di emergenza. Conservare le versioni precedenti del backup per un periodo di alcuni mesi.

### > **Eseguite gli aggiornamenti di sicurezza**

I software obsoleti sono una porta d'accesso molto diffusa per le minacce informatiche. Assicuratevi che i vostri sistemi siano aggiornati. Questo vale anche per il sistema di gestione dei contenuti (CMS), cioè il sistema di gestione del vostro sito web. La maggior parte dei CMS offre una funzione di aggiornamento automatico facile da attivare.

### > **Installate la protezione antivirus**

Installate una protezione antivirus su ogni computer e attivate la protezione in tempo reale. Assicuratevi che sia aggiornato regolarmente e che esegua una scansione completa del sistema ogni giorno.

### > **Protegete l'accesso remoto**

Non proteggete mai l'accesso remoto alla vostra rete con una semplice autenticazione (nome utente e password). Utilizzate almeno l'autenticazione a due fattori o impostate una connessione sicura tramite una rete privata virtuale (VPN). Questo vale anche per l'accesso dei responsabili TIC esterni.



## 4 Cosa considerare quando si esternalizzano i servizi TIC

Se esternalizzate la vostra infrastruttura TIC e la vostra TIC è gestita da una o più aziende esterne, troverete di seguito alcuni suggerimenti. Nella lista di controllo "Quanto è protetto il vostro Comune dagli attacchi informatici?" troverete ulteriori requisiti che dovrebbero essere contemplati nel catalogo dei servizi e nel contratto con il fornitore di servizi TIC. Si noti che la responsabilità non può essere esternalizzata o delegata. In caso di incidente, il Comune può trovarsi alla fine della catena di responsabilità.

### La responsabilità è dei quadri del Comune.

> **Utilizzate i requisiti minimi come guida**

I controlli di sicurezza devono essere effettuati già al momento dell'accettazione di sistemi TIC integrati. Informatevi presso l'ufficio TIC competente del vostro cantone o presso le associazioni comunali sulle condizioni generali e sui requisiti per l'utilizzo dei servizi IT. Questi requisiti dovrebbero far parte del rapporto contrattuale tra voi e i fornitori esterni di servizi TIC. Gli obblighi di riservatezza previsti dalla legge per la manutenzione e il supporto dei sistemi TIC da parte di terzi devono essere regolamentati e non deve essere autorizzato l'accesso non necessario a dati personali particolarmente sensibili. È inoltre necessario prendere accordi e chiarimenti con la rispettiva società di archiviazione dei dati (società di cloud).

> **Scegliete un fornitore di servizi TIC qualificato**

Le certificazioni secondo gli standard riconosciuti di protezione dei dati e di sicurezza delle informazioni o i rapporti di ispezione di terzi indipendenti possono essere utili nella scelta di un'azienda (vedere l'elenco di controllo "Standard e linee guida raccomandati nel settore TIC"). Non è necessario scegliere necessariamente partner certificati. È consigliabile che i fornitori di servizi TIC dimostrino di soddisfare i vostri requisiti e di poter garantire la disponibilità e la sicurezza da voi richieste. Fate controllare o confermare questo aspetto da un organismo indipendente.

> **Eseguite audit di sicurezza**

L'implementazione dei servizi definiti nel contratto deve essere verificata periodicamente secondo standard di audit riconosciuti, ad esempio sulla base del COBIT (Control Objectives for Information and Related Technology) dell'Information Systems Audit and Control Association (ISACA).

A tal fine, è possibile avvalersi dei servizi di centri di revisione indipendenti. La società di servizi TIC può anche far eseguire un cosiddetto ISAE 3402 Type 2 (International Standard on Assurance Engagements), noto anche come rapporto SOC 2 (Service Organisation Control).

L'organismo di controllo valuta gli aspetti di sicurezza, disponibilità, integrità e riservatezza.

> **Unite le forze con altri comuni**

Se la vostra amministrazione comunale non è in grado di acquistare servizi estesi da un fornitore di servizi TIC, unitevi ad altri comuni interessati. Ciò consente di ottenere condizioni di acquisto migliori e di ridurre i costi di approvvigionamento.

Un'altra opzione è quella di esternalizzare questo compito a un comune più grande.

> **Cercate supporto**

Diversi enti, associazioni e organizzazioni ufficiali offrono informazioni rilevanti sull'esternalizzazione dei servizi TIC e strumenti come linee guida, schede informative e contratti campione per lavorare con i fornitori di servizi TIC.

Esempi di enti, associazioni e organizzazioni ufficiali:

**Tecnologie dell'informazione e della comunicazione (TIC)**

- > Gli uffici cantonali per le TIC dispongono di linee guida e ausili, ad esempio l'Ufficio per l'informatica e l'organizzazione del Cantone di Berna (KAIO), [www.be.ch/kaio](http://www.be.ch/kaio)
- > Anche le associazioni comunali possono offrire supporto. Un elenco delle associazioni comunali è disponibile all'indirizzo [www.chgemeinden.ch](http://www.chgemeinden.ch)
- > Presso l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) sono disponibili gli standard minimi per le TIC, [www.bwl.admin.ch](http://www.bwl.admin.ch)
- > Il National Cyber Security Centre<sup>5</sup> (NCSC), [www.ncsc.ch](http://www.ncsc.ch), dispone di informazioni di intelligence e di conoscenze provenienti dai Computer Emergency Response Teams (CERT) di altri Paesi, nonché di misure preventive. Se il vostro fornitore di servizi TIC non è ancora membro, contattate [outreach@ncsc.ch](mailto:outreach@ncsc.ch)
- > Le CG della Conferenza svizzera per l'informatica (SIK) sono adatte per le transazioni TIC nella pubblica amministrazione. Sono disponibili anche modelli di contratto per le CG della SIK, <https://sik.swiss>
- > La Label (marchio) [cyber-safe.ch](http://cyber-safe.ch) è stato sviluppato dall'Associazione svizzera per il marchio di sicurezza informatica. Definisce i requisiti minimi specifici per i Comuni e le PMI. I rischi informatici di comuni e PMI possono essere determinati tramite un questionario online, [www.cyber-safe.ch](http://www.cyber-safe.ch)

**Acquisti**

- > Una panoramica delle pagine dedicate agli acquisti delle amministrazioni federali e cantonali e delle città più grandi è disponibile sui siti web di e-government Svizzera, [www.egovernment.ch](http://www.egovernment.ch), e dell'associazione [simap.ch](http://simap.ch), [www.simap.ch](http://www.simap.ch).

**Datenschutz**

- > Mezzi ausiliari per la protezione dei dati e l'elenco delle rispettive autorità di controllo sono disponibili sul sito della Conferenza dei Commissari svizzeri per la protezione dei dati privatim, [www.privatim.ch](http://www.privatim.ch)
- > L'Incaricato federale della protezione dei dati e delle informazioni (IFPDT) è responsabile del trattamento dei dati da parte dei privati e degli organi federali, [www.edoeb.admin.ch](http://www.edoeb.admin.ch)
- > Cercate supporto  
Diversi enti, associazioni e organizzazioni ufficiali offrono informazioni rilevanti sull'esternalizzazione dei servizi TIC e strumenti come linee guida, schede informative e contratti campione per lavorare con i fornitori di servizi TIC.

---

<sup>5</sup> Dal 1. gennaio 2020 vari compiti della Confederazione in ambito cyber sono stati riuniti sotto l'egida del Centro nazionale per la sicurezza informatica (NCSC). Ciò vale anche per la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI).

# 5 Cosa si deve fare in caso di danni

## Primo soccorso in caso di cyberattacco

### Isolare

- > Disconnettere immediatamente tutti i sistemi dalla rete. Non dimenticate di spegnere la WLAN.

### Contattare

- > Contattare il responsabile TIC e tutti i referenti dell'organizzazione che devono occuparsi dell'attacco.
- > Valutare la possibilità di contattare la polizia e sporgere denuncia. Attendere che la polizia abbia messo al sicuro le prove prima di riavviare i sistemi.

### Segnalare

- > Segnalate l'attacco anche all'NCSC, [www.ncsc.ch](http://www.ncsc.ch). Anche la vostra associazione di comuni dovrebbe essere informata dell'incidente, poiché potrebbero essere coinvolti più comuni.
- > Osservate gli obblighi di segnalazione, ad esempio per quanto riguarda la protezione dei dati.

I responsabili della TIC o altre persone specializzate vi aiuteranno a riparare e, se necessario, a ripristinare la vostra infrastruttura.

Dopo l'attacco è prima dell'attacco. Incorporate le lezioni apprese nel miglioramento della qualità, nei processi interni, nella documentazione, nelle esercitazioni e nella gestione e cultura aziendale.

# 6 Come potete contribuire all'identificazione degli autori del reato

## 6.1 Non siate timidi nel segnalare

L'esperienza dimostra che molti reati informatici sono collegati e presentano analogie. Ogni denuncia e ogni rapporto possono fornire l'indizio decisivo per individuare il colpevole.

La polizia non è interessata ai vostri segreti amministrativi e non interferisce con la vostra infrastruttura. In caso di attacco, cerca solo informazioni e tracce rilevanti per la risoluzione del reato. L'indagine è soggetta al segreto d'ufficio. Inoltre, le indagini devono rispettare le norme sulla protezione dei dati. Il timore di conseguenze negative in caso di denuncia, come il sequestro di computer per un periodo di tempo più lungo o la pubblicazione di un caso, è infondato. La polizia vi prenderà molto sul serio e di solito discuterà prima con voi le misure di perseguimento. Potete anche coinvolgere il vostro consulente legale in qualsiasi momento. Nella maggior parte dei casi è possibile trovare un approccio che vada bene per entrambe le parti.

Agire rapidamente può ridurre i danni in caso di incidente informatico.

## 6.2 Segnalare immediatamente gli incidenti

Segnalare il più rapidamente possibile alla polizia o al ministero pubblico gli episodi penalmente rilevanti, come l'intrusione non autorizzata in un sistema di elaborazione dati. Soprattutto se sono stati causati dei danni. Più si aspetta, maggiore è la probabilità che prove preziose vengano coperte. Inoltre, qualsiasi interferenza può far sì che le tracce non siano più utilizzabili o vengano cancellate. Ogni stazione di polizia accetta una denuncia penale. Sul portale online Suisse ePolice ([www.suisse-epolice.ch](http://www.suisse-epolice.ch)) troverete il numero di telefono della stazione di polizia più vicina a voi.

Si dovrebbe anche prendere in considerazione la possibilità di fare una denuncia volontaria alle autorità di polizia o all'NCSC nel caso di incidenti che non hanno causato alcun danno o che sono già stati scoperti nella fase di tentativo. Tuttavia, le segnalazioni all'NCSC non possono essere utilizzate per l'azione penale o nei procedimenti giudiziari.

# Suggerimenti per gli amministratori comunali per proteggersi dagli attacchi informatici

Un attacco informatico può colpire qualsiasi comune. Tuttavia, potete proteggere meglio il vostro comune con alcune misure precauzionali.

## Chiarire le responsabilità e prendere precauzioni

- > Definite le responsabilità in materia di sicurezza informatica e le interfacce con i vostri partner. Processi ben definiti e percorsi di escalation sono essenziali per mantenere il controllo.

## Protegete i vostri dati

- > Regolamentare la gestione delle informazioni e dei dati. Nessuna informazione riservata deve essere trasmessa attraverso canali impersonali.
- > Fate attenzione quando utilizzate i servizi cloud. Prima di utilizzare un'azienda cloud, leggete i termini e le condizioni e prestate attenzione alle norme sulla protezione dei dati. I dati sensibili non devono mai essere archiviati in modo non criptato nel cloud.
- > Definite un processo che regoli i backup regolari dei dati. Conservare una copia aggiuntiva del backup separatamente (offline) e fuori sede.

## Utilizzate password sicure

- > La lunghezza minima della password deve essere di dodici caratteri e la password deve essere composta da lettere maiuscole e minuscole, numeri e caratteri speciali. L'autenticazione a due fattori offre un'ulteriore protezione. Evitate di usare la stessa password più di una volta. Utilizzate invece un gestore di password e generate una password separata per ogni applicazione.

## Sensibilizzate i vostri dipendenti e il personale di milizia (politici e/o personale esterno)

- > I segretari comunali hanno molte responsabilità all'interno dell'amministrazione comunale e sempre più spesso devono prendere decisioni su questioni relative alle TIC. Si raccomanda che gli impiegati comunali ricevano una formazione speciale in questo settore e che in generale investano in corsi di sensibilizzazione alla sicurezza per i dipendenti e i membri di milizia.

## Fare attenzione quando si tratta di e-mail

- > Bloccate la ricezione di allegati di posta elettronica pericolosi e assicuratevi che non possano essere eseguite macro in documenti Office di origine non sicura. Definite i canali di comunicazione attraverso i quali i dipendenti possono segnalare gli incidenti sospetti (e-mail, computer, telefonate, ecc.). Se possibile, attivate una funzione per la segnalazione di e-mail dubbie.

## Siate sempre aggiornati

- > Implementate un software antivirus e assicuratevi che tutti i computer e i server della vostra rete installino automaticamente gli aggiornamenti di sicurezza.

## Proteggere l'accesso remoto

- > Proteggete l'accesso remoto alla rete con un'autenticazione a due fattori. L'ideale sarebbe utilizzare una connessione sicura tramite una rete privata virtuale (VPN).

## Assicuratevi che il vostro online banking sia sicuro

- > Proteggete il vostro conto bancario online con un computer separato, con un'area delimitata (sandboxing) o con un sistema virtualizzato dedicato e appositamente protetto. Regolamentare i processi di pagamento, ad esempio con un principio di doppio controllo e una firma collettiva.

# Suggerimenti per i dipendenti comunali, per prevenire la criminalità informatica

I quadri comunali hanno il dovere di proteggersi dagli attacchi informatici. Sono inoltre responsabili della sensibilizzazione dei dipendenti. I dipendenti devono attuare le seguenti misure nel loro lavoro quotidiano:

## Gestire le e-mail con attenzione

- > Diffidate dei link o degli allegati contenuti nelle e-mail provenienti da mittenti sconosciuti. Fate particolare attenzione quando aprite i documenti di Office; non attivate mai le macro. Non abbiate timore di chiedere informazioni personali se notate qualcosa di insolito in un'e-mail. Questo vale anche per i mittenti conosciuti! Fate attenzione anche al tasto "Rispondi": verificate se l'e-mail è davvero indirizzata alla persona giusta. L'ideale sarebbe riscrivere l'indirizzo e-mail.

## Utilizzate delle password sicure

- > La lunghezza minima della password deve essere di dodici caratteri e la password deve essere composta da lettere maiuscole e minuscole, numeri e caratteri speciali. Non condividete mai le password, i dati di accesso o le informazioni sul conto per telefono, per e-mail o tramite moduli web aperti da un link.
- > Evitate di usare la stessa password in più situazioni.

## Attenzione ai dati sensibili

- > Pensate bene a quali informazioni divulgare in pubblico, ad esempio sul sito web e sui social network, o discutere in pubblico.
- > Le informazioni riservate devono essere sempre criptate o inviate per posta a organizzazioni esterne.

# Quanto è protetto il vostro comune dagli attacchi informatici?

Quanto è protetta e preparata la vostra amministrazione comunale contro gli attacchi provenienti dal cyberspazio?

Questa lista di controllo vi aiuterà ad affrontare le domande più importanti sulla protezione informatica minima. Per ogni "non so" o "no", fate le dovute precisazioni. Vale quanto segue: le misure di protezione dagli attacchi informatici non possono essere delegate ai dipendenti, ma devono essere affrontate e coordinate dalla direzione comunale.

Se avete esternalizzato le vostre TIC, verificate se i seguenti punti sono contemplati nel contratto con il fornitore di servizi.

|  | Sì                    | No                    | Non lo so             |
|--|-----------------------|-----------------------|-----------------------|
| <b>Compiti, competenze, responsabilità</b>   |                       |                       |                       |
| La vostra amministrazione comunale ha definito chi è responsabile della cybersecurity?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| La persona responsabile ha le conoscenze e le competenze necessarie per gestire la cybersecurity e segue regolarmente corsi di aggiornamento?                | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| La persona responsabile ha la posizione gerarchica necessaria e le competenze corrispondenti per implementare le misure di cybersecurity?                    | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Esistono linee guida per la gestione sicura dei dispositivi e dei dati TIC?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Queste linee guida e le misure di cybersecurity sono implementate in modo coerente e sistematico e vengono riviste regolarmente?                             | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>Sensibilizzazione dei dipendenti e dei collaboratori di milizia</b>   |                       |                       |                       |
| I vostri dipendenti dispongono di linee guida per la gestione sicura di e-mail, dati digitali e Internet?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I dipendenti conoscono e comprendono queste linee guida?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I dipendenti applicano le linee guida in modo coerente e corretto?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I dipendenti vengono regolarmente formati o sensibilizzati in materia di cybersecurity, ad esempio sulla corretta gestione delle e-mail?                     | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>Direttive sulla protezione dei dati</b>   |                       |                       |                       |
| I dati sui vostri sistemi (archivi e memorizzazione dei dati, dispositivi finali e server) sono criptati?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Siete a conoscenza delle norme di legge relative alla conservazione e al trattamento dei dati?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Conoscete i vostri obblighi in relazione alle norme giuridiche sui dati personali?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Le norme sulla protezione dei dati attualmente in vigore sono applicate in modo coerente e corretto nella vostra amministrazione comunale?                   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| L'accesso fisico all'infrastruttura informatica, ai server e alla rete della vostra amministrazione comunale è adeguatamente protetto dall'accesso di terzi? | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>Linee guida per le password e amministrazione degli utenti</b>  |                       |                       |                       |
| La vostra amministrazione comunale ha delle linee guida sull'uso delle password?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Esistono linee guida che definiscono quali dipendenti hanno accesso a quali dati?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Queste linee guida sono implementate in modo coerente e corretto?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>Protezione aggiornata contro il malware</b>   |                       |                       |                       |
| I vostri dispositivi sono protetti da software dannoso (programma antivirus)?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>Firewall configurato e aggiornato</b>   |                       |                       |                       |
| La rete e i sistemi TIC sono protetti da un firewall?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Sono state definite regole speciali del firewall (ad esempio, restrizioni geografiche)?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Il vostro firewall è aggiornato regolarmente?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

|   | Sì                    | No                    | Non lo so             |
|---|-----------------------|-----------------------|-----------------------|
| <b>Segmentazione della rete</b>   |                       |                       |                       |
| Le singole aree dell'amministrazione comunale, ad esempio le risorse umane e la contabilità, sono separate?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Utilizzate un computer o un sistema separato solo per l'online banking?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>Accesso da remoto</b>  |                       |                       |                       |
| L'accesso esterno all'infrastruttura informatica, ai server e alla rete della vostra amministrazione comunale è protetto (VPN, autenticazione a due fattori)?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>Mantenere aggiornati i dispositivi e i sistemi connessi a Internet</b>   |                       |                       |                       |
| Utilizzate l'opzione di aggiornamento automatico del software?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Per i dispositivi e i sistemi il cui software non viene aggiornato automaticamente, viene aggiornato regolarmente, ad esempio dal produttore?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I dispositivi mobili utilizzati nell'amministrazione comunale sono regolarmente aggiornati?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Il sistema di gestione dei contenuti del vostro sito web è aggiornato?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>WLAN protetta e criptata</b>   |                       |                       |                       |
| La vostra WLAN è criptata e protetta?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Esiste una WLAN separata per i dipendenti e gli ospiti?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>Back-up</b>  |                       |                       |                       |
| Utilizzate un processo di backup dei dati?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Controllate regolarmente la funzionalità e la leggibilità del back-up?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Una copia aggiuntiva del backup è conservata separatamente (offline) e fuori sede?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>Precauzioni minime per la gestione delle emergenze</b>   |                       |                       |                       |
| Sono state definite le misure immediate in caso di incidente TIC?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Il responsabile e la persona da contattare in caso di incidente (ad es. malfunzionamento, attacco, ecc.) sono definiti e disponibili?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Esistono piani di risposta operativa e di ripristino?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Sapete come sono organizzati il monitoraggio dei sistemi e il processo di escalation?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| È possibile una forensics interna? Se no: è assicurata esternamente?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| È garantito l'accesso fisico ai sistemi (per la forensics)?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Sono disponibili sufficienti supporti di backup per le prove?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Esiste l'obbligo di documentare tutti i sistemi rilevanti (ad esempio, in un database di gestione della configurazione, CMDB)?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <b>Contratto con il fornitore di servizi TIC</b>  |                       |                       |                       |
| I punti di cui sopra di questa valutazione sono coperti dal contratto con il fornitore di servizi?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| La responsabilità in caso di sinistro e le esclusioni dell'obbligo di prestazione (ad es. forza maggiore) sono disciplinate contrattualmente?   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I livelli di servizio per il funzionamento regolare e di emergenza sono formulati chiaramente (questo vale per i servizi commissionati negli obiettivi di sicurezza richiesti, ad esempio disponibilità, riservatezza o integrità)? Sono stati definiti termini come operazioni di emergenza o incidenti critici? | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| La strategia di uscita è ben studiata e concordata contrattualmente, soprattutto per le soluzioni cloud?  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

# Standard e linee guida raccomandati nel settore delle TIC

Le certificazioni secondo gli standard riconosciuti di protezione dei dati e sicurezza delle informazioni o i rapporti di ispezione di terzi indipendenti possono essere utili nella scelta di un fornitore di servizi TIC. Non dovete necessariamente scegliere partner certificati. È consigliabile che i fornitori di servizi TIC dimostrino di soddisfare i vostri requisiti e di poter garantire la disponibilità e la sicurezza da voi richieste. Fatelo verificare o confermare da un ente indipendente.

Esistono molti standard e linee guida diverse. Le organizzazioni di servizi TIC dovrebbero conoscere e rispettare le norme ISO 27001, ISO 22301, ISO 9001 e ISO 14001.

Se vengono utilizzati altri standard, l'azienda deve fornire la prova della mappatura di conformità. Se le esigenze di protezione sono maggiori, è necessario formulare i propri requisiti aggiuntivi.

Esempi di standard e linee guida:

## Gestione di crisi, Business Continuity, Disaster Recovery

- > ISO 22301, Business Continuity Management System
- > ISO 27031, IT Service Continuity Management System
- > BS 11200, Sistemi di gestione di crisi-System

## Sicurezza dei dati e delle informazioni

- > ISO 27001, Sicurezza delle informazioni
- > ISO 27701, Estensione della norma ISO 27001 per includere la protezione dei dati
- > ISO 30141, Architettura di riferimento per l'Internet of Things (IoT), riservatezza dei dati trattati
- > Allineamento in conformità al Regolamento UE 2016/679, General Data Protection Regulation (GDPR)
- > NIST Cybersecurity Framework

## Direttive tecniche

- > EN 50173, Struttura di cablaggio
- > EN 50600, Centri dati
- > ANSI / TIA-942, Centri dati

## Altro (soprattutto per i fornitori di hardware)

- > ISO 9001, Gestione della qualità
- > ISO 14001, Gestione ambientale

## Linee guida per i clienti

- > ISO 22300, Standard terminologici su sicurezza e resilienza
- > ISO 22318, Standard terminologici supplementari per la sicurezza e la resilienza e Chain Continuity
- > ISO 27036, Sicurezza delle informazioni nella gestione dei fornitori
- > ISO 31010, Gestione del rischio

#### Impressum

Polizia cantonale Berna, Centro nazionale per la cybersicurezza (NCSC) e Rete integrata svizzera per la sicurezza (RSS) per la Rete di supporto alle indagini per la lotta alla criminalità digitale (NEDIK)

Partner: Ufficio per l'informatica e l'organizzazione del Cantone di Berna (KAIO), Associazione dei comuni bernesi (VBG), Associazione dei comuni svizzeri (SGV)

Contatto: Polizia cantonale Zurigo, NEDIK, [cyc\\_nedik@kapo.zh.ch](mailto:cyc_nedik@kapo.zh.ch)

Immagini: iStock

Traduzione in italiano: Dipartimento delle istituzioni del Canton Ticino

|           |                |   |
|-----------|----------------|---|
| Ihre      | <b>POLIZEI</b> | Kantonale und Städtische Polizeikorps   |
| Votre     | <b>POLICE</b>  | Corps de police cantonaux et municipaux |
| La vostra | <b>POLIZIA</b> | Corpi di polizia cantonali e comunali   |