[Sottotitolo facoltativo]

Progetto di crisi ICT
Scuola: [Nome]

|  |  |  |  |
| --- | --- | --- | --- |
| Versione | Data | Persona | Modifiche apportate/osservazioni |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |
| Responsabile: [Responsabile] |  | Redatto da: Autore/autrice |
| Editore/editrice: [Editore]. | Creazione: 18.11.2024 | Va a | CC a: [Destinatario] |

Contenuto

[1 Introduzione e obiettivi 4](#_Toc183437627)

[1.1 Scopo del progetto di sicurezza 4](#_Toc183437628)

[1.2 Campo di applicazione 4](#_Toc183437629)

[1.3 Definizione di termini importanti 4](#_Toc183437630)

[Capitolo 1 - Inventario 5](#_Toc183437631)

[2 Infrastruttura 5](#_Toc183437632)

[2.1 Infrastruttura di rete 5](#_Toc183437633)

[2.2 Componenti della rete 5](#_Toc183437634)

[2.3 Terminali 5](#_Toc183437635)

[3 Gestione dei contratti 5](#_Toc183437636)

[4 Protezione dell'infrastruttura di rete 5](#_Toc183437637)

[4.1 Controllo degli accessi alla rete 5](#_Toc183437638)

[4.2 Segmentazione e gestione delle sottoreti 5](#_Toc183437639)

[4.3 Protezione dagli attacchi esterni (firewall, IPS/IDS ecc.) 5](#_Toc183437640)

[5 Protezione dei componenti della rete 5](#_Toc183437641)

[5.1 Linee guida di sicurezza per il server 5](#_Toc183437642)

[5.2 Gestione dei dispositivi di rete 6](#_Toc183437643)

[5.3 Patch Management 6](#_Toc183437644)

[5.4 Sicurezza fisica 6](#_Toc183437645)

[6 Protezione dei terminali\*\* 6](#_Toc183437646)

[6.1 Linee guida per i terminali 6](#_Toc183437647)

[6.2 Cifratura e software di sicurezza 6](#_Toc183437648)

[6.3 Gestione dei dispositivi mobili (GDM) 6](#_Toc183437649)

[6.4 Linee guida BYOD 6](#_Toc183437650)

[6.5 Requisiti di sicurezza per i dispositivi di proprietà della scuola 6](#_Toc183437651)

[6.6 Separazione dei dati privati dai dati scolastici 6](#_Toc183437652)

[7 Gestione dei dati e backup 7](#_Toc183437653)

[7.1 Progetto di backup 7](#_Toc183437654)

[7.2 Conservazione e archiviazione dei dati 7](#_Toc183437655)

[7.3 Ripristino in caso di emergenza 7](#_Toc183437656)

[Capitolo 2 - Organizzazione e crisi 8](#_Toc183437657)

[8 Analisi e valutazione del rischio 8](#_Toc183437658)

[8.1 Forme dei rischi per la sicurezza 8](#_Toc183437659)

[8.2 Analisi dei punti deboli 9](#_Toc183437660)

[9 Sensibilizzazione e formazione 9](#_Toc183437661)

[9.1 Definizione delle responsabilità 9](#_Toc183437662)

[10 Audit e valutazioni della sicurezza 9](#_Toc183437663)

[11 Misure durante e dopo un incidente 9](#_Toc183437664)

[11.1 Team di intervento 9](#_Toc183437665)

[11.2 Assistenza interna 9](#_Toc183437666)

[11.3 Assistenza esterna 10](#_Toc183437667)

[11.4 Requisiti d'informazione 10](#_Toc183437668)

[11.5 Risorse informative 10](#_Toc183437669)

[12 Analisi della situazione e misure immediate 10](#_Toc183437670)

[12.1 Identificazione dei dati interessati 10](#_Toc183437671)

[12.2 Definire le misure immediate 10](#_Toc183437672)

[Capitolo 3 - Documentazione e reporting 12](#_Toc183437673)

[12.3 Documentazione del progetto di sicurezza ICT 12](#_Toc183437674)

[12.4 Meccanismi di reporting 12](#_Toc183437675)

[Capitolo 4 - Appendici 13](#_Toc183437676)

[13 Elenchi dei contatti 13](#_Toc183437677)

[14 Documentazione dei prodotti 13](#_Toc183437678)

[15 Reporting 13](#_Toc183437679)

[16 Membri del team d'intervento in caso di crisi 13](#_Toc183437680)

***Osservazioni preliminari***

*Non si devono scrivere password e altre informazioni segrete in questo documento. Poiché questo documento deve essere utilizzato nei processi di approvazione e per i corsi di formazione, si consiglia di memorizzare questi dati segreti in un password manager o in un documento di riferimento accessibile alle persone autorizzate.*

*Alcuni dei seguenti capitoli potrebbero non essere rilevanti per la vostra istituzione, altri potrebbero essere mancanti. Vi invitiamo a personalizzare il documento in base alle vostre esigenze.*

*Il progetto di sicurezza ICT esemplificativo è disponibile come documento aperto in formato Microsoft® Word all'indirizzo* [*www.swisscom.com/campus.*](http://www.swisscom.com/campus) *Può essere citato, utilizzato e modificato senza riserve, a condizione che se ne riconosca la paternità.*

# Introduzione e obiettivi

Questo documento serve a descrivere l'inventario dei vari elementi della rete ICT della scuola. Fare clic o digitare direttamente nel documento per aggiungere testo. Inoltre, chiarisce importanti questioni riguardanti i database ad alto rischio, la loro protezione e le misure da adottare in caso di incidente.

Questo documento serve come modello per le scuole e deve essere adattato alla situazione e alle esigenze specifiche di una scuola o di un gruppo scolastico.

## Scopo del progetto di sicurezza

Questo progetto aiuta i responsabili di una scuola ad accedere a informazioni aggiornate sull'infrastruttura di rete ICT in caso di incidente, a classificare e isolare rapidamente il problema e ad avviare le misure immediate necessarie. Non serve a descrivere o a concettualizzare le misure di sicurezza da adottare in anticipo: un progetto di sicurezza viene sviluppato per questi aspetti al momento della creazione dell'architettura di rete ICT.

## Campo di applicazione

Questo progetto di crisi ICT è valido fin dalla sua entrata in vigore e viene applicato in caso di crisi (incidente). Serve come base per il team di intervento della scuola per localizzare l'incidente, identificare le parti della rete interessate, indirizzare i punti di riferimento coinvolti e infine determinare le misure immediate necessarie.

## Definizione di termini importanti

Inserite qui i componenti ICT rilevanti e tutte le unità organizzative della scuola che potrebbero essere importanti in caso di incidente:

|  |  |  |
| --- | --- | --- |
| Termine | Spiegazione | Osservazioni |
| ICT-SPOC | (=Single Point of Contact) Contatto da parte del Comune per le questioni relative all'ICT. | Paolo Esempio+41 58 123 12 12 |
| Sala server "edificio vecchio" | Sala server nell'edificio scolastico "Meieli", piano -1, stanza 123 | Accesso tramite passepartout |
|  |  |  |

Capitolo 1 - Inventario

# Infrastruttura

## Infrastruttura di rete

Aggiungere una descrizione dell'infrastruttura di rete come descritto nel progetto di sicurezza o nel progetto di architettura ICT. Anche in questo caso è utile un piano della rete.

## Componenti della rete

Aggiungere qui i componenti centrali della rete che potrebbero essere interessati in caso di incidente. In particolare, in questo caso sono rilevanti elementi quali: router, transizioni di rete, funzionalità di rete e server.

## Terminali

Descrivere il tipo di terminali e il modo in cui sono collegati o possono essere integrati nella struttura di rete. Descrivete in particolare se e come il BYOD (=Bring Your Own Device) può essere integrato nella rete.

# Gestione dei contratti

Elencare tutti i contratti, compresi i fornitori, che gestiscono o sono responsabili di parti o componenti della rete scolastica tramite i loro servizi. Aggiungete anche i contatti di supporto dei fornitori.

# Protezione dell'infrastruttura di rete

## Controllo degli accessi alla rete

Descrivete gli strumenti utilizzati per consentire l'accesso alla rete, sia virtualmente che fisicamente. In questo modo è possibile identificare rapidamente i possibili punti di ingresso.

## Segmentazione e gestione delle sottoreti

Se l'architettura ICT prevede una segmentazione in sottoreti le cui transizioni includono misure di sicurezza speciali, è possibile descriverle qui.

## Protezione dagli attacchi esterni (firewall, IPS/IDS ecc.)

Specificare qui quali componenti di sicurezza interni alla rete o esterni alla rete sono in uso. Si prega di annotare qui anche eventuali informazioni di accesso o di contatto.

# Protezione dei componenti della rete

## Linee guida di sicurezza per il server

Descrivete qui quali linee guida di sicurezza sono in vigore per infrastrutture server specifiche.

## Gestione dei dispositivi di rete

Descrivete qui come vengono gestiti alcuni dispositivi di rete come i router o gli hotspot WLAN. Specificate anche chi gestisce i componenti corrispondenti.

## Patch Management

Se utilizzate una gestione automatica, semi-automatica o manuale delle Patch, potete descrivere qui il processo e le diverse responsabilità.

## Sicurezza fisica

Definite qui l'accesso e l'autorizzazione di accesso ai componenti centrali della rete, come router, hotspot WLAN, server ecc.

# Protezione dei terminali\*\*

## Linee guida per i terminali

Descrivete quali linee guida si applicano all'accesso dei terminali nella vostra scuola.

## Cifratura e software di sicurezza

Se esiste una cifratura speciale per il traffico all'interno della scuola verso servizi specifici al di fuori della scuola, è possibile aggiungerla qui.

Se sui dispositivi scolastici è installato un software di sicurezza specifico (firewall, filtro dei contenuti), descrivere qui la versione, il livello di funzionalità e l'implementazione.

## Gestione dei dispositivi mobili (GDM)

Descrivete il prodotto, la distribuzione ed eventuali specifiche di sicurezza di un sistema di gestione dei dispositivi mobili utilizzato nella vostra scuola.

## Linee guida BYOD

Indicate se si fa uso del BYOD e se sì: come i terminali non scolastici (laptop, smartphone ecc.) possono accedere alla rete della scuola.

## Requisiti di sicurezza per i dispositivi di proprietà della scuola

Se ci sono direttive specifiche riguardanti i requisiti di sicurezza per l'uso di terminali di proprietà della scuola (ad esempio, lettore di impronte digitali, fotocamera integrata ecc.) indicatele qui.

## Separazione dei dati privati dai dati scolastici

Se si utilizza un modello che consente a studenti e insegnanti di impostare profili di utilizzo privati e scolastici sul proprio dispositivo, descrivete come utilizzare questa opzione.

# Gestione dei dati e backup

##  Progetto di backup

Descrivete quali dati vengono sottoposti a backup e come. I dati sulla frequenza, l'ubicazione e l'accesso a questi backup sono particolarmente importanti.

##  Conservazione e archiviazione dei dati

Se dovessero esserci ulteriori backup (fisici, non basati sulla rete, non automatizzati) dei dati: descrivete qui il processo e la procedura di backup, comprese le persone di contatto e la disponibilità.

##  Ripristino in caso di emergenza

Chiarite con le parti responsabili le modalità di accesso a un set di backup in caso di incidente, le modalità di ripristino e di convalida dell'integrità dei dati ripristinati.

Capitolo 2 - Organizzazione e crisi

# Analisi e valutazione del rischio

## Forme dei rischi per la sicurezza

Formulate qui i possibili rischi per la sicurezza. Di seguito troverete una selezione di rischi:

|  |  |  |
| --- | --- | --- |
| Rischio | Descrizione | Riconoscimento (rilevante/non rilevante; alto-medio-basso) |
| Violazioni della protezione dei dati  | Accesso non autorizzato ai dati personali di studenti/studentesse, insegnanti e personale amministrativo. |  |
| Attacchi informatici  | Questi includono phishing, malware, attacchi ransomware e altre forme di attacchi informatici volti a infiltrarsi nella rete scolastica. |  |
| Perdita di dati  | Perdita di dati importanti a causa di guasti tecnici, errori umani o attacchi informatici. |  |
| Backup dei dati insufficiente  | Procedure di back-up mancanti o inadeguate che non consentono il recupero in caso di perdita di dati. |  |
| Abuso delle risorse ICT  | Uso delle risorse ICT scolastiche per attività inopportune o illegali da parte di studenti/studentesse o personale. |  |
| Rischi del software  | L'utilizzo di software obsoleto o privo di licenza può comportare lacune di sicurezza e problemi giuridici. |  |
| Guasti dell'hardware  | Guasti di sistemi o dispositivi critici che possono causare l'interruzione delle attività didattiche o di amministrazione. |  |
| Sicurezza di rete insufficiente  | Protezione inadeguata della rete dall'accesso non autorizzato o dagli abusi. |  |
| Mancanza di formazione degli e delle utenti  | Insegnanti, alunni/e e personale amministrativo non sono sufficientemente formati all'uso sicuro e responsabile delle risorse ICT. |  |
| Rischi per la sicurezza fisica  | Protezione inadeguata dei dispositivi ICT da furti, atti vandalici o disastri naturali. |  |
| Contenuti online non adeguati  | Accesso a materiale potenzialmente dannoso o inadeguato su Internet. |  |
| Rischi di compliance  | Violazione dei requisiti legali o normativi in materia di protezione e sicurezza dei dati. |  |
| Dipendenza da fornitori di servizi terzi  | Interruzioni dei servizi ottenuti dall'esterno (ad esempio, operatori Internet, servizi cloud). |  |
| Problemi di interoperabilità  | Difficoltà di integrazione delle nuove tecnologie in una struttura ICT esistente o mancanza di compatibilità tra diversi sistemi e applicazioni. |  |
| Social Engineering  | Tattiche utilizzate per invogliare collaboratori/collaboratrici o studenti/studentesse a rivelare informazioni riservate. |  |
| Minacce insider  | Rischi derivanti da persone all'interno dell'organizzazione, sia per dolo che per negligenza. |  |

## Analisi dei punti deboli

Eseguire un'analisi che descriva più dettagliatamente i rischi rilevanti/elevati sopra elencati. Dovreste affrontare aspetti quali la gravità, la probabilità di accadimento, il numero di persone colpite o i rischi finanziari.

# Sensibilizzazione e formazione

## Definizione delle responsabilità

Definite la persona responsabile della sensibilizzazione di tutti i gruppi target della vostra scuola. Questo ruolo ha la responsabilità di garantire che i gruppi siano informati sui rischi potenziali a intervalli regolari. Definite il tipo e la frequenza di queste misure di sensibilizzazione e stabilite un budget adeguato, se necessario.

# Audit e valutazioni della sicurezza

Stabilite con quale frequenza, con quale modalità e da chi deve essere effettuato un audit della sicurezza per la vostra scuola. La scuola ha la possibilità di effettuare tale audit autonomamente, di incaricare il suo fornitore di ICT a farlo o di incaricare una terza parte specializzata.

# Misure durante e dopo un incidente

## Team di intervento

Stabilite un gruppo gestibile di persone e funzioni che, analogamente a un team di pronto intervento in caso di crisi, coordini i primi passi in caso di incidente (vedi sotto, [12.2 Definizione delle misure immediate](#_Sofortmassnahmen_definieren)). A questo punto, descrivete anche la frequenza e la modalità di esercitazione di questo team.

Le responsabilità più importanti devono essere chiarite prima dell'attivazione della squadra di intervento. Questo vale in particolare per il ruolo del responsabile del team di intervento, il ruolo della comunicazione o il coinvolgimento del Comune. Definire anche chi si occupa delle sostituzioni in caso di assenza.

## Assistenza interna

Identificare altri esperti interni (nell'ambito di un'esercitazione) che possano essere chiamati a far parte del team di intervento in caso di incidente.

## Assistenza esterna

Vi sono diversi fornitori di servizi che offrono il cosiddetto CSIRT-as-a-Service. Le informazioni elencate in questo documento e altre informazioni vengono scambiate in anticipo con il fornitore. In questo contesto, un audit viene spesso effettuato per aiutarvi a identificare ed eliminare le aree di rischio.
Descrivete in quali casi e con quali modalità si deve e si può accedere alle risorse del CSIRT. Chiarire anche chi avrà la funzione di SPOC in caso di intervento.

Vi sono diversi fornitori di servizi che formulano un'offerta di risposta rapida. In caso di incidente, questi fornitori vi metteranno a disposizione un team di esperti che vi fornirà supporto per superare la crisi. Chiarire quali compiti e responsabilità saranno assegnati a chi, in caso di intervento del Rapid Response Team.

## Requisiti d'informazione

Prestate grande attenzione al compito di informare le parti interessate con la necessaria urgenza e precisione. Descrivete i possibili gruppi di interesse e le loro esigenze d'informazione.

## Risorse informative

Identificate tutte le informazioni rilevanti di cui si ha bisogno in caso di incidente o che possono aiutare a gestire tale attività. Strutturate le fonti di informazione in modo gerarchico (Comune, Cantone, Governo Federale) e tematico (processi, tecnologia, comunicazione ecc.).

# Analisi della situazione e misure immediate

## Identificazione dei dati interessati

Non appena si hanno indicazioni o sospetti che si sia verificato un incidente, cercate di circoscrivere il più rapidamente possibile i dati interessati dall'incidente. Le informazioni che trovate nel Capitolo 14.2 Segmentierung und Verwaltung von Subnetzenvi aiutano a isolare le singole sottoreti interessate.

## Definire le misure immediate

1. **Eseguire il backup dei dati non interessati.** Se sono interessate solo alcune parti dei dati, mettete in sicurezza l'accesso ai dati rimanenti in relazione al rischio che si è verificato. Ad esempio, scollegate altri server dalla rete, bloccate gli accessi dai terminali interessati o modificate le password ecc.
2. **Create un rapporto** sull'incidente insieme al team d'intervento. Dovete aggiornare regolarmente questo rapporto durante la crisi e diffonderlo attraverso i canali di informazione appropriati, se necessario. In questo modo vi assicurerete che tutte le parti coinvolte abbiano sempre le informazioni più aggiornate.
3. **Create un progetto di informazione.** Determinate chi ha bisogno di quali informazioni e in quale momento. Non sottovalutate questo compito e mettete a disposizione risorse umane sufficienti per esso. Assicuratevi inoltre di utilizzare un canale di informazione che non sia interessato dall'incidente e che goda comunque della fiducia dei destinatari (ad esempio, non utilizzate un indirizzo e-mail privato, ma uno ufficiale).
4. **Assistenza da fonti interne ed esterne.** A seconda dell'organizzazione delle reti ICT, alcune informazioni si trovano in luoghi diversi. Informate immediatamente le autorità con un rapporto. Le risorse4 Schutz der Netz-Infrastrukturelencate vi aiuteranno a prendere le decisioni giuste in caso di crisi.
5. **Linee guida e istruzioni comportamentali.** Stabilite le regole di comportamento per il team d'intervento, le autorità scolastiche, il personale docente, gli alunni/le alunne e, se necessario, i genitori/tutori (se necessario). Tali regole dovrebbero servire a delimitare i danni e, se necessario, a identificare prove e indicazioni.

Capitolo 3 - Documentazione e reporting

## Documentazione del progetto di sicurezza ICT

Descrivete i vari processi di documentazione, in particolare:

1. redazione e aggiornamento del documento
2. Frequenza di controllo delle informazioni elencate (informazioni di contatto, contratti, descrizioni dei prodotti ecc.)
3. Documentazione in caso di incidente

## Meccanismi di reporting

Descrivete qui come e sotto quale forma i dati sul traffico, i siti web visitati, i log di accesso ecc. devono essere raccolti, analizzati, conservati, archiviati e utilizzati.

Capitolo 4 - Appendici

# Elenchi dei contatti

# Documentazione dei prodotti

# Reporting

# Membri del team d'intervento in caso di crisi