Istruzioni sulla sicurezza

SA Base per piani di sicurezza

Swisscom SA

Group Security
Casella postale
3050 Berna

Versione	Data	Persona	Modifiche apportate/Osservazioni
0.1	29.03.2023	Claudio Passafaro	Redazione
0.2	04.04.2023	Daniel Zysset	Revisione
1.0	24.04.2023	Claudio Passafaro	Approvazione

Responsabile: ReSi protezione incendi dell'immobile

Autore: Passafaro Claudio, GSE-PHY

Edito da: ReSi protezione incendi dell'immobile

Data creazione: 29.03.2023

Destinatari: come da 1.2 Campo di applicazione

Contenuto

1 Introduzione

1.1 Situazione di partenza

[1] La gran parte degli edifici per uffici e delle sedi operative di Swisscom si possono costruire e gestire secondo approcci standardizzati.

[2] Quando una superficie o un edificio richiede una protezione speciale, questa necessità di protezione deve essere valutata sulla base di un risk management, in funzione degli obiettivi di protezione e con il coinvolgimento degli utenti. A partire dai risultati di quest'analisi dei rischi, si elabora un piano di protezione specifico per l'oggetto.

[3] I piani di protezione specifici devono essere verificati e autorizzati da Group Security.

[4] Il presente documento contiene il catalogo rischi per la sicurezza fisica e va usato come riferimento per l'analisi e la valutazione dei rischi e la classificazione delle misure, nonché per tutte le considerazioni relative ai rischi all'interno e nei pressi degli edifici e spazi della Swisscom SA. Esso serve per rendere omogenee le valutazioni dei rischi.

1.2 Campo di applicazione

[5] Il presente documento è valido per l'intera Swisscom (Svizzera) SA, incluse tutte le divisioni operative[1] e del Gruppo aventi sede in Svizzera e all'estero[2] (di seguito «Swisscom»).

[6] Le società del Gruppo allestiscono un proprio sistema di Security Management o aderiscono al sistema di Security Management di Swisscom. La responsabilità della security rimane in capo alla società del Gruppo. La decisione è di competenza della società del Gruppo e viene sostenuta da Group Security.

1.3 Documenti di riferimento

[1] Direttiva sicurezza

[2] Security-Policy

[1] Tra le divisioni operative si annoverano Retail Customers («B2C»), Business Customers («B2B»), IT e Network & Infrastructure («INI»).

[2] Tra le divisioni del Gruppo si annoverano Group Business Steering («GBS»), Group Human Resources («GHR»), Group Communications & Responsibility («GCR») e Group Security & Corporate Affairs («GSA»).

2 Esigenze e capacità di protezione di edifici e superfici

2.1 Esigenze di protezione

[7] La classe di protezione di un contenitore, edificio o superficie dipende dalla classe di danno più elevata tra quelle degli oggetti che contiene o si prevede che un giorno possa contenere.

OGGETTO DA PROTEGGERE	Classificazione	Classi			
Informazioni	Confidenzialità	C1 - Public	C2 - General	C3 - Confidential	C4 - Strictly Confidential
	Integrità	I1 - None	I2 - Basic	I3 - Medium	I4 - High
Oggetti materiali	Valore in denaro	M1 - None	M2 - Basic	M3 - Medium	M4 - High

CONTENITORE DI PROTEZIONE	Qualifica	Classi			
Spazio o superficie	*Livello di protezione*	*None*	*Basic*	*Medium*	*High*
	Confidenzialità	pcC1	pcC2	pcC3	pcC4
	Integrità	pcI1	pcI2	pcI3	pcI4
	Valore in denaro	pcM1	pcM2	pcM3	pcM4

2.2 Fattori di valutazione

Per impianti ICT, locali di vendita, locali adibiti a ufficio e archivio e sale conferenze, il riferimento determinante è normalmente la confidenzialità C1-C4.

2.3 Valutazione degli obiettivi di protezione in funzione dei rischi

[8] Un piano di sicurezza comprende una serie di misure di sicurezza coordinate tra loro, che nel loro insieme forniscono l'efficacia protettiva desiderata. Può comprendere misure edilizie, tecniche, organizzative e assicurative.

[9] Le misure devono essere adottate in base a una valutazione del rischio. Questa procedura identifica i pericoli per gli oggetti da proteggere e li valuta individualmente. La valutazione costituisce il punto di partenza per le misure che ne derivano e vengono integrate nel piano di sicurezza.

L'obiettivo dell'analisi è di ottenere una visione d'insieme il più possibile completa dei pericoli, in modo da poterli affrontare con misure adeguate.

2.3.1 Procedura

[10] L'analisi dei rischi comprende i passi riportati nella seguente tabella.

[11] In linea di principio si tratta di applicare le regole contenute nel regolamento operativo sul risk management (link: Regolamento operativo sul risk management _01052022.pdf (swisscom.com). Questo riguarda in particolare le regole applicabili alla tolleranza al rischio.

L'esecuzione dell'analisi dei rischi può usare come riferimento i consigli della direttiva «Risk Impact Assessment» (Link: Direttiva Risk Impact Assessment_IT.pdf (swisscom.com)).

Attività	Contenuto	Risultato
Rilevamento degli obiettivi da proteggere	Prima di tutto bisogna capire quali oggetti si vogliono proteggere con le misure. I principali obiettivi delle misure di protezione e sicurezza presso Swisscom sono definiti nella Security Policy (capitolo 3). Possono inoltre esistere requisiti di legge e richieste dei clienti, che dovranno essere considerati caso per caso.	Gli obiettivi di protezione sono noti.
Identificazione dei rischi	Vengono identificati i pericoli per gli oggetti da proteggere. **Per una panoramica dei potenziali pericoli, consultare il catalogo dei rischi al punto** 3.1. I pericoli che comportano conseguenze prevedibilmente negative sugli oggetti da proteggere vengono classificati come rischi.	I rischi per gli oggetti da proteggere sono noti.
Valutazione dei rischi	I rischi rilevati vengono valutati singolarmente in funzione della probabilità che si concretizzino e dall'entità degli eventuali danni.	I rischi sono valutati.
Identificazione di misure per la gestione dei rischi	Nell'ultima fase vengono adottate misure adeguate per la gestione dei diversi livelli di rischio. Normalmente si tratta di misure per la riduzione del rischio. È però anche possibile che un rischio sia considerato come accettabile. In questo caso, di tratta di seguire il processo di risk management della corrispondente unità organizzativa.	Le misure per la gestione dei rischi sono definite.
Documentazione dei risultati	Nell'ultima fase i risultati vengono registrati nel piano di sicurezza.	Piano di sicurezza

3 Valutazione dei rischi

[12] Al punto 0 è riportato il catalogo dei rischi. Descrive i rischi che possono avere un impatto sugli oggetti da proteggere presso Swisscom, la relativa rilevanza e il contenimento per l'ambito di osservazione Sicurezza fisica.

[13] Il catalogo si può utilizzare per l'analisi dei rischi nell'ambito della sicurezza fisica, la valutazione dei rischi identificati e la definizione delle misure.

[14] Al punto 0 sono riportati gli obiettivi specifici da proteggere

- per rischi attivi, ovvero azioni dirette in modo intenzionale e mirato contro oggetti o persone
- per rischi passivi, ovvero rischi causati da malfunzionamenti ed errori umani o tecnici oppure da eventi naturali.

[15] Nota: gli obiettivi di protezione sono riportati in modo che le misure che possono essere adottate nell'ambito della sicurezza fisica contribuiscano al raggiungimento di tali obiettivi. In parte sono possibili sovrapposizioni con l'ambito della sicurezza delle informazioni, ma la copertura dei relativi obiettivi non è in nessun caso completa.

3.1 Catalogo dei rischi

Identificatore= <numero> Rphy (Rphy="Risk Physical")

					Rischio per gli oggetti da proteggere												
			Rilevante per la sicurezza fisica		Protezione delle persone			Protezione dei beni immateriali			Protezione dei beni materiali			Protezione della performance aziendale		
No	**Rischio**	**Descrizione del rischio**	**J**	**N**	Clienti	Collaboratori	Partner	Informazioni	Know-how	Proprietà intellettuale	Edifici	Impianti tecnologici	Beni mobili / denaro	Reputazione	Prodotti	Ambiente
	Dipendenza da collaboratori e terzi	Creazione consapevole o inconsapevole di know-how da parte di singoli o terzi che in caso di guasto/uscita dall'azienda (incidente, malattia e simili) riducono o impediscono la continuità operativa di impianti e sistemi e/o l'esecuzione di processi chiave		X					•							
	Minacce di violenza fisica	Diffusione di messaggi autentici o fasulli (per telefono o per iscritto) con l'obiettivo di mettere in atto richieste ricattatorie e/o causare guasti o paralisi temporanee dell'azienda	X		•	•	•									
		Minacce contro l'integrità fisica di singoli e/o del loro contesto personale immediato	X		•	•	•							•		
		Rendere incapace di reagire una persona o gruppo di persone facendo leva sulla violenza, una grave minaccia o in altro modo, con l'obiettivo di ottenere un vantaggio patrimoniale illecito	X		•	•	•									
	Attacco contro persone	Attacco violento (fisico o con armi) contro una o più persone	X		•	•	•									
	Attentato/Atto terroristico	Attacco pianificato contro un singolo, un gruppo di persone o un'infrastruttura/un edificio con un'arma o esplosivi, con l'obiettivo di uccidere	X		•	•	•	•	•		•	•	•	•		
	Caduta di oggetti volanti su strutture aziendali	Schianto di un velivolo o di parti di un velivolo su strutture aziendali	X		•	•	•	•	•		•	•	•	•		
	Indisponibilità degli impianti di sicurezza	Indisponibilità temporanea o permanente degli impianti di sicurezza (ad es. impianti antincendio e antintrusione, sistemi di controllo degli accessi)	X								•	•	•			
	Guasto di impianti tecnologici	Guasto temporaneo o permanente di impianti tecnologici rilevanti per l'azienda (gruppi di continuità, distributore principale a bassa	X					•			•	•			•	

Identificatore= <numero> Rphy (Rphy="Risk Physical")

					Rischio per gli oggetti da proteggere												
			Rilevante per la sicurezza fisica		Protezione delle persone			Protezione dei beni immateriali			Protezione dei beni materiali			Protezione della performance aziendale		
No	**Rischio**	**Descrizione del rischio**	**J**	**N**	Clienti	Collaboratori	Partner	Informazioni	Know-how	Proprietà intellettuale	Edifici	Impianti tecnologici	Beni mobili / denaro	Reputazione	Prodotti	Ambiente
	rilevanti per l'azienda	tensione, sistema di controllo, impianti di climatizzazione e raffreddamento ecc.)														
	Guasto a impianti di telecomunicazione	Guasto temporaneo o permanente agli impianti di telecomunicazione		X				•				•			•	
	Guasto a sistemi e reti IT	Guasto temporaneo o permanente ai sistemi IT rilevanti per l'azienda		X				•			•	•			•	
		Guasto temporaneo o permanente ai sistemi di rete (WAN/LAN)		X				•			•	•			•	
	Guasto ai sistemi di alimentazione con risorse	Guasto temporaneo o permanente ai sistemi di alimentazione con corrente elettrica (48 V o 220 V), acqua, calore a distanza e gas così come alle reti di telecomunicazione	X					•			•	•			•	
	Frode/Falsificazione/Appropriazione indebita	Atti o manipolazioni finalizzati a ottenere per sé o per terzi un vantaggio finanziario o materiale		X										•		
	Corruzione	Offrire, promettere, dare o far pervenire a una persona un regalo (materiale/immateriale) o altro vantaggio, in modo che violi i propri obblighi di servizio e funzione		X										•		
	Minaccia di attentato dinamitardo	Diffusione di messaggi autentici o falsi (per telefono o per iscritto) con l'obiettivo di mettere in atto richieste ricattatorie e/o causare guasti o paralisi temporanea dell'azienda.	X		•	•	•				•	•	•	•		
		Minacce contro l'integrità fisica delle persone.	X		•	•	•							•		
	Incendio	Innesco involontario di incendi a seguito di errori umani o tecnici e/o eventi naturali	X		•	•	•	•			•	•	•			
	Incendio doloso	Incendio appiccato con dolo (costituisce una forma speciale di sabotaggio)	X		•	•	•	•			•	•	•			

Identificatore= <numero> Rphy (Rphy="Risk Physical")

					Rischio per gli oggetti da proteggere												
			Rilevante per la sicurezza fisica		Protezione delle persone			Protezione dei beni immateriali			Protezione dei beni materiali			Protezione della performance aziendale		
No	**Rischio**	**Descrizione del rischio**	**J**	**N**	Clienti	Collaboratori	Partner	Informazioni	Know-how	Proprietà intellettuale	Edifici	Impianti tecnologici	Beni mobili / denaro	Reputazione	Prodotti	Ambiente
	Manifestazioni	Manifestazioni collettive pubbliche che riuniscono molte persone su suolo pubblico o privato	X								•	•	•	•		
	Occupazione	Occupazione pacifica o violenta (non autorizzata) di un edificio o parte di esso da parte di persone estranee al servizio (violazione di domicilio) o da parte di collaboratori	X		•	•	•				•	•		•		
	Furto	Sottrazione di valori materiali o immateriali senza effrazione in un edificio	X					•	•	•	•	•	•			
	Calamità naturali	Eventi naturali (ad es. temporali, inondazioni, caduta di fulmini, terremoti) che hanno conseguenze distruttive	X		•	•	•	•			•	•	•	•	•	•
	Scasso	Effrazione in un edificio o spazio chiuso o apertura di un contenitore chiuso con l'obiettivo di sottrarre illegalmente valori materiali o immateriali oppure al fine di perpetrare atti criminali	X					•	•	•	•	•	•	•		
	Epidemia/ Avvelenamento	Avvelenamento di singole persone o gruppi di persone tramite l'immissione di sostanze dannose per la salute o altamente tossiche, dall'esterno o dall'interno, tramite aria/gas, la rete idrica oppure il contatto fisico con gli oggetti/materiali contaminati o persone infette.	X		•	•	•	•	•		•			•		
	Ricatto	Rendere incapace di reagire una persona o gruppo di persone facendo leva sulla violenza, una grave minaccia o in altro modo, con l'obiettivo di ottenere un vantaggio patrimoniale illecito.		X	•	•	•	•		•			•	•		
	Coercizione	Usare la violenza o la minaccia di significativi pregiudizi o altre limitazioni della capacità di agire per costringere una persona o un gruppo di persone a fare, omettere o tollerare un determinato atto.		X	•	•	•	•		•			•	•		

Identificatore= <numero> Rphy (Rphy="Risk Physical")

					Rischio per gli oggetti da proteggere												
					Protezione delle persone			Protezione dei beni immateriali			Protezione dei beni materiali			Protezione della performance aziendale		
No	Rischio	Descrizione del rischio	J	N	Clienti	Collaboratori	Partner	Informazioni	Know-how	Proprietà intellettuale	Edifici	Impianti tecnologici	Beni mobili / denaro	Reputazione	Prodotti	Ambiente
	Rapimento	Sequestro di persona con l'impiego di violenza fisica e psichica, al fine di imporre le proprie richieste. Autori e luogo dove sono trattenute le persone rapite sono sconosciuti.		X	•	•	•							•		
	Esplosione	Reazione chimica fulminea, seguita da onda d'urto con grande forza distruttiva e spesso anche da successivo incendio	X		•	•	•	•	•		•	•	•	•	•	•
	Presa di ostaggi	Sequestro di persone per imporre richieste tramite la minaccia o l'impiego diretto della violenza		X	•	•	•				•		•	•		
	Furto d'identità	Furto e utilizzo dell'identità di un collaboratore o dell'azienda Swisscom	X					•	•	•			•	•		
	Fuga di informazioni	Diffusione non intenzionale o colposa di informazioni sensibili		X				•	•	•				•		
	Furto di informazioni	Sottrazione illegale di informazioni fisiche e/o elettroniche e/o dei relativi supporti dati		X				•	•	•				•		
	Manipolazione di informazioni	Falsificazione (aggiunta, modifica o cancellazione) di informazioni su supporto elettronico o non elettronico (carta, film, supporto audio)		X				•	•	•				•		
	Perdita di informazioni	Distruzione o perdita di informazioni (dati/atti/supporti dati) classificate o essenziali per l'azienda (elettroniche/fisiche)		X				•	•	•				•		
	Contaminazione di cibi e generi di conforto	Avvelenamento doloso o colposo di cibi e generi di conforto con sostanze chimiche o altre sostanze pericolose per la salute		X	•	•	•									•
	Contaminazione radioattiva	Contaminazione radioattiva dell'ambiente (persone, animali, suolo, acqua, aria, fauna ecc.)		X	•	•	•				•	•				•
	Rapina	Applicazione diretta della violenza per imporre richieste di valori materiali o immateriali. Normalmente, le rapine sono violente e impreviste.	X		•	•	•	•		•	•	•	•	•		

Identificatore= <numero> Rphy (Rphy="Risk Physical")

					Rischio per gli oggetti da proteggere												
			Rilevante per la sicurezza fisica		Protezione delle persone			Protezione dei beni immateriali			Protezione dei beni materiali			Protezione della performance aziendale		
No	**Rischio**	**Descrizione del rischio**	**J**	**N**	Clienti	Collaboratori	Partner	Informazioni	Know-how	Proprietà intellettuale	Edifici	Impianti tecnologici	Beni mobili / denaro	Reputazione	Prodotti	Ambiente
	Sabotaggio	Limitazione dolosa, pianificata e intenzionale dei processi aziendali tramite danneggiamento/disattivazione di parti di edifici o impianti rilevanti per l'azienda	X			•		•	•	•	•	•	•		•	
	Spionaggio/Intercettazione di sistemi di comunicazione	Acquisizione illegale di informazioni (ascolto, copia, fotografia ecc.) soprattutto per periodi prolungati di tempo e senza lasciare tracce	X					•	•	•				•	•	
	Sciopero	Rifiuto collettivo da parte dei collaboratori di svolgere determinate attività o processi come misura di lotta per imporre le proprie richieste		X		•								•	•	
	Sovratensione	Breve aumento della tensione nella rete che può provocare danni ai dispositivi elettrici e/o elettronici o distruggerli (ad es. fulmine, sbalzo di tensione nella rete elettrica)	X			•		•			•	•			•	
	Fuga accidentale di sostanze tossiche o infiammabili (perdita chimica)	Contaminazione dell'ambiente con sostanze tossiche,aggressive/corrosive o infiammabili/esplosive allo stato liquido, solido o gassoso (ad es. locali batterie, sale con gruppi di continuità, impianti diesel, stazioni di rifornimento di benzina e diesel, depositi dei detergenti in grandi edifici ecc.)	X		•	•	•				•	•				•
	Vandalismo/Danneggiamenti	Danneggiamento volontario, ma non necessariamente mirato, di parti di edifici o impianti tecnologici	X								•	•		•		
	Danni dovuti all'acqua	Danneggiamento o distruzione involontaria di valori materiali e immateriali conseguente alla fuoriuscita d'acqua (ad es. rottura di condutture) o alla penetrazione d'acqua (acqua di falda, acqua per lo spegnimento di incendi ecc.)	X								•	•	•	•		•

3.2 Obiettivi di protezione specifici a seconda della tipizzazione del rischio

N.	Rischio	Obiettivi di protezione raggiungibili con misure di sicurezza fisica *Obiettivi di protezione raggiungibili con altre misure (non fisiche)*	Incide su
Rischi attivi - Rischi causati da azioni dirette in modo intenzionale e mirato contro oggetti o persone			
	Minacce di violenza fisica	**Carattere minimo** - Il pericolo fisico per le persone e le conseguenze sul funzionamento di Swisscom di una minaccia di attentato dinamitardo sono minimi.	Rphy02 Rphy03 Rphy04
		Realismo - Una valutazione realistica della situazione e un intervento adeguato sono garantiti in ogni momento. Tutte le misure per la perquisizione dell'immobile sono predisposte in modo ottimale.	Rphy02 Rphy03 Rphy04
		Contenimento del panico - Le situazioni di panico devono essere ridotte al minimo. Un'eventuale evacuazione può avvenire in modo rapido e sicuro.	Rphy02 Rphy03 Rphy04
	Attacco contro persone	**Contrasto** - Gli attacchi contro persone da parte di terzi/visitatori sono resi più difficili all'interno degli edifici.	Rphy05
		Tempo di intervento - In caso di evento, le forze di intervento arrivano sul posto in brevissimo tempo.	Rphy05
	Frode/Falsificazione/ Appropriazione indebita	**Riconoscibilità** - I tentativi di frode/falsificazione e appropriazione indebita vengono identificati il più rapidamente possibile	Rphy14
		Analisi - In caso di sospetta frode/falsificazione o appropriazione indebita, si procede immediatamente a un'analisi della situazione per ridurre al minimo i rischi e identificare i colpevoli.	Rphy14
	Incendio doloso	**Prevenzione** - Sono adottati accorgimenti per prevenire gli incendi dolosi	Rphy19
		Contrasto - Sono adottati accorgimenti per rendere particolarmente complicati l'introduzione e il lancio di oggetti incendiari all'interno degli edifici	Rphy19
	Dimostrazioni/Occupazioni	**Orientamento** - Il responsabile sicurezza viene informato tempestivamente di dimostrazioni pianificate o in corso che potrebbero mettere in pericolo i processi aziendali e reagisce adottando contromisure	Rphy20 Rphy21
		Contrasto - Se non è possibile evitare un'occupazione, bisogna per lo meno fare in modo che sia particolarmente difficile da realizzare e abbia conseguenze limitate	Rphy20 Rphy21
	Furto	**Riduzione dell'attrattività** - Fin dall'inizio deve risultare poco attrattivo effettuare dei furti	Rphy22
		Contrasto - Viene fatto il possibile per impedire intrusioni e furti	Rphy22
		Clima di lavoro - Un buon clima di lavoro e una buona politica del personale possono ridurre significativamente il rischio di furti da parte del personale interno	Rphy22
		Prevenzione - Il personale è sensibilizzato sulla prevenzione dei furti	Rphy22
	Scasso	**Assenza di prospettive di riuscita** - Deve essere chiaro che i tentativi di scasso non avranno successo	Rphy24

N.	Rischio	Obiettivi di protezione raggiungibili con misure di sicurezza fisica ***Obiettivi di protezione raggiungibili con altre misure (non fisiche)***	Incide su
		Contrasto - Vengono adottate misure per rendere i furti con scasso difficili durante l'orario di lavoro e molto difficili fuori dall'orario di lavoro	Rphy24
		Rilevamento - I tentativi di scasso in ambienti con elevati requisiti di sicurezza (zona 4: zona di sicurezza) vengono rilevati immediatamente, segnalati e rallentati con misure strutturali in modo da permettere l'intervento tempestivo delle forze di polizia	Rphy24
		Proporzionalità - I tentativi di scasso devono essere impediti con misure adeguate al grado di protezione (misure strutturali) e rilevati con accorgimenti organizzativi e tecnici. Negli edifici con standard di sicurezza elevati serve un servizio di sorveglianza perimetrale (ad es. per eventuali rotture di vetri e cristalli)	Rphy24
	Furto d'identità	**Riduzione del rischio** - Il rischio di furto e utilizzo dell'identità di un collaboratore o dell'azienda Swisscom deve essere ridotto con misure preventive.	Rphy31
	Furto di informazioni	***Protezione tramite tracciabilità*** *- La protezione dell'azienda dal furto di informazioni aziendali o dei clienti in formato elettronico o fisico è garantita rendendo impossibile rubare dati e supporti dati senza lasciare tracce*	Rphy33
	Manipolazione di informazioni	***Misure preventive*** *- La probabilità che avvengano manipolazioni delle informazioni deve essere ridotta tramite adeguate misure preventive*	Rphy34
		Protocollazione *- L'accesso ai dati è regolato e per i database più importanti soggetto a protocollazione*	Rphy34
		Backup dei dati *- Il backup e l'esternalizzazione dei dati sono soggetti a regole specifiche per tutti i sistemi IT e avvengono con frequenza periodica*	Rphy34
		Verifica delle autorizzazioni di accesso *- Le autorizzazioni di accesso vengono verificate almeno una volta all'anno e autorizzate dai responsabili di linea*	Rphy34
	Rapina	**Riduzione dell'attrattività** - Le rapine durante e al di fuori dell'orario di lavoro vengono contrastate e devono risultare fin da subito poco attrattive	Rphy38
		Possibilità di ritirarsi - Sono adottati accorgimenti affinché in caso di rapina siano in pericolo quante meno persone possibile (possibilità di ritirarsi per gli autori della rapina).	Rphy38
		Notifica di allarme e intervento - La notifica di allarme alle forze di intervento è garantita in ogni momento.	Rphy38
		Riduzione dei danni finanziari - Il potenziale ricavato della rapina è sempre inferiore alla somma assicurata	Rphy38
		Condizioni per la cattura - Sono presenti condizioni che in caso di rapina garantiscono alle forze dell'ordine la possibilità di catturare i colpevoli	Rphy38
	Sabotaggio	**Riduzione dei punti deboli** - All'interno e all'esterno degli edifici, i punti suscettibili di sabotaggio da parte di terzi o collaboratori sono ridotti al minimo.	Rphy39
		Protezione adeguata - I sistemi e impianti di sicurezza rilevanti per la sicurezza degli edifici sono dotati di un'adeguata protezione contro i sabotaggi	Rphy39
		Protezione contro il lancio di oggetti e lo sversamento di liquidi - È reso difficoltoso il lancio di oggetti o lo sversamento di fluidi (ad es. liquidi infiammabili) attraverso i punti di contatto con l'esterno più esposti (ad es. aperture di ventilazione)	Rphy39

N.	Rischio	Obiettivi di protezione raggiungibili con misure di sicurezza fisica ***Obiettivi di protezione raggiungibili con altre misure (non fisiche)***	Incide su
		Politica del personale e clima di lavoro *- Il rischio di sabotaggi da parte dei collaboratori è ridotto al minimo attraverso l'adozione di una politica del personale particolarmente avanzata e la creazione di un clima di lavoro gradevole*	Rphy39
	Spionaggio / Intercettazione di sistemi di comunicazione	**Rilevabilità** - Si devono adottare misure adeguate per impedire che lo spionaggio e la sottrazione di informazioni per periodi prolungati passino inosservati. In particolare, occorre garantire che l'appropriazione indebita di informazioni venga rilevata in tempo utile e non si protragga per lunghi periodi.	Rphy40
		Collegamenti non autorizzati, intercettazioni e manipolazioni dei cavi - Vengono adottate misure strutturali e tecniche per ridurre al minimo la possibilità di manipolare i cavi e realizzare collegamenti non autorizzati. Le manipolazioni di cavi e condotte vengono scoperte.	Rphy40
		Spazi da proteggere - Gli spazi particolarmente sensibili (ad es. le sale in cui si riunisce la Direzione aziendale) devono essere protetti con misure più stringenti e adeguate (ad es. per impedire la visione e l'ascolto da parte di persone non autorizzate, schermi di proiezione dalle radiazioni ecc.). I requisiti di sicurezza devono essere rilevati previamente tramite un'analisi mirata dei rischi.	Rphy40
	Vandalismo / Danneggiamenti	**Riduzione dell'attrattività** - Gli atti vandalici all'interno e all'esterno degli edifici vengono contrastati e appaiono poco attrattivi	Rphy44
		Misure immediate - Gli atti vandalici vengono scoperti al più tardi il giorno successivo a quello in cui sono stati commessi. Le corrispondenti misure vengono adottate immediatamente.	Rphy44
Rischi passivi - Rischi causati da malfunzionamenti tecnici ed errori umani oppure da eventi naturali			
	Dipendenza da collaboratori e terzi	***Documentazione*** *- Per tutti gli impianti e sistemi tecnologici rilevanti per il funzionamento dell'azienda si deve tenere una documentazione scritta che copra l'intero periodo di esercizio fino alla sostituzione, in modo da consentire la manutenzione da parte di terzi*	Rphy01
		Dipendenze *- Eventuali casi in cui l'azienda dipenda da collaboratori e terzi sono identificati. In funzione del grado di dipendenza sono previste modalità di sostituzione e procedure alternative disponibili con tempistiche adeguate.*	Rphy01
		Know-how *- Il know-how dell'azienda è documentato indipendentemente dalla documentazione e dagli appunti di singoli collaboratori, salvato e conservato in doppia copia.*	Rphy01
	Caduta di oggetti volanti	**Rischio residuale** - Il pericolo per le persone e gli edifici derivante dall'eventuale caduta di un velivolo o simile viene accettato come rischio residuale	Rphy07
	Guasto di impianti tecnologici rilevanti per l'azienda	**Prevenzione** - Eventuali guasti a impianti tecnologici rilevanti per l'azienda sono monitorati adeguatamente e impediti per quanto più possibile	Rphy09
		Infrastruttura - Le infrastrutture tecnologiche come impianti di riscaldamento, climatizzazione e ventilazione devono essere progettate in modo da garantirne la continuità operativa. Ove necessario, devono essere previsti e installati o predisposti impianti ridondanti e possibilità di commutazione e/o bypass.	Rphy09
		Competenza - Le competenze e responsabilità per progettazione, esercizio, manutenzione e controllo degli impianti tecnologici sono chiaramente definite	Rphy09

N.	Rischio	Obiettivi di protezione raggiungibili con misure di sicurezza fisica ***Obiettivi di protezione raggiungibili con altre misure (non fisiche)***	Incide su
	Guasti tecnici (sistemi IT e di rete)	***Fuori dall'ambito di riferimento*** *- I guasti a sistemi IT non rientrano nell'ambito della sicurezza fisica, ma in quello del Business Continuity Management e/o del Disaster Recovery Planning.*	Rphy11
	Indisponibilità degli impianti di sicurezza	**Disponibilità** - La disponibilità degli impianti tecnologici di sicurezza viene mantenuta ad un livello elevato. Interruzioni e guasti agli impianti di sicurezza vengono comunicati immediatamente a una centrale tramite segnali ottici e acustici	Rphy08
		Protezione - Gli impianti di sicurezza devono essere protetti dai tentativi di sabotaggio e manipolazione.	Rphy08
		Competenze - Le competenze e responsabilità per progettazione, esercizio, manutenzione e controllo degli impianti di sicurezza sono chiaramente definite.	Rphy08
	Guasto agli impianti di telecomunicazione	***Fuori dall'ambito di riferimento*** *- I guasti agli impianti di telecomunicazione non rientrano nell'ambito della sicurezza fisica, ma in quello del Business Continuity Management e/o del Disaster Recovery Planning.*	Rphy10
	Indisponibilità dei sistemi di alimentazione con risorse	**Funzionamento degli elementi relativi alle vie di fuga** - Il funzionamento dell'illuminazione di emergenza e degli elementi tecnologici necessari per l'evacuazione è garantito anche in caso di blackout	Rphy13
		Durata dei guasti - Gli impianti, sistemi e installazioni necessari per l'esercizio senza interruzioni e guasti sono definiti. Il relativo tempo massimo di indisponibilità è definito	Rphy13
		Rilevamento e riparazione dei guasti - I guasti tecnici vengono rilevati in tempi brevi e riparati in funzione dell'urgenza	Rphy13
		Ridondanza - I sistemi di alimentazione e distribuzione (ad es. per energia elettrica, acqua, gas) che alimentano impianti importanti per il funzionamento dell'azienda dispongono delle necessarie ridondanze	Rphy13
	Incendio	**Messa in sicurezza tempestiva** - Indipendentemente da dove e quando scoppia un incendio, tutte le persone devono potere mettersi in salvo per tempo	Rphy18
		Riduzione delle probabilità - La probabilità che scoppi un incendio è ridotta al minimo	Rphy18
		Rilevamento tempestivo - Gli incendi vengono rilevati il prima possibile e segnalati automaticamente.	Rphy18
		Sezioni tagliafuoco - Esistono sezioni tagliafuoco, con dimensioni ridotte al minimo necessario per il funzionamento dell'azienda	Rphy18
		Contenimento delle emissioni - Fumo e gas di combustione restano confinati nella sezione tagliafuoco coinvolta	Rphy18
		Notifica di allarme - La tempestiva notifica ai pompieri è garantita in qualsiasi momento. Le vie di accesso e intervento sono segnalate e mantenute libere in ogni momento	Rphy18
		Esercitazioni antincendio - Tutti i collaboratori partecipano regolarmente a formazioni antincendio (esercitazioni pratiche).	Rphy18

N.	Rischio	Obiettivi di protezione raggiungibili con misure di sicurezza fisica ***Obiettivi di protezione raggiungibili con altre misure (non fisiche)***	Incide su
		Prevenzione degli incendi - Per prevenire gli incendi, vengono effettuati giri periodici di controllo. I risultati vengono registrati. Eventuali migliorie vengono implementate immediatamente.	Rphy18
		Rilevamento di fughe - Eventuali fughe di sostanze infiammabili (riscaldamento) vengono rilevate tempestivamente e segnalate in automatico	Rphy18
		Riduzione dei rischi - In caso di incendio, l'entità dei danni è ridotta al minimo	Rphy18
		Prescrizioni di legge - I sistemi e le procedure antincendio sono conformi alle disposizioni di legge	Rphy18
		Protezione cavi - Gli impianti con cavi elettrici importanti per il funzionamento dell'azienda (linee a corrente forte e debole/linee dati) sono protetti contro gli effetti degli incendi	Rphy18
		Rilevanza *- Un incendio non mette in pericolo l'esistenza di Swisscom. In particolare, i centri di calcolo e le centrali tecniche importanti per il funzionamento dell'azienda restano funzionali anche dopo un incendio (parziale) oppure sono coperti con le dovute ridondanze*	Rphy18
	Fuga di sostanze tossiche o infiammabili/perdita chimica	**Protezione da perdite chimiche** - La penetrazione di sostanze pericolose per la salute o distruttive dall'atmosfera negli edifici è ostacolata con apposite misure organizzative e accorgimenti tecnici conformi ai più recenti sviluppi tecnologici	Rphy43
		Preparazione organizzativa - Per fronteggiare il caso di un evento, vengono adottate adeguate misure organizzative	Rphy43
	Disastri naturali	**Edifici nuovi** - Per la costruzione di edifici nuovi vengono rispettate le norme edilizie e tecnologiche necessarie a renderli resistenti ai disastri naturali	Rphy23
	Esplosione	**Riduzione del rischio** - I rischi di esplosione vengono ridotti significativamente	Rphy29
		Rilevamento tempestivo - Eventuali perdite e fughe di gas vengono rilevate in tempi brevi	Rphy29
	Fuga di informazioni	***Prevenzione*** *- Viene fatto il possibile per impedire, rilevare e interrompere eventuali fughe involontarie e accidentali di informazioni o falsificazioni. Tutti i collaboratori sono istruiti sulla gestione corretta di sistemi di comunicazione d'ufficio, supporti dati e dati (per impedire la perdita di dati)*	Rphy32
		Contrasto - All'interno di archivi, depositi dati e sistemi sono adottate speciali misure di sicurezza edilizie, tecniche e organizzative al fine di rendere più difficile la fuga delle informazioni contenute su supporti cartacei o elettronici.	Rphy32
		Distruzione corretta dei dati *- È garantita la distruzione corretta dei supporti per il salvataggio di dati e informazioni.*	Rphy32
	Perdita di informazioni	***Regolamenti*** *- Salvataggio, stoccaggio, esternalizzazione e distruzione delle informazioni vengono gestiti in base a regole adeguate alle relative esigenze di disponibilità. Questo vale indipendentemente dal tipo di supporto sul quale sono salvate le informazioni (hard disk, USB, nastri, carta ecc.)*	Rphy35
		Regolamentazione degli accessi *- La consultazione e l'accesso alle informazioni sono regolati in modo da garantire la confidenzialità, integrità e disponibilità delle informazioni.*	Rphy35

N.	Rischio	Obiettivi di protezione raggiungibili con misure di sicurezza fisica *Obiettivi di protezione raggiungibili con altre misure (non fisiche)*	Incide su
	Sovratensione	**Limitazione delle conseguenze** - Vengono adottate misure per limitare le conseguenze di eventuali sovratensioni	Rphy42
		Esclusione di danni - Vengono adottate misure tali da rendere improbabili i danni da fulmini	Rphy42
		Protezione CEM - Tutti i sistemi elettronici sono protetti dai danni derivanti da potenziali sovratensioni e perturbazioni elettromagnetiche (CEM)	Rphy42
	Danni dovuti all'acqua	**Rilevamento tempestivo** - Vengono adottate procedure che garantiscono che eventuali danni dovuti all'acqua siano identificati rapidamente	Rphy45
		Riduzione dei danni - I danni a seguito di infiltrazioni di acqua sono ridotti al minimo	Rphy45
		Protezione in caso di rottura di tubazioni - La progettazione delle tubazioni per il trasporto dell'acqua deve avvenire in modo che i centri di calcolo e le centrali tecnologiche non possano essere danneggiati o distrutti in caso di rottura di tubazioni. Le tubazioni non possono essere installate all'interno di ambienti con infrastrutture importanti o critiche per il funzionamento dell'azienda (CC, RZ, centrali con gruppi di continuità ecc.) oppure devono essere protette con apposite compartimentazioni	Rphy45

4 Disposizioni transitorie

[16] Queste disposizioni di sicurezza devono essere applicate dalla data di pubblicazione in caso di nuove edificazioni e ristrutturazioni.

5 Informazioni sul documento

[17] Il presente documento contiene il catalogo rischi per la sicurezza fisica e va usato come riferimento per l'analisi e la valutazione dei rischi e la classificazione delle misure, nonché per tutte le considerazioni relative ai rischi all'interno e nei pressi degli edifici e spazi della Swisscom SA. Esso serve per rendere omogenee le valutazioni dei rischi.

5.1 «Versione 1»

Doc ID	SECDOC-103
Title	SA Base per piani di sicurezza
Classification	C2 General
Scope of application	Swisscom SA
Issue date	29.03.2023
Status	realeased
Document subject	Istruzioni sulla sicurezza
Related	LLV-SYS-008/ LLV-SYS-009