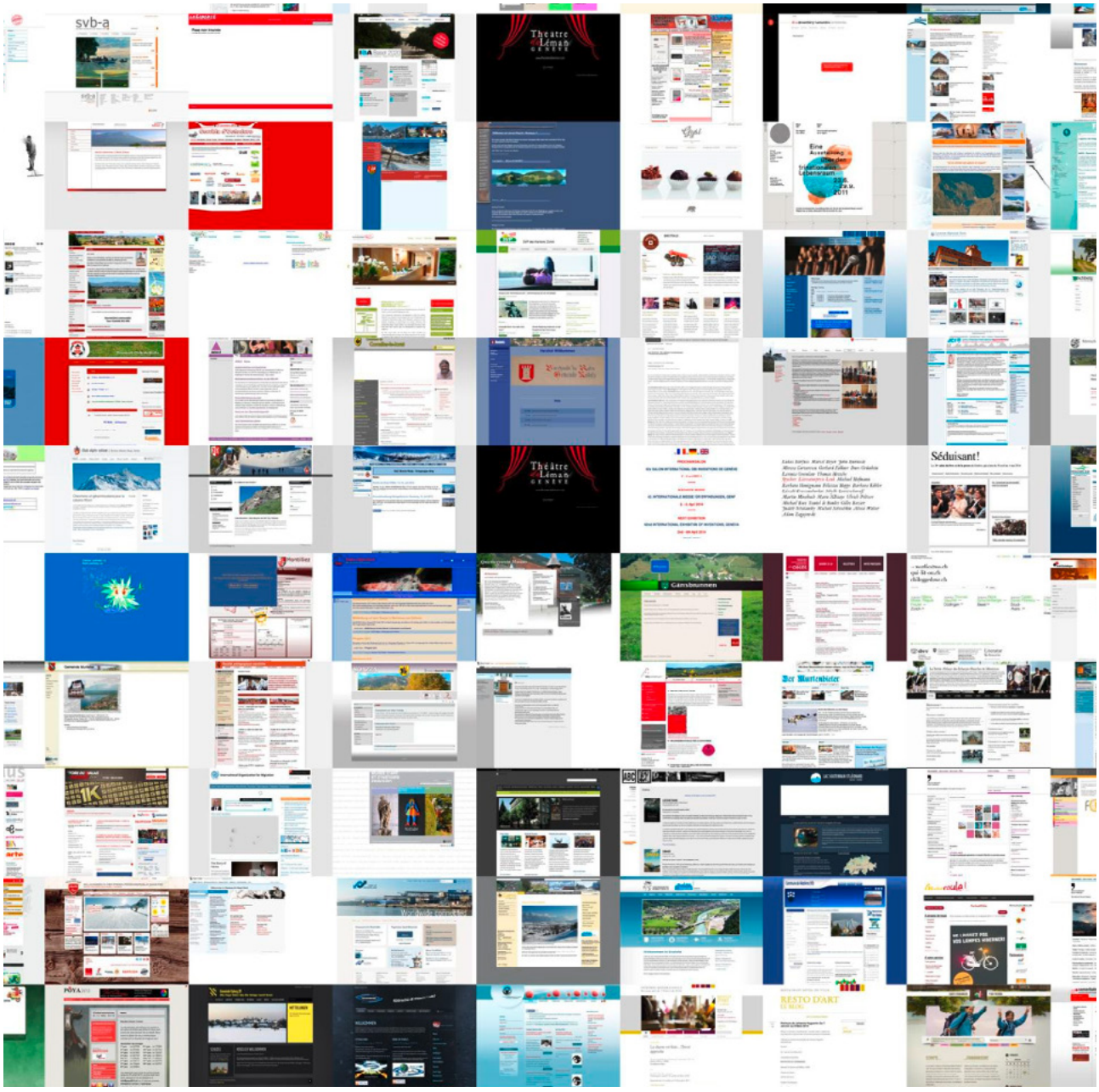
Standard minimo per la sicurezza delle tecnologie dell'informazione e della comunicazione (TIC) relative ai beni culturali digitali



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ufficio federale della protezione della popolazione UFPP

Stato il 19.02.2025

Copertina:
Archivio Web Svizzera, Biblioteca nazionale (BN). Collage tratto dalla pagina d'accesso:
https://www.e-helvetica.nb.admin.ch/collage/

Autore:
Tobias Wildi, Scuola universitaria professionale dei Grigioni, docuteam SA

Editore:
Ufficio federale della protezione della popolazione (UFPP)
divisione Protezione civile e formazione
sezione Basi Protezione civile e formazione
gruppo Protezione dei beni culturali
2024
kulturgueterschutz@babs.admin.ch
www.kgs.admin.ch

Tutti i link sono stati controllati l'ultima volta l'8 luglio 2024.

Premessa

Nella sua «Strategia Svizzera digitale»[1] , il Consiglio federale sottolinea la sua intenzione di sfruttare al meglio le opportunità offerte dalla trasformazione digitale della Svizzera. Oggigiorno è difficile immaginare una gestione degli archivi senza le tecnologie dell'informazione e della comunicazione (TIC). Il presente Standard minimo TIC è incentrato sulla sicurezza dell'archiviazione digitale a lungo termine, in particolare sul backup dei Data at Rest (dati a riposo) nell'ambito dei beni culturali digitali (vedi glossario), ed è inteso come una raccomandazione per le organizzazioni attive nel campo della salvaguardia del patrimonio culturale digitale.

La Commissione federale della protezione dei beni culturali (CFPBC) collabora con l'Ufficio federale della protezione della popolazione (UFPP) e con esperti esterni per aumentare la resilienza dei beni culturali digitali. Il presente standard richiede però anche il consenso delle istituzioni interessate. Questa versione dello Standard minimo TIC dovrà quindi essere regolarmente aggiornata e, se necessario, ampliata.

Con la crescente digitalizzazione dell'amministrazione (gestione elettronica degli affari GEVER, applicazioni specialistiche), il volume del materiale d'archivio digitale è fortemente aumentato negli ultimi anni. Allo stesso tempo, la digitalizzazione dei processi aziendali comporta nuovi rischi, che si devono affrontare. Il rischio di cyberattacchi alle infrastrutture informatiche concerne non solo gli enti statali, ma anche i gestori di infrastrutture critiche e le organizzazioni attive nel campo della salvaguardia del patrimonio culturale (musei e biblioteche). Oggi, la conservazione del patrimonio culturale analogico si basa anche su dati digitali, come database di inventari e cataloghi, copie digitali nonché documentazioni digitali di sicurezza e di reperti archeologici.

I beni culturali digitali assumono ancora più importanza quando gli originali fisici non esistono più o quando sono stati creati in forma born-digital (nato digitale). L'archiviazione a lungo termine di questi oggetti digitali solleva la domanda centrale su cosa significa esattamente «a lungo termine». In pratica si deve garantire che i dati rimangano utilizzabili per molte generazioni di architetture dei processori, sistemi operativi e formati di file. Le misure necessarie vanno oltre il semplice backup dei dati. Pertanto, le riflessioni sulle modalità di archiviazione devono essere di lungo respiro e portare sui prossimi decenni e secoli. Nel presente standard settoriale si è tenuto conto di questa particolare sfida.

1 Vedi https://digital.swiss/it/strategia/strategia-svizzera-digitale.html

Riassunto

Il presente Standard minimo TIC funge da raccomandazione e linea guida per migliorare la resilienza TIC delle organizzazioni che si occupano della salvaguardia e della conservazione dei beni culturali digitali. È destinato principalmente ai gestori di infrastrutture critiche e in particolare ai loro dirigenti e responsabili delle TIC. Fondamentalmente, dovrebbe però fruirne qualsiasi organizzazione attiva nella tutela dei beni culturali. L'obiettivo è individuare i rischi e ridurli a un livello accettabile.

Lo standard minimo TIC fornisce un quadro di riferimento (Framework) incentrato sul backup a lungo termine dei beni culturali digitali e sul raggiungimento di un livello adeguato di sicurezza contro i cyberattacchi e altre minacce. Dopo un incidente, si deve tornare il più rapidamente possibile al funzionamento normale. Per la pianificazione si applica il «NIST Cybersecurity Framework»[2], che permette alle organizzazioni di stimare sistematicamente i loro rischi e di fare il punto sullo stadio d'avanzamento delle contromisure adottate. Il fulcro della raccomandazione è l'attuazione di una cosiddetta strategia Defense in Depth, ossia di una strategia a più livelli contro le cyberminacce.

Lo standard minimo definisce anche i moduli concreti per migliorare la resilienza, che riguardano le seguenti categorie: gestione della sicurezza, processi, sistemi e sicurezza fisica. Questi moduli sono un ausilio sia per le grandi che per le piccole organizzazioni attive nella salvaguardia del patrimonio culturale.

La struttura del presente standard si basa sul modello dello «Standard minimo TIC – 2023»[3] dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE).

2 Standard del National Institute of Standards and Technology (USA): https://www.nist.gov/cyberframework.

3 Il documento è scaricabile dal sito : https://www.bwl.admin.ch/it/standard-minimi-per-le-tic

Indice

1 Situazione di partenza e finalità

Oggigiorno molti beni culturali sono creati in forma digitale e vengono archiviati e utilizzati di conseguenza. Nel patrimonio culturale digitale rientrano, ad esempio, archivi pubblici (come l'Archivio federale e gli archivi di Stato), collezioni di biblioteche (tra cui archivi di immagini, fondi di autori, dati della ricerca) e musei con le loro opere di videoarte e Internet art o fondi fotografici. L'uso e la protezione di questi beni culturali richiedono ausili digitali quali documentazioni di sicurezza, inventari, cataloghi e copie digitali.

La conservazione dei beni culturali digitali è fondamentale e in Svizzera alcuni di questi beni rientrano nelle infrastrutture di rilevanza sistemica. Tali infrastrutture sono indispensabili per il funzionamento della società e per il mantenimento dell'ordine e della sicurezza. I fondi d'archivio contribuiscono in modo significativo alla certezza giuridica poiché custodiscono documenti importanti come testi di legge, contratti, atti e sentenze.

Il presente documento è incentrato sugli archivi, ma i suoi principi si applicano anche ad altre istituzioni che si occupano di beni culturali digitali, tra cui biblioteche, musei, uffici dei monumenti storici, servizi archeologici e centri di documentazione, indipendentemente dal loro stato giuridico. Come tutte le branche, anche i beni culturali digitali sono esposti a vari pericoli. Lo Standard minimo TIC serve ad aiutare le organizzazioni che si occupano di beni culturali a rafforzare la loro infrastruttura informatica. Questo standard segue un approccio basato sui rischi, che consente diversi livelli di protezione adattati alle esigenze specifiche delle organizzazioni.

Il capitolo 3 fornisce una panoramica dei sistemi e dei processi critici da proteggere. Il capitolo 4 spiega il concetto di Defense in Depth, una difesa a più livelli contro le cyberminacce. Il capitolo 5 tratta il NIST Cybersecurity Framework, un approccio basato sui rischi per analizzare e fronteggiare i cyber-rischi. Infine, il capitolo 6 propone misure di sicurezza concrete, suddivise nelle seguenti categorie: gestione della sicurezza, moduli di processo, moduli di sistema e moduli fisici.

1.1 Contesto e panoramica

Nel 2021, l'Ufficio federale della protezione della popolazione (UFPP) ha aggiornato il «Rapporto sulla resilienza del sottosettore critico Beni culturali critici»[4]. Vi si afferma che gli attuali processi d'archiviazione e bibliotecari dipendono fortemente dalle tecnologie dell'informazione e della comunicazione (TIC). In questo contesto, i cyberattacchi agli archivi e alle biblioteche costituiscono un rischio che si estende ben oltre le istituzioni colpite e può avere un impatto sull'intera società.

In futuro ci si deve attendere non solo un marcato aumento di fondi digitali negli archivi e nelle biblioteche, ma anche una progressiva centralizzazione dell'archiviazione dei dati. Ciò si manifesta con la creazione di reti di archivi e cooperazioni e con la gestione congiunta di centri dati, come DIMAG[5] Svizzera, un'associazione di più cantoni. Sebbene permettano di creare sinergie nella gestione di infrastrutture ad alta intensità di manutenzione, queste reti digitali comportano anche un maggiore rischio di cyberattacchi mirati o di interruzioni dei sistemi TIC.

4 Rapporto interno. Una scheda informativa è scaricabile qui: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/21/1209e420-c585-43d9-b9bb-297d4e7b87b2.pdf

5 DIMAG (abbreviazione di Digital Magazine) è un pacchetto di soluzioni software per l'archiviazione digitale a lungo termine di documenti ufficiali. È stato sviluppato dalle amministrazioni archivistiche degli Stati federali tedeschi di Baden-Württemberg e Assia e dello Stato libero di Baviera. Nel 2019, i cantoni di Soletta, Sciaffusa e Argovia hanno fondato la rete di archivi DIMAG Svizzera. Vedi: https://www.eoperations.ch/it/service/lufficio-dimag/.

Un'analisi dettagliata dei rischi, condotta nel succitato rapporto, ha esaminato la possibilità che i processi archivistici vengano compromessi da cyberattacchi contro gli archivi di Stato o i sistemi TIC cantonali. Il rapporto evidenzia che simili attacchi e le conseguenti interruzioni dell'infrastruttura TIC possono pregiudicare a lungo termine l'accessibilità e la disponibilità dei fondi d'archivio e delle reti d'archiviazione. Sussiste inoltre il rischio di distruzione irreversibile o di furto nonché di pubblicazione intenzionale o involontaria di informazioni sensibili.

1.2 Campo d'applicazione e delimitazioni

La responsabilità della protezione dei beni culturali digitali spetta fondamentalmente alle istituzioni preposte alla loro conservazione, che operano sulla base di un mandato legale o a titolo volontario. Laddove il funzionamento delle infrastrutture critiche potrebbe essere compromesso, sussiste anche una responsabilità statale, basata sul mandato della Costituzione federale e della legge federale sull'approvvigionamento economico del Paese (LAP)[6]. Il presente Standard minimo TIC è un'espressione di questa responsabilità dello Stato di proteggere la società, l'economia, le istituzioni e l'amministrazione pubblica.

Questo standard è destinato principalmente ai gestori e responsabili delle infrastrutture critiche del sottosettore Beni culturali, che sono elencate nell'Inventario della protezione delle infrastrutture critiche (Inventario PIC)[7]. Tutti gli oggetti dell'Inventario PIC figurano anche nell'Inventario PBC come oggetti d'importanza nazionale (oggetti A)[8]. La raccomandazione settoriale è incentrata sulle istituzioni (archivi, biblioteche e musei) con archivi digitali, ma può concernere anche altre istituzioni del sottosettore Beni culturali che conservano fondi digitali. Ai gestori delle infrastrutture critiche si raccomanda di applicare lo Standard minimo TIC. Fondamentalmente, lo standard fornisce a tutti gli attori che si occupano della conservazione dei beni culturali un aiuto e moduli concreti che consentono di migliorare la resilienza delle TIC.

I beni culturali digitali vengono spesso suddivisi nelle categorie «born digital» e «retro-digitalizzati». Tuttavia, il presente standard minimo non distingue tra queste due categorie, ma le considera equivalenti. Ciò si spiega con il fatto che negli ultimi anni il confine tra concetti originariamente ben definiti è diventato sempre più labile. Oltre alla conversione analogico-digitale, oggi la retrodigitalizzazione comporta solitamente anche tappe di dataficazione (Datafication). Ne sono un esempio il riconoscimento ottico dei caratteri, il riconoscimento vocale, il riconoscimento di entità nominative (Named Entity Recognition, NER) per convertire il testo in dati strutturati, la vettorializzazione di piani e la scansione 3D in archeologia o degli oggetti museali. Inoltre, le retrodigitalizzazioni servono come copie di sicurezza per materiali analogici originali e ne conservano il carattere originale in caso di perdita. Di conseguenza, il valore dei beni culturali digitali non dipende dal modo in cui sono stati creati (retrodigitalizzati o born digital).

Esistono già diversi standard riconosciuti a livello internazionale per la sicurezza IT (per una panoramica vedi cap. 7, Fonti e siti web). Lo Standard minimo TIC non fa assolutamente concorrenza a questi standard esistenti, ma è compatibile con essi, sebbene abbia un campo d'applicazione più ristretto. Il suo scopo è semplificare l'approccio alla tematica della sicurezza e aiutare a individuare le principali misure per raggiungere un livello di protezione adeguato. La raccomandazione settoriale è incentrata sui processi che hanno un influsso diretto sulla sicurezza dei beni culturali digitali e sul backup dei cosiddetti Data at Rest. Non tratta la sicurezza dell'infrastruttura informatica amministrativa, o solo marginalmente.

6 Legge federale sull'approvvigionamento economico del Paese (legge sull'approvvigionamento economico del Paese, LAP; RS 531) del 17 giugno 2016 (in vigore dal 1° luglio 2023).

7 L'Inventario PIC elenca singole infrastrutture critiche d'importanza strategica. L'inventario di questi edifici e impianti è stato stilato per la prima volta nel 2012 in collaborazione con i cantoni. È un documento classificato e non è accessibile al pubblico. Funge da base per la pianificazione e la definizione delle priorità nella gestione dei rischi e degli eventi da parte delle autorità autorizzate ad accedervi (Confederazione, cantoni e gestori di IC).

8 L'Inventario PBC 2021 è disponibile all'indirizzo: https://www.babs.admin.ch/it/linventario-della-protezione-beni-culturali-con-oggetti-dimportanza-nazionale-e-regionale.

Figura: Perimetro del sottosettore critico Beni culturali

1.3 Obiettivi e struttura dello Standard minimo TIC

Questo standard minimo TIC è inteso come una misura preventiva e formulato come una raccomandazione settoriale.

Il documento è articolato come segue:

- I capitoli 1 e 2 forniscono un'introduzione agli ambiti prioritari della protezione dei beni culturali.
- Il capitolo 3 descrive i sistemi e i processi critici.
- Il capitolo 4 spiega l'approccio Defense in Depth.
- Il capitolo 5 descrive un Framework (quadro di riferimento) per la verifica e la pianificazione della resilienza.
- Il capitolo 6 contiene raccomandazioni specifiche per migliorare la resilienza sotto forma di moduli organizzativi e tecnici.

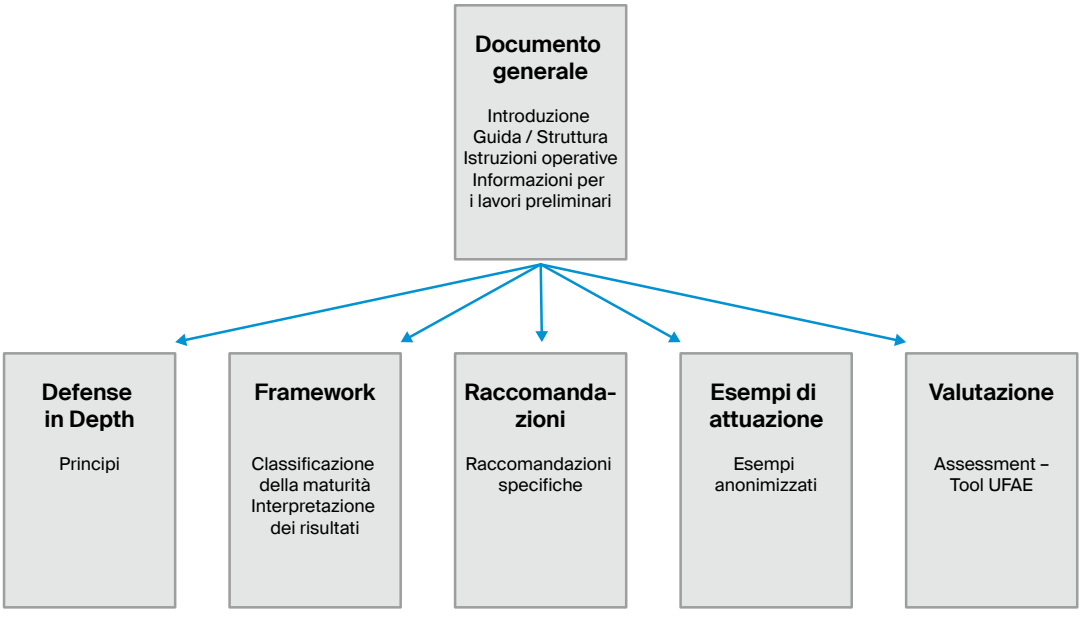


Figura: Panoramica dei documenti dello Standard minimo TIC

L'UFAE mette a disposizione un Assessment-Tool[9] per valutare il livello di maturità dell'azienda o dell'organizzazione. Lo Standard minimo TIC è considerato applicato se, secondo la classificazione del tool di valutazione, il livello di maturità soddisfa almeno i requisiti minimi nell'Overall-Rating (valutazione complessiva), in conformità con l'approccio aziendale basato sui rischi. Di principio, si raccomanda una procedura basata sul processo, in modo da garantire una verifica e un miglioramento regolari e continui.

1.4 Attuazione dello Standard minimo TIC

Il panorama istituzionale della conservazione dei beni culturali è molto eterogeneo, soprattutto per quanto concerne le dimensioni, il mandato e il genere di finanziamento. Non tutte le istituzioni saranno in grado di attuare completamente lo Standard minimo TIC. Quelle più piccole e finanziariamente più deboli si concentreranno su poche misure di protezione essenziali. Le proposte di attuazione del capitolo 6 sono concepite sotto forma di moduli. Ogni istituzione può quindi prioritizzare i moduli più importanti per il suo profilo di collezione e di rischio. A seconda delle dimensioni dell'istituzione, per l'attuazione si applicano le seguenti raccomandazioni:

Genere di istituzione	Esempi	Raccomandazione di attuazione
Piccola, risorse limitate, basso grado di professionalizzazione	Piccolo archivio comunale, archivio speciale con un profilo di collezione mirato	Concentrazione sui moduli più importanti del capitolo 6
Da media a grande, risorse garantite, alto grado di professionalizzazione	Grande archivio comunale, archivio di Stato, Archivio federale, archivio specializzato con un ampio profilo di collezione	Priorizzazione dei moduli del capitolo 6 in funzione del profilo di rischio, applicazione del tool di valutazione

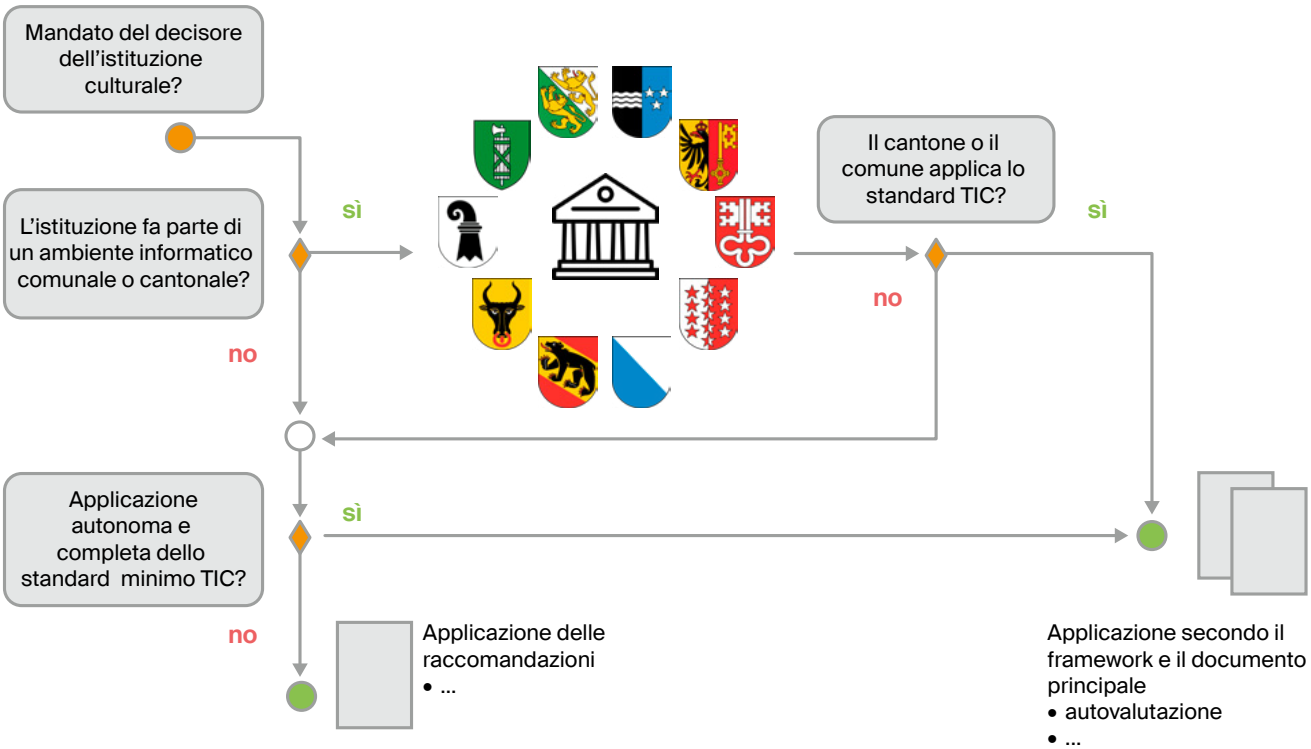


Figura: Diagramma di flusso per l'attuazione dello Standard minimo TIC

9 L'Assessment-Tool è disponibile qui nel formato Excel: https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

Il diagramma di flusso raffigurato qui sotto è un modello per l'attuazione dello Standard minimo TIC. Se i sistemi informatici dell'archivio fanno parte di un'organizzazione più grande (p. es. città, cantone o Confederazione), l'attuazione può avvenire a un livello superiore e includere anche altre infrastrutture. Se ciò non è il caso o se l'archivio deve essere messo in sicurezza in modo autonomo secondo questo standard, si deve innanzitutto procedere a una classificazione delle dimensioni. Le istituzioni di piccole dimensioni implementano solo i moduli del capitolo 6 che sono per loro prioritari. Quelle di medie e grandi dimensioni attuano completamente lo Standard minimo TIC.

Si raccomanda fondamentalmente un approccio basato sul processo (diagramma di flusso), soprattutto per le grandi organizzazioni. Ciò significa che la cybersicurezza non è una condizione statica, bensì un processo da praticare e verificare continuamente. La sicurezza delle TIC non verrà mai completamente raggiunta, ma deve essere continuamente perseguita e periodicamente aggiornata.

1.5 Lavori preliminari e basi legali

In base alla Costituzione federale, i cantoni hanno la sovranità culturale. Sono inoltre responsabili degli archivi di diritto pubblico in conformità con le leggi sugli archivi. La Confederazione può però fornire un supporto sussidiario ai cantoni. In particolare, l'UFPP può assistere e consigliare i cantoni[10] nelle questioni inerenti alla protezione dei beni culturali.

Il 16 giugno 2023, il Consiglio federale ha approvato la Strategia nazionale per la protezione delle infrastrutture critiche (PIC)[11]. Si tratta di un perfezionamento delle prime due strategie del 2012 e del 2017. L'UFPP è incaricato di coordinare i compiti in ambito PIC. La strategia PIC descrive 17 misure volte a migliorare la resilienza sia a livello settoriale che intersettoriale. La «Strategia nazionale per la protezione contro i cyber-rischi»[12] precisa che la Svizzera deve proteggersi dalle cyberminacce dal punto di vista economico e socio-politico per poter sfruttare coerentemente le opportunità offerte dalla digitalizzazione e preservare il vantaggio competitivo di essere un Paese sicuro. I lavori negli ambiti della PIC e della cibernetica sono coordinati tra la Confederazione e i cantoni. Nell'ambito dell'attuazione è stato creato l'Ufficio federale per la cybersicurezza (UFCS), che collabora strettamente con il settore «Trasformazione digitale e governance delle TIC» (TDT) della Cancelleria federale. A tal fine, anche l'UFCS ha pubblicato uno standard minimo per migliorare la resilienza delle TIC.

Nel 2020, la CFPBC ha approvato una strategia 2021-2025 negli ambiti prevenzione/preparazione, intervento e rigenerazione[13], che definisce le principali linee guida per massimizzare la protezione dei beni culturali. Vi si attribuisce grande importanza alla digitalizzazione e alla cybersicurezza dei beni culturali digitali. Si è proceduto alla necessaria precisazione delle nozioni e all'elaborazione di una matrice di valutazione per l'inclusione sistematica degli oggetti nell'Inventario PBC. La conservazione sostenibile e a lungo termine degli oggetti digitali fa parte di questa Strategia PBC.

Su incarico della CFPBC e della sezione PBC dell'UFPP, il Digital Humanities Lab (DH Lab) dell'Università di Basilea ha condotto e valutato dei sondaggi online sui beni culturali digitali.[14] I risultati dei due sondaggi, condotti nel 2016 e nel 2020 per stabilire la quantità di beni culturali digitali e dedurre le esigenze di sicurezza, sono stati utilizzati come base per lo Standard minimo TIC.

10 Art. 4 cpv. b della legge federale del 20 giugno 2014 sulla protezione dei beni culturali in caso di conflitti armati, catastrofi e situazioni d'emergenza (LPBC; RS 520.3)

11 Strategia nazionale per la protezione delle infrastrutture critiche 2023. In giugno 2012 e 2017, il Consiglio federale aveva già adottato le prime due strategie per la protezione delle infrastrutture critiche al fine di migliorare ulteriormente la resilienza (capacità di resistenza, adattamento e rigenerazione) delle infrastrutture critiche della Svizzera: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/03/07/3159c04b-ffc8-4f4e-b72f-ccba6b6a800e.pdf

12 Strategia nazionale per la protezione della Svizzera contro i cyber-rischi: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/03/07/3159c04b-ffc8-4f4e-b72f-ccba6b6a800e.pdf

13 La Strategia PBC è disponibile all'indirizzo: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/732d8094-52f3-49dd-965f-3debd139c8cd.pdf

14 Il rapporto «Valutazione del sondaggio sui beni culturali digitali» del febbraio 2017 può essere richiesto alla sezione PBC dell'UFPP.

2 Il patrimonio culturale digitale della Svizzera

Secondo le convenzioni dell'UNESCO[15], il concetto di *patrimonio culturale* comprende tutti i beni culturali mobili e immobili e il patrimonio culturale immateriale.

- Nei beni culturali **mobili** rientrano le collezioni di archivi, biblioteche e musei. Questa categoria comprende non solo i beni culturali su supporti d'informazione analogici, ma anche il patrimonio culturale digitale sotto forma di fondi digitali negli archivi dell'amministrazione pubblica e nelle istituzioni citate. Ne sono un esempio la videoarte e l'Internet art, i fondi di autori, gli archivi di media audiovisivi (archivi AV), le banche dati, i dati della ricerca, ecc.
- Nei beni culturali **immobili** rientrano edifici, monumenti e siti archeologici. Per questi beni culturali esistono documentazioni di sicurezza sotto forma di piani, fotografie e inventari. Oggi questa documentazione viene creata anche in forma digitale.
- Nel patrimonio culturale **immateriale** rientrano tradizioni, usanze, eventi festivi e arti dello spettacolo.[16] Il patrimonio culturale immateriale è volatile e non può essere archiviato, ma può essere documentato. La documentazione avviene solitamente sotto forma di riproduzioni audiovisive o scritte, che oggi vengono generalmente creati e archiviati in formato digitale.

Questa panoramica mostra che tutte e tre le categorie comprendono oggetti digitali degni di protezione. Si pone però l'accento sui beni culturali mobili con le loro collezioni e archivi digitali. Oggigiorno tali collezioni si trovano presso istituzioni di beni culturali sia pubbliche che private. Il presente Standard minimo TIC è incentrato principalmente sulla protezione degli archivi, in quanto sono considerati particolarmente critici per la loro funzione di certezza giuridica.

15 Le convenzioni dell'UNESCO ratificate dalla Svizzera sono disponibili all'indirizzo https://www.unesco.ch/culture/conventions/

16 Art. 2 della Convenzione per la salvaguardia del patrimonio culturale immateriale (RS 0.440.6) stipulata a Parigi il 17 ottobre 2003.

2.1 Panoramica degli attori

Per il forte carattere tradizionalmente federalista della politica culturale della Svizzera, la custodia e la salvaguardia dei beni culturali non sono nelle mani di poche istituzioni centralizzate, ma vengono garantite da numerose organizzazioni regionali, cantonali e nazionali di varia forma giuridica. La conservazione dei beni culturali in Svizzera non è quindi gestita a livello centrale.

Gli attori di diritto pubblico o privato possono essere attribuiti ai livelli Confederazione (nazionale), cantone e città/comune/regione. In certi casi operano anche a più livelli. La seguente tabella mostra la varietà degli attori:

		Forma giuridica		
		di diritto pubblico con mandato pubblico/legale	**di diritto privato** con mandato pubblico/legale	**di diritto privato** con mandato proprio
Finanziatori principali	**Settore pubblico**	**Attore pubblico** • organizzato secondo il diritto pubblico • con mandato pubblico/legale • finanziato principalmente da enti pubblici (è possibile un finanzziamento parziale da partire di privati)	**Attore ibrido** • organizzato secondo il diritto pubblico • con mandato pubblico/legale • finanziato principalmente da enti pubblici (è possibile un finanziamento parziale da parte di privati)	**Attore ibrido** • organizzato secondo il diritto privato • con mandato privato/proprio • finanziato principalmente da enti pubblici (è possibile un finanziamento parziale da parte di privati)
	Sevttore privato	N/A	N/A	**Attore privato** • organizzato secondo il diritto privato • con mandato privato/proprio • finanziato principalmente da privati (è possibile un finanziamento parziale da parte di enti pubblici)

Tipi principali:

Pubblico	**ibrido**	**privato**

Le tipiche forme organizzative degli attori sono le seguenti:

- **Attori pubblici (statali):** autorità e fondazioni a livello federale, cantonale e cittadino/comunale
- **Attori ibridi (privati/pubblici):** fondazioni e associazioni a livello internazionale, nazionale, cantonale e regionale
- **Attori privati:** fondazioni, associazioni e aziende a livello internazionale, nazionale, cantonale e regionale

Questa panoramica mostra che il settore della salvaguardia del patrimonio culturale è caratterizzato da una marcata eterogeneità, con attori aventi differenti dimensioni, risorse finanziarie e raggi d'azione.

La maggior parte di questi attori operativi nella conservazione del patrimonio culturale sono insediati nei cantoni e nei comuni. La Confederazione li sostiene a titolo sussidiario ed assume compiti di coordinamento. A livello nazionale, l'Ufficio federale della cultura (UFC) è competente per la conservazione e la catalogazione dei beni culturali, mentre l'UFPP per la protezione dei beni culturali in caso di conflitti armati e catastrofi. A livello cantonale e comunale, i rispettivi enti cantonali e comunali sono competenti per la cultura, la protezione dei beni culturali, la protezione dei siti, la salvaguardia dei monumenti e l'archeologia. Inoltre, numerosi attori privati si impegnano per la conservazione e la protezione dei beni culturali in Svizzera, la maggior parte dei quali è organizzata come fondazione privata o associazione. Un'intera serie di attori ibridi ha un mandato pubblico, ma è organizzata secondo il diritto privato.[17]

17 Edzard Schade, Tobias Wildi (2022). Panoramica / Inventario del patrimonio culturale in Svizzera. Rapporto commissionato dall'Ufficio federale della cultura.

La Confederazione e i cantoni sono responsabili dei beni culturali in loro possesso. Le responsabilità per la conservazione e la catalogazione dei beni culturali sono generalmente disciplinate a livello federale nella legge sulla protezione della natura e del paesaggio (LPN).[18] Esiste inoltre un'ampia legislazione cantonale con disposizioni pertinenti (p. es. diritto in materia di archivi, salvaguardia dei monumenti e archeologia). La responsabilità per i beni culturali in caso di conflitti armati, catastrofi e situazioni d'emergenza è disciplinata dalla corrispondente legge federale sulla protezione dei beni culturali in caso di conflitti armati, catastrofi e situazioni d'emergenza (LPBC).[19]

2.2 Archivi e struttura degli archivi in Svizzera

Il presente Standard minimo TIC è incentrato principalmente sugli archivi, poiché una parte degli archivi della Svizzera è classificata come infrastruttura critica.[20] Questi rientrano nelle infrastrutture critiche poiché contribuiscono alla certezza giuridica. In questo documento, il termine archivio non si riferisce però solo a un tipo di istituzione della memoria, ma più in generale anche a funzioni e sistemi di memorizzazione e conservazione di oggetti digitali con un valore culturale. Il compito di un archivio consiste nel prendere in consegna i beni culturali e garantire che rimangano utilizzabili a lungo termine. A tal fine, si deve preservare l'integrità (inalterabilità) e l'autenticità (attendibilità) dei documenti. Anche un altro tipo di attore, come una biblioteca o un museo, può assumere questa funzione.

La Svizzera dispone di un panorama archivistico pubblico a più livelli, con l'Archivio federale, 26 archivi di Stato, archivi cantonali e archivi cittadini e comunali. A questi si aggiungono importanti archivi ecclesiastici, aziendali e speciali, nonché fondi archivistici di biblioteche, musei e centri di documentazione. Nell'Inventario PIC, i 26 archivi di Stato e l'Archivio federale sono stati classificati come oggetti di rilevanza sistemica.

In Svizzera non esiste una struttura archivistica centralizzata a livello federale, cantonale o comunale. Il diritto d'uso e gli obblighi di conservazione e notifica non sono definiti da alcuna disposizione costituzionale. La legislazione sugli archivi è disciplinata su base federalista: ogni cantone ha una propria legge o ordinanza sugli archivi. Ciascuno dei 26 archivi di Stato ha quindi una propria tradizione storico-giuridica.

Lo sviluppo del diritto archivistico è stato fortemente influenzato dalla legislazione sulla protezione dei dati negli anni Novanta. I punti principali da regolamentare erano l'obbligo di versamento di documenti agli archivi, il diritto d'uso e la protezione della privacy (protezione dei dati). Nel frattempo, la maggior parte dei cantoni ha emanato una propria legge sugli archivi accanto a quella federale. Di principio, ogni cittadino svizzero ha il diritto di visionare documenti ufficiali, a meno che non vi siano interessi pubblici o privati prevalenti per il mantenimento del segreto.

La legge federale sull'archiviazione (LAr)[21] disciplina l'archiviazione degli atti della Confederazione nell'Archivio federale. Vi vengono archiviati documenti federali di grande valore giuridico, politico, economico, storico, sociale o culturale. La LAr non ha però conseguenze dirette per i cantoni e i comuni.

18 Legge federale del 1° luglio 1966 sulla protezione della natura e del paesaggio (LPN; RS 451)

19 Art. 3 e 5 della legge federale del 20 giugno 2014 sulla protezione dei beni culturali in caso di conflitti armati, catastrofi e situazioni d'emergenza (LPBC; SR 520.3).

20 Vedi https://www.babs.admin.ch/it/le-infrastrutture-critiche.

21 Legge federale sull'archiviazione (legge sull'archiviazione, LAr; RS 152.1) del 26 giugno 1998

3 Panoramica dei sistemi e dei processi di rilevanza sistemica

3.1 Archivi di rilevanza sistemica

Negli archivi di rilevanza sistemica rientrano l'Archivio federale, gli archivi di Stato e alcuni archivi comunali e speciali.

Archivio federale svizzero (AFS)

L'Archivio federale svizzero (AFS) ha il mandato legale[22] di mantenere sempre disponibili le informazioni rilevanti della Confederazione. Ciò consente all'Amministrazione di rendere conto delle sue attività e la sostiene nel suo lavoro. L'AFS aiuta e consiglia l'Amministrazione federale nella creazione, organizzazione e gestione di dati e documenti. Inoltre, sceglie insieme agli enti amministrativi i documenti che meritano di essere archiviati e ne garantisce la disponibilità e la conservazione a lungo termine. La valutazione si basa su criteri sistematici e le decisioni vengono pubblicate regolarmente.[23] L'AFS crea anche copie digitali di documenti d'archivio analogici e le mette a disposizione del pubblico. Per alcuni temi scelti, collabora alle ricerche storiche e le rende accessibili al grande pubblico.

Archivi di Stato e archivi comunali

Gli archivi di Stato e gli archivi comunali svolgono al loro livello essenzialmente gli stessi compiti che l'AFS svolge a livello nazionale. Prendono in consegna, catalogano e conservano i documenti d'archivio delle autorità tenute a versarli agli archivi e sono responsabili delle misure di conservazione e dell'accessibilità. Contribuiscono alla trasmissione della conoscenza storica e alla ricerca storica per le esigenze del cantone, della scienza e della cultura. Valutano i documenti in funzione del loro valore archivistico, consigliano le autorità e i privati e, in certi casi, emanano anche direttive sul versamento dei documenti e sugli strumenti di ricerca.

Archivi speciali

Gli archivi speciali sono archivi specializzati in determinati temi o aree precise. Raccolgono, conservano e rendono disponibili documenti su temi specifici. Possono ad esempio essere archivi di arte, musica, storia, storia naturale, tecnologia, scienza o medicina. Servono per la ricerca, la formazione e la cultura e sono fonti importanti per scienziati, storici, giornalisti, artisti e il grande pubblico. Svolgono un'importante funzione sociale poiché documentano l'operato della società civile e di attori non statali in modo complementare ai documenti statali. Tra questi rientrano movimenti sociali, partiti politici, comunità religiose, associazioni, organizzazioni non governative (ONG), ecc.

3.2 Prestazioni degli archivi nel sottosettore Beni culturali

Gli archivi pubblici sono attori importanti per la garanzia della certezza giuridica in Svizzera. Conservano documenti che sono di fondamentale importanza per la tutela e l'applicazione dei diritti e degli obblighi, come ad esempio testi di legge, contratti, atti, sentenze o titoli di proprietà fondiaria. Assicurano che i documenti siano archiviati secondo le leggi, le norme e gli standard vigenti al fine di garantire l'integrità e l'autenticità del materiale archivistico.

Attraverso la conservazione permanente di documenti amministrativi, gli archivi garantiscono la tracciabilità delle decisioni e delle attività, soprattutto nel settore pubblico. In tal modo contribuiscono alla trasparenza e alla responsabilità dei processi governativi e amministrativi, aumentando la fiducia dei cittadini nelle istituzioni e nello Stato di diritto. L'Archivio federale riassume perfettamente questo concetto nel motto «niente democrazia senza archivi».

22 Vedi legge federale sull'archiviazione (LAr, RS 152.1)

23 Le decisioni di valutazione dell'AFS sono disponibili all'indirizzo: https://www.bar.admin.ch/bar/it/home/gestione-dell-informazione/valore-archivistico/decisioni-di-valutazione.html

A complemento degli archivi pubblici, gli archivi speciali sono socialmente utili poiché garantiscono la conservazione e la fruibilità di beni culturali mobili che non sono stati direttamente creati nell'ambito dell'Amministrazione pubblica. Sono incentrati su temi e aree specifiche, come ad esempio la storia sociale, la storia economica o la storia delle donne. Hanno un grande valore per l'identificazione culturale del nostro Paese e rientrano quindi (almeno in parte) nelle infrastrutture critiche.

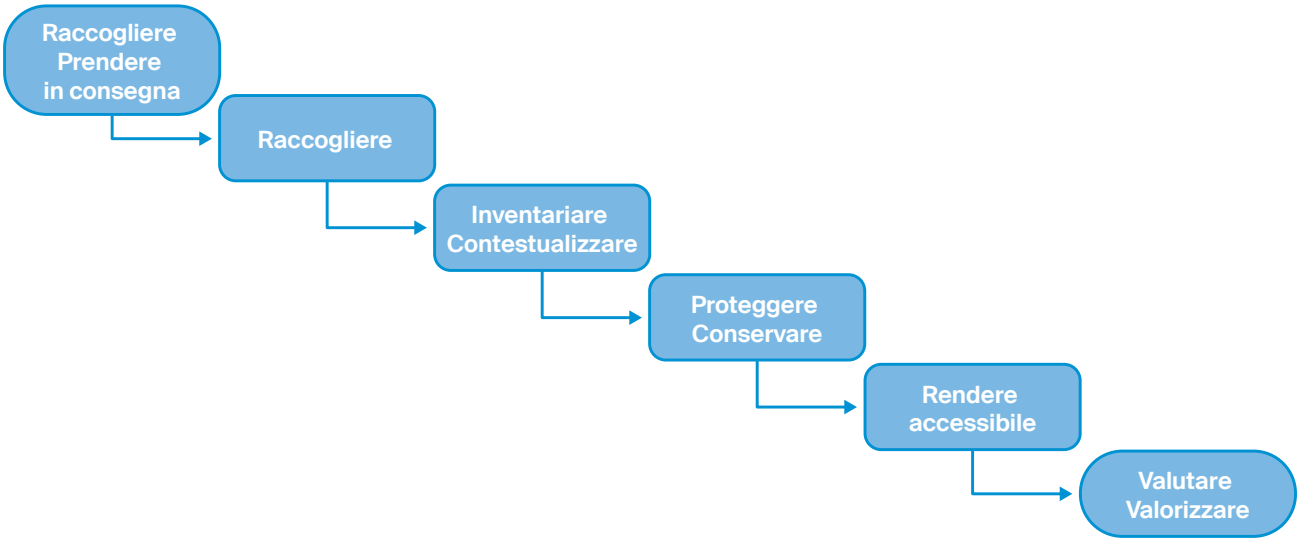
3.3 Panoramica dei processi critici

I processi aziendali di tutti gli attori coinvolti nella conservazione e nella salvaguardia del patrimonio culturale possono essere descritti con l'ausilio del diagramma di flusso raffigurato qui sotto. I campi d'attività sono possibilmente denominati con termini generici e le fasi sono denominate in modo diverso a seconda del tipo di attore (archivio, biblioteca, museo, centro di documentazione, servizio per la salvaguardia dei monumenti) e del bene culturale (mobile, immobile, immateriale). Dal diagramma si evince che il sottosettore critico Beni culturali dipende fortemente dai sistemi TIC, in particolare per l'inventariazione, la ricerca e la protezione/conservazione.

Nel quadro del presente Standard minimo TIC, alcuni campi d'attività non vengono presi in considerazione o fanno parte di altri sottosettori delle infrastrutture critiche:

- Sistemi a monte come GEVER, gestione dei documenti, gestione dei record, applicazioni speciali
- Valutazione, selezione, scelta dei beni culturali da archiviare
- Sistemi a valle come sistemi di valutazione e infrastrutture di ricerca

Il processo di presa in consegna, custodia e messa a disposizione dei beni culturali digitali prevede le seguenti tappe:



Raccogliere
Prendere in consegna e preparare dati e metadati (Ingest). Questo compito è supportato da sistemi basati sul workflow che automatizzano e orchestrano operazioni quali il controllo antivirus, la validazione, l'estrazione di metadati, la migrazione del formato dei file, l'integrità (scrittura di checksum), ecc.

Inventariare e contestualizzare
Registrare, elencare, ordinare, documentare e catalogare. A seconda del tipo di organizzazione, questo compito è supportato da sistemi archivistici, bibliotecari o di gestione delle collezioni. Inoltre, si acquisiscono conoscenze contestuali e informazioni sulla provenienza e sul contesto di creazione e d'uso.

Proteggere e conservare
Salvare (procedimento iniziale), mettere in sicurezza (compito permanente: salvaguardare i dati, controllare la memoria). Pianificare la conservazione (Preservation Planning) e adottare eventuali misure di conservazione.

Rendere accessibile
Permettere la ricerca di dati (OPAC, sala di lettura digitale, accesso al web), fornire i dati (per la valutazione automatica o per un ulteriore utilizzo su interfacce tecniche).

Valutare e valorizzare
Trasmettere e riattualizzare sotto forma di trasmissione didattica e mediatica e attraverso la pratica.

3.4 Da quali pericoli proteggersi?

Il rapporto sui pericoli e sulla resilienza nel sottosettore Beni culturali, stilato dall'UFPP nel 2022, analizza i rischi causati da interruzioni e perturbazioni di questa infrastruttura critica. Per i beni culturali sono state individuate le seguenti quattro categorie di pericolo principali:

- Un **cyberattacco** e/o un'interruzione delle TIC compromettono, probabilmente per diverse settimane, la disponibilità dei fondi digitali di un'organizzazione che custodisce beni culturali. Sono anche possibili una distruzione irreversibile, il furto o la pubblicazione (intenzionale o meno) di informazioni sensibili. I fondi d'archivio possono essere ripristinati solo se sono state preventivamente adottate delle misure adeguate. La pubblicazione di documenti riservati può causare ingenti danni alla reputazione di persone e organizzazioni. Il rischio di un cyberattacco sussiste anche per il fatto che spesso le istituzioni culturali devono cavarsela con poche risorse e non sono in grado di tenere il passo con il rapido progresso tecnologico.
  Tappe del processo minacciate: tutte le tappe sono minacciate da cyberattacchi.
- Per **i pericoli naturali** come terremoti e inondazioni si calcolano ingenti costi per la gestione dell'evento e il ripristino. Questi due eventi colpiscono infatti numerosi beni culturali nella regione interessata. Gli archivi rimangono indisponibili per mesi o addirittura per anni. Ciò comporta ingenti costi consecutivi per la popolazione, le autorità e la ricerca.
  Tappe del processo minacciate: soprattutto la tappa «Proteggere e conservare» è minacciata dai percoli naturali.
- Un **attentato convenzionale** a un archivio o a un bene culturale è considerato un attacco all'identità del cantone o del Paese e comporta ingenti danni dovuti all'incertezza percepita dalla popolazione e dall'economia. Un attentato convenzionale a un centro dati può causare una grave perdita di dati.
  Tappe del processo minacciate: è minacciata da attentati convenzionali soprattutto la tappa «Proteggere e conservare».
- Una **pandemia** porta all'assenza di personale specializzato, necessario per l'esercizio degli archivi digitali e il backup dei record. Questo pericolo è particolarmente marcato nelle istituzioni culturali più piccole, dove le conoscenze specialistiche sono detenute da una o poche persone.
  Tappe del processo minacciate: tutte le tappe del processo sono minacciate dall'assenza di personale specializzato, ma soprattutto la tappa «Proteggere e conservare».

Come in altri sottosettori, i cyber-rischi rappresentano un elevato rischio per i beni culturali a causa della crescente digitalizzazione dei processi aziendali e della centralizzazione delle infrastrutture informatiche. Inoltre, la frequenza di simili attacchi è fortemente aumentata negli ultimi anni. Un maggiore potenziale di danno si delinea anche a causa delle emergenti reti regionali e sovraregionali per l'archiviazione digitale e della crescente quantità di oggetti digitali presi a carico dagli archivi.

4 Defense in Depth

Per proteggersi dai succitati pericoli, viene qui introdotto il cosiddetto approccio di Defense in Depth (difesa in profondità). Questo si basa sul principio che non basta un'unica misura di sicurezza per proteggere completamente i sistemi o le reti. Si deve invece perseguire un approccio complessivo, che comprende diverse misure di sicurezza implementate a diversi strati o livelli. Lo scopo di questo capitolo è spiegare più in dettaglio l'approccio Defense in Depth per la cybersicurezza e illustrare quali categorie di misure potrebbero adottare le organizzazioni per perseguire questo approccio. Sulla base di questi principi, nel capitolo 6 vengono citati i moduli per migliorare la sicurezza delle informazioni.

4.1 Il concetto di Defense in Depth

La strategia di sicurezza TIC di un'organizzazione deve essere orientata alla protezione dei sistemi e delle applicazioni necessarie per i suoi campi di attività e processi. Ciò presuppone un approccio a più strati, noto come Defense in Depth, che consiste nell'applicazione coordinata di più livelli di protezione, secondo il principio per cui è più difficile superare un sistema di difesa a più strati che un'unica barriera. Allo stesso tempo, si studiano i metodi e gli approcci dei potenziali aggressori al fine di preparare dispositivi di difesa adeguati. L'obiettivo della Defense in Depth è individuare le violazioni della sicurezza TIC nonché ridurre al minimo o mitigare le loro conseguenze. La Defense in Depth persegue un approccio olistico che cerca di proteggere tutte le risorse operative (TIC) da qualsiasi rischio. Le risorse di un'organizzazione devono essere impiegate in modo da garantire una protezione efficace contro i rischi noti e monitorare i potenziali rischi futuri. Vi rientrano persone, processi, oggetti, dati e dispositivi. Un aggressore costituisce una minaccia per un sistema TIC solo quando riesce a sfruttare una vulnerabilità esistente in uno di questi elementi. Le organizzazioni e le aziende sono tenute a sorvegliare costantemente le misure e, se necessario, adattarle alle nuove minacce.

Gli elementi di un approccio Defense in Depth possono essere sommariamente suddivisi in misure organizzative, tecniche e fisiche.

4.2 Misure organizzative (processi)

In questo gruppo di misure rientrano i seguenti moduli:

- Difesa (Defense) come compito permanente di un'organizzazione nell'ambito della gestione della sicurezza; regolamentazione delle responsabilità all'interno dell'organizzazione
- Elaborazione di un profilo di rischio, identificazione dei rischi per la sicurezza
- Aspetti organizzativi e inerenti alla sicurezza del personale
- Concetti e procedure standardizzate, ad esempio per quanto concerne la protezione dei dati, la cancellazione e la distruzione di dati e dei loro supporti, lo scambio di informazioni all'interno dell'organizzazione o con terzi
- Gestione dell'insieme delle risorse operative TIC (Asset Management)
- Panoramica degli oggetti digitali archiviati
- Aspetti di sicurezza nell'esercizio operativo, sia in proprio che da parte di terzi (centro dati esterno, cloud); questo ambito comprende anche la separazione tra l'informatica amministrativa e il sistema archivistico
- Gestione delle patch (correttivi) e dei punti deboli
- Processi di elaborazione e verifica delle misure di sicurezza adottate, individuazione degli incidenti per la sicurezza e dei processi di gestione degli incidenti (Incident Management)
- Organizzazione della gestione della continuità operativa (Business Continuity Management)
- Documentazione

4.3 Misure tecniche (sistemi)

In questo gruppo di misure rientrano i seguenti moduli:

- Messa in sicurezza di applicazioni e servizi, specificamente negli ambiti: comunicazione, memorizzazione e applicazioni aziendali e client
- Messa in sicurezza dei singoli sistemi informatici, come server e desktop
- Messa in sicurezza della rete, delle connessioni e dei componenti di rete e della comunicazione tramite la rete; suddivisione della rete in segmenti e zone di sicurezza
- Messa in sicurezza dei componenti di rete attivi (firewall, router, switch, ecc.)

4.4 Misure fisiche

La messa in sicurezza fisica dei fondi archiviati è una preoccupazione che concerne soprattutto il materiale analogico, che deve essere protetto da incendi, dall'acqua o da atti vandalici. Per gli archivi digitali giocano piuttosto un ruolo i seguenti ambiti:

- Messa in sicurezza dell'accesso ai locali server e ai centri dati
- Protezione dei locali dei server e dei centri dati contro i pericoli naturali
- Distribuzione geografica dei sistemi di memorizzazione e di backup
- Backup su memoria offline (Offline Storage) o memoria fredda (Cold Storage). Come per qualsiasi tipo di memorizzazione, si deve eseguire un controllo periodico dell'integrità

4.5 Separazione dell'informatica d'ufficio dal sistema archivistico

Un punto centrale della strategia Defense in Depth è la separazione sistematica e sistemica dell'informatica amministrativa dai fondi d'archivio digitali (il sistema archivistico). Un «sistema archivistico» comprende fondamentalmente i compiti descritti nello standard ISO 14721, «Open Archival Information System» (OAIS).

La seguente tabella illustra, sulla base di esempi, come questi due ambiti funzionino secondo logiche e processi di pianificazione differenti e debbano quindi essere presi in considerazione in modo diverso. Il presente Standard minimo TIC, e in particolare i moduli per migliorare la sicurezza delle informazioni (vedi cap. 6), si riferiscono principalmente alla protezione dei beni culturali digitali e non all'informatica d'ufficio.

Tema inerente alla sicurezza	TIC (p. es. informatica d'ufficio)	Sistema archivistico basato sull'OAIS
Principi normativi	Norme e standard	Legislazione nazionale e cantonale sugli archivi, Convenzione dell'UNESCO per la salvaguardia dei beni culturali, norme e standard
Antivirus	Diffusi su larga scala. Facili da distribuire e aggiornare. Gli utenti hanno la possibilità di personalizzarli. La protezione antivirus può essere configurata a livello di dispositivo o di azienda.	I virus rappresentano una duplice sfida: 1) si devono proteggere i server del sistema d'archiviazione e 2) si deve evitare che file contaminati da virus entrino nell'archivio a lungo termine attraverso l'Ingest.
Aggiornamenti della sicurezza (Update Management)	Chiaramente definiti, eseguiti in tutta l'azienda e automatizzati tramite accesso remoto	Lunghi tempi di preparazione e di pianificazione fino all'installazione riuscita delle patch; aggiornamenti sempre specifici al produttore; possono causare interruzioni (temporanee) nell'OAIS. È necessario definire il rischio accettabile.
Ciclo di vita della tecnologia (Technology Support Lifecycle)	2–3 anni, più fornitori, sviluppo e aggiornamenti continui	10–20 anni, solitamente lo stesso offerente/fornitore di servizi per l'intero ciclo di vita; la fine del ciclo di vita comporta nuovi pericoli per la sicurezza.

Tema inerente alla sicurezza	TIC (p. es. informatica d'ufficio)	Sistema archivistico basato sull'OAIS
Metodi di test e audit (Testing and Audit Methods)	Applicazione di metodi moderni (possibilmente automatizzati). Di solito, i sistemi sono sufficientemente resilienti e affidabili da consentire valutazioni anche mentre sono in funzione.	I metodi di valutazione automatizzati potrebbero, ad esempio, essere inadeguati a causa dell'elevato grado di sviluppo individuale. C'è una maggiore probabilità d'errore durante la valutazione. Pertanto, le valutazioni delle TIC in funzione sono tendenzialmente più difficili.
Gestione dei cambiamenti (Change Management)	Pianificata e programmata a intervalli regolari. Conforme alle direttive dell'organizzazione per la durata d'uso minima/massima.	Processo complesso con un potenziale impatto sull'attività dell'archivio. È necessaria una pianificazione strategica individuale.
Classificazione dell'inventario (Asset Classification)	Si esegue solitamente ogni anno. Le spese e gli investimenti vengono pianificati in funzione dei risultati.	Per quanto concerne l'archiviazione, è soprattutto la classificazione dei dati a porre un problema. Senza un inventario e senza conoscere la sensibilità dei dati, è difficile pianificare contromisure efficaci.
Reazione e analisi degli incidenti (Incident Response and Forensics)	Facile da sviluppare e attuare. A seconda delle circostanze, ci si deve attenere alle disposizioni normative (protezione dei dati).	Si concentra principalmente sulla ripresa del sistema nell'ambito del ripristino dei dati e del Disaster Recovery.
Sicurezza fisica (Physical Security)	Varia da debole (ufficio IT) a forte (centri dati irrobustiti).	In genere, la sicurezza fisica è molto buona. Nel caso degli archivi di Stato, l'OAIS viene solitamente gestito dai centri dati cantonali.
Sviluppo di sistemi sicuri (Secure Software Development)	Parte integrante del processo di sviluppo	I primi archivi digitali a lungo termine erano spesso concepiti come sistemi fisicamente isolati e costituivano un corpo estraneo nell'infrastruttura informatica. I moderni OAIS sono invece progettati e implementati come parte integrante dell'infrastruttura informatica cantonale anche in termini di sicurezza.
Sicherheitsvorgaben	Regole generali, a seconda del settore (non per tutti i settori)	Le regole di sicurezza degli standard settoriali sono incentrate sulla conservazione a lungo termine dei dati e dei metadati e non entrano in merito di aspetti di sicurezza più ampi. A tal fine, è opportuno applicare standard generali come il NIST o l'ISO 27001.

Tabella 1: Differenze tra l'informatica d'ufficio e il sistema archivistico basato sull'OAIS

5 Misure NIST Framework Core

5.1 Panoramica

NIST Framework Core

L'obiettivo del «Cybersecurity Framework»[24] del «National Institute of Standards and Technology (USA)» è fornire ai gestori delle infrastrutture critiche uno strumento per aumentare in modo proattivo la loro resilienza ai cyber-rischi. Inoltre, tiene conto dei propositi di redditività ed efficienza, nonché della riservatezza e della protezione dei dati. Il framework si basa su una scelta di standard, linee guida e buone pratiche (Best Practice) già esistenti e non vincolati a una determinata tecnologia.

Il NIST Framework Core è un approccio basato sui rischi volto ad affrontare e gestire consapevolmente i cyber-rischi. Comprende cinque funzioni:

1. Identificare (Identify)
2. Proteggere (Protect)
3. Individuare (Detect)
4. Reagire (Respond)
5. Ripristinare (Recover)

Queste cinque funzioni costituiscono nel loro insieme la base del concetto di sicurezza.

Il NIST Framework prevede quattro livelli di implementazione (Implementation Tiers). Questi descrivono il livello di sviluppo o di protezione che un'azienda ha già raggiunto. Si va da un livello *parziale* (Tier 1) fino a un livello *adeguato al pericolo* (Tier 4). Per stabilire il *livello di protezione* auspicato (Tier Level), un'organizzazione dovrebbe avere una visione d'insieme delle proprie pratiche di gestione dei rischi, della situazione di pericolo, dei requisiti legali e normativi, degli obiettivi aziendali e delle direttive organizzative. Solo così diventa chiaro contro cosa si vuole veramente proteggere l'azienda.

Il prossimo capitolo è articolato secondo le cinque funzioni del NIST Framework Core. I compiti da svolgere sono classificati come segue:

- Le prime due lettere (p. es. ID = Identify) designano una delle cinque funzioni.
- La seconda coppia di lettere designa la categoria (p. es. AM = Asset Management).
- Il numero designa il singolo compito. I compiti sono numerati in ordine crescente all'interno della categoria. Esempio di lettura: ID.AM-1 corrisponde al primo compito della categoria Asset Management della funzione Identify.

La seguente tabella fornisce una panoramica delle funzioni e delle categorie del NIST Framework:

Abbreviazione	Italiano	Inglese
ID	**Identificare**	**Identify**
ID.AM	Gestione dell'inventario	Asset Management
ID.BE	Ambiente aziendale	Business Environment
ID.GV	Direttive	Governance
ID.RA	Analisi dei rischi	Risk Assessment
ID.RM	Strategia di gestione dei rischi	Risk Management Strategy
ID.SC	Gestione dei rischi nella catena di fornitura	Supply Chain Riskmanagement

24 https://www.nist.gov/cyberframework

5 Misure NIST Framework Core

Abbreviazione	Italiano	Inglese
PR	**Proteggere**	**Protect**
PR.AC	Gestione e controllo degli accessi	Access Control
PR.AT	Sensibilizzazione e formazione	Awareness and Training
PR.DS	Sicurezza dei dati	Data Security
PR.IP	Linee guida per la protezione delle informazioni	Information Protection Processes and Procedures
PR.MA	Manutenzione	Maintenance
PR.PT	Impiego di tecnologie di protezione	Protective Technology
DE	**Individuare**	**Detect**
DE.AE	Anomalie e incidenti	Anomalies and Events
DE.CM	Sorveglianza	Security Continous Monitoring
DE.DP	Processo di individuazione	Detection Processes
RS	**Reagire**	**Respond**
RS.RP	Piano di intervento	Response Planning
RS.CO	Comunicazione	Communications
RS.AN	Analisi	Analysis
RS.MI	Mitigazione dei danni	Mitigation
RS.IM	Miglioramenti	Improvements
RC	**Ripristinare**	**Recover**
RC.RP	Piano di ripristino	Recovery Planning
RC.IM	Miglioramenti	Improvements
RC.CO	Comunicazione	Communications

Tabelle 2: Panoramica delle funzioni e delle categorie del NIST Framework

A ogni tabella con i compiti del NIST Framework Core segue un'altra tabella con riferimenti ad altri standard internazionali. Ciascuna di queste tabelle si riferisce alla rispettiva categoria, per esempio Asset Management. Ciò facilita la classificazione agli utenti che organizzano i compiti di sicurezza TIC secondo altri standard. Per l'ambito dei beni culturali digitali si fa riferimento anche alla norma ISO 16363 (vedi qui sotto).

NIST Framework e norma ISO 16363:2012
Un importante standard settoriale per valutare l'affidabilità degli archivi digitali è la norma ISO 16363:2012 «Audit and certification of trustworthy digital repositories». Questa norma è suddivisa in tre parti:

- Quadro organizzativo
- Gestione degli oggetti digitali
- Gestione dei rischi per l'infrastruttura e la sicurezza

La seguente tabella mostra come sono correlate le funzioni e le categorie del NIST Framework e della norma ISO 16363:

5 Misure NIST Framework Core

Function	NIST Framework Core	ISO 16363
Identify	Asset Management	5.1 Technical Infrastructure Risk Management
	Business Environment	3.3 Procedural Accountability and Preservation Policy Framework
	Governance	3.1 Governance and Organizational Viability 3.3 Procedural Accountability and Preservation Policy Framework 3.4 Financial Sustainability
	Risk Assessment	5.1 Technical Infrastructure Risk Management 5.2 Security Risk Management
	Risk Management Strategy	5.1 Technical Infrastructure Risk Management 5.2 Security Risk Management
	Supply Chain Management	3.5 Contracts, Licenses, and Liabilities
Protect	Identity management and access control	4.6 Access management
	Awareness and Training	3.2 Organizational Structure and Staffing
	Data Security	5.1 Technical Infrastructure Risk Management
	Information Protection	3.3 Procedural Accountability and Preservation Policy Framework 4.1 Ingest: Acquisition of Content 4.2 Ingest: Creation of the AIP 4.5 Information Management
	Maintenance	4.3 Preservation Planning
	Protective Technology	4.4 AIP Preservation
Detect	Anomalies and Events	
	Security continuous monitoring	
	Detection Processes	
Respond	Response Planning	
	Communications	
	Analysis	
	Mitigation	
	Improvements	
Recover	Recovery Planning	
	Improvements	
	Communications	

Tabelle 3: Correlazione tra le categorie del NIST Framework e la norma ISO 16363:2012

Dalla tabella si evince che la norma ISO 16363:2012 copre ampiamente le funzioni NIST *Identify* e *Protect* e si può generalmente affermare che gli attori siano ben consapevoli dell'importanza di questi due ambiti. Ma si evince anche che le funzioni *Detect*, *Respond* e *Recover* non sono coperte. Ciò risulta anche confrontando le categorie NIST con il catalogo *nestor*[25] dei criteri per gli archivi digitali a lungo termine, uno strumento ampiamente utilizzato, perlomeno nei Paesi di lingua tedesca. Questo catalogo copre infatti gli stessi ambiti della norma ISO 16363:2012.

25 nestor-Arbeitsgruppe Vertrauenswürdige Archive - Zertifizierung. (2008). Kriterienkatalog vertrauenswürdige digitale Langzeitarchive. http://nbn-resolving.de/urn:nbn:de:0008-2008021802

5.2 Identificare (Identify)

Gestione dell'inventario (Asset Management)

Si tratta di identificare, catalogare e valutare i dati, le persone, i dispositivi, i sistemi e gli impianti dell'organizzazione. La loro criticità deve essere valutata in funzione dei processi aziendali da attuare e della strategia di rischio dell'organizzazione.

La stesura di inventari è una misura centrale per la protezione dei beni culturali digitali. Gli inventari non offrono solo una visione d'insieme e un controllo dei beni culturali da proteggere, ma documentano anche la loro origine (provenienza), la storia della loro creazione e contribuiscono a garantire la loro autenticità. Esistono sia inventari trasversali, come quello della PBC, sia inventari interni alle istituzioni, come i sistemi d'informazione archivistici, i cataloghi delle biblioteche o le banche dati per la gestione delle collezioni.

Designazione	Compito
ID.AM-1	Elaborate un processo d'inventariazione che garantisca la disponibilità permanente di un inventario completo delle risorse operative TIC (asset).
ID.AM-2	Inventariate tutte le piattaforme, le licenze e le applicazioni software all'interno della vostra organizzazione.
ID.AM-3	Catalogate tutti i flussi interni di comunicazione e di dati.
ID.AM-4	Catalogate tutti i sistemi TIC esterni che sono rilevanti per la vostra organizzazione.
ID.AM-5	Prioritzzate le risorse inventariate (dispositivi, applicazioni, dati) in funzione della loro criticità.
ID.AM-6	Definite chiaramente i ruoli e le responsabilità in materia di cybersicurezza.

Tabelle 4: Compiti ID.AM

Standard	Riferimento
CCS CSC 1	1, 2
COBIT 2019	BAI09.01, BAI09.02, BAI09.05, Dss05.02, APO02.02, APO03.03, APO03.04, PO01.02, Dss06.03
ISO 27001:2013	A.5.2, A.5.3, A.5.9, A.7.9, A.5.12, A.5.14 A.5.32, Clause 7.1, Clause 7.2
NIST-SP-800-53 Rev. 5	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-20, PS-7, PM-2, PM-5, PM-29, SA-17, SC-6, RA-9
BSI 100-2	M 2.225, M 2.393, B 2.10, M 2.193
ISO 16363	5.1

Tabelle 5: Riferimenti ID.AM

Ambiente aziendale (Business Environment)
Si tratta di priorizzare e valutare gli obiettivi, i compiti e le attività dell'azienda. Queste informazioni servono come base per attribuire le responsabilità.

Designazione	Compito
ID.BE-1	Identificate, documentate e comunicate il ruolo della vostra azienda nella catena (critica) di approvvigionamento.
ID.BE-2	Identificate e comunicate l'importanza della vostra organizzazione come infrastruttura critica e la sua posizione all'interno del settore critico.
ID.BE-3	Die Ziele, Aufgaben und Aktivitäten innerhalb der Organisation sind bewertet und priorisiert.
ID.BE-4	Definite le interdipendenze e le funzioni critiche per l'erogazione di servizi critici.
ID.BE-5	Definite per tutte le circostanze operative (p. es. sotto coazione/attacco, durante il ripristino, durante il normale funzionamento) i requisiti di resilienza per supportare l'erogazione di servizi critici.

Tabella 6: Compiti ID.BE

Standard	Riferimento
CCS CSC 1	1, 2
COBIT 2019	BAI09.01, BAI09.02, BAI09.05, Dss05.02, APO02.02, APO03.03, APO03.04, PO01.02, Dss06.03
ISO 27001:2013	A.5.19, A.5.21, A.5.23, A.5.24, A.5.28, A.5.29, A.5.30, A.5.31, A.5.33, A.5.37, A.6.2, A.7.11, A.7.12, A.7.5, A.8.14, A.8.6, A.8.30, Clause 4.1
NIST-SP-800-53 Rev. 5	CP-2, CP-8, PM-8, PM-11, PE-9, PE-11, RA-9, SA-20, SR-1, SR-2, SR-3
BSI 100-2	B 1.11, M 2.256, B 2.2, B 2.12, M 2.214
ISO 16363	3.3

Tabella 7: Riferimenti ID.BE

Direttive (Governance)
La governance regola le competenze, sorveglia e garantisce il rispetto dei requisiti normativi, giuridici e operativi dell'ambiente aziendale.

Designazione	Compito
ID.GV-1	Definite e comunicate le direttive per la sicurezza delle informazioni all'interno della vostra azienda.
ID.GV-2	Coordinate i ruoli e le responsabilità nell'ambito della sicurezza delle informazioni con i ruoli interni (p. es. della gestione dei rischi) e con i partner esterni.
ID.GV-3	SAssicuratevi che la vostra organizzazione rispetti tutte le direttive giuridiche e normative in materia di cybersicurezza, incluse quelle sulla protezione dei dati.
ID.GV-4	Assicuratevi che i cyber-rischi facciano parte della gestione aziendale dei rischi.

Tabella 8: Compiti ID.GV

Standard	Riferimento
COBIT 2019	APO01.03, EDM01.01, EDM01.02, APO13.02, MEA03.01, MEA03.04, Dss04.02
ISO 27001:2013	A.5.1, A.5.19, A.5.30, A5.31, A.6.2, A.6.6, A.8.27, A.8.30, A15.1.1, Clause 6
NIST-SP-800-53 Rev. 5	PM-1, PS-7, PM-9, PM-11
BSI 100-2	M 2.192, M 2.193, M 2.336, B 1.16
ISO 16363	3.1, 3.3, 3.4

Tabella 9: Riferimenti ID.GV

Analisi dei rischi (Risk Assessment)
L'organizzazione conosce gli effetti dei cyber-rischi sulle attività aziendali, sulle risorse operative e sul personale, inclusi i rischi per la reputazione.

Designazione	Compito
ID.RA-1	Identificate e documentate le vulnerabilità (tecniche) delle vostre risorse operative
ID.RA-2	Acquisite informazioni aggiornate sulle cyberminacce attraverso scambi regolari in forum e gruppi d'interesse.
ID.RA-3	IIdentificate e documentate le cyberminacce interne ed esterne.
ID.RA-4	Valutate il potenziale impatto delle cyberminacce sull'attività aziendale e la loro probabilità d'insorgenza
ID.RA-5	Valutate i rischi per la vostra organizzazione basandovi su minacce, vulnerabilità, impatto (sull'azienda) e probabilità d'insorgenza.
ID.RA-6	Definite e priorizzate le possibili misure urgenti da adottare quando insorge un rischio.

Tabella 10: Compiti ID.RA

Standard	Riferimento
COBIT 2019	APO12.01, APO12.02, APO12.03, APO12.04, APO 12.05, APO 13.02, Dss04.02
ISO 27001:2013	A.5.37, A.5.6, A.5.7, A.6.1, A.8.12, A8.14, A.8.16, A,8.2, A.8.3, A.8.7, A.8.8, Clause 6.1.2, Clause 6.1.3, Clause 8, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 5	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16, RA-3, PM-12, RA-2, PM-9, PM-11, SA-14
BSI 100-2	M 2.35, M 2.199, M 2.546
ISO 16363	3.4.3 (financial risks), 5.1, 5.2

Tabella 11: Riferimenti ID.RA

Strategia di gestione dei rischi
(Risk Management Strategy)
Si tratta di definire le priorità, i limiti e i rischi massimi tollerabili per l'organizzazione. I rischi operativi vengono valutati su questa base.

Designazione	Compito
ID.RM-1	Stabilite i processi di gestione dei rischi, gestiteli attivamente e fateli confermare dalle persone coinvolte e dai gruppi di riferimento.
ID.RM-2	Definite e comunicate i rischi massimi tollerabili per la vostra organizzazione.
ID.RM-3	Assicuratevi di valutare i rischi massimi tollerabili, tenendo conto dell'importanza della vostra organizzazione quale gestrice di un'infrastruttura critica. Tenete conto anche delle analisi settoriali dei rischi.

Tabella 12: Compiti ID.RM

Standard	Riferimento
COBIT 2019	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06
ISO 27001:2013	A.6.1, A.8.2, A.8.3, Clause 6.1.3, Clause 8.3, Clause 9.3
NIST-SP-800-53 Rev. 5	PM-8, PM-9, PM-11, PM-28, RA-9
ISO 16363	3.4.3 (financial risk management), 5.1, 5.2

Tabella 13: Riferimenti ID.RM

Gestione dei rischi per la catena di fornitura (Supply Chain Risk Management)
Si tratta di definire le priorità, i limiti e i rischi massimi che l'organizzazione è disposta a sopportare in relazione ai rischi legati ai fornitori.

Designazione	Compito
ID.SC-1	Identificate, stabilite, valutate e amministrate i processi per la gestione dei rischi nella catena di fornitura informatica. Gli attori coinvolti sono d'accordo sui processi scelti.
ID.SC-2	Identificate e priorizzate i fornitori e gli erogatori di sistemi informativi, componenti e servizi e valutateli secondo un processo di valutazione dei rischi per la catena di fornitura informatica (vedi ID.SC-1).
ID.SC-3	Controllate regolarmente i fornitori e gli offerenti terzi tramite audit, test o altre forme di valutazione per assicurarvi che rispettino gli obblighi contrattuali.
ID.SC-4	Applicate un monitoring per assicurarvi che tutti i vostri fornitori ed erogatori di servizi rispettino i loro obblighi secondo le direttive. Fatevelo confermare regolarmente nei rapporti degli audit o dai risultati dei test tecnici.
ID.SC-5	Definite i processi d'intervento e di ripristino con i vostri fornitori ed erogatori di servizi in caso di incidenti di cybersicurezza. Testate questi processi nell'ambito di esercitazioni.

Tabella 14: Compiti ID.SC

Standard	Riferimento
COBIT 2019	APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05
ISO 27001:2013	A.5.19, A.5.20, A.5.21, A.5.22, A.5.29, A.6.6, A.8.30, Clause 8.3
NIST-SP-800-53 Rev. 5	SA-9, SA-12, PM-9, RA-2, RA-3, SA-14, SA-15, SA-11, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
BSI	B 1.11, B 1.17, M 2.256, B 1.3
ISO 16363	3.5

Tabella 15: Riferimenti ID.SC

5.3 Proteggere (Protect)

Gestione e controllo degli accessi (Access Control)
L'accesso fisico e logico alle risorse operative e alle installazioni TIC è possibile solo per le persone, i processi e i dispositivi autorizzati. Allo stesso modo, l'accesso è possibile solo per le attività consentite.

Designazione	Compito
PR.AC-1	Stabilite un processo chiaro per la concessione e la gestione delle autorizzazioni e dei dati d'accesso per gli utenti, i dispositivi e i processi.
PR.AC-2	Assicuratevi che solo le persone autorizzate abbiano accesso fisico alle risorse operative TIC. Adottate misure (edilizie) per proteggere le risorse operative TIC contro qualsiasi accesso fisico non autorizzato.
PR.AC-3	Stabilite i processi per la gestione dell'accesso remoto.
PR.AC-4	Definite i diritti d'accesso e le autorizzazioni tenendo conto dei principi del privilegio minimo e della separazione dei compiti.
PR.AC-5	Assicuratevi che l'integrità della vostra rete sia protetta. Separate logicamente e fisicamente la vostra rete, se necessario e ragionevole.
PR.AC-6	Assicuratevi che le identità digitali siano assegnate a persone o processi inequivocabilmente verificati.
PR.AC-7	Autentificate gli utenti, i dispositivi e altri asset (p. es. autenticazione a uno o più fattori) in funzione del rischio della transazione (p. es. rischi per la sicurezza e la protezione dei dati personali e altri rischi aziendali).

Tabella 16: Compiti PR.AC

Standard	Riferimento
COBIT 2019	Dss05.04, Dss06.03, Dss01.04, Dss05.05, APO13.01, Dss01.04, Dss05.03, Dss05.04, Dss05.07, BAI08.03
ISO 27001:2013	A.5.14, A.5.15, A.5.16, A.5.17, A.5.18, A.5.21, A.5.22, A.5.23, A.5.3, A.5.34, A.6.1, A.6.7, A.7.1, A.7.2. A.7.3, A.7.4, A.7.5, A.7.6, A.7.9, A.8.1, A.8.5, A.8.11, A.15, A.8.16, A.8.18, A.8.2, A.8.3, A.8.5, A.8.20, A.8.22, A.8.27, A.8.31
NIST-SP-800-53 Rev. 5	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-10, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, SC-15, IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12, PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9, SC-7, SC-10, SC-20, PS-3
BSI	M 2.30, M 2.220, M 2.11, M 4.15, M 1.79, M 2.17, B 2.2, B 2.12, B 5.8, B 4.1, M 2.393, M 2.5, B 1.18, M 2.8, M 4.135, B 4.1, M 5.77, M 2.393, M 3.33, M 2.31, M 2.586
ISO 16363	4.6

Tabella 17: Riferimenti PR.AC

Sensibilizzazione e formazione (Awareness and Training)
Si tratta di formare e addestrare regolarmente e adeguatamente i collaboratori e i partner esterni in tutti gli aspetti della cybersicurezza. Essi devono svolgere i loro compiti inerenti alla sicurezza secondo le direttive e i processi pertinenti.

Designazione	Compito
PR.AT-1	Assicuratevi che tutti i collaboratori siano informati e formati sulla cybersicurezza.
PR.AT-2	Assicuratevi che gli utenti con livelli di autorizzazione elevati siano consapevoli del loro ruolo e delle loro responsabilità.
PR.AT-3	Assicuratevi che tutti gli attori esterni alla vostra azienda (fornitori, clienti, partner) siano consapevoli del loro ruolo e delle loro responsabilità.
PR.AT-4	Assicuratevi che tutti i quadri siano consapevoli del loro ruolo e delle loro responsabilità.
PR.AT-5	Assicuratevi che i responsabili della sicurezza fisica e della sicurezza delle informazioni siano consapevoli del loro ruolo e della loro responsabilità.

Tabella 18: Compiti PR.AT

Standard	Riferimento
COBIT 2019	APO07.03, BAI05.07, APO07.02, Dss06.03, APO07.03, APO10.04, APO10.05
ISO 27001:2013	A.5.19, A.5.2, A.5.4, A.6.2, A.6.3, A.6.6, A.7.2, A.7.3, A.7.6, A.8.18, A.8.2, A.8.3, A.8.30, Clause 5.1, Clause 5.3
NIST-SP-800-53 Rev. 5	AT-2, AT-3, PM-13, PS-7, SA-9, PM-7
BSI	M 2.193, B 1.13
ISO 16363	3.2

Tabella 19: Riferimenti PR.AT

Sicurezza dei dati (Data Security)
Si tratta di gestire le informazioni, i dati e i supporti dati in modo tale da proteggere la riservatezza, l'integrità e la disponibilità dei dati secondo la strategia contro i rischi adottata dall'azienda.

Designazione	Compito
PR.DS-1	Assicuratevi che i dati memorizzati siano protetti (da violazioni di riservatezza, integrità e disponibilità).
PR.DS-2	Assicuratevi che i dati siano protetti durante la loro trasmissione (da violazioni di riservatezza, integrità e disponibilità).
PR.DS-3	Assicuratevi che per le vostre risorse operative TIC venga stabilito un processo formale finalizzato a proteggere i dati quando queste risorse vengono soppresse, spostate o sostituite.
PR.DS-4	Assicuratevi che le vostre risorse operative TIC abbiano capacità di riserva sufficienti per garantire la disponibilità dei dati.
PR.DS-5	Assicuratevi che vengano adottate misure adeguate contro la fuga di dati (Data Leak).
PR.DS-6	Stabilite un processo per verificare l'integrità dei firmware, sistemi operativi, software applicativi e dati.
PR.DS-7	Create un ambiente informatico per lo sviluppo e i test che sia completamente indipendente dai sistemi produttivi.
PR.DS-8	Stabilite un processo per verificare l'integrità dell'hardware utilizzato.

Tabella 20: Compiti PR.DS

Standard	Riferimenti
COBIT 2019	APO01.06, BAI02.01, BAI06.01, Dss06.06, BAI09.03, APO13.01, BAI07.04, BAI03.05.4
ISO 27001:2013	A.5.7, A.5.10, A.5.13, A.5.14, A.5.15, A.5.23, A.5.24, A.5.29, A.5.33, A.5.34, A.6.1, A.6.2, A.6.5, A.6.6, A.7.5, A.7.8, A.7.9, A.7.10, A.7.14, A.8.1, A.8.11, A.8.12, A.8.13, A.8.14, A.8.16, A.8.18, A.8.19, A.8.2, A.8.20, A.8.22, A.8.23, A.8.24, A.8.26, A.8.28, A.8.29, A.8.31, A.8.34, A.8.3, A.8.4, A.8.6, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-4, AC-5, AC-6, AU-4, AU-13, CM-2, CM-8, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, CP-2, PE-11, PE-16, PE-19, PE-20, PS-6, SA-10, SC-5, SC-7, SC-8, SC-11, SC-28, SI-4, SI-7, SI-10
BSI	M 2.217, B 4.1, M 2.393, B 5.3, B 5.4, B 5.21, B 5.24, B 1.7, M 2.3, B 1.15, M 5.23, M 3.33, M 2.226, M 3.2, M 3.6, B 1.18, M 2.220, M 2.8, M 4.135, M 4.494, M 5.77, M 2.393, B 5.3, M 3.55, B 5.4, B 5.21, B 5.24, B 1.6, B 1.9, M 2.62, M 2.4
ISO 16363	5.1

Tabella 21: Riferimenti PR.DS

Linee guida per la protezione delle informazioni (Information Protection Processes and Procedures)
Esistono linee guida per la protezione dei sistemi informativi e delle risorse operative TIC. Esse descrivono almeno lo scopo, il campo d'applicazione, i ruoli e le responsabilità e regolano il coordinamento in seno all'organizzazione. Si tratta di applicare queste linee guida per proteggere i sistemi informativi e le risorse operative.

Designazione	Compito
PR.IP-1	Definite una configurazione standard per l'infrastruttura di informazione e comunicazione e per i sistemi di controllo industriali. Assicuratevi che questa configurazione sia conforme ai principi di sicurezza abituali (p. es. ridondanza N-1, configurazione minima, ecc.).
PR.IP-2	Stabilite un processo di ciclo di vita per l'utilizzo delle risorse operative TIC.
PR.IP-3	Stabilite un processo per controllare le modifiche di configurazione.
PR.IP-4	Assicuratevi che le copie di sicurezza (backup o sincronizzazione) dei vostri dati vengano eseguite, gestite e testate regolarmente (testate la ripristinabilità delle copie).
PR.IP-5	Assicuratevi che tutte le direttive (normative) e le linee guida concernenti i mezzi operativi fisici vengano rispettate.
PR.IP-6	Assicuratevi che i dati vengano distrutti secondo le direttive.
PR.IP-7	Assicuratevi che i vostri processi per la sicurezza delle informazioni vengano continuamente sviluppati e migliorati.
PR.IP-8	Discutete l'efficacia delle diverse tecnologie di protezione con i vostri partner.
PR.IP-9	Stabilite i processi di reazione agli incidenti informatici (Incident Response-Planning, Business Continuity Management, Incident Recovery, Disaster Recovery).
PR.IP-10	Testate i piani d'intervento e di ripristino.
PR.IP-11	Tenete conto degli aspetti della cybersicurezza già nel processo d'assunzione di personale (p. es. tramite controlli del background/controlli di sicurezza relativi alle persone).
PR.IP-12	Sviluppate e implementate un processo per trattare i punti deboli individuati.

Tabella 22: Compiti PR.IP

Standard	Riferimento
COBIT 2019	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI06.01, BAI01.06, APO13.01, Dss01.04, Dss05.05, BAI09.03, APO11.06, Dss04.05, Dss04.03, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
ISO 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.16.1.6, A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3, A.12.6.1, A.18.2.2
NIST-SP-800-53 Rev. 5	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8, CP-4, CP-6, CP-9, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18, MP-6, A-2, CA-7, CP-2, IR-8, PL-2, PM-6, AC-21, CA-7, SI-4, CP-2, IR-8, IR-3, PM-14, RA-3, RA-5, SI-2
BSI	B 1.4, B 1.3, M 2.217, B 1.14, B 1.9, M 2.62, B 5.27, M 4.78, M 2.9, B 1.0, M 2.80, M 2.546, B 5.27, B 5.21, B 5.24
ISO 16363	3.3, 4.1, 4.2, 4.5

Tabella 23: Riferimenti PR.IP

Manutenzione (Maintenance)
Si tratta di eseguire i lavori di manutenzione e riparazione dei componenti del sistema TIC secondo le linee guida e i processi vigenti.

Designazione	Compito
PR.MA-1	Assicuratevi che l'esercizio, la manutenzione e le eventuali riparazioni delle risorse operative vengano registrati e documentati (Logging). Assicuratevi che queste operazioni vengano eseguite tempestivamente e solo con mezzi testati e approvati.
PR.MA-2	Assicuratevi che i lavori di manutenzione sui vostri sistemi che sono eseguiti in remoto vengano registrati e documentati. Assicuratevi che non sia possibile alcun accesso non autorizzato.

Tabella 24: Compiti PR.MA

Standard	Riferimento
COBIT 2019	BAI09.03, Dss05.04, APO11.04, Dss05.02, APO13.01
ISO 27001:2013	A.5.14, A.5.15, A.5.19, A.5.22, A.6.7, A.7.13, A.8.2, A.8.9, A.8.15, A.8.16
NIST-SP-800-53 Rev. 5	MA-1, MA-2, MA-3, MA-4, MA-5, MA-6
BSI	M 2.17, M 2.4, M 2.218, B 1.11, B 1.17, M 2.256
ISO 16363	4.3, 5.2.1

Tabella 25: Rifermimenti PR.MA

Impiego di tecnologie di protezione (Protective Technology)
Si tratta di installare soluzioni tecniche di sicurezza per garantire la sicurezza e la resilienza dei sistemi TIC e dei dati secondo le direttive e i processi.

Designazione	Compito
PR.PT-1	Definite le direttive per gli audit e le registrazioni dei registri (log). Create e controllare regolarmente i log secondo le direttive e le linee guida.
PR.PT-2	Assicuratevi che i supporti rimovibili siano protetti e vengano utilizzati solo in conformità alle linee guida.
PR.PT-3	Assicuratevi che il vostro sistema sia configurato in modo da garantire sempre la funzionalità minima.
PR.PT-4	Assicuratevi che le vostre reti di comunicazione e di comando siano protette.
PR.PT-5	Assicuratevi che siano implementati i meccanismi (p. es. fail-safe, bilanciamento del carico, hot-swap) volti a garantire la sicurezza contro le interruzioni sia in situazioni normali che avverse.

Tabella 26: Compiti PR.PT

Standard	Riferimento
COBIT 2019	APO11.04, Dss05.02, APO13.01, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, Dss01.05
ISO 27001:2013	A.5.14, A.5.15, A.5.18, A.5.29, A.5.30, A.5.34, A.5.37, A.8.11, A.8.13, A.8.14, A.8.15, A.8.16, A.8.20, A.8.21, A.8.22, A.8.2, A.8.3, A.8.34, A.8.5, A.8.6, A.8.9, A.9.2, A.5.10, A.6.7, A.7.10, A.7.14, A.8.24
NIST-SP-800-53 Rev. 5	AC-3, AC-4, AC-17, AC-18, AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16, CM-7, CP-7, CP-8, CP-11, CP-12, CP-13, MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, PE-11, PL-8, SC-6, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
BSI	B 5.22, M 2.500, M 2.220, M 2.64, M 4.227, M 2.64, B 1.18, B 4.1, M 2.393, B 1.3, B 2.4, B 2.9
ISO 16363	4.4

Tabella 27: Riferimento PR.PT

5.4 Individuare (Detect)

Anomalie e incidenti (Anomalies and Events)

Si tratta di fare in modo che i collaboratori individuino tempestivamente le anomalie e gli incidenti rilevanti per la sicurezza e conoscano le loro potenziali conseguenze.

Designazione	Compito
DE.AE-1	Definite valori standard per le operazioni di rete consentite e i flussi di dati attesi per gli utenti e i sistemi. Adeguate continuamente questi valori.
DE.AE-2	Assicuratevi che gli incidenti di cybersicurezza individuati vengano analizzati in relazione ai loro obiettivi e metodi.
DE.AE-3	Assicuratevi che le informazioni sugli incidenti di cybersicurezza provenienti da varie fonti e vari sensori vengano raggruppate e trattate.
DE.AE-4	Stabilite le conseguenze di possibili eventi.
DE.AE-5	Definite i valori di soglia per l'allerta sugli incidenti.

Tabella 28: Compiti DE.AE

Standard	Riferimento
COBIT 2019	Dss03.01, APO12.06
ISO 27001:2013	A.5.24, A.5.25, A.5.27, A.5.28, A.5.37, A.8.1, A.8.12, A.8.15, A.8.16, A.8.20, A.8.21, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-4, AU-6, CA-3, CA-7, CM-2, CP-2, SI-4, IR-4, IR-5, IR-8, SC-16, SI-4, RA-3, RA-5
BSI	B 1.8

Tabella 29: Riferimenti DE.AE

Sorveglianza (Security Continuous Monitoring)
Si tratta di sorvegliare a intervalli regolari il sistema TIC, incluse tutte le risorse operative, da un lato per individuare gli incidenti di cybersicurezza, e dall'altro per verificare l'efficacia delle misure di protezione.

Designazione	Compito
DE.CM-1	Istituite un monitoraggio continuo della rete per individuare potenziali incidenti di cybersicurezza.
DE.CM-2	Istituite un monitoraggio/una sorveglianza continua di tutte le risorse operative fisiche e degli edifici al fine di individuare gli incidenti di cybersicurezza.
DE.CM-3	Sorvegliate le attività dei collaboratori per individuare potenziali incidenti di cybersicurezza.
DE.CM-4	Assicuratevi che sia possibile individuare i malware.
DE.CM-5	Assicuratevi che sia possibile individuare i malware sui dispositivi mobili.
DE.CM-6	Assicuratevi che le attività dei fornitori di servizi esterni vengano sorvegliate al fine di individuare eventuali incidenti di cybersicurezza.
DE.CM-7	Sorvegliate costantemente il vostro sistema per individuare le attività/gli accessi da parte di persone, dispositivi e software non autorizzati.
DE.CM-8	Eseguite scansioni delle vulnerabilità.

Tabella 30: Compiti DE.CM

Standard	Riferimento
COBIT 2019	Dss05.01, Dss05.07, APO07.06, BAI03.10
ISO 27001:2013	A.5.14, A.5.15, A.5.18, A.5.19, A.5.21, A.5.23, A.5.7, A.6.7, A.7.1, A.7.2, A.7.4, A.7.8, A.7.9, A.8.1, A.8.11, A.8.12, A.8.15, A.8.16, A.8.19, A.8.2, A.8.20, A.8.21, A.8.23, A.8.28, A.8.3, A.8.30, A.8.5, A.8.7, A.8.8
NIST-SP-800-53 Rev. 5	AC-2, AU-12, AU-13, CA-7, CM-3, CM-8, CM-10, CM-11, PE-6, PE-20, PS-7, RA-5, SA-4, SA-9, SC-5, SC-7, SC-18, SC-44, SI-3, SI-4, SI-8
BSI	B 5.22, M 2.500, B 1.6, B 2.9, B 1.9, B 5.25, B 1.11, M 2.256, M 2.35

Tabella 31: Riferimenti DE.CM

Processo di individuazione (Detection Processes)
Si tratta di gestire, testare e aggiornare i processi e le istruzioni per individuare gli incidenti di cybersicurezza.

Designazione	Compito
DE.DP-1	Definite ruoli e responsabilità inequivocabili, in modo che sia ben chiaro chi è responsabile di cosa e chi ha quali competenze.
DE.DP-2	Assicuratevi che i processi di individuazione rispettino tutte le direttive e condizioni vigenti.
DE.DP-3	Testate i vostri processi di individuazione
DE.DP-4	Comunicate gli incidenti individuati alle parti competenti (fornitori, clienti, partner, autorità, ecc.).
DE.DP-5	Migliorate continuamente i processi di individuazione.

Tabella 32: Compiti DE.DP

Standard	Riferimento
COBIT 2019	Dss05.01, APO13.02, APO12.06, APO11.06, Dss04.05
ISO 27001:2013	A.5.2, A.5.26, A.5.27, A.5.3, A.5.35, A.5.4, A.6.3, A.6.8, A.7.4, A.8.12, A.8.15, A.8.16, A.8.17, A.8.27, A.8.6, A.8.7, A.8.8, A.8.9, Clause 5.3, Clause 7.2, Clause 9.2, Clause 10.1
NIST-SP-800-53 Rev. 5	AC-1, AT-1, AU-1, AU-6, CA-1, CA-2, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-1, PM-14, PS-1, PT-1, RA-1, RA-5, SA-1, SC-1, SI-1, SI-3, SI-4, SR-1, SR-9, SR-10
BSI	M 2.193, M 2.568, B 1.8

Tabella 33: Riferimenti DE.DP

5.5 Reagire (Respond)

Piano d'intervento (Response Planning)

È disponibile un piano d'intervento per gestire gli incidenti di cybersicurezza individuati. Si tratta di adottare le misure volte a garantire che il piano d'intervento venga attuato correttamente e tempestivamente in caso d'incidente.

Designazione	Compito
RS.RP-1	Assicuratevi che il piano d'intervento venga attuato correttamente e tempestivamente durante o dopo un incidente di cybersicurezza individuato.

Tabella 34: Compiti RS.RP

Standard	Riferimento
COBIT 2019	BAI01.10
ISO 27001:2013	A.5.26, A.5.28, A.5.29
NIST-SP-800-53 Rev. 5	CP-2, CP-10, IR-4, IR-8
BSI	B 1.8

Tabella 35: Riferimenti RS.RP

Comunicazione (Communications)
Si tratta di coordinare i processi d'intervento con tutti gli attori interni ed esterni. In caso d'incidente, ci si deve assicurare di ricevere il supporto degli organi statali, se necessario e opportuno.

Designazione	Compito
RS.CO-1	Assicuratevi che tutti i collaboratori conoscano i loro compiti e la sequenza per reagire a un incidente di cybersicurezza.
RS.CO-2	Definite i criteri per la segnalazione e assicuratevi che gli incidenti di cybersicurezza vengano segnalati e trattati secondo questi criteri.
RS.CO-3	Condividete secondo i criteri predefiniti le informazioni e i risultati sugli incidenti di cybersicurezza individuati.
RS.CO-4	Coordinatevi con tutti i partecipanti e i gruppi di riferimento conformemente ai piani d'intervento e secondo i criteri predefiniti
RS.CO-5	Scambiate regolarmente e volontariamente informazioni con gli attori esterni al fine di aumentare la consapevolezza dell'attuale situazione di cybersicurezza.

Tabella 36: Compiti RS.CO

Standard	Riferimento
COBIT 2019	nessuno
ISO 27001:2013	A.5.2, A.5.24, A.5.26, A.5.3, A.5.30, A.5.37, A.5.5, A.5.6, A.6.3, A.6.8, A.7.4
NIST-SP-800-53 Rev. 5	AU-6, CP-2, CP-3, IR-3, IR-4, IR-6, IR-8, PM-15, SI-5
BSI	B 1.3, B 1.8, M 2.193

Tabella 37: Riferimenti RS.CO

Analisi (Analysis)
Si tratta di svolgere delle analisi periodiche in modo che sia possibile reagire adeguatamente agli incidenti di cybersicurezza.

Designazione	Compito
RS.AN-1	Assicuratevi che si tenga conto delle segnalazioni dei sistemi di individuazione e che vengano avviate le indagini.
RS.AN-2	Assicuratevi che si conoscano e capiscano le conseguenze di un incidente di cybersicurezza.
RS.AN-3	Eseguite analisi forensi dopo un incidente di cybersicurezza.
RS.AN-4	Stabilite processi per individuare, analizzare e colmare le lacune di cui la vostra organizzazione viene a conoscenza da fonti interne ed esterne.

Tabella 38: Compiti RS.ANv

Standard	Riferimento
COBIT 2019	Dss02.07
ISO 27001:2013	A.5.19, A.5.25, A.5.26, A.5.27, A.5.28, A.5.35, A.5.5, A.5.6, A.6.3, A.8.15, A.8.16, A.10.2
NIST-SP-800-53 Rev. 5	AU-6, AU-7, CA-1, CA-2, CA-7, CP-2, IR-4, IR-5, IR-8, PE-6, PM-4, PM-15, RA-1, RA-3, RA-5, RA-7, SI-4, SI-5, SR-6
BSI	B 5.22, M 2.500, M 2.64, B 1.8

Tabella 39: Riferimenti RS.AN

Mitigazione dei danni (Mitigation)
Si tratta di agire in modo da evitare la propagazione di un incidente di cybersicurezza e limitare i potenziali danni.

Designazione	Compito
RS.MI-1	Assicuratevi che sia possibile contenere gli incidenti di cybersicurezza e impedire la loro propagazione.
RS.MI-2	Assicuratevi che sia possibile mitigare le conseguenze degli incidenti di cybersicurezza
RS.MI-3	Assicuratevi che le nuove vulnerabilità identificate vengano ridotte o documentate come rischi accettabili.

Tabella 40: Compiti RS.MI

Standard	Riferimento
COBIT 2019	nessuno
ISO 27001:2013	A.5.26, A.8.23, A.8.8
NIST-SP-800-53 Rev. 5	IR-4, CA-2, CA-7, RA-3, RA-5, RA-7
BSI	B 1.6, B 1.8, M 2.35

Tabella 41: Riferimenti RS.MI

Miglioramenti (Improvements)
Si tratta di migliorare continuamente la reattività dell'organizzazione in caso di incidenti di cybersicurezza, traendo insegnamento dagli incidenti precedenti.

Designazione	Compito
RS.IM-1	Assicuratevi che i risultati e gli insegnamenti tratti dai precedenti incidenti di cybersicurezza confluiscano nei vostri piani d'intervento.
RS.IM-2	Aggiornate le vostre strategie d'intervento.

Tabella 42: Compiti RS.IM

Standard	Riferimento
COBIT 2019	BAI01.13
ISO 27001:2013	A.5.27, A.10.1, Clause 10
NIST-SP-800-53 Rev. 5	CP-2, IR-4, IR-8
BSI	B 1.8

Tabella 43: Riferimenti RS.IM

5.6 Ripristinare (Recover)

Piano di ripristino (Recovery Planning)
Si tratta di preparare ed eseguire i processi di ripristino in modo tale da poter ripristinare rapidamente i sistemi.

Designazione	Compito
RC.RP-1	Assicuratevi che sia possibile attuare correttamente il piano di ripristino dopo un incidente di cybersicurezza.

Tabella 44: Compiti RC.PR

Standard	Riferimento
COBIT 2019	Dss02.05, Dss03.04
ISO 27001:2013	A.5.29, A.5.30, A.5.37
NIST-SP-800-53 Rev. 5	CP-10, IR-4, IR-8

Tabella 45: Riferimenti RC.PR

Miglioramenti (Improvements)
Si tratta di migliorare continuamente i processi di ripristino traendo insegnamento dai ripristini precedenti.

Designazione	Compito
RC.IM-1	Assicuratevi che i risultati e gli insegnamenti tratti da precedenti incidenti di cybersicurezza confluiscano nei vostri piani di ripristino.
RC.IM-2	Aggiornate la vostra strategia di ripristino.

Tabella 46: Compiti RC.IM

Standard	Riferimento
COBIT 2019	BAI05.07
ISO 27001:2013	A.5.27, A.10.1, Clause 10
NIST-SP-800-53 Rev. 5	CP-2, IR-4, IR-8

Tabella 47: Riferimenti RC.IM

Comunicazione (Communications)
Si tratta di coordinare le attività di ripristino con partner interni ed esterni (p. es. provider di servizi Internet, CERT, autorità, integratori di sistemi, ecc.).

Designazione	Compito
RC.CO-1	Elaborate preventivamente un piano di comunicazione per le relazioni pubbliche in caso di incidenti di cybersicurezza.
RC.CO-2	Ripristinate la buona reputazione della vostra organizzazione dopo un incidente di cybersicurezza.
RC.CO-3	Comunicate le attività di ripristino a tutti gli attori interni ed esterni, in particolare ai membri del management e della direzione aziendale.

Tabella 48: Compiti RC.CO

Standard	Riferimento
COBIT 2019	EDM03.02
ISO 27001:2013	A.5.24, A.5.26, A.5.5, A.6.3, Clause 7.4
NIST-SP-800-53 Rev. 5	CP-2, IR-4

Tabella 49: Riferimenti RC.CO

6 Moduli per migliorare la sicurezza delle informazioni

L'Assessment Framework (quadro di valutazione) utilizzato nel capitolo 5 è un valido ausilio per rilevare la cybersicurezza e pianificare i miglioramenti nelle istituzioni della memoria. Le organizzazioni più grandi (p. es. a livello cantonale o federale) con risorse adeguate e personale qualificato saranno in grado di attuare integralmente questa raccomandazione. È possibile che stiano già utilizzando il Framework proposto in questo documento o uno simile. Alla salvaguardia del patrimonio culturale partecipano però attori molto eterogenei. Alcune infrastrutture critiche sono paragonabili per dimensioni (numero di collaboratori e risorse disponibili per la sicurezza delle informazioni) a piccole aziende o microimprese. L'attuazione completa del Framework metterebbe queste istituzioni di fronte a grandi sfide. Per tenerne conto e attuare comunque una strategia Defense in Depth efficace, si raccomanda alle istituzioni più piccole di concentrarsi sui moduli essenziali, menzionati in questo capitolo, per migliorare la sicurezza delle informazioni.

Una piccola istituzione ha normalmente piccole collezioni digitali, poca affluenza di pubblico e risorse umane e finanziarie limitate. Potrebbe ad esempio trattarsi dell'archivio comunale di una piccola città o di un archivio specializzato che raccoglie fondi e lasciti su una particolare area tematica. Questo capitolo spiega come un'istituzione di questo tipo possa attuare i punti centrali della strategia Defense in Depth (vedi cap. 4) con scarse risorse. Le piccole istituzioni della memoria sono spesso integrate in organizzazioni informatiche più grandi (p. es. servizi informatici cittadini, cantonali o universitari). Esse devono quindi fare tutto il possibile per sfruttare le sinergie e integrarsi nell'unità sovraordinata più grande.

Le singole istituzioni non devono quindi adottare per forza tutte le misure, ma solo quelle che sono necessarie per proteggere i loro processi critici e i loro sistemi informatici. Una raccolta di misure e raccomandazioni per migliorare la sicurezza delle informazioni è stata compilata dall'ufficio federale tedesco competente (Bundesamt für Sicherheit in der Informationstechnik, BSI).[26] I moduli sono suddivisi nelle seguenti tre categorie, già descritte nel capitolo 4 Defense in Depth:

- Misure organizzative (gestione della sicurezza, organizzazione e processi)
- Misure tecniche (sistemi)
- Misure fisiche (edifici, locali)

Il NIST Framework dice cosa si deve fare per la valutazione (Assestement). Questo capitolo sui moduli per la protezione dell'informazione dà un'idea su come procedere.

26 I moduli del BSI possono essere scaricati dall'indirizzo: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

6.1 Gestione della sicurezza

L'obiettivo di questo modulo è stabilire una gestione globale della sicurezza nell'istituzione, al fine di ancorare la sicurezza delle informazioni come un processo continuo.

Nelle misure previste da questo modulo rientrano la definizione degli obiettivi e dei requisiti di sicurezza, l'introduzione dei processi di sicurezza, la definizione delle responsabilità e delle competenze, la formazione e la sensibilizzazione dei collaboratori nonché l'elaborazione di piani d'emergenza.

Con questo modulo si vuole instaurare una cultura di miglioramento sistematico e continuo della sicurezza delle informazioni in seno all'organizzazione. Attraverso una gestione globale della sicurezza si riducono al minimo i rischi e si raggiunge un livello di sicurezza adeguato per i sistemi e i dati informatici.

Standard	Riferimento
BSI IT-G 2023	ISMS.1

6.2 Moduli di processo

Organizzazione

L'obiettivo di questo modulo è creare un'**organizzazione** efficiente ed efficace, in grado di individuare proattivamente e di ridurre al minimo i rischi per la sicurezza informatica.

Nelle misure previste da questo modulo rientrano tra l'altro la definizione delle strutture organizzative e dei processi per la sicurezza delle informazioni, l'attribuzione delle responsabilità e delle competenze e l'elaborazione di linee guida per la sicurezza. Dato che la maggior parte degli archivi è integrata in una struttura informatica ufficiale e sovraordinata, è molto importante chiarire le competenze specialistiche e tecniche.

Il modulo **Organizzazione** attribuisce molto peso anche alla stretta collaborazione e comunicazione tra le divisioni e i collaboratori di un'azienda o di un'autorità. L'obiettivo è creare una consapevolezza comune dell'importanza della sicurezza delle informazioni e coinvolgere tutte le parti nei processi di sicurezza. Come già accennato, ciò è di grande importanza per coordinare le esigenze professionali e tecniche tra gli archivi e i servizi informatici.

Adottando le misure di questo modulo, un'istituzione può sviluppare la sua forma **organizzativa** in modo tale che la sicurezza delle informazioni diventi parte integrante della sua attività aziendale.

Standard	Riferimento
BSI IT-G 2023	ORP.1

Personale

Questo modulo tratta il tema della sicurezza delle informazioni in relazione ai collaboratori di un'istituzione. L'obiettivo è garantire che i collaboratori siano sufficientemente sensibilizzati e formati per contribuire alla sicurezza dei sistemi informatici e dei dati.

Nelle misure previste da questo modulo rientrano tra l'altro la definizione dei requisiti di sicurezza per i collaboratori, la sensibilizzazione e la formazione sulla sicurezza delle informazioni e il rispetto delle norme di sicurezza. Si tratta di adottare precauzioni per ridurre al minimo la perdita di know-how in caso d'assenza di personale, per esempio durante una pandemia. Inoltre, le qualifiche dei collaboratori addetti alla sicurezza delle informazioni devono essere sviluppate in modo mirato.

Un'ulteriore misura per le istituzioni con dati sensibili e rilevanti per la sicurezza è quella di eseguire un controllo di sicurezza relativo alle persone al momento dell'assunzione di nuovo personale.[27]

Standard	Riferimento
BSI IT-G 2023	ORP.2

27 A livello federale compete all'organo di controllo della sicurezza relativo alle persone (CSP) del DDPS: https://www.sepos.admin.ch/it/controllo-di-sicurezza-relativo-alle-persone

Sensibilizzazione e formazione

L'obiettivo di questo modulo è sensibilizzare e formare i collaboratori di aziende e autorità sulla sicurezza delle informazioni. Solo così potranno svolgere adeguatamente i loro compiti nell'ambito della sicurezza delle informazioni e contribuire a ridurre al minimo i rischi.

Nelle misure previste da questo modulo rientrano tra l'altro la definizione degli obiettivi di formazione e sensibilizzazione, la scelta di formati e metodi didattici adeguati, la pianificazione e l'esecuzione di corsi nonché le misure di sensibilizzazione.

Le misure di formazione e sensibilizzazione devono essere adattate ai bisogni e alle esigenze specifiche dei collaboratori, anche in funzione dei pericoli specifici a cui l'istituzione è esposta. Queste misure dovrebbero essere adottate regolarmente, soprattutto con i nuovi collaboratori, e si dovrebbe coinvolgere anche la direzione per sottolineare l'importanza della sicurezza dell'informazione nell'istituzione.

Standard	Riferimento
BSI IT-G 2023	ORP.3

Gestione delle identità e delle autorizzazioni

Questo modulo tratta la gestione delle identità e delle autorizzazioni all'interno di un'istituzione. Il suo obiettivo è garantire che solo le persone autorizzate abbiano accesso ai sistemi e ai dati informatici.

Nelle misure previste da questo modulo rientrano tra l'altro la definizione dei ruoli e delle autorizzazioni per i collaboratori, l'implementazione di meccanismi di controllo degli accessi, la verifica delle identità e delle autorizzazioni nonché lo svolgimento di audit sul controllo degli accessi. Una misura fondamentale è separare la gestione delle identità e delle autorizzazioni dall'informatica d'ufficio e dall'archivio digitale.

Il modulo Gestione delle identità e delle autorizzazioni comprende anche la gestione appropriata dei dati di accesso e l'uso dell'autenticazione a due fattori per aumentare la sicurezza degli accessi.

Standard	Riferimento
BSI IT-G 2023	ORP.4

Gestione della conformità (Compliance Management)

Questo modulo tratta la conformità ai requisiti legali, normativi e contrattuali nell'ambito della sicurezza delle informazioni. Il suo obiettivo è garantire che l'istituzione rispetti le condizioni essenziali e riduca quindi al minimo i rischi giuridici e normativi.

Nelle misure previste da questo modulo rientrano tra l'altro l'identificazione e la sorveglianza dei requisiti legali, normativi e contrattuali, l'integrazione dei requisiti di conformità nel concetto di sicurezza informatica, la documentazione dei requisiti di conformità e l'esecuzione dei controlli di conformità. Questi requisiti comprendono in particolare anche norme e standard di archiviazione e buone pratiche (Best Practices).

Il modulo Gestione della conformità comprende inoltre un controllo periodico della conformità ai requisiti e l'integrazione degli aspetti di conformità nella pianificazione e nella realizzazione dei progetti informatici. Si presentano qui delle interfacce con il sottosettore critico dell'amministrazione, poiché si deve già tenere conto dell'archiviazione nella pianificazione e nell'introduzione di nuovi sistemi.

Standard	Riferimento
BSI IT-G 2023	ORP.5

Protezione dei dati
Questo modulo tratta la protezione dei dati personali all'interno di un'organizzazione. Il suo obiettivo è garantire che i dati personali vengano trattati e protetti secondo le disposizioni legali.

Nelle misure previste da questo modulo rientrano tra l'altro la stima delle conseguenze per la protezione dei dati, l'adozione di misure tecniche e organizzative per la protezione dei dati personali, la formazione dei collaboratori sul trattamento dei dati personali e il controllo del rispetto delle norme di protezione dei dati.

Il modulo Protezione dei dati è incentrato sulla conformità ai principi di protezione dei dati, come l'economia dei dati, la finalità e la trasparenza, nonché sulla tutela dei diritti delle persone interessate, come ad esempio il diritto di accesso, cancellazione o rettifica dei dati.

Adottando le misure di questo modulo, l'istituzione garantisce che i dati personali vengano trattati e protetti secondo le disposizioni legali, il che rafforza la fiducia degli enti che li forniscono e degli utenti e riduce al minimo i rischi giuridici.

Standard	Riferimento
BSI IT-G 2023	CON.2

Concetto per il backup dei dati
Questo modulo tratta l'elaborazione e l'attuazione di un concetto per il backup dei dati archiviati e dei metadati. Il suo obiettivo è garantire la disponibilità e l'integrità di questi dati e ridurre al minimo il rischio di perdita dei dati.

Nelle misure previste da questo modulo rientrano tra l'altro l'elaborazione di un concetto per il backup dei dati che precisa la frequenza e il tipo di backup, la memorizzazione delle copie di sicurezza e la verifica dei backup. Si tratta inoltre di regolare il ripristino e il controllo dell'integrità dei dati dopo una perdita di dati nonché l'attuazione di procedure di backup.

Per il materiale d'archivio digitale, si deve scegliere un concetto per il backup dei dati basato su almeno tre copie indipendenti, che vengono sincronizzate. Se insorge un errore in una delle copie, i dati vengono ripristinati da un'altra copia. Per l'elaborazione del concetto si deve tenere conto soprattutto di quanto segue:

- Sistemi di memorizzazione geograficamente distribuiti sul territorio
- Utilizzo di compartimenti antincendio differenti per i sistemi di produzione e quelli di backup
- Memoria offline
- Sistemi di memorizzazione con meccanismi di auto-riparazione (Self-Healing) per correggere eventuali errori
- Attivazione manuale anziché automatica dei processi di backup e di replicazione al fine di impedire la propagazione di ransomware

Il modulo **Concetto per il backup dei dati** comprende anche l'identificazione e la valutazione dei rischi correlati al backup dei dati nonché l'adeguamento del concetto alla continua evoluzione delle esigenze e dei rischi.

Standard	Riferimento
BSI IT-G 2023	CON.3

Cancellazione e distruzione
Esistono casi in cui si devono cancellare dati d'archivio, ad esempio perché i loro formati sono diventati obsoleti e sono stati convertiti in nuovi formati o perché una nuova valutazione ha dimostrato che non sono più idonei all'archiviazione.

Questo modulo tratta la cancellazione sicura e definitiva dei dati nonché la distruzione dei supporti dati di un'istituzione. Il suo obiettivo è evitare che i dati archiviati (in particolare quelli riservati o personali) finiscano nelle mani sbagliate e possano essere utilizzati senza autorizzazione.

Nelle misure previste da questo modulo rientrano tra l'altro l'elaborazione di linee guida e procedure per la cancellazione sicura dei dati, l'identificazione precisa dei dati e dei metadati da cancellare e la definizione delle procedure per distruggere i supporti dati. Ciò prevede la documentazione della procedura di cancellazione. Vengono inoltre trattate la formazione dei collaboratori sulla cancellazione sicura dei dati e il controllo del rispetto delle procedure di cancellazione e distruzione.

Standard	Riferimento
BSI IT-G 2023	CON.6

Esercizio in proprio
Questo modulo tratta la messa in sicurezza dei sistemi e delle infrastrutture informatiche da parte dell'istituzione stessa. Il suo obiettivo è garantire la disponibilità, l'integrità e la riservatezza dei dati e dei sistemi informatici, in modo da ridurre al minimo il rischio di panne e cyberattacchi.

Nelle misure previste da questo modulo rientrano tra l'altro l'elaborazione di linee guida per la sicurezza informatica, l'esecuzione di controlli degli accessi e delle autorizzazioni, la sorveglianza dei sistemi e delle reti informatiche e lo svolgimento di audit periodici sulla sicurezza informatica. Vengono inoltre trattate la messa in sicurezza fisica dei locali dei server e la pianificazione d'emergenza. Il modulo comprende la pianificazione di queste misure e rimanda ai moduli di sistema necessari.

Il modulo **Esercizio** in proprio tiene conto anche dei nuovi sviluppi e delle nuove tecnologie nonché dell'adeguamento delle misure di sicurezza informatica alla continua evoluzione dei rischi e delle minacce.

Rientrano spesso in questa categoria le piccole istituzioni, in parte basate sul volontariato. Le esigenze poste dall'**esercizio in proprio** sono però elevate e si raccomanda quindi a queste istituzioni di valutare a fondo **un esercizio da parte di terzi** (Cloud).

Standard	Riferimento
BSI IT-G 2023	OPS.1

Esercizio da parte di terzi (Cloud)
Questo modulo tratta la messa in sicurezza di sistemi e infrastrutture informatiche gestiti da parte di un fornitore di servizi esterno. Il suo obiettivo è garantire la disponibilità, l'integrità e la riservatezza dei dati e dei sistemi informatici, in modo da ridurre al minimo il rischio di panne e cyberattacchi.

Nelle misure previste da questo modulo rientrano tra l'altro la definizione dei requisiti di sicurezza per il fornitore di servizi, l'esecuzione di controlli di sicurezza del fornitore di servizi, la definizione delle responsabilità e degli obblighi nel contratto di outsourcing e lo svolgimento di audit periodici sulla sicurezza informatica. Vengono inoltre trattate la sorveglianza dei contratti sul livello di servizio (Service-Level-Agreement; SLAs) e la pianificazione d'emergenza.

Nella stesura dei contratti è importante scegliere provider adeguati e tenere conto degli aspetti di sicurezza.

Standard	Riferimento
BSI IT-G 2023	OPS.2

6.3 Moduli di sistema

Server

Questo modulo tratta la messa in sicurezza dei server e degli ambienti dei server nei sistemi informatici. Il suo obiettivo è garantire la disponibilità, l'integrità e la riservatezza dei dati e dei sistemi informatici, in modo da ridurre al minimo il rischio di guasti e attacchi.

Nelle misure previste da questo modulo rientrano tra l'altro la messa in sicurezza fisica dei locali dei server, l'esecuzione di controlli degli accessi e delle autorizzazioni, la comunicazione criptata, l'esecuzione periodica di update di sicurezza e l'implementazione di meccanismi di backup e ripristino. Vengono inoltre trattate la sorveglianza dei server e la pianificazione d'emergenza.

È importante tenere conto dei nuovi sviluppi e delle nuove tecnologie e adeguare continuamente le misure di sicurezza informatica all'evoluzione dei rischi e delle minacce.

Standard	Riferimento
BSI IT-G 2023	SYS.1

Soluzioni di memorizzazione

Questo modulo tratta la messa in sicurezza delle soluzioni di memorizzazione nei sistemi informatici. Il suo obiettivo è garantire la disponibilità, l'integrità e la riservatezza dei dati e dei sistemi informatici, in modo da ridurre al minimo il rischio di panne e cyberattacchi. Questo modulo mette fondamentalmente in atto il concetto per il backup dei dati del modulo CON.3.

Nelle misure previste da questo modulo rientrano tra l'altro la messa in sicurezza fisica dei sistemi di memorizzazione, l'esecuzione di controlli degli accessi e delle autorizzazioni, la comunicazione criptata, l'esecuzione periodica di update di sicurezza e l'implementazione di meccanismi di sincronizzazione e backup.

L'adozione di queste misure mira a proteggere adeguatamente le soluzioni di memorizzazione nonché a individuare e affrontare rapidamente eventuali panne o cyberattacchi..

Standard	Riferimento
BSI IT-G 2023	SYS.1.8

Sistemi desktop

Questo modulo tratta la messa in sicurezza dei sistemi desktop negli ambienti informatici. Il suo obiettivo è garantire la disponibilità, l'integrità e la riservatezza dei dati e dei sistemi informatici, in modo da ridurre al minimo il rischio di panne e cyberattacchi.

Nelle misure previste da questo modulo rientrano tra l'altro la messa in sicurezza fisica delle postazioni di lavoro, l'esecuzione di controlli degli accessi e delle autorizzazioni, la comunicazione criptata, l'esecuzione periodica di update di sicurezza e l'implementazione di meccanismi di backup e ripristino. Ci si deve assicurare che il sistema operativo, i software installati e la protezione antivirus siano sempre aggiornati. I software obsoleti o non più necessari devono essere disinstallati. Vengono inoltre trattate la sorveglianza dei sistemi desktop e la pianificazione d'emergenza.

È importante tenere conto dei nuovi sviluppi e delle nuove tecnologie nonché adeguare continuamente le misure di sicurezza informatica all'evoluzione dei rischi e delle minacce.

Standard	Riferimento
BSI IT-G 2023	SYS.2

Supporti di memorizzazione rimovibili
Questo modulo tratta l'uso sicuro di chiavi USB, dischi rigidi esterni e altri supporti di memorizzazione mobili nei sistemi informatici. Il suo obiettivo è ridurre al minimo i rischi di perdita, furto o manipolazione dei dati tramite supporti di memorizzazione rimovibili e garantire la riservatezza, l'integrità e la disponibilità dei dati.

Nelle misure previste da questo modulo rientrano tra l'altro la definizione di linee guida per l'uso dei supporti rimovibili, l'implementazione di meccanismi volti a individuare e contrastare i malware sui supporti rimovibili nonché la formazione e la sensibilizzazione dei collaboratori sull'uso sicuro di questi supporti. La perdita o il furto di un supporto dati è possibile, ma grazie a misure adeguate come la crittografia si possono ridurre al minimo le conseguenze. Può inoltre capitare che i supporti rimovibili siano difettosi. Si possono utilizzare come parte di una strategia di backup, ma mai come unica copia dei dati.

È importante sorvegliare e documentare le attività eseguite con supporti rimovibili nonché verificare e aggiornare periodicamente le misure di sicurezza.

Standard	Riferimento
BSI IT-G 2023	SYS 4.5

Rete
Questo modulo tratta la sicurezza delle reti nei sistemi informatici. Il suo obiettivo è garantire la riservatezza, l'integrità e la disponibilità dei dati nelle reti e ridurre al minimo il rischio di attacchi e perdite di dati.

Nelle misure previste da questo modulo rientrano tra l'altro la definizione di linee guida e processi per l'architettura di rete, la segmentazione e la gestione della rete. Ulteriori misure prevedono l'implementazione di firewall, sistemi di rilevamento di intrusioni e la crittografia delle connessioni di rete. Una misura centrale è la separazione dell'informatica d'ufficio dagli archivi digitali a livello di rete. Sul firewall si devono inoltre creare delle regole non solo per il flusso di dati in entrata, ma anche per quello in uscita, in modo da evitare un flusso incontrollato di dati in uscita. Fondamentalmente, tutte le connessioni di rete tra i diversi ambiti e i singoli computer devono essere criptate. Durante la trasmissione di dati d'archivio, si deve garantire l'integrità transazionale confrontando le somme di controllo (checksum) prima e dopo la trasmissione.

Il modulo Rete attribuisce anche molto peso alla sorveglianza e documentazione delle attività di rete, al controllo e aggiornamento periodico dei dispositivi e dei sistemi di rete nonché alla formazione e sensibilizzazione dei collaboratori sull'uso sicuro delle reti.

Standard	Riferimento
BSI IT-G 2023	NET.1

6.4 Moduli fisici

Edifici in generale
Questo modulo tratta gli aspetti fisici della sicurezza degli edifici in cui vengono gestiti i sistemi informatici. Il suo obiettivo è garantire la riservatezza, l'integrità e la disponibilità dei sistemi informatici e dei dati adottando misure di sicurezza adeguate nell'edificio. Si tratta di impedire l'accesso fisico non autorizzato a luoghi sensibili come locali dei server o centri dati.

Nelle misure previste da questo modulo rientrano la messa in sicurezza di ingressi, finestre e altri punti d'accesso all'edificio, il controllo dei visitatori e degli ospiti e l'installazione di impianti di sicurezza come telecamere di sorveglianza, sistemi d'allarme e sistemi di controllo degli accessi.

In questo modulo rientrano anche la disponibilità di piani d'emergenza e la formazione dei collaboratori sulla gestione di emergenze come incendi, inondazioni o altre catastrofi naturali.

Standard	Riferimento
BSI IT-G 2023	INF.1

Centro dati, locale dei server
DQuesto modulo tratta i requisiti specifici per la sicurezza dei centri dati e dei locali dei server in cui vengono utilizzati i sistemi informatici. Il suo obiettivo è garantire la riservatezza, l'integrità e la disponibilità dei sistemi informatici e dei dati adottando misure di sicurezza adeguate.

Nelle misure di questo modulo rientrano la messa in sicurezza degli accessi ai centri dati e ai locali dei server, il controllo dei visitatori e degli ospiti e l'installazione di impianti di sicurezza come telecamere di sorveglianza, sistemi di allarme e sistemi di controllo degli accessi. Questo modulo comprende anche adeguati sistemi di climatizzazione e di estinzione degli incendi per evitare danni causati da surriscaldamento o incendi.

A queste misure di carattere generale si aggiungono misure specifiche per gli archivi digitali. Almeno tre copie dei fondi d'archivio devono essere conservate in almeno due sedi, ubicate in zone sismiche diverse. Se si scelgono solo due sedi per le tre copie, l'hardware presente in doppio in una sede deve trovarsi in zone antincendio separate.

Il modulo *Centro dati, locale dei server* comprende anche raccomandazioni per la progettazione dell'infrastruttura tecnica, come l'alimentazione elettrica, l'architettura di rete e l'infrastruttura dei server.

Standard	Riferimento
BSI IT-G 2023	INF.2

Archivio dei supporti dati
Questo modulo tratta la conservazione e l'archiviazione sicura dei supporti dati nei sistemi informatici. Il suo obiettivo è garantire la riservatezza, l'integrità e la disponibilità dei dati sui supporti di memorizzazione, al fine di ridurre al minimo il rischio di perdita, furto o manipolazione. Le misure previste dai due *moduli Supporti di memorizzazione rimovibili* e *Archivio dei supporti dati* proteggono i dati anche in caso di blackout e costituiscono un'importante rete di sicurezza per il recupero dei dati dopo un incidente (Disaster Recovery).

Nelle misure previste da questo modulo rientrano tra l'altro la definizione di processi per il controllo dell'accesso fisico e logico ai locali dell'archivio dei supporti dati, l'adozione di misure di sicurezza per i supporti dati, come la crittografia e l'etichettatura (Labeling), nonché la definizione di procedure per la distruzione sicura dei supporti dati alla fine del loro ciclo di vita.

Il modulo *Archivio dei supporti dati* comprende inoltre la verifica e l'aggiornamento periodico delle misure di sicurezza nonché la formazione e la sensibilizzazione del personale che ha accesso all'archivio dei supporti dati.

Standard	Riferimento
BSI IT-G 2023	INF.6

7 Fonti e siti web

BSI
Bundesamt für Sicherheit in der Informationstechnik (Deutschland). BSI 100-2 (Ufficio federale tedesco per la sicurezza nella tecnologia dell'informazione).
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.html

BSI IT-G (2023)
Bundesamt für Sicherheit in der Informationstechnik (Deutschland). IT-Grundschutz-Bausteine (Ufficio federale tedesco per la sicurezza nella tecnologia dell'informazione: moduli per la protezione informatica).
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

COBIT
Control Objectives for Information and related Technology (COBIT). (Obiettivi di controllo per le tecnologie informatiche e correlate).
https://www.isaca.org/resources/cobit

CoreTrustSeal
La CoreTrustSeal Foundation offre una certificazione degli archivi e depositi digitali sulla base dei «Core Trustworthy Data Repositories Requirements».
https://www.coretrustseal.org/why-certification/requirements/

ENISA
EU Agency for Cybersecurity. Good Practice Guide on National Cyber Security Strategies.
https://www.enisa.europa.eu/topics/national-cyber-security-strategies

Guida alla protezione delle infrastrutture critiche
Ufficio federale della protezione della popolazione (ed.) (2018).
https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/9c51cf46-602d-4ba1-9da7-03be93f84469.pdf

ISO 14721
Open archival information system (OAIS) – Reference model (Sistema informativo archivistico aperto – Modello di riferimento)
https://www.iso.org/standard/57284.html
Testo identico:
https://public.ccsds.org/Pubs/650x0m2s.pdf

ISO 16363
Audit and certification of trustworthy digital repositories. (Audit e certificazione di archivi digitali affidabili)
https://www.iso.org/standard/56510.html
Testo identico:
https://public.ccsds.org/Pubs/652x0m2.pdf

ISO 2700x
L'International Organization for Standardization (ISO) ha pubblicato una dozzina di norme complementari per la sicurezza delle informazioni, raccolte nella «serie 2700x». La più nota è la norma ISO 27001, che specifica i requisiti per la creazione, l'attuazione, il mantenimento e il miglioramento continuo di un sistema documentato per gestire la sicurezza delle informazioni, tenendo conto del contesto dell'organizzazione.
https://www.iso.org/standard/73906.html

nestor-Kriterienkatalog
Gruppo di lavoro nestor Archivi affidabili - Certificazione (2008). Catalogo dei criteri per gli archivi digitali affidabili a lungo termine.
https://d-nb.info/1000083241/34

NIST Framework
National Institute of Standards and Technology (USA). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.
(Istituto nazionale per gli standard e la tecnologia (USA). Quadro di riferimento per migliorare la cybersicurezza delle infrastrutture critiche, versione 1.1)
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST-SP-800-53 Rev. 5
National Institute of Standards and Technology (USA). Security and Privacy Controls for Information Systems and Organizations, Revision 5.
(Istituto nazionale per gli standard e la tecnologia (USA). Controlli sulla sicurezza e sulla privacy per i sistemi informativi e le organizzazioni, 5a revisione.)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

8 Glossario e abbreviazioni

AFS	Archivio federale svizzero
Archivio AV	Archivio dei supporti audiovisivi
Asset	In questo contesto: dati, persone, dispositivi, sistemi e impianti di un'organizzazione
Autenticità	Nel settore dell'archiviazione digitale, il termine viene utilizzato per indicare che un file contiene effettivamente ciò che dichiara di essere. È largamente usato come sinonimo di affidabilità.
Backup	Un backup è una copia dei dati creata per consentire il ripristino in caso di perdita o danneggiamento dei dati. Queste copie vengono eseguite regolarmente e salvate in un luogo sicuro.
Bene culturale	Secondo la «Convenzione dell'Aia per la protezione dei beni culturali in caso di conflitto armato» del 1954, sono considerati beni culturali «i beni, mobili o immobili, che siano di grande importanza per il patrimonio culturale dei popoli, come i monumenti architettonici, artistici o storici, religiosi o laici, i luoghi archeologici, gli insiemi di costruzioni che, come tali, offrono un interesse storico o artistico, le opere d'arte, i manoscritti, libri e altri oggetti d'interesse artistico, storico o archeologico, le collezioni scientifiche e le collezioni importanti di libri, di archivi o di riproduzioni di tali beni».[28] Va evidenziata la suddivisione in beni culturali mobili e immobili.
Bene culturale digitale	Il concetto di bene culturale, come definito nell'articolo 1 della Convenzione dell'Aia del 1954 per la protezione dei beni culturali in caso di conflitto armato, funge da criterio centrale per la scelta degli oggetti digitali. Per beni culturali digitali intendiamo sia gli oggetti creati digitalmente (born digital), sia quelli digitalizzati (retro-digitalizzazione). In questo contesto, il termine «collezione» è assimilabile a quello utilizzato per gli archivi, le biblioteche e i musei. Si tratta di una collezione di materiali d'archivio digitali. Oltre agli archivi digitali (p. es. quotidiani digitalizzati o archivi di programmi audiovisivi presso una biblioteca cantonale), i beni culturali creati digitalmente comprendono anche l'arte digitale (p. es. una collezione museale di fotografie creata digitalmente), la riproduzione digitale di oggetti d'arte e dati di ricerca (p. es. documentazione dei siti archeologici di un ente archeologico cantonale sotto forma di immagini riprese da droni o di modelli 3D), documentazioni di sicurezza create digitalmente, ecc. Per essere inclusi nell'Inventario PBC, gli oggetti PBC digitali vengono rilevati e classificati come collezioni.
Bitstream Preservation	Definisce il processo di conservazione e ripristino a lungo termine dei flussi di bit digitali per garantire l'integrità e la riproducibilità dei contenuti digitali.

28 Art. 1 Convenzione dell'Aia per la protezione dei beni culturali in caso di conflitto armato (RS 0.520.3), stipulata all'Aia il 14 maggio 1954.

8 Glossario e abbreviazioni

BN	Biblioteca nazionale
CFPBC	Commissione federale della protezione dei beni culturali
Compliance	È il termine economico e giuridico utilizzato per descrivere la conformità normativa di un'azienda, ossia il rispetto di determinate leggi, direttive e codici volontari.
Cybersicurezza	Per cybersicurezza si intende la protezione di computer, reti e dati contro attacchi provenienti da Internet o altre reti. Comprende misure di difesa contro le minacce informatiche (minaccia) per proteggere le infrastrutture digitali.
Data at Rest	Per Data at Rest si intendono dati memorizzati o a riposo che si trovano su supporti di memorizzazione fisici o digitali.
Data in Transit	Per Data in Transit si intendono dati in spostamento su reti o canali di comunicazione.
Defense in Depth	Si tratta di una strategia di cybersicurezza che implementa più livelli di meccanismi di sicurezza per proteggere sistemi e dati. L'obiettivo è creare barriere di sicurezza ridondanti, in modo che se un meccanismo di sicurezza fallisce, un altro prende immediatamente il suo posto per non compromettere l'intera sicurezza.
DH Lab	Digital Humanities Lab, Università di Basilea
DIMAG	Digitales Magazin. Soluzione condivisa per l'archiviazione digitale negli archivi pubblici.
Entità dei danni	Per entità dei danni si intendono le conseguenze stimate per la popolazione e le sue basi vitali, causate dall'interruzione di uno o più → processi critici nel caso in cui la → minaccia dovesse concretizzarsi. Risulta dalla somma dei danni causati al momento dell'insorgenza dell'evento e di quelli che possono verificarsi durante l'intera fase di ripristino.
GEVER	GEschäftsVERwaltung: gestione (elettronica) degli affari
Infrastrutture critiche	Per infrastrutture critiche si intendono processi, sistemi e installazioni essenziali per il funzionamento dell'economia o il benessere della popolazione.
Integrità	Prova che i dati sono corretti e invariati. Le somme di controllo (Checksum) sono un ausilio importante a tal fine.
LAP	Legge sull'approvvigionamento del Paese
LAr	Legge federale sull'archiviazione (legge sull'archiviazione, LAr; RS 152.1) del 26 giugno 1998
LPBC	Legge federale del 20 giugno 2014 sulla protezione dei beni culturali in caso di conflitti armati, catastrofi e situazioni d'emergenza (LPBC; RS 520.3)
LPN	Legge federale del 1° luglio 1966 sulla protezione della natura e del paesaggio (RS 451)
Minaccia	Per minaccia si intende un pericolo concreto che sussiste per un bene protetto. La minaccia corrisponde quindi a un potenziale evento o sviluppo con possibili conseguenze per il bene protetto.
NIST	Il National Institute of Standards and Technology (NIST, Istituto nazionale di standardizzazione e tecnologia) è un'agenzia federale degli Stati Uniti che ha pubblicato un quadro di riferimento (Framework) per la gestione dei cyber-rischi.
OAIS	Open Archival Information System, ISO 14721. Modello di riferimento per gli archivi digitali
OPAC	Open Public Access Catalog

8 Glossario e abbreviazioni

Patrimonio culturale	Utilizzato come termine generico che comprende tutti i beni culturali immobili e mobili nonché il patrimonio culturale immateriale.
Patrimonio culturale immateriale	Per patrimonio culturale immateriale s'intendono (secondo la definizione della Convenzione dell'UNESCO) «le pratiche, rappresentazioni, espressioni, sapere e capacità, come pure gli strumenti, oggetti, manufatti e spazi culturali associati, che le comunità, i gruppi e, in alcuni casi anche i singoli individui, riconoscono come parte integrante del loro patrimonio culturale».[29] La Convenzione dell'UNESCO individua cinque settori: A. Tradizioni ed espressioni orali, incluso il linguaggio in quanto veicolo del patrimonio culturale immateriale B. Arti dello spettacolo C. Consuetudini sociali, riti ed eventi festivi D. Conoscenze e pratiche sulla natura e l'universo E. Artigianato tradizionale
PBC	Protezione dei beni culturali
Preservation Planning	La Preservation Planning (pianificazione della conservazione) nell'ambito dell'archiviazione a lungo termine persegue l'obiettivo di mantenere disponibili sul lungo periodo i contenuti archiviati.
Probabilità d'insorgenza	Per probabilità d'insorgenza si intende la probabilità, stimata o basata su valori statistici, che un evento si verifichi entro un determinato lasso di tempo (p. es. entro 10 anni).
Processi critici	Nel contesto della protezione delle infrastrutture critiche, per processo critico s'intende un processo essenziale per il funzionamento dell'infrastruttura critica e la cui interruzione avrebbe gravi ripercussioni sulla popolazione e sulle sue basi vitali.
Protezione delle infrastrutture critiche	La protezione delle infrastrutture critiche comprende le misure volte a ridurre la → probabilità d'insorgenza e/o l' → entità dei danni causati da una perturbazione, un'interruzione o una distruzione di → infrastrutture critiche e quindi la durata della loro interruzione.
Records Management	Comprende la gestione sistematica dei record e delle informazioni durante tutto il loro ciclo di vita, dalla creazione o acquisizione, alla memorizzazione e conservazione, fino all'archiviazione definitiva o alla distruzione.
Resilienza	Per resilienza si intende la capacità di un sistema, di un'organizzazione o di una società di resistere a perturbazioni interne d esterne e di mantenere o ripristinare possibilmente il funzionamento. La resilienza si compone di quattro elementi: 1) la robustezza dei sistemi (p. es. → infrastrutture critiche, Stato, economia e società) di per sé; 2) la disponibilità di ridondanze; 3) la capacità di mobilitare misure di sostegno efficaci; 4) la tempestività e l'efficienza delle misure di sostegno.
Rischio	Il rischio è un metro di misura per le dimensioni di una → minaccia e implica la → probabilità d'insorgenza e l' → entità dei danni di un evento indesiderato.
RS	Raccolta sistematica del diritto federale
Sicurezza delle informazioni	La sicurezza delle informazioni protegge le informazioni e i sistemi informativi contro accessi, utilizzi, divulgazioni, modifiche o distruzioni illecite. L'obiettivo è garantire la riservatezza, l'integrità e la disponibilità dei dati.

29 Art. 2 Convenzione per la salvaguardia dei beni culturali immateriali (RS 0.440.6), stipulata a Parigi il 17 ottobre 2003

8 Glossario e abbreviazioni

Sincronizzazione	È il processo volto a sincronizzare i dati tra due o più sistemi affinché abbiano tutti lo stesso stato di dati. Ciò avviene in tempo reale o a intervalli regolari per garantire che i dati siano coerenti e aggiornati.
Sottosettore	In Svizzera, le → infrastrutture critiche sono state suddivise in 27 sottosettori. Questi comprendono diverse categorie, come industrie, settori economici e altre suddivisioni di carattere economico. Si tratta nella fattispecie dei seguenti sottosettori: acque reflue, approvvigionamento alimentare, approvvigionamento di elettricità, approvvigionamento di gas, approvvigionamento di petrolio, approvvigionamento idrico, beni culturali, chimica e agenti terapeutici, esercito, media, parlamento / governo / giustizia / Amministrazione, organizzazioni di pronto intervento, prestazioni mediche e ospedaliere, protezione civile, ricerca e insegnamento, rifiuti, servizi assicurativi, servizi di laboratorio, servizi informatici, servizi finanziari, servizi postali, telecomunicazioni, teleriscaldamento e calore di processo, traffico aereo, traffico ferroviario, traffico navale, traffico postale e traffico stradale.
TDT	Settore «Trasformazione digitale e governance delle TIC» della Cancelleria federale
TIC	Tecnologie dell'informazione e della comunicazione
UFAE	Ufficio federale per l'approvvigionamento economico del Paese
UFC	Ufficio federale della cultura
UFCS	Ufficio federale della cybersicurezza
UFPP	Ufficio federale della protezione della popolazione

Per ulteriori glossari e definizioni di termini si veda anche:

- Glossario sui rischi, Ufficio federale della protezione della popolazione UFPP, 29.4.2013. https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/6e53cc48-dfd0-496e-8516-54bd2f227e76.pdf

- Glossario nella Guida alla protezione delle infrastrutture critiche, 2018. Microsoft Word - 20181217_Leitfaden_SKI_i.docx (admin.ch)

8 Glossario e abbreviazioni

Autori ed esperti della prima edizione

Cognome	Nome	Organizzazione	Funzione
Wildi	Tobias	CFPBC Scuola universitaria professionale dei Grigioni	CP / autore principale
Fornaro	Peter	Digital Humanities Lab, Università di Basilea	Revisione
Müller	Stefanie	Scuola universitaria professionale dei Grigioni	Revisione

Cronologia

Data	Breve descrizione
2018	Decisione della CFPBC di elaborare lo standard minimo per le TIC
gennaio – luglio 2023	Stesura della prima bozza
agosto – novembre 2023	Consultazione di uffici e cantoni
dicembre 2023	Stesura della seconda bozza
gennaio – marzo 2024	Consultazione dei cantoni
aprile – luglio 2024	Rielaborazione e versione definitiva
novembre 2024	Approvazione da parte della CFPBC
agosto – dicembre 2024	Traduzione e pubblicazione