Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS

Versione 5.1

Si001 – Protezione IT di base nell'Amministrazione federale

del 5 luglio 2024

Indice

1 Disposizioni generali ... 3
1.1 Oggetto ... 3
1.2 Campo d'applicazione e condizioni quadro giuridiche ... 3
1.3 Deroghe ... 4
2 Definizioni ... 4
3 Principi ... 7
4 Requisiti di sicurezza ... 8
5 Entrata in vigore ... 19
Abbreviazioni ... 19
Riferimenti ... 21
Allegato A: Modello delle zone della Confederazione ... 22
Allegato B: Livelli di sicurezza per i mezzi di autenticazione e identificazione ... 24
Allegato C: *Zone policy* per il «dominio di rete blu» ... 26
C.1 Requisiti e direttive per i sistemi TIC ... 26
C.2 Requisiti e direttive per il dominio di rete blu ... 26
C.3 Requisiti e direttive per le comunicazioni consentite ... 26
C.3.1 Comunicazione interna ... 26
C.3.2 Comunicazione esterna ... 26
Allegato D: Matrice d'accesso per il dominio di rete blu e la SSZ ... 28

1 Disposizioni generali

1.1 Oggetto

[1] Ai sensi dell'articolo 29 capoverso 1 OSIn[1], la presente direttiva disciplina i requisiti minimi del livello di sicurezza «protezione di base» secondo l'articolo 17 capoverso 1 LSIn[2] per tutti gli oggetti informatici che non devono essere attribuiti a un livello di sicurezza più elevato. Ai sensi dell'articolo 18 capoverso 2 LSIn, tutti i mezzi informatici devono soddisfare tali requisiti.

[2] Ogni unità amministrativa (UA) è responsabile in prima persona della sicurezza dei propri mezzi informatici e a tal fine deve garantire l'attuazione e l'osservanza della presente direttiva, ovvero controllare che la stessa venga attuata e osservata.

[3] L'attuazione e l'osservanza della presente direttiva devono essere documentate in modo ricostruibile dall'UA responsabile (ad es. sulla base del documento [Si001-Hi01]). La documentazione deve essere verificata e firmata almeno

a) dal/dalla responsabile degli oggetti da proteggere (secondo il n. 2 cpv. 1),
b) dall'incaricato/a della sicurezza informatica dell'UA responsabile (ISIU, secondo articolo 36 OSIn),
c) dal committente (se si tratta di un progetto) e
d) dal responsabile dei processi aziendali.

Apponendo la loro firma, essi confermano altresì che a loro giudizio tutti i fornitori di prestazioni (FP) coinvolti nella gestione del mezzo informatico soddisfano i requisiti previsti.

[4] L'UA responsabile deve documentare in modo ricostruibile anche l'avvenuto controllo dell'attuazione e dell'osservanza della presente direttiva. Le modalità di esecuzione di tale controllo dipendono anche dall'oggetto informatico da proteggere e dal suo bisogno di protezione, e devono quindi essere concordate con l'ISIU e documentate. Nel caso di un oggetto da proteggere che viene utilizzato da uno o più FP interni su incarico dell'UA responsabile, il controllo si considera effettuato se il documento «Attuazione delle misure per la protezione IT di base nell'Amministrazione federale» è stato firmato anche dai rispettivi FP.

1.2 Campo d'applicazione e condizioni quadro giuridiche

[1] Ai sensi dell'articolo 29 capoverso 1 OSIn, il campo d'applicazione della presente direttiva per tutte le organizzazioni è disciplinato dall'articolo 2 capoverso 1-3 OSIn.

[2] Ulteriori condizioni quadro giuridiche si possono evincere

a) dall'ordinanza sulla protezione delle informazioni della Confederazione (ordinanza sulla protezione delle informazioni [OPrl]) e dalle istruzioni concernenti le prescrizioni dettagliate in materia di protezione delle informazioni (istruzioni sul trattamento, disponibili solo in tedesco),
b) dalla legislazione federale sulla protezione dei dati per quanto riguarda il trattamento dei dati personali, nonché

[1] RS 128.1

[2] RS 128

c) dalla legislazione federale in materia di archiviazione per quanto riguarda l’archiviazione dei dati.

1.3 Deroghe

[1] Se non è in grado di soddisfare uno o più requisiti previsti dalla presente direttiva per un oggetto informatico da proteggere, l’UA deve richiedere una deroga ai sensi dell’articolo 9 capoverso 1 OSIn. Tale deroga può essere richiesta secondo una delle modalità specificate nei capoversi 2–4 seguenti.

[2] Dal punto di vista della sicurezza informatica dell’Amministrazione federale i requisiti contrassegnati con un asterisco (*) al numero 4 sono associati a un rischio minore e lasciano spazio alla possibilità di deroghe, purché debitamente motivate e documentate nel documento «Attuazione delle misure per la protezione IT di base nell’Amministrazione federale» o nel piano SIPD. In tal caso la deroga si intende autorizzata dai responsabili menzionati al numero 1.1 capoverso 3.

[3] L’incaricato/a della sicurezza informatica dell’UA responsabile (ISIU) può autorizzare in prima persona una richiesta formale di deroga se sono soddisfatte (cumulativamente) le condizioni indicate di seguito.

a) L’ISIU è coinvolto/a nel processo di autorizzazione della deroga a tal punto da potersene assumere la responsabilità.
b) La deroga riguarda esclusivamente l’utilizzo di informazioni dell’UA responsabile o altri oggetti informatici da proteggere che non presentano un bisogno di protezione elevato o il cui bisogno di protezione, ancorché elevato, è basato unicamente su requisiti in materia di protezione di dati.
c) La deroga non riguarda né i servizi standard TIC né un’altra UA.
d) È comprovato che tutte le persone menzionate al numero 1.1 capoverso 3 come anche il responsabile dell’UA o un membro della direzione dell’UA sono d’accordo con la deroga.
e) L’ISIU tiene un elenco aggiornato delle deroghe accordate e, su richiesta, le comunica al servizio specializzato della Confederazione per la sicurezza delle informazioni.

[4] Tutte le altre richieste di deroga possono essere inoltrate all’NCSC mediante il processo P035 («IKT-Anforderungs- und Vorgabenmanagement Bund»). Nella richiesta si devono indicare i motivi per cui ci si intende scostare dalla protezione IT di base e si devono illustrare e analizzare le misure possibili e quelle previste per ridurre i rischi.

[5] Le deroghe di cui al capoverso 4 vengono sempre accordate per un tempo limitato (di norma due anni).

2 Definizioni

[1] Ai sensi dell'articolo 17 capoverso 1 LSIn, il livello di sicurezza «protezione di base» si applica a tutti i mezzi informatici, salvo a quelli che devono essere attribuiti a un livello di sicurezza più elevato. L'espressione «tutti i mezzi informatici» utilizzata nella legge comprende sia singoli mezzi informatici sia diversi mezzi informatici analoghi o correlati, in quanto la LSIn/OSIn mira a fornire una copertura di sicurezza completa. Nella prassi dell'Amministrazione federale, in particolare, tali mezzi informatici sono spesso considerati

come unità interconnesse, che vengono pertanto indicate di seguito nella presente direttiva come **oggetti informatici da proteggere**. Questo approccio consente un'identificazione e una gestione più precisa delle unità da proteggere e contribuisce alla chiarezza e all'efficienza nell'attuazione delle successive misure di sicurezza. Per ogni oggetto da proteggere deve essere **designato/a un/una responsabile degli oggetti informatici da proteggere**.

[2] Nella presente direttiva vengono inoltre utilizzati i termini e le espressioni seguenti.

a) **Analisi del bisogno di protezione:** metodo strutturato di rilevamento del bisogno di protezione di un oggetto informatico da proteggere. Al riguardo si distingue tra protezione di base e bisogno di protezione elevato.

b) **Piano per la sicurezza dell'informazione e la protezione dei dati (SIPD):** descrizione strutturata dei requisiti di sicurezza di un oggetto informatico da proteggere, delle misure di sicurezza previste e di quelle attuate nonché degli ulteriori rischi residui.

c) **Informazioni:** dati salvati, trattati e/o trasmessi in forma elettronica[3]. Se i dati si riferiscono a una persona identificata o identificabile, si tratta di **dati personali** ai sensi della legislazione sulla protezione dei dati.

d) **Sistema IT (sistema):** sistema tecnico informatico che viene gestito come un software (di sistema) su un hardware dedicato o virtuale oppure su un dispositivo virtuale[4]. Nel secondo caso si parla di sistema IT virtuale.

e) Un sistema IT è[5]

- un **sistema di server**, quando fornisce principalmente prestazioni IT;
- un **sistema client**, quando è principalmente il beneficiario di prestazioni IT;
- un **client della Confederazione**, se è un sistema client gestito nel servizio standard TIC Burotica. Può trattarsi di un sistema di postazioni di lavoro (SPL) oppure di un sistema client virtuale gestito su uno smart device all'interno di una *sandbox* con una gestione dei dispositivi mobili (*Mobile Device Management*, MDM) conformemente alla direttiva [E021] (sistema MDM);
- una **periferica**, quando rappresenta un'estensione funzionale di altri sistemi IT e, a tal fine, deve essere integrata o installata (driver), ad esempio stampanti, dispositivi multifunzione o sistemi di presentazione per sale conferenze;
- un **apparecchio di misurazione**, quando il suo compito principale consiste nel trasmettere i valori misurati[6] da un sensore, presente sul luogo della misurazione, a un secondo sistema IT lontano attraverso una connessione dedicata che non può essere utilizzata per altri scopi. Il sistema IT ricevente può soltanto raccogliere e registrare i valori misurati o può anche analizzarli ed elaborarli ulteriormente. Le comunicazioni possono essere effettuate bilateralmente e comprendere, ad esempio, la trasmissione di informazioni di controllo all'apparecchio di misurazione. Gli apparecchi di misurazione sono

[3] Nella presente direttiva il termine «informazioni» è utilizzato in senso generico per intendere «informazioni e dati», mentre si parla di dati solo quando ci si riferisce ai dati personali così come intesi nell'ambito della protezione dei dati.
[4] Il sistema IT che mette a disposizione l'hardware virtuale o un dispositivo virtuale (*hypervisor*) è a sua volta un software ed è quindi considerato un sistema IT autonomo.
[5] La differenza tra sistema client e sistema di server non è precisa, e quindi un sistema IT può fungere contemporaneamente sia da sistema client sia da sistema di server.
[6] I valori misurati possono essere anche segnali acustici e/o ottici.

utilizzati soprattutto in applicazioni dell'Internet delle cose (*Internet of Things*, IoT);

- un **componente di rete**, se serve principalmente per il trasporto di dati tra sistemi IT, ad esempio switch, router o filtri di pacchetti statici semplici (firewall IP). Nel modello di riferimento OSI (*Open Systems Interconnection*) i componenti di rete funzionano fino al livello 5 compreso (livello di sessione);
- un ***policy enforcement point*** **(PEP)**, quando serve principalmente ad applicare regole (derivanti da una *policy*) come ad esempio filtri di pacchetti dinamici, gateway per protocolli applicativi, server proxy e server proxy inversi. Nel modello di riferimento OSI, i PEP intervengono fino al livello 7 compreso (livello applicativo), e in questo senso controllano anche il/i protocollo/i di comunicazione trasmesso/i.

f) **Applicazione:** software applicativo utilizzato nei sistemi IT di una o più UA per svolgere i processi aziendali. Le applicazioni dell'IoT si differenziano da altre applicazioni soprattutto per il fatto che le informazioni utilizzate sono generate principalmente da apparecchi di misurazione.

g) **Rete:** infrastruttura tecnica (composta principalmente da componenti di rete e connessioni) per lo scambio di dati tra sistemi IT.

h) **Segmento di rete (segmento):** parte di una rete che, per ragioni di bilanciamento del carico e/o di sicurezza, è normalmente separata dalle altre parti della rete mediante componenti di rete.

i) **Zona:** raggruppamento logico di sistemi informatici che presentano requisiti di sicurezza simili e che sottostanno alla medesima *zone policy*. In particolare, una zona non è limitata a un determinato luogo (ad es. centro di calcolo). La connessione a livello di rete degli elementi di una zona avviene tramite i componenti di rete, mentre l'applicazione delle regole della *zone policy* è effettuata dai PEP.

j) **Sottozona:** una zona può essere suddivisa in sottozone se la *policy* corrispondente lo prevede. Ogni sottozona costituisce a sua volta una zona. In particolare, ogni sottozona deve avere una *policy* che preveda requisiti più severi rispetto alla zona superiore. In altre parole, questa *policy* può contenere soltanto requisiti o prescrizioni supplementari (non sono ammessi requisiti più semplici). Una sottozona può essere ulteriormente suddivisa in sottozone supplementari, ma soltanto in caso di necessità.

k) ***Zone policy*****:** descrizione strutturata dei requisiti e delle direttive concernenti una zona, ossia

- i sistemi IT gestiti nella zona;
- la zona stessa, ad esempio se può essere segmentata sulla rete e, in caso affermativo, in che modo;
- l'autenticazione delle persone e dei processi automatizzati che accedono ai sistemi IT e alle applicazioni gestiti nella zona; e
- le comunicazioni interne (anche quelle tra segmenti) ed esterne (anche quelle che esulano dall'ambito della *policy enforcement zone* [PEZ]) ammesse nella zona, cioè le comunicazioni consentite in entrata e in uscita[7]. Una

[7] Una comunicazione è considerata in uscita se il relativo scambio di dati è attivato da un sistema IT della zona interessata. Per contro, è considerata in entrata se lo scambio di dati, pur essendo attivato da un sistema IT al di fuori della zona, riguarda un sistema IT nella zona. In entrambi i casi i dati possono essere scambiati nelle due direzioni.

comunicazione tra due o più zone simili[8] è considerata interna se le interfacce tra le zone sono conformi alle *policy* e sono controllate in una PEZ comune.

l) **Modello delle zone della Confederazione:** modello generico utile a definire le zone nell'Amministrazione federale (cfr. allegato A).

3 Principi

[1] **Modalità di fornitura delle prestazioni:** la protezione IT di base deve essere garantita a tutti gli oggetti informatici da proteggere, indipendentemente dalla modalità di fornitura delle prestazioni. In altri termini, sia i FP interni sia quelli esterni devono attuare i requisiti e le misure di sicurezza che li riguardano. Per quanto concerne i FP esterni, occorre assicurarsi in particolare che osservino le direttive in materia di sicurezza informatica[9] e che ottengano il relativo consenso dell'autorità preposta conformemente ai processi specifici dell'ufficio o del dipartimento (cfr. [Si001-Hi04]).

[2] **Virtualizzazione:** la protezione IT di base deve essere garantita indipendentemente dal fatto che un oggetto informatico da proteggere sia gestito su un hardware dedicato o su un hardware virtuale utilizzato in comune. Se il bisogno di protezione è elevato, l'utilizzo di eventuali tecnologie e soluzioni di virtualizzazione deve essere motivato e documentato nel piano SIPD.

[3] **Principio «zero trust»:** il dispositivo di sicurezza di un oggetto informatico da proteggere deve, per quanto possibile, essere configurato in modo che i requisiti di sicurezza di cui al numero 4 possano essere soddisfatti autonomamente e che l'oggetto sia isolato e separato dal suo ambiente in maniera da ridurre al minimo le preoccupazioni circa la sicurezza dell'ambiente.

[4] **Principio della difesa in profondità («defense in depth»):** se possibile ed economicamente sostenibile, un oggetto deve essere protetto con misure di sicurezza diverse e complementari, così da creare un sistema ridondante idoneo a soddisfare i requisiti di sicurezza definiti. Nel complesso, le misure di sicurezza devono perseguire un triplice scopo: prevenire gli attacchi, rilevare la presenza di un attacco in corso e rispondere agli attacchi.

[5] **Stato della tecnica:** tutte le misure di sicurezza messe in atto (per prevenire gli attacchi, rilevare la presenza di un attacco in corso e rispondere agli attacchi) devono essere conformi allo stato della tecnica[10], preferibilmente standardizzate e di comprovata efficacia sul piano operativo. Le misure divenute ormai obsolete o di cui sono noti vulnerabilità o punti deboli rilevanti devono essere migliorate o sostituite con tempestività e indipendentemente dal «ciclo di vita».

[6] **Principio del privilegio minimo («least privilege») o del «need to know»:** agli utenti deve essere attribuito il livello minimo di accesso e di privilegi. Questa regola vale ad esempio per gli utenti di sistemi IT e di applicazioni[11], per l'attivazione di servizi e di

[8] Queste zone possono anche avere proprietari diversi.
[9] L'osservanza delle direttive in materia di sicurezza informatica può ad esempio essere disciplinata contrattualmente e/o garantita da verifiche e certificati adeguati.
[10] Nel campo della crittografia, informazioni sullo stato della tecnica sono reperibili nelle «Raccomandazioni in materia di sicurezza per la protezione IT di base– metodi crittografici: algoritmi e protocolli» della BAC CEO CRITT del 24.01.2023.
[11] Per l'assegnazione dei diritti di accesso agli utenti idealmente si deve prevedere un piano dei ruoli (nell'ambito di un controllo degli accessi basato sui ruoli).

funzionalità aggiuntive (*feature*) di sistemi IT e applicazioni e per le comunicazioni consentite nell'ambito delle *zone policy*[12].

[8] **Principio della «security by design»:** quando si sviluppano componenti hardware e software o li si utilizzano in sistemi IT e applicazioni, la sicurezza deve essere considerata fin dall'inizio e aggiornata affinché i sistemi e le applicazioni non presentino, per quanto possibile, vulnerabilità o punti deboli e i potenziali attacchi siano ridotti al minimo.

[9] **Principio della «security by default»:** gli oggetti informatici da proteggere devono essere sviluppati, configurati e gestiti in maniera che tutte le misure di sicurezza utili in uno specifico ambiente siano attivate per impostazione predefinita e possano produrre i loro effetti senza che gli utenti debbano preoccuparsene.

[10] **Neutralità rispetto ai prodotti:** in linea di massima, le direttive e le raccomandazioni sono formulate in termini neutrali rispetto ai prodotti. Indicazioni a favore o contro l'utilizzo di determinati prodotti vengono fornite solo quando riguardano un servizio standard TIC[13] o quando sussistono altri motivi importanti dal punto di vista della sicurezza informatica.

4 Requisiti di sicurezza

[1] Per ogni oggetto informatico da proteggere si deve tener conto dei principi esposti al capitolo 3 e si devono soddisfare i requisiti di sicurezza di cui al capoverso 2. I requisiti sono stati in parte ripresi dallo standard ISO/IEC 27002:2013 e sono strutturati in conformità al nuovo standard ISO/IEC DIS 27002[14].

[2] I requisiti di sicurezza che riguardano l'organizzazione (O), il personale (P), la tecnica (T) e le informazioni (I) devono essere sempre soddisfatti, mentre i requisiti previsti per i sistemi IT (S), le applicazioni (A) e le zone (Z) devono essere soddisfatti solo quando si utilizzano anche oggetti informatici da proteggere.

Organizzazione	
O1	Responsabilità Per l'oggetto informatico da proteggere deve essere designata una persona (appartenente all'UA responsabile) che fungerà da responsabile dell'oggetto informatico da proteggere e a cui spetterà l'attuazione della presente direttiva. Questa persona deve essere consapevole della responsabilità che le viene affidata e deve avere le competenze tecniche necessarie per farsene carico.
O2	Documentazione O2.1 Per l'oggetto informatico da proteggere deve essere disponibile una documentazione aggiornata e il cui contenuto sia stato concordato con i

[12] In linea di principio i protocolli di comunicazione sono consentiti solo quando necessari sul piano operativo.
[13] Per quanto riguarda, ad esempio, la crittografia asimmetrica si dovranno utilizzare preferibilmente certificati rilasciati dalla Swiss Government PKI (SG-PKI) e per la cifratura di file classificati come CONFIDENZIALI sul SPL si utilizzerà il software di cifratura dell'Amministrazione federale (shell 1).
[14] Contrariamente allo standard ISO/IEC 27002:2013, in questa nuova versione viene fatta una distinzione tra controlli organizzativi (sezione 5), personali (sezione 6), fisici (sezione 7) e tecnici (sezione 8). La corrispondenza tra i controlli indicati nello standard ISO/IEC DIS 27002 e i controlli di cui allo standard ISO/IEC 27002:2013 è sintetizzata nell'allegato B dello standard ISO/IEC DIS 27002.

	FP coinvolti. La documentazione deve coprire l'intero ciclo di vita dell'oggetto e comprendere in particolare anche a) la catena di fornitura (*supply chain*); b) le misure di protezione fisiche, posto che la necessità di adottare misure edilizie e tecniche per proteggere fisicamente i sistemi IT deve, laddove necessario, essere concordata con l'UFCL, con armasuisse e con il Servizio federale di sicurezza; c) i componenti, le funzioni e le impostazioni rilevanti ai fini della sicurezza; d) la gestione delle chiavi in caso di utilizzo di metodi crittografici; e) le modalità e i processi da applicare in caso di modifica (nel quadro della gestione del cambiamento), di riparazione, di smaltimento e di smarrimento; f) gli accordi contrattuali; e g) i processi e le attività di audit[15] necessari per controllare che la presente direttiva venga effettivamente attuata e rispettata. O2.2 Se l'oggetto informatico da proteggere (sistema IT o applicazione) non è gestito in una zona dell'Amministrazione federale (ad es. in un cloud pubblico), la documentazione deve indicare a) come poter soddisfare il bisogno di protezione dell'oggetto in questo ambiente; e b) quali misure di sicurezza complementari adottare per garantire che gli altri oggetti informatici da proteggere dell'Amministrazione federale non siano esposti a ulteriori minacce e rischi.
O3	Continuità operativa Per l'oggetto informatico da proteggere, la continuità operativa deve essere garantita e documentata nell'ambito di un processo di *IT Service Continuity Management* (ITSCM) o di *Business Continuity Management* (BCM) conformemente al bisogno accertato in sede di analisi del bisogno di protezione.
O4	Ciberincidenti L'oggetto informatico da proteggere deve essere incluso nel processo di gestione dei ciberincidenti.
Personale	
P1	Sensibilizzazione e formazione P1.1 Tutti coloro che utilizzano l'oggetto informatico da proteggere devono essere sensibilizzati e formati sul tema della sicurezza informatica, secondo il loro livello e la loro funzione.

[15] I processi e le attività di audit devono essere eseguiti da un servizio indipendente e concepiti in maniera da pregiudicare il meno possibile la disponibilità degli oggetti informatici da proteggere (limitando quindi il più possibile i malfunzionamenti e le interruzioni).

	P1.2 Tutti coloro che utilizzano l'oggetto informatico da proteggere devono conoscere le direttive delle applicazioni rilevanti e sono tenuti a rispettarle[16].
P2	Obbligo di segnalazione Tutti coloro che utilizzano l'oggetto informatico da proteggere devono segnalare il più rapidamente possibile al servizio competente (ad es. al service desk del FP) qualsiasi evento critico ai fini della sicurezza, come un comportamento anomalo e sospetto del sistema o una perdita fisica.
Tecnica	
T1	Gestione L'oggetto informatico da proteggere deve essere gestito conformemente allo stato della tecnica e tenendo debitamente conto delle prescrizioni e delle raccomandazioni in materia di sicurezza usuali nel settore («buone pratiche»).
T2	Configurazione e impostazione T2.1 Prima di essere messo in funzione per la prima volta, l'oggetto informatico da proteggere deve essere configurato e impostato in modo da a) essere protetto contro ogni eventuale accesso da parte di persone non autorizzate; b) poter contare, per quanto tecnicamente possibile, su una protezione ottimizzata e funzionare nella configurazione minima necessaria per lo svolgimento dei compiti e non modificabile dall'utente (le interfacce, le funzioni e i moduli non utilizzati devono quindi essere disattivati), e c) consentire di registrare le attività e gli eventi rilevanti ai fini della sicurezza (anche con indicazione dell'ora) e di valutarli tempestivamente. T2.2 Le configurazioni e le impostazioni di sicurezza possono essere attivate, modificate, disattivate e disinstallate solo previa autorizzazione.
T3	Ambiente di produzione L'ambiente di produzione dell'oggetto informatico da proteggere deve essere separato dagli altri eventuali ambienti (ad es. quelli per lo sviluppo e/o i test). Se la separazione segue un criterio logico, i relativi provvedimenti e le misure di sicurezza devono essere motivati e documentati.
T4	Punti deboli e vulnerabilità Per individuare eventuali punti deboli e vulnerabilità, l'oggetto informatico da proteggere deve essere sottoposto a controlli regolari e preferibilmente automatizzati (ad es. con un *security scanner*) prima di essere messo in funzione e, se il suo bisogno di protezione e la sua esposizione a Internet lo

[16] Questo requisito si applica in particolare all'utilizzo di sistemi MDM e/o di dispositivi periferici privati durante il lavoro mobile. Una panoramica di tutte le direttive delle applicazioni è disponibile all'indirizzo: https://intranet.dti.bk.admin.ch/isb_kp/it/home/ikt-vorgaben/einsatzrichtlinien.html

	giustificano, anche durante la fase operativa. In caso di punti deboli e vulnerabilità critici occorre coinvolgere l'NCSC.
T5	Autenticazione e autorizzazione T5.1 Ogni accesso a un oggetto informatico da proteggere deve essere autenticato[17] in funzione del suo bisogno di protezione e autorizzato nel rispetto del principio del privilegio minimo o «need to know». T5.2 Tutti i diritti di accesso all'oggetto informatico da proteggere devono essere amministrati nel quadro di un processo definito e documentato[18] ed essere tenuti sempre aggiornati. In particolare, dovranno essere controllati almeno una volta all'anno per accertarsi che siano corretti e ancora necessari; i diritti (e gli account) che non servono più dovranno essere cancellati. T5.3 Per l'oggetto informatico da proteggere si possono utilizzare soltanto mezzi di autenticazione e identificazione gestiti nel quadro di un processo definito e documentato che copra l'intero ciclo di vita del mezzo (incluse le possibilità di accesso per emergenze, blocco, ripristino, revoca e smaltimento).
T6	Autenticazione dell'utente T6.1 Per accedere a un SPL o a un sistema di server l'utente deve autenticarsi con un mezzo di autenticazione e identificazione che presenti almeno il livello di sicurezza «medio» secondo l'allegato B o tramite un'autenticazione a due fattori[19]. T6.2 Per accedere a un sistema MDM l'utente deve autenticarsi sulla base di una procedura supportata dal rispettivo sistema operativo, come l'inserimento di un PIN[20] o un'autenticazione biometrica (ad es. Touch ID o Face ID per dispositivi iOS). Il PIN deve essere composto da almeno 6 caratteri e non deve essere troppo semplice. T6.3 Per accedere a un componente di rete l'utente deve autenticarsi con un mezzo di autenticazione e identificazione che presenti almeno il livello di sicurezza «elevato» secondo l'allegato B.
T7	Password I requisiti per l'autenticazione dell'utente tramite password sono i seguenti. T7.1* La password a) deve essere personale[21];

[17] L'autenticazione può avvenire a livello locale o tramite una o più connessioni di rete. Nel secondo caso l'autenticazione è considerata nella sua totalità (ossia autenticazione locale su un terminale ed eventuali autenticazioni sui server proxy).

[18] Nell'ambito di questo processo si dovrà, per quanto possibile e opportuno, considerare e documentare la separazione dei poteri tra autorizzazione e assegnazione di diritti di accesso.

[19] La necessità di un'autenticazione a due fattori deriva da una decisione del Consiglio federale del 4.6.2010. Per i dipendenti della Confederazione si usano certificati di classe B della SG-PKI. Nel caso di un sistema di server, l'autenticazione dell'utente si applica a livello di sistema operativo.

[20] Le differenze concettuali tra una password e un PIN sono spiegate nella considerazione tecnologica «Password vs. PIN» del 29.6.2012. Pertanto, i requisiti minimi esposti in questa sede per i PIN si applicano solo in misura limitata.

[21] Account funzionali impersonali possono essere assegnati solo in casi debitamente motivati (cfr. [Si002-Hi01]) e

	b) deve essere unica[22]; c) non può essere trasmessa a terzi; d) non deve essere annotata e deve essere conservata in un luogo protetto oppure gestita con un programma di cifratura di password[23]; e) deve essere composta da almeno 10 caratteri (18 caratteri per gli utenti con privilegi elevati) appartenenti ad almeno tre delle quattro categorie seguenti: lettere maiuscole, lettere minuscole, cifre e caratteri speciali; f) non deve essere troppo semplice né poter essere associata all'utente, ossia non deve contenere attributi quali ID utente, cognome, nome o data di nascita. T7.2* Le password iniziali assegnate dall'amministratore di sistema devono essere modificate al primo accesso. T7.3* Quando si modifica la password, occorre assicurarsi che la nuova password non corrisponda a una delle ultime dieci utilizzate. T7.4* Dopo un massimo di cinque tentativi di accesso falliti, la password deve essere bloccata e potrà essere riattivata solo nell'ambito di un processo ben definito. T7.5 Se si ha il sospetto che persone non autorizzate siano venute a conoscenza della password o che ne sia stato fatto un uso indebito, si deve immediatamente modificare la password. T7.6* A livello del server, si deve garantire che la password non possa essere letta sotto forma di testo né essere compromessa facilmente nell'ambito di un altro tipo di attacco.
T8	Accessi amministrativi e accessi remoti T8.1 Gli accessi amministrativi all'oggetto informatico da proteggere devono avvenire in modo controllato e documentato. In particolare, questi accessi devono essere protetti da un sistema di crittografia ed essere registrati e valutati in maniera ricostruibile. T8.2 I sistemi IT utilizzati per gli accessi amministrativi devono essere stati progettati appositamente per questo compito ed essere gestiti preferibilmente in una zona di gestione. L'utilizzo dei relativi account (privilegiati) deve poter essere attribuito a una persona. Inoltre, gli account possono disporre solo dei diritti di accesso minimi necessari e per il minor tempo possibile[24], devono essere assegnati a uno dei livelli che formano un'architettura a livelli[25] e possono essere utilizzati soltanto per scopi amministrativi all'interno del livello specifico (per evitare una *privilege escalation*). In particolare, gli account non possono essere utilizzati per accedere a Internet per scopi non amministrativi.

possono essere usati unicamente per accedere a oggetti informatici da proteggere con un bisogno di protezione non elevato (protezione di base).

[22] Nello specifico, non è consentito utilizzare la medesima password per autenticarsi e accedere a più sistemi IT e applicazioni.

[23] Sui SPL si utilizzerà la gestione personale delle password (shell 1).

[24] L'ideale è che gli account siano gestiti nell'ambito di una soluzione di *Privileged Access Management* (PAM) e siano validi solo per il tempo necessario per eseguire una determinata attività amministrativa.

[25] Un'architettura a livelli di questo tipo è definita ad esempio nella direttiva d'architettura AR012.

	T8.3 Un accesso remoto diretto da parte di un fornitore esterno è consentito se a) il titolare dell'oggetto è d'accordo e ha acconsentito a possibili violazioni del segreto d'ufficio conformemente ai processi specifici dell'ufficio o del dipartimento (cfr. [Si001-Hi03, Si001-Hi04); b) l'accesso avviene tramite un account dedicato e l'autenticazione dell'utente si basa su un mezzo di autenticazione e identificazione che presenta almeno il livello «medio» secondo l'allegato B; c) l'utilizzo di tale account è limitato nel tempo e monitorato; d) se tecnicamente possibile, l'accesso avviene tramite un *jump server*; e) la connessione tecnica di rete usata per l'accesso è protetta da un sistema di crittografia (ad es. tramite il protocollo SSH); e f) la possibilità di controllare i processi esternalizzati è sempre garantita.
Informazioni (dati)	
I1*	Ammissibilità dei sistemi IT Le informazioni rilevanti per l'attività possono essere memorizzate e trattate unicamente su sistemi IT di proprietà di un'UA dell'Amministrazione federale o per i quali l'osservanza dei requisiti tecnici di sicurezza previsti dalla presente direttiva è disciplinata contrattualmente (ad es. nell'ambito di una soluzione cloud).
I2	Confidenzialità e integrità I2.1 La confidenzialità e l'integrità delle informazioni rilevanti per l'attività devono essere sempre salvaguardate con l'ausilio di metodi crittografici[26], in funzione del bisogno di protezione e tenendo conto delle particolarità fisiche (questo requisito si applica anche ai dati di prova e ai dati produttivi usati a fini sperimentali). Se le informazioni vengono crittografate, le chiavi utilizzate devono essere gestite in modo da poter recuperare e quindi decrittare in qualsiasi momento tali informazioni. Di norma, ciò richiede una gestione complessa delle chiavi (con un meccanismo di *key recovery*) nonché la necessità di verificare periodicamente la possibilità di recuperare le informazioni. I2.2 I sistemi IT utilizzati devono essere atti a garantire che la confidenzialità e l'integrità delle informazioni siano salvaguardate adeguatamente[27].
I3	Disponibilità I3.1 La disponibilità delle informazioni rilevanti per l'attività deve essere garantita in qualsiasi momento, conformemente al bisogno di protezione.

[26] In particolare, devono essere protette con un sistema di crittografia del disco rigido le informazioni che presentano un bisogno di protezione elevato e che sono memorizzate su dischi rigidi facenti parte di sistemi di server che fisicamente non beneficiano di una protezione specifica.

[27] Sui sistemi MDM, ad esempio, in linea di principio non è consentito memorizzare e trattare informazioni classificate come CONFIDENZIALI né dati personali degni di particolare protezione o profili della personalità. È consentito farlo solo nel quadro di comunicazioni vocali crittografate [E027].

	I3.2 L'UA responsabile delle informazioni deve disporre di una strategia di backup[28] e deve metterla in atto. Questa strategia deve prevedere uno schema di rotazione dei backup denominato «Grandfather-Father-Son» (GFS) e un salvataggio offline dei dati importanti, in modo da renderne possibile il recupero anche in presenza di un malware che cifra i dati («ransomware»).
I4	Supporti di dati I supporti su cui vengono memorizzate le informazioni rilevanti per l'attività devono sempre essere protetti conformemente al bisogno di protezione delle informazioni. Soprattutto per quanto riguarda la riparazione e lo smaltimento dei supporti di dati[29], si devono definire e mettere in atto processi adeguati.
Sistemi IT	
S1	Appartenenza a una zona Il sistema IT deve essere assegnato a una zona ed essere gestito conformemente alla relativa zone policy[30].
S2	Aggiornamenti e correzioni di errori Il produttore del sistema IT deve garantire, per l'intera durata del ciclo di vita del sistema, la disponibilità di aggiornamenti e correzioni di errori (*patch*) che verranno tempestivamente verificati e installati[31]; in alternativa deve essere garantita la gestione del sistema IT in una zona dedicata e quanto più possibile isolata (ad es. zona tecnica) nonché la disponibilità di misure di sicurezza complementari atte a escludere la possibilità che altri oggetti informatici da proteggere dell'Amministrazione federale siano esposti a ulteriori minacce e rischi. Se è prevista una sostituzione, il sistema IT può continuare a essere utilizzato per un massimo di due anni, purché si provveda a descrivere in un piano SIPD come sarà garantita la continuità operativa.
S3	Account di servizio S3.1 Gli account utilizzati dai servizi di sistema (account di servizio) devono essere specifici[32] e dotati solo dei diritti minimi necessari per fornire il servizio previsto. S3.2* Gli account di servizio devono essere gestiti in maniera automatizzata e richiedono un'autenticazione tramite un metodo di crittografia forte. Questa autenticazione si basa preferibilmente sull'utilizzo della crittografia asimmetrica, e le chiavi private usate a tal fine devono essere

[28] Se l'UA responsabile è un beneficiario di prestazioni (BP), la strategia di backup può anche essere definita dal FP. Il BP deve però verificarla e, se la ritiene adeguata, accettarla. In questo caso è di fondamentale importanza verificare con regolarità l'efficacia della strategia: la possibilità di recuperare i dati in caso di perdita deve essere oggetto di controlli periodici e deve essere confermata dal BP.

[29] In caso di smaltimento di supporti di dati occorre in particolare accertarsi che non sia possibile recuperare il loro contenuto o i dati in essi memorizzati.

[30] Un sistema IT che non può essere assegnato a nessuna zona appartiene a Internet. In questo caso non esiste nessuna *zone policy* da rispettare. Ci possono essere altresì componenti di rete che non appartengono né a una zona né a Internet. Questi componenti devono essere documentati.

[31] Per i SPL che non sono costantemente collegati alla rete occorre garantire l'installazione di aggiornamenti e *patch* almeno una volta al mese.

[32] Un account di servizio è specifico se viene utilizzato per un solo servizio.

	conservate in un luogo sicuro. Se l'autenticazione si basa invece su password, queste devono essere chiaramente più complesse (e più lunghe) di quelle usate per l'autenticazione degli utenti.
S4	Protezione dell'integrità e contro i malware S4.1 L'integrità dei componenti software installati nel sistema IT deve essere garantita (ad es. per mezzo di firme digitali). In particolare, tutti i sistemi di server che presentano un bisogno di protezione elevato devono essere sottoposti a una verifica periodica della loro integrità[33]. S4.2 Se viene rilevata una perdita di integrità, il sistema IT deve essere immediatamente disconnesso dalla rete, messo in sicurezza e analizzato. Se la compromissione viene confermata, il sistema IT deve essere completamente rimosso e reinstallato. S4.3 Il sistema IT deve essere integrato in un piano di protezione contro i malware, redatto sulla base della strategia [SB003], che definisca in particolare i provvedimenti da adottare in caso di attacco da malware, quali servizi devono essere informati e secondo quali modalità.
S5	Client della Confederazione S5.1 Sul client della Confederazione le memorie interne non volatili (ad es. dischi rigidi) devono essere crittografate in maniera trasparente. Per i sistemi MDM si deve inoltre prevedere la possibilità di ripristinare da remoto le impostazioni di fabbrica del sistema e di cancellare tutte le informazioni memorizzate a livello locale. S5.2 In assenza di attività da parte dell'utente, l'accesso al client della Confederazione deve essere bloccato automaticamente (sui SPL dopo un massimo di 15 minuti e sui sistemi MDM dopo un massimo di 3 minuti). L'accesso al sistema deve poter essere bloccato anche manualmente. Se per motivi tecnici non è possibile attivare il blocco, l'accesso ai client della Confederazione incustoditi ma con sessione attiva deve essere protetto fisicamente (ad es. chiudendo a chiave il locale). S5.3 Nessuna funzione di esecuzione automatica (*autorun*) può essere attivata sul client della Confederazione in caso di collegamento di supporti di dati esterni (ad es. chiavette USB). S5.4 Gli utenti di un SPL non possono disporre di diritti locali di amministratore. S5.5 L'accesso amministrativo al SPL per fornire assistenza è consentito unicamente previa autorizzazione esplicita degli utenti.
S6	Periferiche S6.1 L'utilizzo delle periferiche è consentito se a) la periferica è stata acquistata da un servizio d'acquisto della Confederazione, e

[33] Decisione del Consiglio federale del 16.12.2009.

	b) la sua integrabilità[34] e la sua sicurezza di base sono state debitamente confermate dal FP. S6.2 La periferica deve essere configurata dal FP con le funzionalità minime richieste ed essere protetta da modifiche (della configurazione) non autorizzate. S6.3 Se il dispositivo viene utilizzato per stampare documenti classificati a) deve essere gestito a livello locale o esserci la possibilità di autenticare le persone che lo utilizzano, e b) le memorie interne non volatili (ad es. dischi rigidi) devono poter essere sovrascritte conformemente alle raccomandazioni applicabili[35]; la sovrascrittura deve poter essere avviata manualmente dall'utente o attivarsi automaticamente. S6.4 Per quanto riguarda l'utilizzo di periferiche private durante il lavoro mobile, occorre osservare la direttiva delle applicazioni [E026].
Applicazioni	
A1	Acquisto / sviluppo A1.1 Le applicazioni devono essere acquistate e sviluppate nel quadro di un processo metodico (preferibilmente conforme a HERMES[36]) e tenendo conto fin dall'inizio delle prescrizioni e raccomandazioni applicabili in materia di sicurezza[37] («buone pratiche»). A1.2 Durante lo sviluppo di software applicativi occorre assicurarsi in particolare che a) il codice sorgente sia conservato in un luogo sicuro; b) l'accesso ai relativi archivi (*repository*) sia chiaramente regolamentato e venga controllato in maniera ricostruibile; c) i processi di compilazione (*build*) siano monitorati ed eventuali modifiche alla «pipeline di compilazione» possano essere apportate unicamente sotto supervisione; d) il software venga sottoposto a test regolari; e e) l'integrità del software sia sempre garantita (ad es. per mezzo di firme digitali).
A2	Cura e manutenzione Sia per l'applicazione sia per i suoi componenti (ad es. librerie software) devono essere garantite una cura e una manutenzione professionali nell'arco del loro intero ciclo di vita. Queste attività comprendono, in particolare, anche l'installazione regolare degli aggiornamenti e delle correzioni di errori (*patch*) necessari ai fini della corretta operatività e della sicurezza.
Zone	

[34] Integrabilità significa, ad esempio, che il dispositivo può essere collegato agli elenchi dei collaboratori dell'Amministrazione federale per funzioni quali ScanToMail.
[35] P. es. DoD 5220.22-M o NIST SP 800-88.
[36] https://www.hermes.admin.ch/it
[37] Per lo sviluppo di applicazioni web si dovrà tener conto, ad esempio, delle direttive e delle raccomandazioni dell'«Open Web Application Security Project» (OWASP), che contemplano anche la gestione sicura dei codici di programma.

Z1	Conformità Z1.1 La zona deve essere conforme al modello delle zone della Confederazione e avere un proprietario, un nome univoco[38], una *zone policy* e un gestore[39] (non vale per Internet e per la zona Internet). Se la zona comprende sistemi IT e applicazioni gestiti al di fuori dell'Amministrazione federale (ad es. in un cloud pubblico), la connessione degli elementi a livello di rete deve essere descritta nella *zone policy*. Z1.2 Il gestore deve garantire che possano avere luogo soltanto le comunicazioni da e verso la zona consentite dalla *zone policy* e che, con l'ausilio di adeguate misure di sicurezza complementari (ad es. isolamento e segmentazione), tali comunicazioni non espongano a ulteriori minacce e rischi altri sistemi IT e applicazioni all'interno e all'esterno della zona. Z1.3 La zona deve essere inclusa nell'elenco tenuto dall'ISIU competente. Un ISIU è competente quando il proprietario o il gestore della zona è un'unità amministrativa del dipartimento di sua competenza.
Z2	Accessi Z2.1 L'accesso limitato[40] a una zona è consentito unicamente a persone e a processi automatizzati che si autenticano con un mezzo di autenticazione e identificazione almeno di livello «medio» (per gli apparecchi di misurazione è sufficiente il livello «basso»). Sono ammesse le seguenti deroghe: a) accessi anonimi e personalizzati creati nel quadro delle applicazioni di Governo elettronico e di cui può beneficiare una larga fascia della popolazione in una zona server. I siti Internet corrispondenti devono essere protetti mediante certificati TLS (HTTPS) e i moduli protetti contro eventuali attacchi automatizzati (ad es. mediante CAPTCHA); b) accessi limitati nel tempo per caricare dati su un sistema di server[41]; c) accessi automatizzati eseguiti con il consenso del proprietario della zona nell'ambito di controlli della sicurezza di pagine web (*scan*). Se si accede a una zona con un elevato bisogno di protezione (ad es. SZ+), il mezzo di autenticazione e identificazione deve presentare almeno il livello di sicurezza «elevato» secondo l'allegato B e, in tal caso, le deroghe a) e b) di cui sopra non sono ammesse.

[38] L'univocità può essere ottenuta, ad esempio, associando l'identificativo del proprietario al nome come suffisso (ad es. SZ-BAC per una zona server gestita dalla Base d'aiuto alla condotta [BAC]). Se un proprietario attiva più volte una zona, i nomi corrispondenti devono essere chiaramente distinguibili.

[39] Il gestore è un FP che gestisce la zona per conto del proprietario dal punto di vista della tecnologia delle reti. Se il proprietario della zona è un FP, il proprietario e il gestore possono coincidere. Nel caso in cui il proprietario di una (sotto)zona modifichi la *policy*, al gestore deve essere concesso un termine adeguato per l'attuazione della stessa.

[40] Un accesso si dice limitato quando, mediante provvedimenti tecnici (ad es. filtraggio pacchetti IP), è limitato a uno o pochi sistemi IT definiti o a una o poche applicazioni definite e ai protocolli obbligatoriamente necessari per l'accesso. Altrimenti, l'accesso si dice illimitato.

[41] In questo caso la distinzione dei sistemi di server corrispondenti dagli altri sistemi IT nella stessa zona deve essere documentata nella *zone policy* oppure nella documentazione sulla sicurezza dell'applicazione insieme a tutte le misure di sicurezza complementari prese allo scopo di minimizzare i rischi. Naturalmente, anche il proprietario della zona deve essere d'accordo con l'esercizio dei sistemi di server.

	Z2.2 L'accesso illimitato a una zona è consentito unicamente a persone che si collegano tramite un client della Confederazione, sono autenticate con un mezzo di autenticazione e identificazione almeno di livello «elevato» secondo l'allegato B e utilizzano una connessione protetta da un sistema di crittografia (ad es. con SSH).
Z3	Comunicazione tra zone Qualsiasi comunicazione tra zone deve passare attraverso una PEZ[42]. Essa deve garantire che la comunicazione sia conforme alla pertinente *zone policy*. A tal fine, i modelli e le relazioni di comunicazione autorizzati devono essere definiti con la massima precisione nelle *zone policy*, idealmente a livello applicativo e sotto forma di «elenco dei contatti autorizzati» (*allow list*). Se non è possibile verificare la conformità in una PEZ (ad es. nel caso di una comunicazione end-to-end crittografata), la verifica può essere effettuata anche tramite i sistemi IT nelle zone stesse (sotto forma di PEP). Occorre tuttavia prevedere e documentare l'adozione di misure complementari e di attenuazione dei rischi.
Z4	PEZ Z4.1 I PEP gestiti in una PEZ possono essere gestiti virtualmente solo all'interno della relativa zona: ciò significa che nell'hardware utilizzato in comune non è consentito gestire sistemi IT di altre zone. Z4.2 Il proprietario di una PEZ o di un'infrastruttura web proxy deve disciplinare le modalità di accesso alle risorse in Internet e gli accessi consentiti. Tale regolamentazione può essere definita nella *zone policy* della PEZ o in una direttiva separata. Nell'ambito del servizio standard TIC Comunicazione di dati, la regolamentazione viene definita nel quadro della direttiva [Si004]. Z4.3 La connessione di una PEZ a Internet deve essere altamente disponibile ed eventualmente ridondante. Inoltre, il gestore deve garantire con misure appropriate che i sistemi IT separati da Internet tramite la PEZ siano adeguatamente protetti da attacchi DoS e DDoS.
Z5	Monitoraggio Z5.1 All'interno di una zona, la comunicazione deve essere monitorata in modo da poter individuare gli attacchi nel modo più affidabile possibile (ad es. con l'ausilio di sistemi di individuazione degli attacchi [IDS] o di prevenzione degli attacchi [IPS]) e da permettere al gestore di reagire rapidamente e in maniera adeguata in caso di necessità. Z5.2 Le informazioni di cui si viene a conoscenza durante il monitoraggio devono essere conservate in conformità alle disposizioni legali (in particolare, alla legislazione sulla protezione dei dati e all'ordinanza del 22 febbraio 2012 sul trattamento di dati personali derivanti dall'utilizzazione dell'infrastruttura elettronica della Confederazione) e protette da successive manipolazioni.

[42] Sebbene ciò si applichi in linea di principio anche alle comunicazioni da una sottozona alla zona sovrastante, si può derogare in casi giustificati e documentati nelle politiche delle rispettive sottozone.

5 Entrata in vigore

[1] La presente direttiva entra in vigore il 5 luglio 2024

[2] Per quanto riguarda gli oggetti informatici da proteggere che sono stati messi in funzione prima dell’entrata in vigore della presente direttiva restano valide le direttive in vigore al momento della loro messa in funzione.

Abbreviazioni

BAC	Base d’aiuto alla condotta
BCM	Business Continuity Management (gestione della continuità operativa)
BP	Beneficiario di prestazioni
CA	Certification Authority
CaF	Cancelleria federale
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CC	Client della Confederazione
CZ	Client Zone
DDoS	Distributed Denial of Service
DIS	Draft International Standard
DNS	Domain Name System
DoS	Denial of Service
EAL	Evaluation Assurance Level
FIDO	Fast ID Online
FP	Fornitore di prestazioni
IAM	Identity and Access Management
ID	Identificatore
IDS	Intrusion Detection System (sistema di individuazione delle intrusioni)
IEC	International Electrotechnical Commission
IKE	Internet Key Exchange
IoT	Internet of Things (Internet delle cose)
IP	Internet Protocol
IPS	Intrusion Prevention System (sistema di prevenzione delle intrusioni)
IPsec	IP security
ISID	Incaricato della sicurezza informatica del dipartimento
ISIU	Incaricato della sicurezza informatica dell’unità amministrativa
ISO	International Organization for Standardization
LoA	Level of Assurance
LSIn	Legge sulla sicurezza delle informazioni
IT	Information Technology (tecnologie dell’informazione)
ITSCM	IT Service Continuity Management
JSON	JavaScript Object Notation
JWT	JSON Web Token
MDM	Mobile Device Management
NCSC	Centro nazionale per la cibersicurezza
NW	Network Full Access (accesso illimitato alla rete)
OCiber	Ordinanza sui ciber-rischi
OPrI	Ordinanza sulla protezione delle informazioni
OSI	Open Systems Interconnection

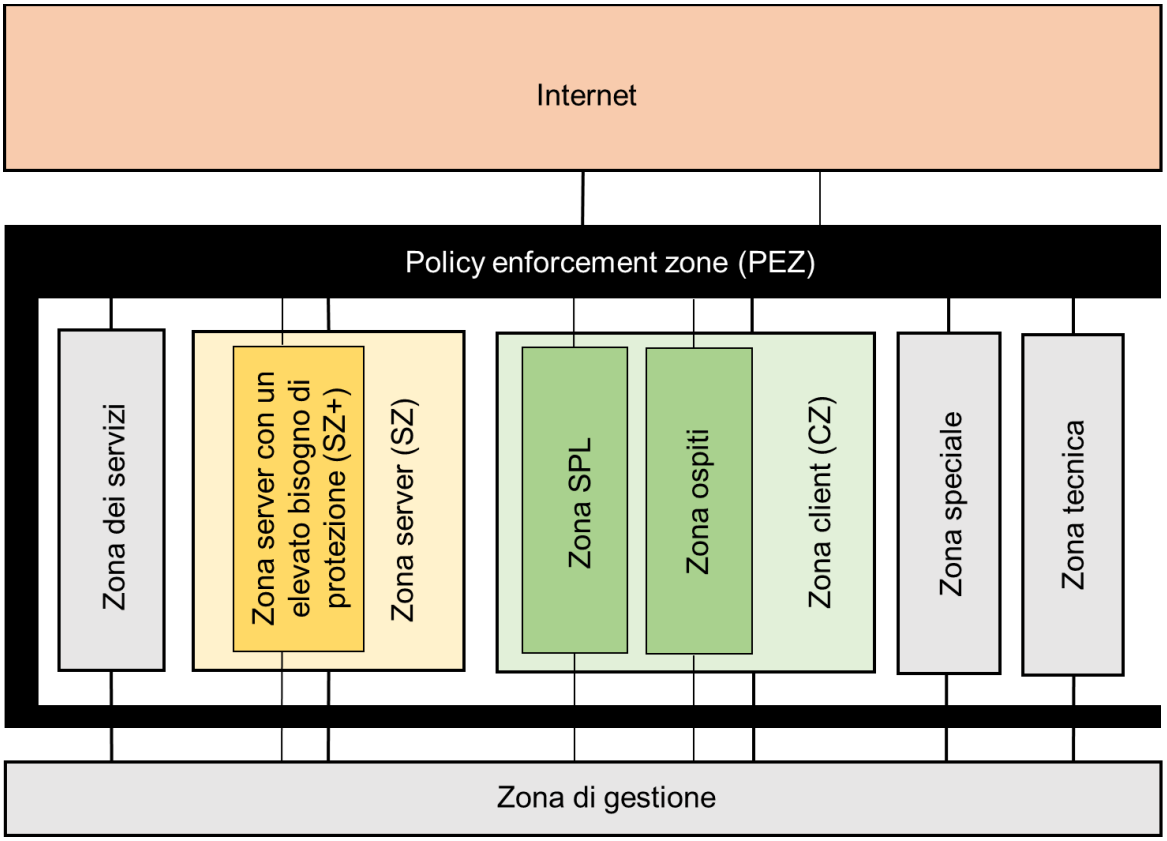
OTP	One-Time Password
OWASP	Open Web Application Security Project
PAM	Privileged Access Management
PEP	Policy Enforcement Point
PEZ	Policy Enforcement Zone
PIN	Personal Identification Number (numero d’identificazione personale)
PKI	Public Key Infrastructure (infrastruttura a chiave pubblica)
RA	Restricted Access (accesso limitato alla rete)
SAML	Security Assertion Markup Language
SG-PKI	Swiss Government PKI
SIPD	Sicurezza delle informazioni e protezione dei dati
SMS	Short Message Service
SPL	Sistema di postazioni di lavoro
SS	Servizio standard
SSH	Secure Shell
SSO	Single Sign-On
SSZ	Shared Service Zone
SZ	Server Zone (zona server)
SZ+	Server Zone+ (zona server con un elevato bisogno di protezione)
TCP	Transmission Control Protocol
TDT	Trasformazione digitale e governance delle TIC (settore della CaF)
TE	Terminale esterno
TIC	Tecnologie dell’informazione e della comunicazione
TLS	Transport Layer Security
TPM	Trusted Platform Module
UA	Unità amministrativa
UFCL	Ufficio federale delle costruzioni e della logistica
UFCS	Ufficio federale della cibersicurezza

Riferimenti

[OCiber]	Ordinanza del 27 maggio 2020 sui ciber-rischi (OCiber)
[E021]	TDT, E021 – Direttiva delle applicazioni «Smartphone/Smarttablet Sync», versione 2.1 del 9 giugno 2020 (disponibile solo in tedesco e francese)
[E026]	TDT, E026 – Direttiva delle applicazioni «Arbeitsplatzsystem», versione 1.0 dell’11 giugno 2019 (disponibile solo in tedesco e francese; in corso di rielaborazione con riferimento al lavoro mobile)
[E027]	TDT, E027 – Direttiva delle applicazioni concernente la comunicazione vocale crittografata (CVC), versione 1.1 del 1° ottobre 2021
[LSIn]	Legge federale del 18 dicembre 2020 sulla sicurezza delle informazioni in seno alla Confederazione (Legge sulla sicurezza delle informazioni, LSIn)
[OSIn]	Ordinanza dell’8 novembre 2023 sulla sicurezza delle informazioni in seno all’Amministrazione federale e all’esercito (ordinanza sulla sicurezza delle informazioni, OSIn)
[SB003]	NCSC, «Malwareschutz Strategie in der Bundesverwaltung», 2021 (disponibile solo in tedesco)
[Si001-Hi01]	Attuazione delle misure per la protezione di base delle TIC nell’Amministrazione federale, versione 4.6 del 31 marzo 2021
[Si001-Hi03]	Direttive per evitare i rischi di violazione del segreto d’ufficio nell’Amministrazione federale, versione 1.4 del 31 marzo 2021
[Si001-Hi04]	Raccomandazione per l’applicazione operativa della procedura di ottenimento del consenso in relazione all’articolo 320 CP, 15 dicembre 2020
[Si002-Hi01]	Richiesta di autorizzazione speciale per account impersonali (account E e F), 15 dicembre 2020
[Si004]	«Regelung der Zugriffe auf Ressourcen im Internet, Web Proxy Richtlinie BV», versione 1.3 del 4 ottobre 2016 (stato: 1° aprile 2019, disponibile solo in tedesco e francese)

Allegato A: Modello delle zone della Confederazione

Il modello delle zone della Confederazione (cfr. figura A.1) è un modello generico che serve a definire le zone nell'Amministrazione federale. Esso stabilisce i sistemi IT e le reti dell'Amministrazione federale che devono essere organizzati e gestiti in zone e sottozone.



igura A.1: Modello delle zone della Confederazione

Nel modello delle zone della Confederazione si fa una distinzione tra le seguenti zone e sottozone:

a) **Internet:** zona che non corrisponde a nessun criterio delle altre zone e per la quale non può essere definito nessun requisito (di sicurezza);
b) ***policy enforcement zone* (PEZ):** zona per i PEP necessari per l'applicazione delle regole relative alla comunicazione esterna con altre zone;
c) **zona dei servizi (*service zone*):** zona destinata ai sistemi di server necessari per la fornitura di servizi infrastrutturali (ad es. server DNS e *time server*);
d) **zona server (server zone, SZ):** zona destinata ai sistemi di server;
e) **zona server con un elevato bisogno di protezione (SZ+):** sottozona della SZ per i sistemi di server sui quali sono gestite in particolare applicazioni che presentano un bisogno di protezione elevato secondo l'analisi del bisogno di protezione;
f) **zona client (client zone, CZ):** zona per i sistemi client. L'esercizio di sistemi di server nella CZ o in una sottozona è ammesso se la *policy* corrispondente lo prevede e se i sistemi di server sono utilizzati principalmente dai sistemi client della stessa (sotto)zona (ad es. server locale per la burotica o di stampa);

g) **zona SPL:** sottozona della CZ per i sistemi client che funzionano come sistemi di postazioni di lavoro (SPL) e sono utilizzati esclusivamente dal servizio standard TIC Burotica/UCC;
h) **zona ospiti:** sottozona della CZ per i sistemi client che non sono gestiti da un’UA della Confederazione, ad esempio dispositivi utilizzati da collaboratori esterni o da dipendenti dell’Amministrazione federale nell’ambito della politica «Bring Your Own Device»;
i) **zona speciale:** zona per i sistemi IT dell’Amministrazione federale che presentano caratteristiche speciali ed esigenze corrispondenti, come ad esempio l’autonomia operativa o la connessione alla rete a banda stretta, e che possono essere gestiti dalla zona di gestione (ad es. rete di trasporto con requisiti specifici);
j) **zona tecnica:** zona specifica per i sistemi IT e IoT, come ad esempio i sistemi per l’impiantistica degli edifici o per il *facility management*, i sistemi di rilevamento del tempo di lavoro, i sistemi di misurazione e i sistemi di supporto diagnostico a distanza;
k) **zona di gestione:** zona specifica per i sistemi IT che sono utilizzati esclusivamente per amministrare i sistemi IT di altre zone.

Ogni (sotto)zona del modello delle zone dell’Amministrazione federale può essere attivata più volte.

Allegato B: Livelli di sicurezza per i mezzi di autenticazione e identificazione

I mezzi di autenticazione e di identificazione attualmente disponibili o in uso con i relativi sistemi federati sono suddivisi nei seguenti quattro livelli di sicurezza (basso, medio, elevato e molto elevato) [43]:

a) **basso:** le credenziali di autenticazione trasmesse attraverso la rete sono statiche e identiche per ogni autenticazione, vale a dire che possono essere intercettate da un aggressore e utilizzate illecitamente, ad esempio durante un *replay-attack*, nel quale viene simulata l'identità del titolare delle credenziali. Tipici esempi di credenziali di questo tipo sono il nome utente e la password. Se sono utilizzate come token per l'autenticazione federata ai sensi del documento I050, le credenziali di autenticazione devono essere protette solo marginalmente contro gli attacchi all'integrità e associate al contesto dell'utente. Possibili esempi sono diversi token d'accesso come i cookies;

b) **medio:** le credenziali di autenticazione cambiano a ogni accesso e risultano dunque dinamiche. Tali credenziali non possono quindi essere utilizzate illecitamente durante un *replay-attack*, nel quale viene simulata l'identità del titolare delle credenziali. Esempi di credenziali di questo tipo sono il nome utente e la password con codice di verifica via SMS o vincolati al dispositivo, le soluzioni software OTP (ad es. Google Authenticator), implementazioni FIDO2 (p. es. passkey) con opzioni di sincronizzazione ed esportazione di chiavi nonché i certificati di software emessi dalla SG-KPI (classe C, D o E). Le credenziali utilizzate come token per l'autenticazione federata devono essere protette contro gli attacchi all'integrità e associate al contesto dell'utente (p. es. «sessione») conformemente allo stato della tecnica. Esempi di credenziali di questo tipo sono i cosiddetti ticket Kerberos delle foreste di risorse del servizio standard TIC Burotica nonché i token d'accesso trasmessi tramite SAML o OIDC/OAuth come JWT;

c) **elevato:** le credenziali di autenticazione sono dinamiche e protette da una chiave crittografica memorizzata in un modulo hardware dedicato, dal quale non può essere letta (con un dispendio ragionevole). Se il mezzo di autenticazione e identificazione è personale, la registrazione della persona interessata o la consegna del mezzo di identificazione ad essa deve essere effettuata sulla base di un documento d'identità ufficiale (ad es. passaporto o carta d'identità). Se l'identità della persona viene verificata all'atto della registrazione, il mezzo di identificazione deve essere consegnato con raccomandata. La consegna può anche essere protetta mediante un codice segreto (ad es. password o PIN) o un elemento biometrico (ad es. Touch ID o Face ID per Apple o Hello per Windows). Esempi di credenziali di questo tipo sono i token OTP, le soluzioni OTP basate su un *Trusted Platform Module* (TPM), implementazioni FIDO2 (p. es. passkey) senza opzioni di sincronizzazione ed esportazione di chiavi e Swisscom Mobile ID. Le credenziali utilizzate come token per l'autenticazione federata devono essere protette contro gli attacchi all'integrità e associate al contesto dell'utente conformemente allo stato della tecnica. Nel complesso, il sistema federato deve corrispondere a un profilo di protezione equivalente ai Common Criteria EAL4+. Esempi di credenziali di questo tipo sono SSO-Identity e SSO-Federation del portale SSO e i ticket Kerberos delle foreste di

[43] Lo standard TIC I050 definisce quattro livelli di affidabilità (*Level of Assurance*, LoA), ai quali si potrebbe ricorrere per specificare i requisiti minimi di sicurezza dei mezzi di autenticazione e identificazione da impiegare..

utenti, se questi sono stati emessi sulla base di un'autenticazione dell'utente con certificato di classe B rilasciato dalla SG-PKI;

d) **molto elevato:** i mezzi di autenticazione e identificazione soddisfano i requisiti del livello «elevato» (compresi quelli relativi al sistema federato). Inoltre, sia il modulo hardware che il rispettivo processo di registrazione devono essere riconosciuti per essere utilizzati nell'Amministrazione federale. Gli unici esempi in questo caso sono i certificati emessi dalla SG-PKI sulle smart card (classe B).

Gli esempi menzionati e riassunti nella tabella B.1 non sono esaustivi.

Livello di sicurezza	Esempi di mezzi di autenticazione e identificazione
Basso	• Nome utente e password • Token d'accesso (ad es. cookie)
Medio	• Nome utente e password con codice di verifica via SMS[44] • Nome utente e password vincolati al dispositivo • Soluzione software OTP (ad es. Google Authenticator) • Implementazioni FIDO2 (p. es. passkey) con opzioni di sincronizzazione ed esportazione di chiavi • Certificato di software emesso dalla SG-PKI (classe C, D o E) • Ticket Kerberos delle foreste di risorse del servizio standard TIC Burotica • Token d'accesso trasmessi tramite SAML o OIDC/OAuth come JWT
Elevato	• Token OTP (ad es. RSA, Vasco ecc.) • Soluzione OTP basata su un TPM • implementazioni FIDO2 (p. es. passkey) senza opzioni di sincronizzazione ed esportazione di chiavi Swisscom Mobile ID • Swisscom Mobile ID • SSO-Identity e SSO-Federation del portale SSO • Ticket Kerberos delle foreste di utenti (SG-PKI[45]) • Token SAML emesso nell'ambito di eIAM (SG-PKI)
Molto elevato	• Certificato emesso dalla SG-PKI su smart card (classe B)

Tabella B.1: Livelli di sicurezza di alcuni mezzi di autenticazione e identificazione

In linea di principio il livello di sicurezza non può essere aumentato accumulando diversi mezzi di autenticazione e identificazione. Ciò significa che un certificato software emesso dalla SG-PKI continua a mantenere, ad esempio, il livello di sicurezza «medio» anche se combinato con nome utente e password con codice di verifica via SMS.

[44] In linea di massima, le procedure di autenticazione basate su SMS vanno usate solo in assenza di alternative migliori.

[45] Secondo le spiegazioni del testo, sia i ticket Kerberos che i token SAML devono essere stati emessi sulla base dell'autenticazione dell'utente con un certificato di classe B emesso dalla SG-PKI.

Allegato C: *Zone policy* per il «dominio di rete blu»

C.1 Requisiti e direttive per i sistemi TIC

[1] Il «dominio di rete blu» e la Shared Service Zone (SSZ) sono ancora disponibili per motivi di retrocompatibilità. Per la SSZ è disponibile una *zone policy*.

[2] Fino a quando non sarà chiarita la proprietà del dominio di rete blu e non saranno emesse le direttive corrispondenti, fanno fede sia la *zone policy* dell'allegato C con tutte le autorizzazioni di deviazione (eccezioni) e gli accordi[46] che la matrice d'accesso dell'allegato D.

[3] Un sistema TIC può essere utilizzato nel dominio di rete blu se soddisfa i requisiti della procedura di sicurezza ai sensi dell'articolo 16 LSIn e dell'articolo 27 OSIn.

C.2 Requisiti e direttive per il dominio di rete blu

[1] Il dominio di rete blu può essere segmentato sulla rete.

[2] È possibile effettuare una suddivisione in sottozone ai sensi del numero 2 capoverso 2 lettera j.

C.3 Requisiti e direttive per le comunicazioni consentite

C.3.1 Comunicazione interna

[1] La comunicazione interna può essere effettuata direttamente e non soggiace ad alcuna restrizione derivante da una segmentazione della rete.

C.3.2 Comunicazione esterna

[1] La comunicazione esterna non deve essere effettuata direttamente ma deve avvenire tramite uno o più PEP (ad es. in una PEZ).

[2] Si deve garantire che un sistema TIC del dominio di rete blu non possa mantenere contemporaneamente più comunicazioni esterne con i sistemi TIC di altre zone.

[3] Per le comunicazioni in entrata valgono i requisiti e le direttive seguenti.

a) È possibile utilizzare soltanto protocolli noti e standardizzati o per i quali esiste un server proxy inverso affidabile. Per i servizi web si devono utilizzare i protocolli e i formati di dati SOAP/XML, REST/XML e/o REST/JSON.
b) La comunicazione viene garantita da un server proxy inverso che (i) autentica la persona che inizia la comunicazione, (ii) protegge il traffico dati e (iii) registra e valuta tempestivamente i relativi dati secondari. Nel caso dei servizi web è sufficiente autenticare i processi (consumatori e fornitori di questi servizi) in base a certificati SSL/TLS riconosciuti, e la protezione del traffico dati deve essere effettuata verificando il contenuto dei messaggi[47] nonché autenticando e crittografando i dati in maniera trasparente in base all'HTTPS.

[46] Si tratta di accordi stipulati con i Servizi del Parlamento.
[47] Se è necessaria una crittografia end-to-end tra il consumatore e il fornitore del servizio web e se il firewall di questo servizio non può verificare direttamente il contenuto dei messaggi, devono essere adottate misure complementari per garantire che il contenuto dei messaggi sia controllato almeno indirettamente.

c) Un accesso illimitato alla rete è possibile soltanto da un sistema TIC gestito da un’unità organizzativa dell’Amministrazione federale.

4 Alle comunicazioni in uscita si applica la direttiva sui web proxy dell’Amministrazione federale [Si004].

Allegato D: Matrice d'accesso per il dominio di rete blu e la SSZ

Le seguenti tabelle sono riprese dalla versione 4.0 della matrice d'accesso (precedentemente Si002) e valgono per l'autenticazione di persone al dominio di rete blu e alla SSZ (tabella D.1) o per l'autenticazione di sistemi partner e processi (tabella D.2). Restano valide le eccezioni riguardanti le applicazioni di Governo elettronico (requisito Z2.1 lett. a).

	Livello di protezione	**Base (LP0)**				**1 (LP1)**				**2 (LP2)**			
	Terminale utente	CC	CC	TE	TE	CC	CC	TE	TE	CC	CC	TE	TE
	Metodo di accesso	NW	AL	NW	AL	NW	AL	NW	AL	NW	AL	NW	AL
Dominio di rete blu	Hard Crypto Token	Sì	Sì	No	Sì	Sì	Sì	No	Sì	Sì	Sì	No	Sì
	OTP	Sì	Sì	No	Sì	Sì	Sì	No	Sì	Sì	Sì	No	Sì
	OTP senza dispositivo	No	Sì	No	Sì	No	Sì	No	Sì	No	No	No	No
	Soft Crypto Token	No	No	No	No	No	No	No	No	No	No	No	No
	Password o PIN token	No	No	No	No	No	No	No	No	No	No	No	No
SSZ	Hard Crypto Token	Sì[48]	Sì	No	Sì	Sì[50]	Sì	No	Sì	Sì[50]	Sì	No	Sì
	OTP	Sì[50]	Sì	No	Sì	Sì[50]	Sì	No	Sì	Sì[50]	Sì[50]	No	Sì
	OTP senza dispositivo	No	Sì	No	Sì	No	Sì	No	Sì	No	No	No	No
	Soft Crypto Token	No	Sì	No	Sì	No	Sì	No	Sì	No	No	No	No
	Password o PIN token	No	Sì	No	Sì	No	Sì	No	Sì	No	No	No	No

Tabella D.1: Autenticazione di persone al dominio di rete blu o alla SSZ

	Livello di protezione	**Base (LP0)**		**1 (LP1)**		**2 (LP2)**	
	Metodo di accesso	NW	AL	NW	AL	NW	AL
Dominio di rete blu / SSZ	Hard Crypto Token	No	Sì	No	Sì	No	Sì
	OTP / OTP senza dispositivo	Nessuna applicazione pratica					
	Soft Crypto Token	No	Sì	No	Sì	No	Sì[49]
	Password o PIN token	No	Sì[50]	No	No	No	No

Tabella D.2: Autenticazione di sistemi partner e relativi processi

[48] L'unico caso è l'amministrazione di sistemi tramite rete Admin-LAN (zona di gestione del FP).
[49] Concesso soltanto per l'accesso a Sedex e ad altre applicazioni, attraverso le quali possono essere scambiati unicamente messaggi standardizzati e/o possono essere seguiti processi definiti.
[50] Concesso soltanto per dati telemetrici (apparecchi di misurazione).