Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Centro nazionale per la cibersicurezza NCSC
Sicurezza informatica della Confederazione

Versione 4.5

P041 – Analisi del bisogno di protezione

del 19 dicembre 2013 (stato: 1° aprile 2021)

Ai sensi dell'articolo 11 capoverso 1 lettera e dell'ordinanza del 27 maggio 2020 sui ciber-rischi (OCiber), il delegato alla cibersicurezza emana la seguente direttiva per l'analisi del bisogno di protezione di cui all'articolo 14*b* OCiber.

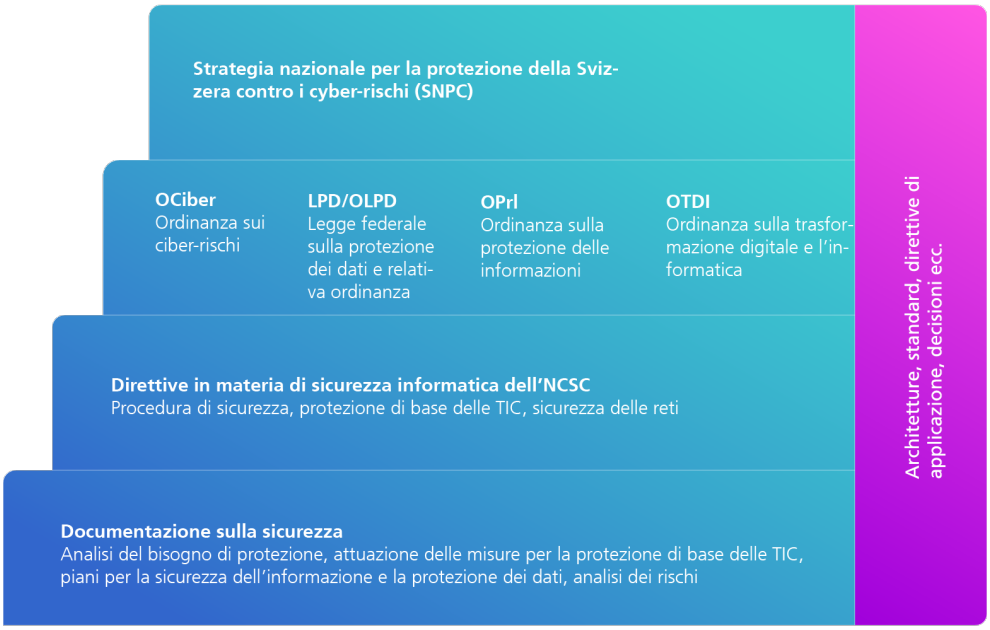

Immagine 1: Struttura delle basi per la sicurezza informatica

Indice

1 Analisi del bisogno di protezione

L'analisi del bisogno di protezione consiste nel rilevamento dei requisiti di sicurezza degli oggetti informatici da proteggere. Essa deve essere verificata almeno dall'incaricato della sicurezza informatica dell'unità amministrativa (ISIU)[1] nonché approvata dal committente e dal responsabile dei processi aziendali.

Nell'analisi del bisogno di protezione si devono rilevare almeno i seguenti dati.

1.1 Dati riferiti all'oggetto informatico da proteggere

- Nome del progetto/dell'oggetto da proteggere (per l'oggetto da proteggere esistente)
- Dipartimento/Ufficio
- Numero del progetto/ID del progetto
- Processi aziendali supportati
- Classificazione del documento (non classificato, AD USO INTERNO, CONFIDENZIALE, SEGRETO)
- Responsabile del processo aziendale (nome, UA)
- Capoprogetto (CP BP) (nome, UA)
- Responsabile della sicurezza delle informazioni e della protezione dei dati dell'unità amministrativa (nome, UA), *se già deciso*
- Incaricato della della sicurezza informatica ISIU (nome, UA)
- Documento compilato da (nome, UA)

- Risultato della classificazione (rappresentazione della classificazione)

- Controllo delle modifiche

- Firme
    - Verificato: ISIU (data, nome, UA)
    - Approvato: committente (data, nome, UA)
    - Approvato: responsabile del processo aziendale (data, nome, UA)

Ulteriori dati possono essere richiesti in singoli casi.

1.2 Validità dell'analisi del bisogno di protezione

L'analisi del bisogno di protezione è valida per cinque anni al massimo.

[1] Nel caso dei servizi standard, la verifica compete al rispettivo incaricato della sicurezza informatica.

1.3 Classificazione

Nell'analisi del bisogno di protezione è necessario valutare i seguenti elementi.

Elementi valutati	*Domanda*	*Risposte*	*Spiegazioni*
Confidenzialità	Con questo oggetto da proteggere si devono trattare dati personali ai sensi della normativa sulla protezione dei dati? In caso affermativo, che tipo di dati personali sono interessati?	Nessun dato personale	
		Dati personali	Tutte le informazioni relative a una persona identificata o identificabile sono *dati personali*. Essi vengono chiamati *dati personali non sensibili* se non sono degni di particolare protezione.
		Dati personali degni di particolare protezione o profili della personalità	Si definiscono *dati personali degni di particolare protezione («sensibili»)* i dati concernenti: le opinioni o attività religiose, filosofiche, politiche o sindacali, la salute, la sfera intima o l'appartenenza a una razza, le misure d'assistenza sociale e i procedimenti o le sanzioni amministrativi e penali. Un *profilo della personalità* è una compilazione di dati che permette di valutare caratteristiche essenziali della personalità di una persona fisica.
		Dati personali il cui uso improprio comporta rischi elevati per la vita o l'incolumità delle persone interessate	Se la divulgazione di dati degni di particolare protezione può comportare una minaccia, in particolare per la vita o l'incolumità della persona interessata, si parla *dati personali molto sensibili (d'importanza vitale)*.
	[Con questo oggetto da proteggere] si devono trattare le informazioni classificate ai sensi dell'ordinanza sulla protezione delle informazioni (OPrI)? In caso affermativo, quali informazioni e a quali livelli di classificazione (cfr. art. 5−7 OPrI) sono interessati?	Nessuna classificazione	*Nota bene*: Sono da osservare in particolare le istruzioni concernenti prescrizioni dettagliate sulla protezione delle informazioni (istruzioni sul trattamento) e le istruzioni sulla classificazione (catalogo di classificazione)[2]. *Aiuto:* Per maggiori informazioni riguardo alla classificazione dei dati, rivolgersi all'incaricato della protezione delle informazioni del dipartimento o all'organo di coordinamento per la protezione delle informazioni in seno alla Confederazione (annesso al DDPS).

[2] Vedi le prescrizioni in materia di protezione delle informazioni del DDPS (documento 52.064 d, disponibile solo in tedesco).

	Classificazione: AD USO INTERNO	Sono classificate *AD USO INTERNO* le informazioni la cui conoscenza da parte di persone non autorizzate può pregiudicare gli interessi nazionali e che non possono essere classificate a un livello superiore (art. 7 OPrl).
	Classificazione: CONFIDENZIALE	Sono classificate *CONFIDENZIALE* le informazioni la cui conoscenza da parte di persone non autorizzate può causare un danno agli interessi nazionali (art. 6 OPrl).
	Classificazione: SEGRETO	Sono classificate *SEGRETO* le informazioni la cui conoscenza da parte di persone non autorizzate può causare un danno grave agli interessi nazionali (art. 5 OPrl).
[Con questo oggetto da proteggere] si devono trattare informazioni o dati che devono essere particolarmente protetti per un motivo preciso (normative speciali[3])? In caso affermativo, quanto devono essere elevati i requisiti di protezione?	Non sono necessari requisiti di riservatezza elevati	*Livello di protezione dei dati* • Le informazioni o i dati da trattare sono soggetti a prescrizioni speciali sulla tutela della riservatezza come ad esempio l'articolo 11 lettera e della legge federale sugli acquisti pubblici (LAPub), l'articolo 21 della legge sull'organizzazione del Governo e dell'Amministrazione (LOGA) o l'articolo 110 della legge sull'imposta federale diretta (LIFD)? • Con l'oggetto da proteggere si devono trattare informazioni o dati di cui occorre proteggere la riservatezza conformemente ad accordi con uno o più parti contraenti? • Un accesso non autorizzato alle informazioni o ai dati da trattare può essere considerato una violazione del segreto d'ufficio, professionale, d'affare o di fabbricazione rilevante dal punto di vista penale? *Nessun requisito particolare*: le misure per la protezione di base delle TIC sono già comprese.

[3] Normative speciali riguardanti il sistema sanitario, finanziario ecc.

		Requisiti di riservatezza elevati	*Requisiti elevati* devono essere stabiliti a seconda della situazione. Essi comprendono almeno le misure per la protezione di base delle TIC. Costituiscono un esempio le seguenti ulteriori misure: • nessuna pubblicazione su Intranet/Internet; • accesso sicuro con password monouso (one-time password), SMS di login (i soli nome utente e password non bastano) o persino mediante l'autenticazione a due fattori (hard crypto token); • crittografia del canale di trasmissione; • crittografia dei dati.
Disponibilità	Durata massima consentita di inattività	Inattività per più di 12 ore	I dati riguardanti l'inattività corrispondono alle definizioni riportate nell'elenco dei servizi standard della TDT[4].
		Inattività per 12 ore al massimo	Elenco dei servizi: classe di disponibilità 1
		Inattività per 8 ore al massimo	Elenco dei servizi: classe di disponibilità 2
		Inattività per 2 ore al massimo	Elenco dei servizi: classe di disponibilità 3
	Orari di servizio[5]	Orari di servizio standard (11 h / 5 gg.)	Dal lunedì al venerdì, ore 7.00-18.00; conformemente all'accordo contenuto nel SLA (vedi anche l'elenco dei servizi TIC del FP).
		Orari di servizio prolungati (11 h / 5 gg., CF)	Dal lunedì al venerdì, ore 7.00-18.00; orario prolungato fino alle 21.00 in occasione delle sedute del CF; descrivere i requisiti per gli orari di servizio prolungati.
		Orari di servizio continuati 24 h / 7 gg.	Servizio 24 ore su 24; se si tratta di un orario standard per un'UA/un FP, non è richiesto alcun piano SIPD aggiuntivo. I requisiti precisi devono essere definiti nel dettaglio in un SLA.
	L'IT Service Continuity Management (ITSCM) è rilevante [per questo oggetto da proteggere] ai fini del Business Continuity Management (BCM) per i processi	ITSCM/BCM non necessario	*Domande suggerite* • Cosa accade se il centro di calcolo (CC) non è più operativo? Ad es. causa incendio. • Cosa accade se le postazioni di lavoro (uffici) non sono più accessibili?

[4] Consultabile alla pagina: intranet.dti.bk.ch > Direttive TIC > Servizi standard > SD100 - Servicekatalog SD (disponibile in tedesco).
[5] Secondo l'elenco dei servizi standard
intranet.dti.bk.admin.ch > Direttive TIC > Servizi standard > SD100 - Catalogo dei servizi standard.

	aziendali critici?		• Ci sono soluzioni da adottare in caso di catastrofe? • Ci sono scenari d'emergenza? *Effetti possibili* • Le misure di prevenzione delle emergenze (inattività di un solo computer) devono essere adottate in ogni caso. • In caso di catastrofe (inattività di interi centri di calcolo per un periodo prolungato), i dati devono essere archiviati presso una terza sede esterna.
Integrità	Deve poter essere garantita l'autenticità, la correttezza e/o l'integrità dei dati?	Nessun requisito particolare	*Nessun requisito particolare*: le misure per la protezione di base delle TIC sono già comprese. *Domande suggerite* • Cosa accade se i dati sono incompleti? • L'elaborazione / la valutazione dei dati è a rischio?
		Requisiti particolari	*Effetti possibili* a) violazione delle leggi, delle prescrizioni o dei contratti vigenti; b) compromissione dei risultati; c) impedimento all'esecuzione dei compiti; d) impatto verso l'esterno negativo (ad es. immagine dell'AF); e) effetti finanziari (per l'Ufficio o l'AF, sotto il profilo dell'economia pubblica); f) che impatto ha sull'esecuzione dei compiti? Esempi di dati interessati: • dati riguardanti la salute; • rendiconti; • dati giuridicamente vincolanti; • backup; • ecc.

Tracciabilità	Devono essere comprovati determinati processi lavorativi?	Nessun requisito particolare	*Nessun requisito particolare*: le misure per la protezione di base delle TIC sono già comprese. *Aiuto* Per maggiori informazioni riguardanti la tracciabilità, rivolgersi al Controllo federale delle finanze (CDF) oppure all'IFPDT (Incaricato federale della protezione dei dati e della trasparenza).
		Requisiti particolari	*Domande suggerite* • Sono dati rilevanti dal punto di vista finanziario (ad es. dati contabili o di inventario)? • Vengono eseguiti controlli di sicurezza conformemente al manuale d'esercizio, del piano o di organizzazione? • Sono compromessi i principi della prova documentata? *Effetti possibili* • Violazione delle leggi, delle prescrizioni o dei contratti vigenti; • limitazione dell'obbligo d'informazione (diritto della personalità, privacy); • impedimento all'esecuzione di compiti; • ripercussioni finanziarie (per l'AF, sotto il profilo dell'economia pubblica).
Rilevanza per il processo di verifica RINA	L'oggetto da proteggere rischia di essere compromesso dallo spionaggio dei servizi d'informazione (o simili) e/o occorre prevedere acquisti delicati?	No, non è rilevante per il processo di verifica RINA.	
		Sì, è rilevante per il processo di verifica RINA.	Se la risposta alla domanda è affermativa, sussiste una rilevanza per il processo di verifica RINA. In questo caso è necessario verificare i criteri conformemente alle istruzioni del processo RINA[6] e adottare le misure del caso.

In casi specifici si possono richiedere ulteriori criteri di valutazione.

[6] Vedi intranet.ncsc.admin.ch > Direttive e ausili > Procedura di sicurezza > Valutazione del bisogno di protezione > P041 - Analisi del bisogno di protezione > P041-Hi02 - Guida al processo di verifica RINA (metodo di gestione dei rischi per ridurre lo spionaggio dei servizi d'informazione).

2 Bisogno di protezione elevato

Non appena uno dei campi classificati come confidenziali o più di due criteri negli ambiti disponibilità, integrità o tracciabilità sono contrassegnati in rosso, sussiste un bisogno di protezione elevato. Conformemente all'articolo 14d OCiber, in casi di bisogno di protezione elevato comprovato si deve elaborare un piano per la sicurezza e la protezione dei dati (piano SIPD) in cui devono essere definite, documentate e attuate ulteriori misure di sicurezza specifici per il progetto o l'oggetto informatico da proteggere, oltre all'attuazione delle direttive in materia di sicurezza per la protezione di base e facendo capo a un'analisi dei rischi.

Nel caso sussistano requisiti elevati soltanto negli ambiti disponibiltà, integrità o tracciabilità (due criteri al massimo), devono essere documentati ulteriori misure di sicurezza a estensione della protezione di base TIC. Tali requisiti devono essere inseriti preferibilmente nel documento «Attuazione delle misure per la protezione di base delle TIC», ad esempio in un capitolo aggiuntivo.

Se uno dei criteri per definire la rilevanza di RINA è soddisfatto, si deve eseguire il relativo processo di verifica per ridurre lo spionaggio dei servizi d'informazione (secondo la Guida al processo di verifica RINA[7]). Qualora, dal processo di verifica RINA, emergano casi rilevanti per i rischi, occorre svolgere integralmente il processo di verifica e documentarne l'attuazione. RINA è principalmente un processo di sensibilizzazione in cui vengono illustrate le possibili minacce derivanti dallo spionaggio dei servizi d'informazione.

[7] Vedi Intranet.ncsc.admin.ch > Direttive e ausili > Procedura di sicurezza > Valutazione del bisogno di protezione > P041 - Analisi del bisogno di protezione > P041-Hi02 - Guida al processo di verifica RINA (metodo di gestione dei rischi per ridurre lo spionaggio dei servizi d'informazione).