



Judith Schneider-Köppel, 18.10.2020

Pubblico

Sistema di gestione della sicurezza delle informazioni (SGSI) UFSPO

Manuale sulla sicurezza delle informazioni UFSPO

Verifica del documento	
Valido da / fino a	18.10.2021
Versione	5.0
Stato	Autorizzato
Tipo di documento	Manuale
Distribuzione	
Proprietà	Felix Sandra BASPO
Campo d'applicazione	UFSPO
Luogo d'archivio	GRCS

Controllo

Nome	Ruolo	Data/versione
Roland Häusler	Capo IT UFSP0	18.10.2018
Roland Häusler	Capo IT UFSP0	14.11.2019
Roland Häusler	Capo IT UFSP0	31.07.2020
Roland Häusler	Capo IT UFSP0	16.09.2021

Validazione

Nome	Ruolo	Data/versione
Sandra Felix	Responsabile sicurezza informazione	22.10.2018
Sandra Felix	Responsabile sicurezza informazione	03.12.2019
Sandra Felix	Responsabile sicurezza informazione	20.10.2020
Sandra Felix	Responsabile sicurezza informazione	18.10.2021

Indice

1	Introduzione/contesto.....	5
1.1	Introduzione	5
1.2	Scopo	5
1.3	Campo d'applicazione.....	5
1.4	Formulazione non sessista.....	6
1.5	Termini e definizioni.....	6
1.6	Ambiti coperti dalla sicurezza delle informazioni	6
1.6.1	Protezione delle informazioni.....	6
1.6.2	Sicurezza dell'informatica (TIC).....	6
1.6.3	Protezione dei dati	6
1.7	Interfacce.....	7
1.8	Altri documenti applicabili.....	7
1.9	Allegati	7
2	Obiettivi della sicurezza delle informazioni	8
3	Campo d'applicazione SGSI	8
4	Fattori d'influenza (di natura interna/esterna)	9
5	Parti interessate e requisiti.....	9
6	Direttive.....	9
6.1	Direttive superiori	9
6.2	Direttive specifiche all'UFSPPO.....	10
6.2.1	Rispetto dei requisiti ISO 27001.....	10
6.2.2	Dichiarazione di applicabilità.....	10
6.2.3	Inventario degli oggetti da proteggere.....	10
6.2.4	Formazione e sensibilizzazione	10
6.2.5	Informazione e comunicazione	10
6.2.6	Gestione dei documenti.....	10
6.2.7	Rapporti e resoconti.....	10
7	Struttura organizzativa	11
7.1	Funzioni e ruoli	12
7.1.1	Responsabile della sicurezza delle informazioni.....	12
7.1.2	Consulente per la protezione dei dati (CDP)	12
7.1.3	Incaricato della sicurezza informatica dell'unità amministrativa ISIU	13
7.1.4	Responsabile SGSI.....	13
7.1.5	Operatore SGSI.....	13
7.1.6	Titolare dell'oggetto di sicurezza informazione	13
7.1.7	Titolari del rischio	13
7.1.8	Titolari.....	14
7.2	Organi.....	14
7.2.1	Conferenza dei responsabili della sicurezza delle informazioni DDPS	15
7.2.2	Organo specializzato sicurezza delle informazioni DDPS.....	15
7.2.3	Conferenza per la protezione dei dati DDPS.....	15
8	Organizzazione del processo	16
8.1	Panoramica SGSI UFSPPO	16
8.2	Esercizio SGSI.....	16
9	Entrata in vigore	17

Indice delle figure

Figura 1: organigramma UFSPPO.....	8
Figura 2: SGSI UFSPPO.....	16

Indice delle tabelle

Tabella 1: allegati.....	8
Tabella 2: Titolari UFSPPO.....	14

1 Introduzione/contesto

1.1 Introduzione

La sicurezza delle informazioni deve garantire adeguatamente la **disponibilità**, l'**integrità**, la **confidenzialità** e la **verificabilità** di tutti i tipi di informazioni (elettroniche, cartacee, orali) in conformità con i requisiti dei titolari delle informazioni.

Conformemente alle Istruzioni concernenti la sicurezza delle informazioni in seno al DDPS (ISI DDPS numero 1 cpv. 2) la sicurezza delle informazioni comprende i seguenti 3 ambiti:

- protezione delle informazioni (v. cap. 1.6.1),
- TIC sicurezza informatica (v. cap. 1.6.2) e
- protezione dei dati (v. cap. 1.6.3).

Le informazioni che rappresentano un valore per l'UFSPO devono essere adeguatamente protette (in base al rischio). La necessità di protezione e i rischi determinano tutte le misure di sicurezza.

La sicurezza delle informazioni è stabilita, gestita e migliorata costantemente in un sistema di gestione della sicurezza delle informazioni (SGSI) secondo la norma SN ISO/IEC 27001:2015 (numero ISI 1 cpv. 1) in conformità alle basi giuridiche della Confederazione e tenendo conto dei requisiti interni ed esterni. Le direttive (v. cap. 1.8 / 6.1) per la sicurezza delle informazioni in seno all'UFSPO comprendono i principi del DDPS sulla sicurezza delle informazioni e le direttive pertinenti sulla sicurezza delle informazioni nel DDPS. L'UFSPO si fonda sui principi del DDPS sulla sicurezza delle informazioni, in particolare gli obiettivi e i principi ivi elencati. Inoltre, l'UFSPO definisce i propri principi e le proprie procedure specifiche con il presente manuale e gli allegati.

La sicurezza delle informazioni è un aspetto parziale della sicurezza integrale, per la quale il comitato di direzione UFSPO ha approvato un concetto specifico.

Tutti gli allegati secondo il cap. 1.9 sono parte integrante di questo manuale.

1.2 Scopo

Il manuale sulla sicurezza delle informazioni UFSPO regola il processo e la struttura organizzativa (comprese le responsabilità) nel campo della sicurezza delle informazioni in seno all'UFSPO nella misura in cui ciò non sia già specificato nel piano sulla sicurezza integrale UFSPO o non sia disciplinato da prescrizioni dell'organizzazione centrale responsabile della sicurezza DDPS (SGSI DDPS).

Il funzionamento del SGSI è supportato dall'applicazione „**Governance-Risiko-Compliance-Sicherheit**“ (GRCS UFSPO) nel quale sono archiviate e aggiornate le direttive e i documenti giustificativi.

1.3 Campo d'applicazione

Il presente manuale è valido per tutti i collaboratori e le collaboratrici dell'UFSPO.

1.4 Formulazione non sessista

Per non compromettere la leggibilità, nel documento è sempre utilizzata la sola forma maschile. Naturalmente tutte le espressioni vanno riferite a persone di entrambi i sessi.

1.5 Termini e definizioni

Il documento ISI (numero 2) definisce i termini fondamentali che riguardano la sicurezza delle informazioni, come

- sistema di gestione della sicurezza delle informazioni (SGSI)
- oggetto da proteggere "Informazione" e
- titolare dell'oggetto da proteggere "Informazione".

1.6 Ambiti coperti dalla sicurezza delle informazioni

La sicurezza delle informazioni copre gli ambiti elencati di seguito.

1.6.1 Protezione delle informazioni

La protezione delle informazioni disciplina tutte le questioni attinenti la protezione delle informazioni contro la divulgazione non autorizzata. La protezione delle informazioni deve garantire la **confidenzialità** delle informazioni.

L'ordinanza sulla protezione delle informazioni della Confederazione (ordinanza sulla protezione delle informazioni OPrl) disciplina la protezione delle informazioni dell'Amministrazione federale e dell'esercito nella misura in cui è necessaria nell'interesse del Paese. In particolare essa ne stabilisce la classificazione e il trattamento.

1.6.2 Sicurezza dell'informatica (TIC)

La sicurezza TIC deve garantire il trattamento protetto e sicuro delle informazioni.

La sicurezza TIC è disciplinata dall'ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale (Ordinanza sui ciber-rischi, OCiber) e dalle istruzioni concernenti la sicurezza delle informazioni in seno al DDPS (ISI).

La OCiber regola l'organizzazione dell'Amministrazione federale nel campo della prevenzione di ciber-rischi, la procedura di protezione (analisi del bisogno di protezione, piano per la sicurezza e per la protezione dei dati) e la sicurezza della rete. Esse stabiliscono i requisiti riguardo a tecnica, infrastruttura, organizzazione e personale e definiscono i requisiti al fine di garantire una protezione adeguata della confidenzialità, della disponibilità, dell'integrità e della tracciabilità degli oggetti da proteggere, delle tecnologie dell'informazione e della comunicazione dell'Amministrazione federale.

1.6.3 Protezione dei dati

Lo scopo della protezione dei dati è quello di proteggere la personalità da un trattamento illegale o sproporzionato dei dati personali.

La legge federale sulla protezione dei dati (LPD) e l'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD) prescrivono i principi che devono essere rispettati per il trattamento di dati di persone fisiche.

- In particolare i dati personali possono essere trattati soltanto in modo lecito.
- Il trattamento dei dati deve essere conforme al principio della buona fede e della proporzionalità.
- I dati possono essere trattati soltanto per lo scopo indicato all'atto della loro raccolta, risultante dalle circostanze o previsto da una legge.
- Chi tratta dati personali deve accertarsi della loro esattezza.
- La LPD regola la comunicazione di dati all'estero come pure il diritto d'accesso.

Gli articoli 16 – 25 LPD regolano il trattamento di dati personali da parte di organi federali.

- Gli organi federali hanno il diritto di trattare dati personali se ne esiste una base legale.
- I dati personali degni di particolare protezione e i profili della personalità possono essere trattati soltanto se lo prevede esplicitamente una legge in senso formale.
- La comunicazione di dati personali a terzi è soggetta a un fondamento giuridico fatta riserva delle eccezioni menzionate all'art. 19 cpv. 1 LPD.
- I dati personali possono essere resi accessibili solo tramite una procedura di richiamo qualora ciò sia previsto esplicitamente.

1.7 Interfacce

Le interfacce e le dipendenze della sicurezza dell'informazione verso altre aree di sicurezza sono considerate nel SGSI. Lo stesso vale per le dipendenze da fornitori interni ed esterni (ad es. UFIT, BAC) e parti interessate.

Business Continuity Management (BCM)

La gestione della continuità operativa (Business Continuity Management BCM) ha lo scopo di garantire la normale operatività il più rapidamente possibile dopo che si è verificato un incidente (di sicurezza). La continuazione e il mantenimento dell'attività si basa sulle prescrizioni del Capo DDPS concernenti il Business Continuity Management (BCM).

1.8 Altri documenti applicabili

Le basi legali sono indicate nel SGSI DDPS. Le prescrizioni specifiche all'UFSPO sono pubblicate nell'internet UFSPO e le basi specifiche del figurano in GRCS UFSPO.

1.9 Allegati

Gli allegati elencati di seguito (in tedesco) costituiscono parte integrante del presente manuale sulla sicurezza delle informazioni UFSPO.

No.	Titolo
A1	Gestione del rischio della sicurezza delle informazioni
A2	Gestione dei documenti
A3	Gestione delle modifiche
A4	Eccezioni
A5	Incidenti della sicurezza
A6	Valutazione della prestazione
A7	Miglioramenti continui
A8	IT Service Continuity Management

A9 Campo d'applicazione SGSI

Tabella 1: allegati

2 Obiettivi della sicurezza delle informazioni

Vengono adottati i principi del DDPS sulla sicurezza delle informazioni. L'UFSPÖ definisce e ricava i propri obiettivi misurabili in materia di sicurezza dell'informazione da questi principi, che vengono rivisti e ridefiniti annualmente nell'ambito della valutazione della gestione.

3 Campo d'applicazione SGSI

Il campo d'applicazione SGSI si fonda sul regolamento interno dell'UFSPÖ e sulle informazioni che derivano dai processi amministrativi¹.

Organigramma

Ufficio federale dello sport UFSPÖ
1.10.2021

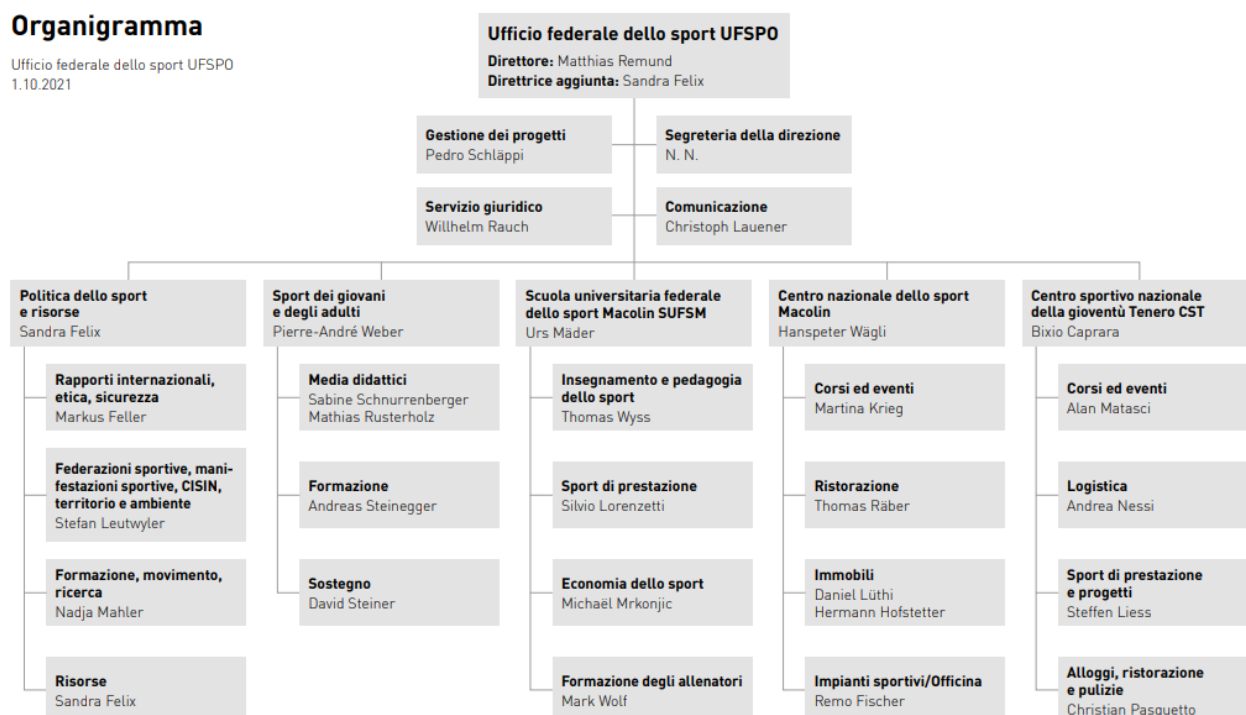


Figura 1: organigramma UFSPÖ

¹ v. regolamento interno UFSPÖ (tedesco o francese, capitolo 3.1)

Il campo d'applicazione SGSI comprende l'intero Ufficio federale dello sport (UFSPO) e le sue sedi e si estende a tutte le informazioni dell'UFSPO e ai valori assegnati (titolari delle informazioni) quali

- persone/depositari di segreti,
- oggetti di protezione TIC e
- oggetti fisici,

nella misura in cui questi rientrano nella sfera di responsabilità dell'UFSPO.

Il campo d'applicazione SGSI è definito nell'allegato A9 del manuale.

4 Fattori d'influenza (di natura interna/esterna)

I fattori (secondo ISO 27001 fattori interni ed esterni) che influiscono sulla sicurezza delle informazioni e su SGSI all'UFSPO sono elencati e aggiornati nell'apposito documento (in tedesco: „Einflussfaktoren ISMS BASPO“).

I fattori d'influenza vengono rivisti e adeguati annualmente nell'ambito della valutazione della gestione. Le modifiche a breve termine sono valutate dal responsabile della sicurezza informazione e dall'operatore SGSI.

5 Parti interessate e requisiti

Le parti interessate (o anche: stakeholder) avanzano richieste sulla sicurezza dell'informazione e che riguardano quindi SGSI UFSPO. Questi soggetti interni ed esterni e le loro esigenze sono elencati e aggiornati nell'elenco degli stakeholder.

L'elenco degli stakeholder viene rivisto e adeguato ogni anno nell'ambito della valutazione della gestione. Le modifiche a breve termine sono valutate dalla responsabile della sicurezza informazione e presi in considerazione dall'operatore SGSI.

6 Direttive

6.1 Direttive superiori

L'elenco delle basi legali per la sicurezza delle informazioni è disponibile nel SGSI DDPS gestito dalla Sicurezza delle informazioni e degli oggetti SIO. Esso elenca tutte le leggi, le ordinanze e le direttive DDPS rilevanti (ad es. prescrizioni, regolamenti) valide anche per l'UFSPO. Tutte le direttive di livello superiore sono vincolanti anche per i terzi/fornitori di servizi esterni che lavorano per conto dell'UFSPO. Tutti i contratti sono depositati presso il servizio competente dell'UFSPO.

La [voce intranet](#) sicurezza delle informazioni DDPS offre una breve panoramica dei decreti, documenti e promemoria sulla sicurezza dell'informazione.

6.2 Direttive specifiche all'UFSPO

Laddove le direttive federali e le direttive SGSI DDPS non sono sufficienti o devono essere concretizzate, l'UFSPO elabora direttive o requisiti specifici che non siano meno severi dello standard minimo. Per la loro attuazione sono stabilite delle misure di sicurezza.

6.2.1 Rispetto dei requisiti ISO 27001

Il rispetto dei requisiti ISO 27001 è documentato e comprovato in GRCS UFSPO.

6.2.2 Dichiarazione di applicabilità

La dichiarazione di applicabilità riguardo alle 114 contromisure (controls) (v. allegato A) è gestita e aggiornata nel GRCS UFSPO. Per i controlli sono stabilite delle misure la cui attuazione è concretizzata nel piano triennale.

6.2.3 Inventario degli oggetti da proteggere

Tutti gli oggetti da proteggere (informazioni e valori assegnati) e i dettagli collegati (livello di protezione, responsabile dell'oggetto di protezione, dipendenze, ecc.) vengono registrati nell'inventario degli oggetti da proteggere e sono gestiti e aggiornati dal titolare degli oggetti da proteggere.

6.2.4 Formazione e sensibilizzazione

La formazione e la sensibilizzazione sui temi della sicurezza dell'informazione sono realizzate secondo il piano di formazione per la sicurezza integrale. Per i corsi di formazione specifici al SGSI viene elaborato un piano di formazione che conferma anche la partecipazione.

6.2.5 Informazione e comunicazione

L'informazione e la comunicazione in materia di sicurezza delle informazioni avviene secondo la strategia di comunicazione dell'UFSPO. Le parti interessate interne ed esterne sono informate in funzione delle esigenze. I temi attinenti la sicurezza delle informazioni sono comunicati alla CII tramite il rapporto annuale (in conformità con il Istr GOSic).

6.2.6 Gestione dei documenti

Tutti i documenti rilevanti in materia di sicurezza delle informazioni e SGSI UFSPO sono creati, aggiornati e gestiti nel GRCS in conformità con l'apposito documento (in tedesco, allegato A2 "Dokumentenmanagement").

6.2.7 Rapporti e resoconti

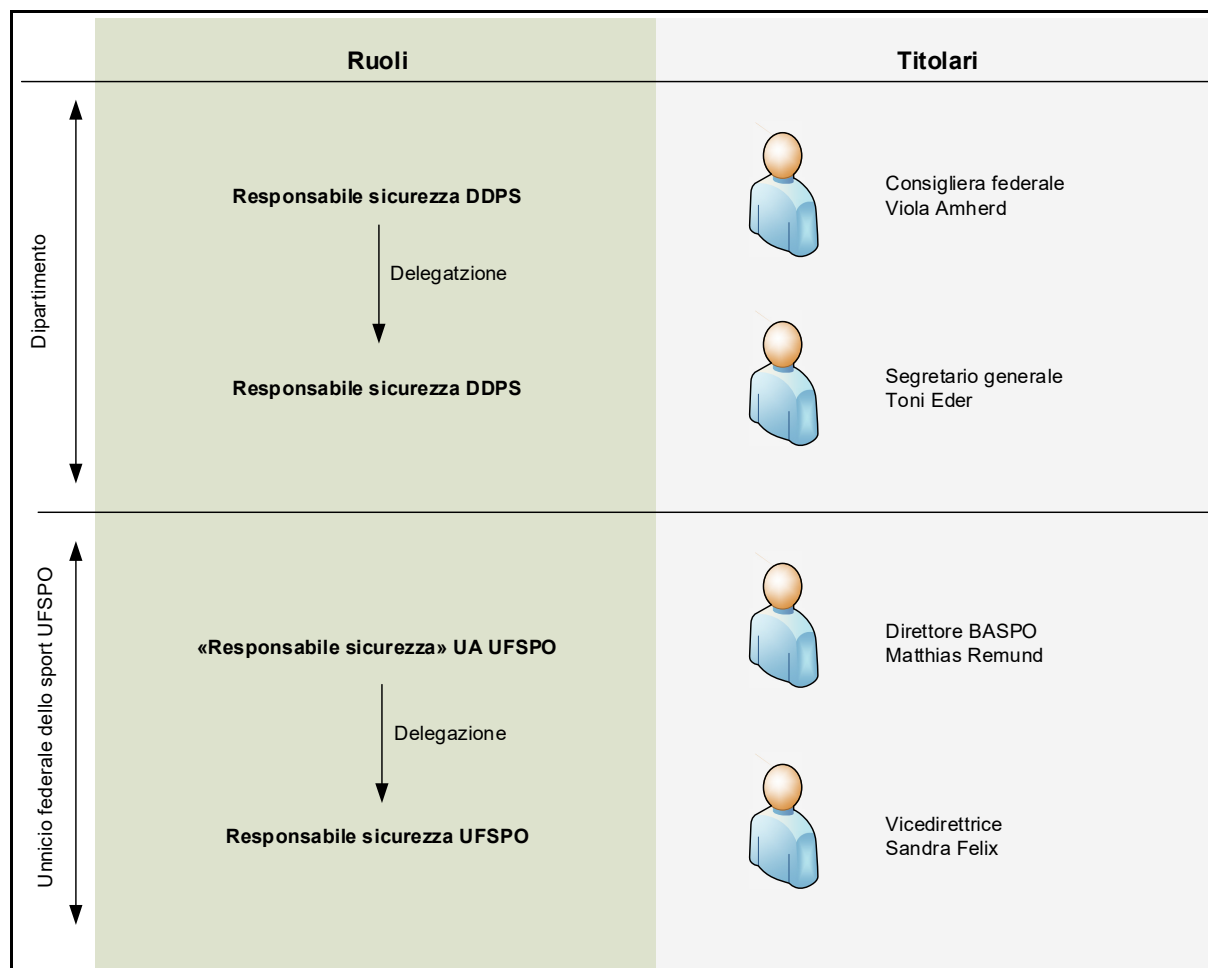
I rapporti e i resoconti sulla sicurezza delle informazioni sono elaborati in conformità alle istruzioni del DDPS sulla sicurezza delle informazioni (ISI, numero 24). L'operatore SGSI UFSPO riferisce regolarmente al SGSI centrale del DDPS e internamente al responsabile SGSI UFSPO e al responsabile sicurezza informazione UFSPO, soprattutto in vista della valutazione della gestione.

7 Struttura organizzativa

Dipartimento

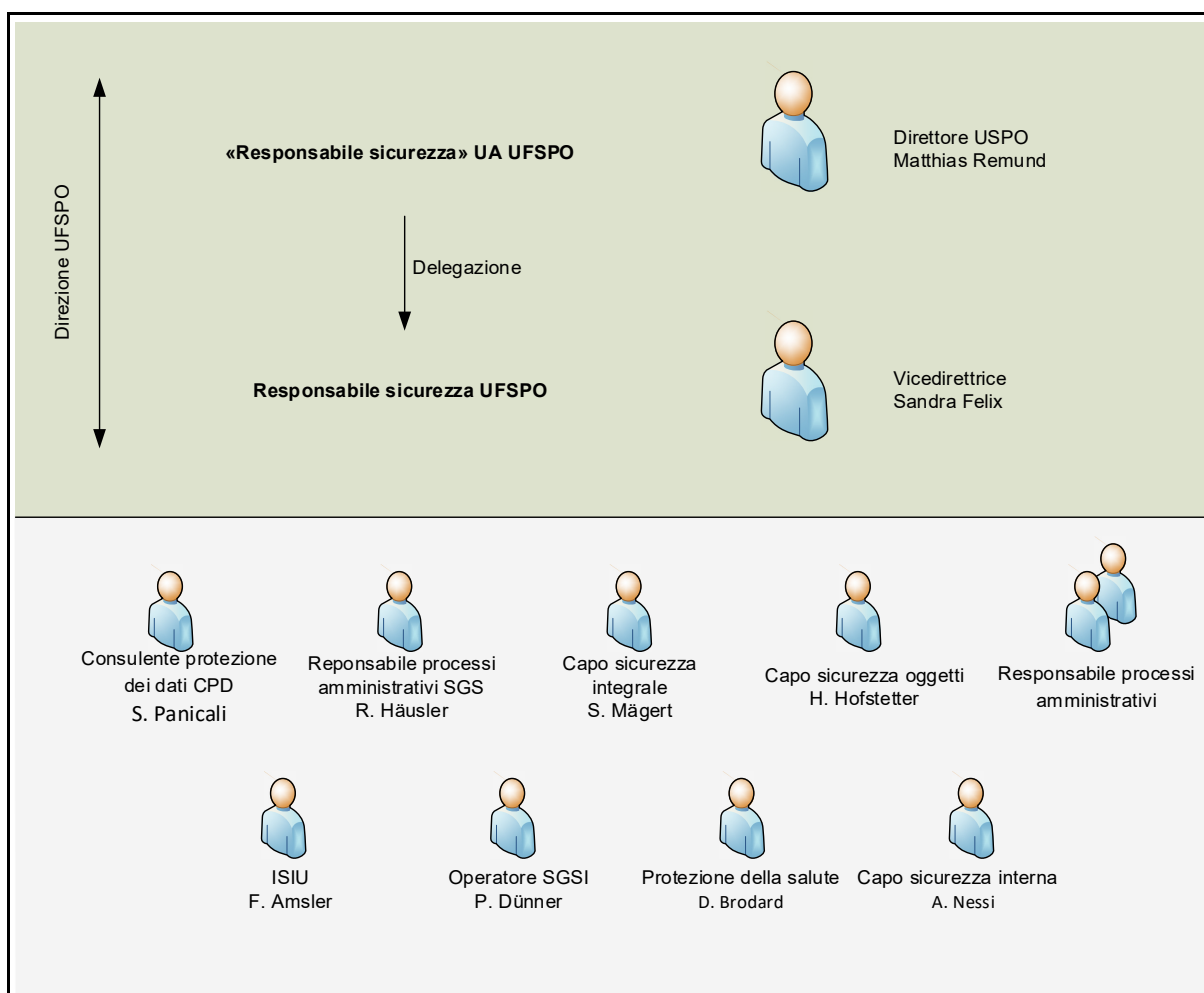
Il responsabile sicurezza DDPS (Consigliera federale) è l'autorità suprema del Dipartimento e quest'organo ha delegato i suoi compiti al Segretario generale del DDPS.

Ogni unità amministrativa (UA) ha un responsabile della sicurezza delle informazioni che in genere è anche il responsabile dell'UA. In seno all'UFSPPO questo compito è stato assegnato alla direttrice supplente.



Organizzazione della sicurezza UFSPPO

L'organizzazione della sicurezza dell'UFSPPO è subordinata alla responsabile sicurezza UFSPPO. La gestione operativa è affidata al capo sicurezza UFSPPO. Si tratta di un'organizzazione a matrice. Il funzionamento e la responsabilità SGSI UFSPPO sono affidati al settore Informatica (Politica dello sport e risorse, sotto settore Risorse).



La struttura organizzativa così come le funzioni/ruoli e le loro responsabilità in materia di sicurezza delle informazioni presso l'UFSPPO sono assegnati ai dipendenti UFSPPO come spiegato nei seguenti capitoli.

7.1 Funzioni e ruoli

Per tutte le funzioni e i ruoli sono nominati dei sostituti.

7.1.1 Responsabile della sicurezza delle informazioni

I **CCR** (compiti, competenze, responsabilità) sono definiti nelle direttive DDPS sulla sicurezza dell'informazione (ISI numero 6).

Il **ruolo** è ricoperto dal responsabile politica dello sport e risorse (PSR) che in qualità di responsabile della sicurezza è responsabile della sicurezza generale.

7.1.2 Consulente per la protezione dei dati (CDP)

I **CCR** sono definiti nelle Istruzioni sulla protezione dei dati nel DDPS (numero 5).

Il ruolo di consulente per la protezione dei dati (CDP) è aggregato al servizio giuridico UFSPPO e dotato di 0.2 FTE.

Profilo dei requisiti

- Studi completi di giurisprudenza (giurista)

- Conoscenza delle disposizioni di legge, delle norme specifiche di protezione dei dati e delle relative disposizioni speciali
- Autonomia nell'adempimento dei compiti, elevata specializzazione e affidabilità

7.1.3 Incaricato della sicurezza informatica dell'unità amministrativa ISIU

Le **prescrizioni** sono definite nell'ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale (Ordinanza sui ciber-rischi, OCiber), art. 14.

In seno all'UFSP il ruolo ISIU è aggregato al settore Informatica dotato di 0.4 ETP.

Profilo dei requisiti

- Studi (universitari di alta scuola specializzata) completi di informatica o informatica aziendale (o formazione equivalente)
- Esperienza professionale pluriennale nel campo dell'informatica e/o della sicurezza informatica

7.1.4 Responsabile SGSI

Il responsabile SGSI è responsabile dell'attuazione interna all'ufficio delle direttive del responsabile della sicurezza delle informazioni DDPS conformemente alle IS.

Profilo dei requisiti

- Studi (universitari di alta scuola specializzata) completi di informatica o informatica aziendale (o formazione equivalente)
- Conoscenze specializzate delle norme ISO 27000 segg., del SGSI o di altri sistemi di gestione
- Conoscenze specializzate in materia di gestione dei rischi, gestione delle emergenze e delle crisi

7.1.5 Operatore SGSI

Su mandato del responsabile SGSI, l'operatore SGSI gestisce il sistema di gestione secondo le istruzioni del DDPS e dell'UFSP.

I **CCR** sono stabiliti nella descrizione del posto.

Il ruolo dell'operatore SGSI UFSP è aggregato a IT UFSP e dotato di 0.3 ETP.

Profilo dei requisiti

- Studi (universitari di alta scuola specializzata) completi di informatica o informatica aziendale (o formazione equivalente)
- Conoscenze specializzate delle norme ISO 27001 e 27002
- Conoscenze della gestione di progetti e dei rischi, costituzione e gestione dell'inventario degli oggetti protetti

7.1.6 Titolare dell'oggetto di sicurezza informazione

I **CCR** sono definiti nelle Istruzioni sulla protezione dei dati nel DDPS (numero 11).

7.1.7 Titolari del rischio

I **CCR** sono definiti nelle Istruzioni sulla protezione dei dati nel DDPS (numero 10) nonché

nelle Direttive sulla gestione dei rischi presso la Confederazione (cap. 3 Funzioni e responsabilità).

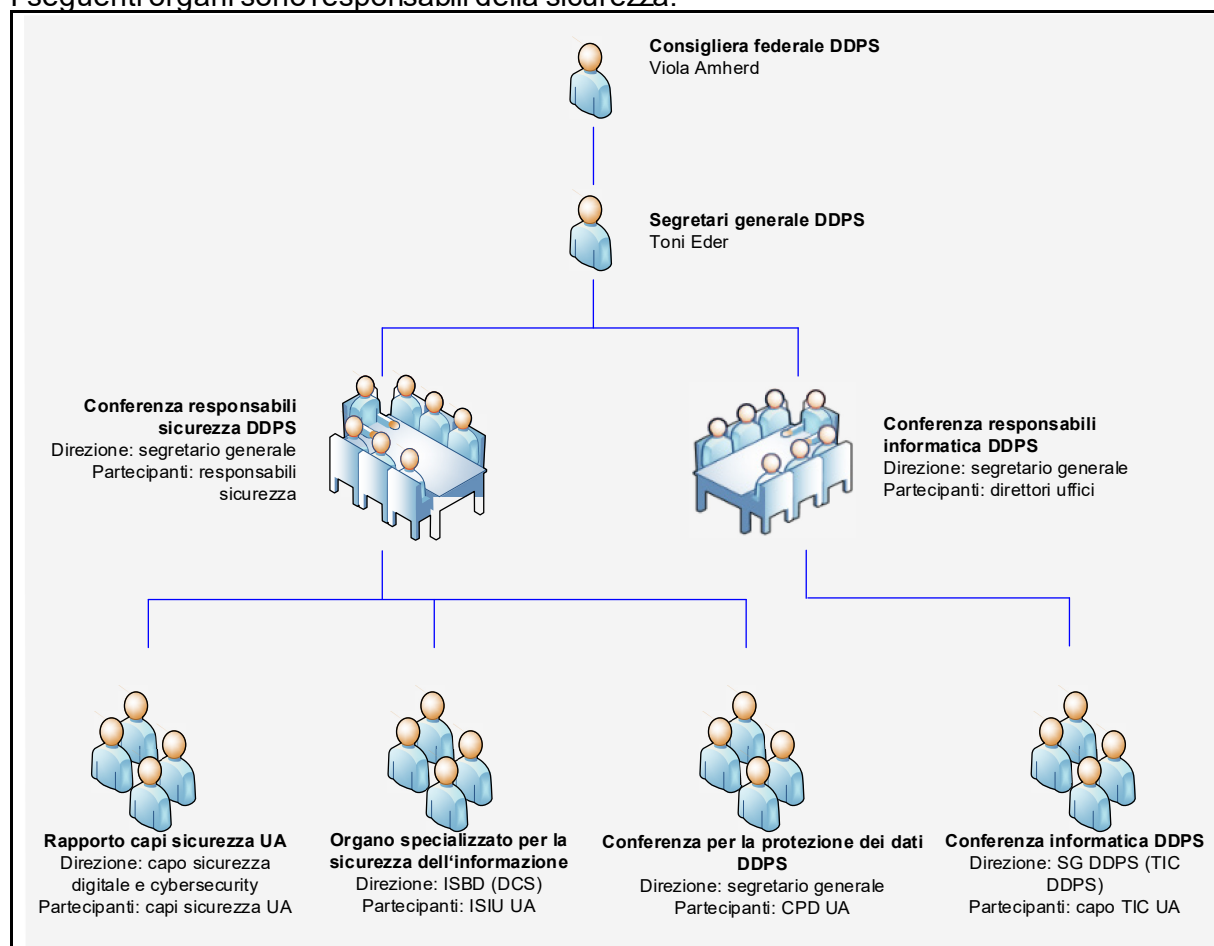
7.1.8 Titolari

Ruolo	Nome/cognome	Settore	Funzione gerarchica
Responsabile sicurezza	Felix Sandra	PSR	Direttrice supplente
Consulente protezione dati	Panicali Sabrina	DIR / servizio giuridico	Giurista servizio giuridico
ISIU	Amsler Fritz	PSR / IT	ISIU / capoprogetto
Responsabile SGSI	Häusler Roland	PSR / IT	Capo IT
Operatore SGSI RPO	Schneider-Köppel Judith	PSR / IT	Controlling TIC / responsabile esercizio SGSI
Capo sicurezza UFSPÖ	Mägert Stefanie	PSR	Giurista Politica dello sport e affari amministrativi

Tabella 2: Titolari UFSPÖ

7.2 Organi

I seguenti organi sono responsabili della sicurezza:



Conferenza responsabili DDPS

3-4 riunioni all'anno.

Si occupa di argomenti relativi alla sicurezza generale e di questioni interdipartimentali a livello strategico.

Conferenza responsabili informatica DDPS

3-4 riunioni all'anno.

Si occupa di argomenti relativi alla sicurezza informatica e di questioni interdipartimentali a livello strategico.

Rapporto capi sicurezza UA

4 riunioni all'anno.

Si occupa di argomenti relativi alla sicurezza delle UA.

Organo specializzato per la sicurezza dell'informazione

10-12 riunioni all'anno.

Si occupa a livello operativo di argomenti relativi alla sicurezza delle informazioni e ha carattere consultativo.

Conferenza per la protezione dei dati DDPS

1-2 riunioni all'anno.

Organo specializzato per la protezione dei dati.

Conformemente alle Istruzioni concernenti la sicurezza delle informazioni, v. sotto.

Conferenza informatica DDPS

8-10 riunioni all'anno.

Direzione operativa TIC DDPS.

Si occupa di argomenti TIC strategici e temi operativi interni al DDPS nonché di questioni interdipartimentali.

Secondo le Istruzioni concernenti la sicurezza delle informazioni DDPS riguardo alla sicurezza delle informazioni sono prescritti i seguenti organi.

7.2.1 Conferenza dei responsabili della sicurezza delle informazioni DDPS

Secondo le Istruzioni concernenti la sicurezza delle informazioni DDPS (cifra 7) il responsabile della sicurezza delle informazioni è membro della Conferenza dei responsabili della sicurezza delle informazioni DDPS.

7.2.2 Organo specializzato sicurezza delle informazioni DDPS

Le Istruzioni concernenti la sicurezza delle informazioni DDPS (cifra 8) non prescrivono chi è membro dell'organo specializzato sicurezza delle informazioni. Per l'UFSPPO è stato designato l'incaricato della sicurezza informatica dell'unità amministrativa ISIU come membro di quest'organo.

7.2.3 Conferenza per la protezione dei dati DDPS

L'UFSPPO è rappresentato in questa conferenza dal CPD conformemente alle direttive sulla protezione dei dati DDPS (numero 6).

8 Organizzazione del processo

Lo scopo del sistema di gestione della sicurezza delle informazioni SGSI (secondo ISO DDPS) è quello di assicurare la gestione, la misurazione e il controllo della disponibilità, dell'integrità, della confidenzialità e della verificabilità delle informazioni attraverso regolamenti, processi, prescrizioni e meccanismi di miglioramento tenendo conto dei rischi esistenti. Attraverso il SGSI UFSP i requisiti del sistema sono integrati nei processi amministrativi dell'organizzazione.

8.1 Panoramica SGSI UFSP

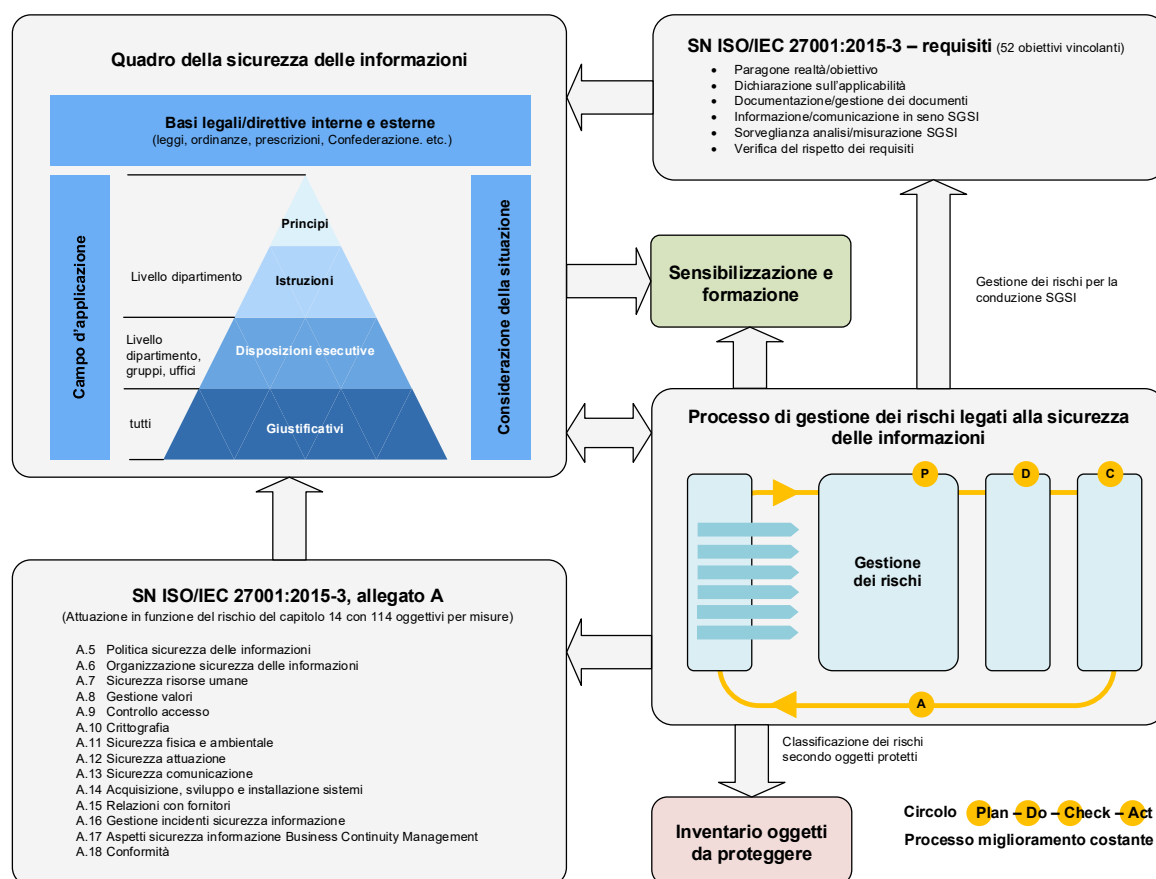


Figura 2: SGSI UFSP

L'organizzazione del processo dell'UFSP si basa sulla norma ISO 27001/2. I principi, i processi e le definizioni della gestione dei rischi in materia di sicurezza delle informazioni sono descritti in dettaglio nel Manuale di gestione dei rischi per la sicurezza delle informazioni (ISRM) [A1].

8.2 Esercizio SGSI

In seno all'UFSP il SGSI è gestito e curato dall'operatore SGSI UFSP (v. organizzazione strutturale cap. 7.1.4) che a sua volta è sottoposto al capo SGSI che risponde al responsabile della sicurezza.

9 Entrata in vigore

Il manuale entra in vigore con la firma del responsabile della sicurezza delle informazioni UFSPO.

Macolin,

.....

Sandra Felix

Responsabile della sicurezza delle informazioni UFSPO