|  |  |
| --- | --- |
|  | Classificazione |

|  |
| --- |
|  |

P042-Hi03 - Piano di emergenza

<Nome del progetto / dell’oggetto da proteggere>

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Classificazione | Non classificato / AD USO INTERNO / CONFIDENZIALE / SEGRETO |
| Stato | In corso di elaborazione / in corso di verifica / approvato |
| Numero del progetto |  |
| Capoprogetto (CP BP) |  |
| Versione | Template – versione 3.1 |
| Data |  |
| Committente |  |
| Elaborato da |  |

Controllo delle modifiche

|  |  |  |  |
| --- | --- | --- | --- |
| Versione | Data | Descrizione / Osservazioni | Nome |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribuzione

|  |  |  |
| --- | --- | --- |
| Funzione | Nome | Dipartimento / Ufficio |
| ISIU |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Indice

1 Considerazioni generali 4

1.1 Descrizione 4

1.2 Responsabilità 5

1.2.1 Beneficiari delle prestazioni 5

1.2.2 Fornitori delle prestazioni 5

1.3 Scopo del documento 5

1.4 Procedura 5

1.5 Documentazione BCM sovraordinata 6

1.6 Processi aziendali supportati 6

2 Prevenzione delle emergenze 7

2.1 Informazioni generali 7

2.2 Misure preventive 7

2.3 Esecuzione di esercitazioni di emergenza 7

3 Misure di emergenza 7

3.1 Descrizione dell’oggetto da proteggere 7

3.2 Misure immediate 7

4 Allegato A: ausili BCM 9

4.1 Campo di applicazione 9

4.2 Provvedimenti consigliati per il BCM 9

4.3 Gestione delle crisi / dei casi di emergenza 10

4.3.1 Orientamento strategico della gestione dei casi di emergenza 10

4.3.2 Spiegazioni relative a guasti, emergenze, crisi e catastrofi 10

4.3.3 Scenari di emergenza e interlocutori 10

4.3.4 Valutazione della situazione 11

4.4 Comunicazione e pubbliche relazioni in caso di crisi 11

4.4.1 Locale per lo Stato maggiore di crisi / centro di analisi della situazione 11

5 Allegato B: riferimenti 12

5.1 Elenco dei documenti 12

5.2 Definizioni 12

# Considerazioni generali

**Indicazioni per la compilazione del documento**

I seguenti standard e raccomandazioni fungono da ausilio per l’elaborazione del piano di emergenza:

* [Standard 100-4 Gestione delle emergenze](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html) (standard per la protezione di base IT)
* Standard ISO/IEC 27001, 27002 e 27031
* [Raccomandazioni per il Business Continuity Management (BCM)](http://www.swissbanking.ch/print/20130829-3040-VEB-rev_BCM_Empfehlungen_online-AKN.pdf) dell’Associazione svizzera dei banchieri, SwissBanking, riconosciute dalla FINMA come standard minimi di autoregolamentazione
* [Direttiva concernente il Business Continuity Management (BCM) nell’Amministrazione federale](https://intranet.ncsc.admin.ch/dam/ncscintra/de/dokumente/empfehlungen/Begriffserklaerungen_KaVor_v01-1.pdf.download.pdf/Begriffserklaerungen_KaVor_v01-1.pdf)

Il testo in azzurro è un ausilio per la compilazione del documento.

## Descrizione

Il requisito O3 della protezione IT di base (Si001) sul tema della "continuità operativa" permette di dedurre la necessità di un piano di emergenza.

Il punto di partenza del piano di emergenza è costituito dal piano SIPD. Il piano di emergenza si riferisce allo stesso oggetto da proteggere descritto nel piano SIPD. Fondamentale per la stesura del piano di emergenza è l’analisi dei rischi eseguita nell’ambito del piano SIPD.

Il seguente grafico illustra l’inserimento del piano di emergenza nel contesto del piano SIPD e la relativa delimitazione rispetto ad altri settori.

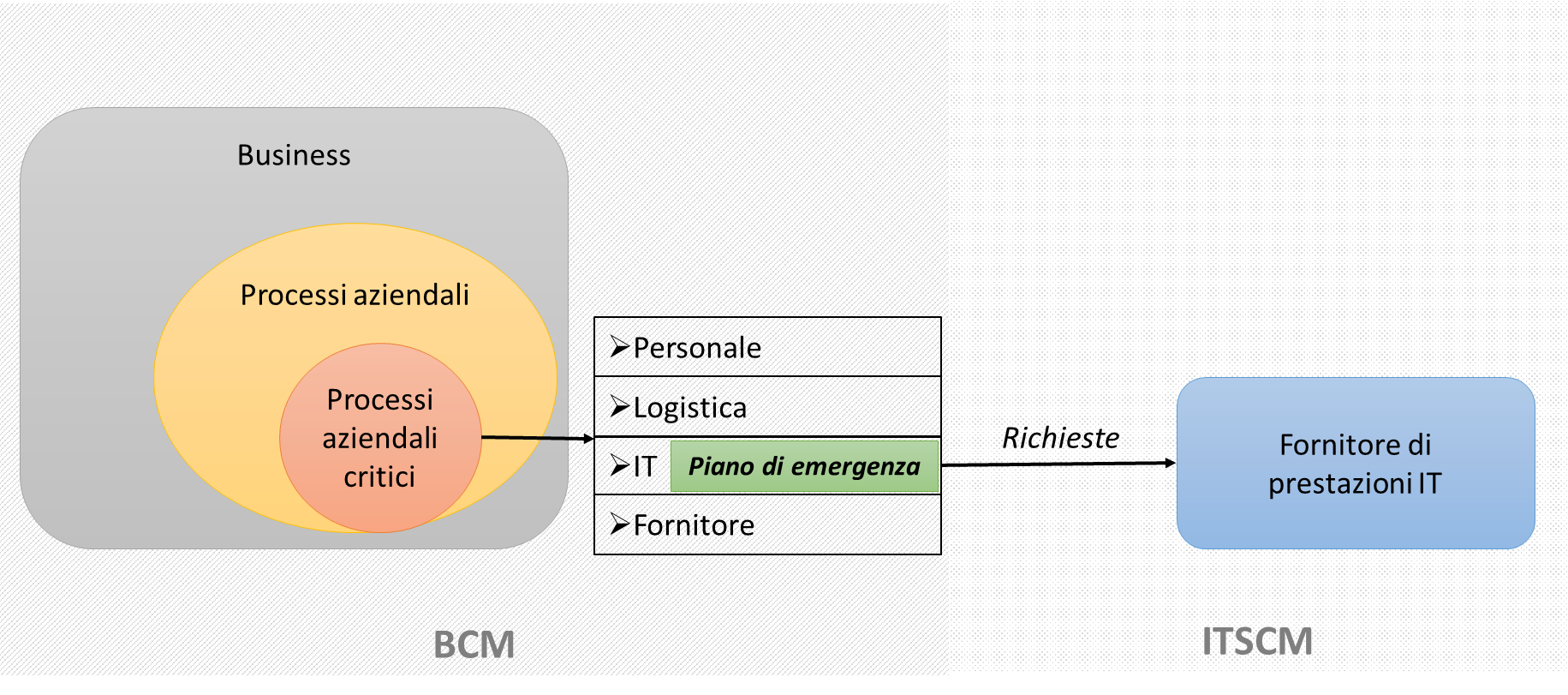


Figura 1: Classificazione del piano di emergenza

## Responsabilità

### Beneficiari delle prestazioni

Il beneficiario delle prestazioni è responsabile del rispetto delle direttive TIC, nonché delle decisioni del Consiglio federale, del DFF, dell’ODIC e dei dipartimenti o della Cancelleria federale nel loro settore di competenza (art. 21 cpv. 2 OIAF).

In relazione alla gestione dei casi di emergenza ciò significa in particolare:

* controllo dei service level agreements (SLA) con i fornitori delle prestazioni
* backup dei dati, possibilità di ripristino dei dati
* gestione dei diritti e degli accessi ai dati
* ….

### Fornitori delle prestazioni

I fornitori delle prestazioni sono responsabili del rispetto delle direttive TIC, nonché delle decisioni del Consiglio federale, del DFF, dell’ODIC e dei dipartimenti o della Cancelleria federale nel loro settore di competenza (art. 23 cpv. 2 OIAF).

In relazione alla gestione dei casi di emergenza ciò significa in particolare:

* gestione dei casi di emergenza e sicurezza in caso di emergenza centro di calcolo
* infrastruttura sostitutiva.

## Scopo del documento

Il piano di emergenza descrive la pianificazione dei casi di emergenza e la continuazione della capacità operativa dell’oggetto da proteggere, al fine di garantire il mantenimento e il ripristino dell’operatività in situazioni straordinarie.

Obiettivo del piano di emergenza è anche verificare gli SLA esistenti con il fornitore di prestazioni, che se necessario devono essere opportunamente integrati.

## Procedura

Il seguente grafico illustra la procedura da rispettare per la stesura del piano di emergenza.

Questa procedura parte dal presupposto che l’ufficio dispone di un BCM che controlla regolarmente per verificarne l’attualità (in particolare per quanto riguarda le variazioni relative alla responsabilità e ai dati di contatto) e integra opportunamente.

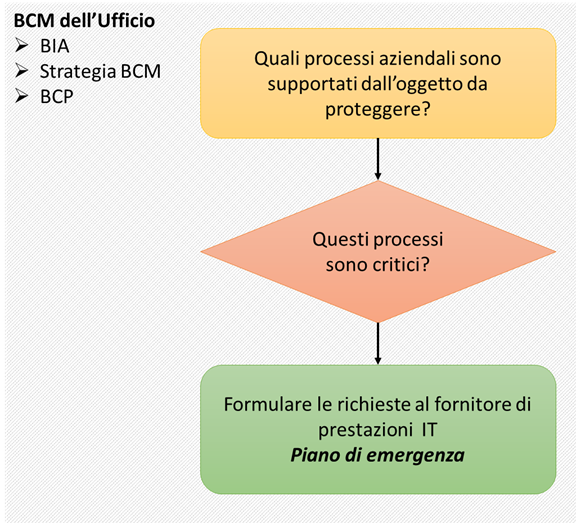


Figura 2: Procedura per la stesura del piano di emergenza

## Documentazione BCM sovraordinata

La seguente documentazione è stata elaborata a livello di ufficio.

|  |  |
| --- | --- |
| BCM | |
| Business lmpact Analysis (BIA) |  |
| Strategia BCM |  |
| Business Continuity Plan (BCP) |  |
| … |  |

## Processi aziendali supportati

I seguenti processi aziendali sono supportati dall’oggetto da proteggere.

|  |  |  |
| --- | --- | --- |
| Criticità (c) | Processo aziendale | Responsabile dei processi aziendali |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Prevenzione delle emergenze

## Informazioni generali

La prevenzione delle emergenze costituisce la base per l’attuazione delle strategie di continuità. Essa descrive le condizioni contingenti e contiene tutte le informazioni disponibili durante la pianificazione. Tutti gli aspetti organizzativi e concettuali nonché tutte le misure e attività della gestione dei casi di emergenza che non contribuiscono alla gestione diretta di un’emergenza dovrebbero essere descritti nell’organizzazione dei casi di emergenza.

## Misure preventive

In questa fase vengono identificate le misure adeguate ai singoli oggetti da proteggere, che sono opportune dal punto di vista economico e/o concordate con i provvedimenti esistenti dei fornitori delle prestazioni.

**Domande di controllo**

* Le misure definite nel piano SIPD o già attuate dal fornitore delle prestazioni sono state coordinate / prese in considerazione con le misure pianificate?
* È presente un’apposita prevenzione delle emergenze ad esempio presso il fornitore delle prestazioni?
* Le misure derivanti dall’analisi del bisogno di protezione sono state prese in considerazione?
* Ne tenete conto nel vostro SLA?
* …

## Esecuzione di esercitazioni di emergenza

Il funzionamento delle misure e della gestione dei casi di emergenza dovrebbe essere opportunamente verificato attraverso esercitazioni di emergenza, al termine delle quali si deve procedere a una valutazione del processo utilizzato con gli uffici interessati.

# Misure di emergenza

Questo capitolo deve essere strutturato in modo tale da consentire anche a un esperto indipendente di eseguire le misure di emergenza qui descritte.

## Descrizione dell’oggetto da proteggere

La descrizione viene eseguita conformemente al piano SIPD.

**Domande di controllo**

* In questo contesto sono presenti altri oggetti da proteggere?
* ...

## Misure immediate

Le misure immediate mirano a una reazione appropriata e tempestiva in caso di incidente e devono essere coordinate in particolare con quelle del piano SIPD.

**Domande di controllo**

* Le misure immediate sono state definite? Quali devono essere adottate a seconda delle emergenze?
* Sono stati definiti dei compiti per singoli individui/ruoli in caso di emergenza?
* Sono disponibili delle istruzioni operative per emergenze speciali?
* ...

# Allegato A: ausili BCM

Se il BCM esistente nell’ufficio non è ancora stato regolamentato, fungono da ausilio i seguenti punti.

## Campo di applicazione

In questo paragrafo si devono inserire nel piano SIPD i limiti del sistema dal punto di vista del piano di emergenza.

**Domande di controllo**

* Quali interfacce con un BCM sovraordinato sono presenti?
* ...

## Provvedimenti consigliati per il BCM

Devono essere elaborati determinati provvedimenti consigliati, ad esempio:

* definizione di emergenza e relativo responsabile
* analisi delle alternative interne ed esterne
* regolamentazione delle responsabilità in caso di emergenza
* piano d’allerta
* piani di emergenza per determinati sinistri
* elaborazione di un programma di salvataggio dei dati
* piano di acquisti sostitutivi
* coordinamento degli accordi dei fornitori
* esecuzione di esercitazioni di emergenza
* linee di comunicazione ridondanti
* ...

## Gestione delle crisi / dei casi di emergenza

La gestione dei casi di emergenza mira a garantire che l’unità amministrativa possa espletare direttamente le proprie mansioni principali in situazioni straordinarie entro i termini stabiliti. È pertanto fondamentale procedere a un’osservazione completa, prendendo in considerazione tutti gli aspetti richiesti per la prosecuzione dei processi aziendali critici al verificarsi di un sinistro.

### Orientamento strategico della gestione dei casi di emergenza

Gli obiettivi strategici della gestione dei casi di emergenza elencati di seguito devono essere stabiliti in anticipo.

**Domande di controllo**

* Quali obiettivi aziendali devono essere tutelati?
* Quali sono i principali scenari di sinistro?
* Quali tipi di interruzioni operative vengono ritenuti in grado di compromettere l’esistenza di un ente (ad es. danni d’immagine)?
* Entità dell’accettazione del rischio?
* Tipo ed entità delle misure?
* Obiettivo principale della gestione delle emergenze?
* ...

### Spiegazioni relative a guasti, emergenze, crisi e catastrofi

Descrizione chiara dei concetti di guasto, emergenza, crisi o catastrofe che devono essere opportunamente concordati sia con i responsabili del committente sia con i fornitori delle prestazioni.

### Scenari di emergenza e interlocutori

Per i casi di emergenza può essere adottata una suddivisione dei ruoli diversa rispetto a quella prevista per l’esercizio corrente e/o a quella definita nel piano SIPD.

Definire i rispettivi utenti/interlocutori a seconda del livello di aggravamento della situazione.

|  |  |  |
| --- | --- | --- |
| Tipo di incidente di sicurezza | Interlocutore | Dati di contatto |
| Definizione degli scenari di emergenza |  | … |
| * Guasti di lieve entità che riguardano l’operatività per un breve periodo (cfr. SLA) * … | Service Desk  1st Level Support  (Incident Management) | … |
| * Guasti che compromettono l’operatività per un certo numero di ore... * ... | Service Desk  2nd Level Support  (Intervention) | … |
| * … | … | … |
| * … | … | … |

**Domande di controllo**

* Gli scenari di emergenza e i rispettivi fattori scatenanti sono stati definiti?
* Si è stabilito quale interlocutore è responsabile per quale scenario di emergenza?
* I rispettivi ruoli, responsabilità e competenze sono stati definiti?
* Documentazione delle procedure di segnalazione e dei livelli di aggravamento della situazione?
* Regolamentazione delle sostituzioni?
* Designazione degli interlocutori?
* È stata individuata la causa dell’aggravamento della situazione?
* Lo svolgimento (processo) e la relativa descrizione sono disponibili e noti?
* Gli ausili per le decisioni in caso di escalation sono disponibili?
* Le modalità con cui procedere in caso di escalation sono state definite?
* Gli scenari di emergenza e i fattori scatenanti definiti sono stati concordati con il fornitore / i fornitori delle prestazioni?
* Gli SLA sono stati concepiti su tali basi?
* ...

### Valutazione della situazione

In questo paragrafo si deve indicare come può essere valutata e classificata una situazione eccezionale.

**Domande di controllo**

* Sono stati creati degli appositi ausili per le decisioni per la valutazione della situazione?
* Come si procede a un’analisi e a una valutazione della gestione delle emergenze?
* Si è stabilito come e con quali modalità stilare un’apposita documentazione?
* Sono stati definite le fasi di ripristino della normalità?
* ...

## Comunicazione e pubbliche relazioni in caso di crisi

In questo paragrafo si deve descrivere come gestire la comunicazione verso l’interno e l’esterno in caso di crisi.

**Domande di controllo**

* Chi è autorizzato a comunicare verso l’esterno?
* Sussistono delle riserve in merito alla comunicazione?
* ...

### Locale per lo Stato maggiore di crisi / centro di analisi della situazione

In caso di emergenza si devono mettere a disposizione dei locali che consentano lo svolgimento dell’attività dello Stato maggiore di crisi e che soddisfino determinati requisiti in termini di ubicazione e dotazione.

**Domande di controllo**

* Le sedi sono documentate e note a tutti gli individui/uffici coinvolti?
* La relativa reperibilità è assicurata?
* Sono stati definiti appositi processi e lavori?
* ...

# Allegato B: riferimenti

## Elenco dei documenti

Comprende l’elenco delle leggi, ordinanze, istruzioni, regolamenti, specifiche tecniche ecc. rilevanti nell’ambito della gestione dei casi di emergenza. L’elenco deve essere completato con i documenti dei singoli dipartimenti e/o uffici.

|  |  |
| --- | --- |
| Tipologia di documento | Titolo |
| Leggi | Base legale del processo aziendale e/o dell’applicazione  (da completare da parte dell’autore) |
|  | [Legge federale sulla protezione dei dati (LPD; RS *235.1*)](https://www.admin.ch/opc/it/classified-compilation/19920153/index.html) |
| Ordinanze | Ordinanza concernente l’informatica e la telecomunicazione nell’Amministrazione federale (OIAF; [RS *172.010.58*](https://www.admin.ch/opc/it/classified-compilation/20081009/index.html) ) |
|  | [Ordinanza relativa alla legge federale sulla protezione dei dati (OLPD; RS *235.11*)](https://www.admin.ch/opc/it/classified-compilation/19930159/index.html) |
| Istruzioni | [ODIC – Istruzioni del Consiglio federale sulla sicurezza TIC nell’Amministrazione federale](https://www.isb.admin.ch/isb/it/home/ikt-vorgaben/grundlagen/w002-weisungen_bundesrat_ikt-sicherheit_bundesverwaltung_wisb.html)) |
| Metodologie | [HERMES – il metodo svizzero per la gestione di progetti](https://www.isb.admin.ch/isb/it/home/themen/projektmanagement/hermes.html) |
| Documenti  propri | … |

## Definizioni

Per le definizioni si vedano le raccomandazioni sui concetti in ambito BCM e ITSCM a livello di Confederazione («Begriffserklärungen im Umfeld BCM / ITSCM auf Stufe Bund»).