SISTEMA SANITARIO REGIONALE
ARES 118

REGIONE LAZIO

DELIBERAZIONE N° **1212** del **30/12/2025**

Struttura proponente: U.O.C. INFORMATION COMMUNICATION TECHNOLOGY	**Proposta n.** 1148 **del** 29/12/2025
Oggetto: Approvazione regolamento per la gestione degli incidenti di cybersicurezza (incident management), del modulo per la segnalazione degli incidenti, del registro degli incidenti e del Team di gestione degli incidenti. Approvazione delle procedure di gestione degli incidenti, di gestione del rischio e della valutazione della sicurezza delle terze parti, approvazione delle politiche di back up, di controllo accessi e di crittografia. Individuazione del referente CSIRT nell'ambito del contratto di migrazione al PSN .	
L'estensore: Nicola D'Agostino	
Il presente provvedimento è composto da n. 128 pagine di cui n. 121 di allegati	
Parere del Direttore Amministrativo	
Paola Longo: *Favorevole*	
Firma Paola Longo	*Data* 30/12/2025
Parere del Direttore Sanitario	
Simona Ursino: *Favorevole*	
Firma Simona Ursino	*Data* 30/12/2025
Il Direttore Generale	
Narciso Mostarda	
Firma Narciso Mostarda	*Data* 30/12/2025
Compilato dalla U.O.C. Proponente	
Non comporta impegno di spesa	
Firma Nicola D'Agostino	*Data* 29/12/2025

Il Dirigente e il Responsabile del procedimento	
Con la sottoscrizione del presente atto, a seguito dell'istruttoria effettuata attestano che l'atto è legittimo nella forma e nella sostanza ed è utile per il servizio pubblico	
Firma del Responsabile del Procedimento Nicola D'Agostino	*Data* 29/12/2025
Firma del Dirigente Nicola D'Agostino	*Data* 29/12/2025

Il Direttore UOC Information and Communication Technology relaziona al Direttore Generale e propone il seguente schema di deliberazione:

- **VISTI**

la Legge Regionale 3 agosto 2004, n. 9, con cui veniva istituita l'Azienda Regionale per l'Emergenza Sanitaria;

il D. Lgs. 30 dicembre 1992, n. 502 e successive modificazioni e integrazioni, nonché l'art. 9 della L.R. n. 18/94 e successive modificazioni ed integrazioni;

l'Atto Aziendale dell'ARES 118, formalizzato da ultimo con deliberazione 16 febbraio 2021, n. 127 e approvato con Determinazione Regionale della Direzione Salute e Integrazione Sociosanitaria 25 marzo 2021, n. G03256, pubblicata sul BURL Lazio n. 33 del 1° aprile 2021;

la Legge Regionale n. 45/96;

il D.lgs. 31 marzo 2023, n. 36 – Codice dei contratti pubblici in attuazione dell'art. 1 della legge 21 giugno 2022 n. 78 recante delega al Governo in materia di contratti pubblici.

- **PREMESSO**

Che la Legge Regionale n.9/2004, istituiva l'Azienda Regionale Emergenza Sanitaria (Ares 118) affidando alla stessa in via esclusiva per il territorio regionale del Lazio, l'attività di soccorso in emergenza-urgenza extraospedaliera, compresa l'emergenza neotanale, di trasporto collegato alla trapiantologia, di trasporti legati al primo intervento.

- **CONSIDERATO**

Che, nel tempo, la Regione Lazio ha affidato all'ARES 118 una serie di altre funzioni di natura assistenziale e di natura organizzativo gestionale, sull'intero territorio, quali le attività collegate al NEA 116117, il coordinamento delle reti di patologia, il coordinamento e l'integrazione tra i diversi ambiti assistenziali del SSR.

- **CONSIDERATO**

Che le attività dell'ARES 118 presuppongono per una gestione centralizzata, nelle sedi delle Centrali Operative aziendali, per le diverse funzioni, una gestione esterna, relativamente ai mezzi di soccorso e di trasporto sul territorio e alle strutture sanitarie coinvolte nelle attività assistenziali e di coordinamento affidata all'Azienda.

- **CONSIDERATO**

Che l'ARES 118, per svolgere la sua attività, sia relativamente alla tipologia che alla complessità che agli oneri quantitativi delle prestazioni da erogare, deve disporre, come elemento imprescindibile, di specifica piattaforma tecnologica, declinate in reti connettività, server di conservazione dati ed applicativi gestionali per le specifiche funzioni.

- **CONSIDERATO**

Che l'ARES 118 ha come obiettivo quello di garantire su tutto il territorio regionale:

* la gestione della fase di allarme, e la direzione ed il coordinamento, della risposta extraospedaliera alle emergenze-urgenze sanitarie, ivi compresa l'emergenza neonatale,

materno-assistita ed i trasporti secondari legati al primo intervento;

* la gestione dei trasporti sanitari connessi all'attività trapiantologica;

* la gestione dei trasporti secondari;

E che altresì l'ARES 118, promuove, tra l'altro, d'intesa con la Regione, i modelli organizzativi più funzionali da adottare per la gestione dell'emergenza extraospedaliera, in raccordo con i diversi Enti del Servizio Sanitario Regionale e con i Medici di Medicina Generale, addetti alla continuità assistenziale, nell'ambito del sistema di emergenza sanitaria territoriale e che per effettuare tali servizi necessariamente deve utilizzare la piattaforma applicativa e tecnologica definita SIE118 e che quindi tale piattaforma è da ritenersi di fondamentale importanza per l'esecuzione dei servizi stessi

- TENUTO CONTO

  - che la Direttiva UE n. 2022/2255 (Direttiva NIS2) - recepita nell'ordinamento italiano dal D. Lgs. n. 138/2024- introduce requisiti più stringenti per la gestione del rischio e la resilienza operativa, con un'attenzione particolare alla sicurezza della supply chain. Nello specifico, la Direttiva prescrive in maniera mandatoria per gli Enti cosiddetti Essenziali una moltitudine di adempimenti in tema di cyber sicurezza e cyber resilienza;
  - che l'Ente, nella propria qualifica di Soggetto Essenziale NIS, dovrà operare nel rispetto del cronoprogramma NIS2 di cui alla Determinazione ACN n.164179 del 14/04/2025 come di seguito: *(i)* adozione - entro il 31.12.2025- di una procedura e delle connesse azioni sia organizzative che tecniche per la gestione dell'incident reporting; *(ii)* sviluppo -entro il 31.10.2026- di tutte le altre azioni, sia di analisi e mappatura dei processi, tali da consentire il pieno adempimento della normativa NIS2;
  - che, per le motivazione sopra esposte, l'Ente ha definito politiche e procedure al fine di mettere in campo le azioni previste dalla NIS2, allegate al presente provvedimento quale parte integrante e sostanziale;

- CONSIDERATO

  - che la Determinazione ACN n. 333017/2025, art. 7, rende obbligatoria la nomina del referente aziendale incaricato di garantire i rapporti con il CSIRT nazionale (Computer Security Incident Response Team nazionale), di assicurare la corretta gestione delle comunicazioni relative agli incidenti di sicurezza informatica e di trasmettere le notifiche di incidenti significativi (come definiti dalla Determinazione ACN n. 164179) e le notifiche volontarie di informazioni rilevanti sulla cybersicurezza;
  - nelle FAQ promulgate da ACN viene precisato che il Referente CSIRT può essere qualsiasi persona fisica che disponga di competenze di base in materia di cybersicurezza e gestione degli incidenti informatici, nonché di un'adeguata conoscenza dei sistemi e delle reti dell'organizzazione.
  - che all'interno dell'amministrazione e nella contenuta organizzazione tecnica informatica aziendale non sono presenti figure professionali con tali caratteristiche oltre alle figure già designate di Punto di Contatto e Sostituto del punto di contatto;
  - che ACN ha chiarito che la Determinazione ACN 333017/2025 non vieta l'esternalizzazione di tale figura e, pertanto, è ammessa anche la designazione di professionisti esterni;
  - che, in tale prospettiva, l'Ente ha formalizzato la nomina nei confronti del Sig. Gianluigi Angotti, essendo già CISO aziendale nell'ambito del contratto di migrazione verso il PSN, per lo svolgimento delle funzioni di Referente CSIRT per garantire i rapporti con il CSIRT nazionale;

Per tutto quanto esposto in narrativa, si propone al Direttore Generale:

- di considerare le premesse parte integrante del presente dispositivo;
- di approvare e adottare i documenti allegati alla presente delibera e, nello specifico:

a) Procedura di gestione degli incidenti;

b) Politica di backup e ripristino delle informazioni;

c) Politica di controllo degli accessi logici;

d) Politica di crittografia;

e) Procedura di gestione del rischio;

f) Procedura di valutazione della sicurezza per le terzi parti;

Politiche saranno oggetto di attività per la definizione di relative procedure

- di conferire mandato al Sig. Gianluigi Angotti, già CISO aziendale nell'ambito del contratto PSN, per lo svolgimento delle funzioni e dei connessi adempimenti, di cui rispettivamente al D. lgs. n. 138/2024;
- di dare comunicazione al personale interessato mediante pubblicazione sul Sito Intranet aziendale
- di nominare il Dr. Nicola D'Agostino quale Responsabile Unico del Procedimento del presente atto

Si dichiara che il presente schema di deliberazione è stato proposto dal Direttore UOC Information Communication Technology, il quale, consapevole delle disposizioni di cui al D.lgs. 165/2001 in tema di responsabilità dirigenziale, attesta che il presente provvedimento, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall'art. 1 della Legge n. 20/1994 e successive modifiche, nonché alla stregua dei criteri di economicità ed efficacia di cui all'art. 1, primo comma, della Legge n. 241/1990 come modificato dalla Legge n. 15/2005.

IL DIRETTORE UOC INFORMATION COMMUNICATION TECHNOLOGY

Dott. Nicola D'Agostino

Il Direttore Generale, con i poteri di cui alla Deliberazione ARES 118 n. 394 del 04.11.2024 di formalizzazione del Decreto del Presidente della Regione Lazio n. T 00164 del 31.10.2024: "Prosecuzione incarico di Direttore Generale dell'ARES 118 e contestuale differimento del termine di scadenza contrattuale", vista la relazione contenuta nella presente proposta di delibera inoltrata dal Direttore della UOC Information and Communication Technology

VISTI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario

DELIBERA

Per le motivazioni richiamate in premessa, che qui si intendono integralmente riportate unitamente agli atti allegati:

- di approvare e adottare, quali parti integranti e sostanziali del presente provvedimento, i seguenti documenti allegati:

a) Procedura di gestione degli incidenti

b) Politica di backup e ripristino delle informazioni

c) Politica di controllo degli accessi logici

d) Politica di crittografia

e) Procedura di gestione del rischio

f) Procedura di valutazione della sicurezza per le terze parti

Politiche saranno oggetto di attività per la definizione di relative procedure

- di conferire mandato al Sig. Gianluigi Angotti, già CISO aziendale nell'ambito del contratto PSN, per lo svolgimento delle funzioni di Referente CSIRT ai sensi dell'art. 7 della Determinazione ACN n. 333017/2025, per garantire i rapporti con il CSIRT nazionale, assicurare la corretta gestione delle comunicazioni relative agli incidenti di sicurezza informatica e trasmettere le notifiche di incidenti significativi e le notifiche volontarie di informazioni rilevanti sulla cybersicurezza, ai sensi del D. Lgs. n. 138/2024;
- di dare comunicazione al personale interessato mediante pubblicazione sul Sito Intranet aziendale;
- di nominare il Dr. Nicola D'Agostino quale Responsabile Unico del Procedimento del presente atto

- di precisare che il presente provvedimento rientra nelle previsioni dell'art. 29 del D.Lvo 118/2011 e rispetta l'autorizzazione ex Delibera Giunta Regione Lazio n.991/2023 e Delibera Ares 118 36/2024;

La presente deliberazione è composta di n. 6 pagine di cui di allegati

Gli eventuali allegati citati e facenti parte integrante della presente deliberazione sono custoditi presso la UOC Affari Generali e oggetto di ostensione a richiesta degli interessati legittimati.

Il presente atto è pubblicato nell'Albo dell'Azienda nel sito internet aziendale www.ares118.it per 15 giorni consecutivi, ai sensi della Legge Regionale n. 45/96.

Il Direttore Generale

(Dott. Narciso Mostarda)

Modulo di segnalazione di un eventuale incidente di sicurezza

Il presente modulo deve essere utilizzato per segnalare un eventuale incidente di sicurezza con impatto significativo in banche dati, portali, sistemi amministrativi e/o diagnostici, ecc. di cui è titolare ARES 118.

Un **incidente di sicurezza** è un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi.

Il modulo compilato in tutte le sue parti va inviato tramite e-mail all'indirizzo:

dalla casella di posta elettronica aziendale [1]

1 Per la data del documento fa fede la data di invio dell'email dalla casella di posta istituzionale.

Dati di contatto di chi effettua la segnalazione (*campi obbligatori):

Nome e Cognome*:

Recapiti per comunicazioni al team di gestione degli incidenti:

Indirizzo e-mail*:

Telefono*:

Indirizzo (Via/Piazza, numero civico, città e CAP) *:

Afferenza organizzativa*:

Struttura/Ufficio di appartenenza:

Ruolo/ funzione ricoperta:

Nominativo del Responsabile della Struttura:

Dispositivo oggetto dell'incidente di sicurezza (può essere segnalata più di una voce):

☐ computer

☐ rete

☐ dispositivo mobile

☐ pen drive

☐ file o parte di un file

☐ strumento di backup

☐ workstation

☐ firewall

☐ VPN

☐ server

☐ antivirus

☐ domini di amministrazione

☐ altro:

Causa presunta dell'incidente di sicurezza: (può essere segnalata più di una voce):

☐ azione intenzionale interna

☐ azione accidentale interna

☐ azione intenzionale esterna

- ☐ phishing
- ☐ malware
- ☐ ransomware

☐ azione accidentale esterna

☐ sconosciuta

☐ altro:

Servizi interrotti/compromessi a causa dell'incidente ivi segnalato (compilare se sono note, può essere selezionata più di una voce):

☐ processi amministrativi e gestionali di ARES 118

☐ attività di programmazione sanitaria, economica e gestionale dell'Ente di ARES 118

☐ altro, specificare:

Indicatori di compromissione (IOC): (compilare se sono note, può essere selezionata più di una voce):

☐ indirizzi IP

☐ hash di file

☐ pattern di traffico anomali

☐ anomalie negli accesso

☐ altro, specificare:

Probabili conseguenze dell'incidente di sicurezza (può essere segnalata più di una voce):

☐ **Interruzione delle attività lavorative:**

- ☐ per il singolo utente
- ☐ per il team/dipartimento
- ☐ per l'azienda o per i clienti
- ☐ altro, specificare:
- ☐ in corso di valutazione

☐ **Impatto su dati e/o informazioni:**

- ☐ perdita o corruzione di dati e/o informazioni
- ☐ inaccessibilità dei dati e/o informazioni
- ☐ altro, specificare:
- ☐ in corso di valutazione

☐ **Compromissione della sicurezza:**

- ☐ sospetto di accesso non autorizzato
- ☐ sospetto infezione malware/ransomware
- ☐ altro, specificare:
- ☐ in corso di valutazione

☐ **Impatto economico o reputazionale:**

- ☐ impatto economico diretto
- ☐ rischio di danno di immagine
- ☐ altro, specificare:
- ☐ in corso di valutazione

Potenziale impatto operativo dell'incidente (può essere segnalata più di una voce):

☐ interruzione del lavoro individuale

☐ interruzione del lavoro di un team

☐ interruzione di un servizio aziendale critico

☐ impatto sui clienti o partner esterni

☐ rischio di perdita o corruzione di dati e/o informazioni

☐ sospetto accesso o divulgazione non autorizzata di dati e/o informazioni

☐ rischio di perdita economica diretta

Stima della gravità complessiva dell'incidente di sicurezza (selezionare solo UNA voce):

☐ trascurabile

☐ bassa

☐ media

☐ alta

☐ critica

☐ non definita

Quando si è verificato l'incidente di sicurezza? (selezionare solo UNA voce):

☐ è possibile identificare la data precisa dell'incidente il

ed esso è ancora in corso;

☐ è possibile identificare la data precisa dell'incidente il

ed esso non è più in corso;

☐ l'incidente è avvenuto presumibilmente nel seguente intervallo temporale:

dal al

Ulteriori soggetti coinvolti (indicare i riferimenti dei soggetti coinvolti e il ruolo svolto):

1. Denominazione:

C.F./P. IVA:

Ruolo:

Stabilimento sito in Paese UE/SEE/EFTA, indicare quale:

Stabilimento sito in Paese Extra UE, indicare quale:

2. Denominazione:

C.F./P. IVA:

Ruolo:

Stabilimento sito in Paese UE/SEE/EFTA, indicare quale:

Stabilimento sito in Paese Extra UE, indicare quale:

3. Denominazione:

C.F./P. IVA:

Ruolo:

Stabilimento sito in Paese UE/SEE/EFTA, indicare quale:

Stabilimento sito in Paese Extra UE, indicare quale:

Eventuali ulteriori informazioni utili relative all'incidente di sicurezza:

Luogo e data

REGISTRO DEGLI INCIDENTI ARES 118

COMPONENTI TEAM DI GESTIONE INCIDENTI E RELATIVI DATI DI CONTATTO	Ruolo	Informazioni di contatto		Tempo di archiviazione
		TEL:	mail	
(INSERIRE NOME E COGNOME)	Direttore Generale			Permanente
(INSERIRE NOME E COGNOME)	Direttoe Amministrativo			
(INSERIRE NOME E COGNOME)	Direttoe Sanitario			
(INSERIRE NOME E COGNOME)	Direttore Area ICT			
(INSERIRE NOME E COGNOME)	Referente per la Cybersicurezza Aziendale			
(INSERIRE NOME E COGNOME)	Punto di contatto NIS 2			
(INSERIRE NOME E COGNOME)	Sostituto Punto di contatto NIS 2			
(INSERIRE NOME E COGNOME)	Referente Privacy Aziendale			
(INSERIRE NOME E COGNOME)	Referente CSIRT			
(INSERIRE NOME E COGNOME)				
(INSERIRE NOME E COGNOME)				
		LUOGO DI ARCHIVIAZIONE DEL PRESENTE REGISTRO		
LUOGO DI ARCHIVIAZIONE DELLA PROCEDURA DI INCIDENT MANAGEMENT				
Armadio con chiave di sicurezza in stanza accesso limitato		pc aziendale:		
RESPONSABILE DELL'ARCHIVIAZIONE				
REFERENTE CSIRT				
AUTORIZZATI AL CONTROLLO DEL PRESENTE REGISTRO				
REFERENTE CSIRT				

DECISIONI DOCUMENTATE DELLE RUNIONI DEL TEAM DI GESTIONE INCIDENTI

LUOGO DI ARCHIVIAZIONEDELLE DECISIONI DOCUMENTATE	Tempo di archiviazione
Armadio con chiave di sicurezza in stanza accesso limitato	5 anni
RESPONSABILE DELL'ARCHIVIAZIONE	
REFERENTE CSIRT	
AUTORIZZATO AL CONTROLLO PER LA PROTEZIONE DEI DOCUMENTI	
REFERENTE CSIRT	

DATA	DECISIONE DOCUMENTATA
	ADOZIONE PROCEDURA DI RISPOSTA IN CASO DI INCIDENTE - PROTOCOLLO AZIENDALE IN MATERIA DI INCIDENT MANAGEMENT

COMUNICAZIONI DELL'INCIDENTE A SOGGETTI ESTERNI

LUOGO DI ARCHIVIAZIONE DELLE COMUNICAZIONI	Tempo di archiviazione
Armadio con chiave di sicurezza in stranza accesso limitato	5 anni
RESPONSABILE DELL'ARCHIVIAZIONE	
REFERENTE CSIRT	
AUTORIZZATO AL CONTROLLO PER LA PROTEZIONE DELLE COMUNICAZIONI	
REFERENTE CSIRT	

DATA	COMUNICAZIONI EFFETTUATE

REGISTRO DELLE NOTIFICHE DI INCIDENTE ICT AL CSIRT ITALIA

LUOGO DI ARCHIVIAZIONE DELLE NOTIFICHE	Tempo di archiviazione
Armadio con chiave di sicurezza in stranza accesso limitato	5 anni
RESPONSABILE DELL'ARCHIVIAZIONE	
REFERENTE CSIRT	
AUTORIZZATO AL CONTROLLO PER LA PROTEZIONE DELLE NOTIFICHE	
REFERENTE CSIRT	

DATA	NOTIFICHE EFFETTUATE

REGISTRO DEGLI INCIDENTI ICT NON SIGNIFICATIVI

LUOGO DI ARCHIVIAZIONE DELLE NOTIFICHE	Tempo di archiviazione
Armadio con chiave di sicurezza in stranza accesso limitato	5 anni
RESPONSABILE DELL'ARCHIVIAZIONE	
REFERENTE CSIRT	
AUTORIZZATO AL CONTROLLO PER LA PROTEZIONE DELLE NOTIFICHE	
REFERENTE CSIRT	

DATA	REPORT FINALE DOCUMENTATO

SISTEMA SANITARIO REGIONALE
ARES
118

REGIONE
LAZIO

ALLEGATO 3

Contenuto

1. Composizione del team di gestione incidenti

Il team di gestione degli incidenti sarà composto da soggetti interni all'Azienda e soggetti esterni.

Le figure interne saranno le uniche deputate a poter determinare la configurazione di un incidente, la gravità del medesimo, nonché le attività da porre in essere e, nello specifico, sono le seguenti:

- Direttore Generale
- Direttore Amministrativo
- Direttore Sanitario
- Direttore UOC ICT
- Responsabile per la Cybersicurezza Aziendale
- CISO (ove nominato)
- Referente CSIRT
- Punto di Contatto NIS 2
- Sostituto Punto di Contatto NIS 2
- Referente Privacy Aziendale
- Sistemisti aziendali interni ed esterni.

Alle riunioni programmate dal team di gestione incidenti potranno anche partecipare ***(i)*** rappresentanti della Società Leonardo S.p.A., in forza di quanto previsto dal contratto di migrazione al PSN nonché ***(ii)*** rappresentanti della Società Scudomed S.r.l., in quanto fornitore della Società Leonardo S.p.A., ***(iii)*** il CISO nominato dall'azienda e ***(IV)*** il DPO. Tali figure potranno essere consultate al fine di ottenere parere in merito a eventi occorsi e/o attività da porre in essere, ma non potranno assumere decisioni vincolanti per l'Azienda.

2. Incidenti significativi, evidenze e temini per la notifica

Gli incidenti significativi da considerarsi per ARES 118, nella propria qualifica di Soggetto Essenziale NIS, sono riportati nell'allegato 4 della determina 164179/2025 dell'Agenzia per la Cybersicurezza Nazionale (ACN).

Ogni tipologia di incidente significativo è costituita da un **codice identificativo** e da una **descrizione**. Nel complesso sono state definite **4** tipologie di incidenti significativi per i soggetti essenziali.

Con evidenza dell'incidente si intende che il soggetto dispone di elementi oggettivi dai quali si evince che si è verificato un incidente di sicurezza informatica. L'acquisizione dell'evidenza è tipicamente successiva al verificarsi dell'incidente e definisce il momento dal quale decorre il termine per la trasmissione della pre-notifica (24 ore) e della notifica (72 ore), mediante piattaforma telematica messa a disposizione dal CSIRT Italia. Entro i 30 giorni successivi, ARES 118 dovrà trasmettere, sempre telematicamente, una relazione finale sull'accaduto.

SISTEMA SANITARIO REGIONALE
ARES 118

REGIONE LAZIO

POLICY PER IL BACKUP E RISPRISTINO DELLE INFORMAZIONI

118.PO.SEC.0XX – V1.0

Contenuto

1. Policy Statement

Il backup delle informazioni in formato elettronico deve essere effettuato secondo criteri di criticità dei dati e continuità operativa, garantendo la protezione e il ripristino tempestivo delle informazioni necessarie all'erogazione dei servizi sanitari.

I sistemi critici per la gestione delle emergenze devono essere soggetti a strategie di backup e ripristino con obiettivi di disponibilità compatibili con la continuità del servizio.

2. Definizioni

Termine	Definizione
Backup	Creazione di copie dei dati in modo che possano essere utilizzate per ripristinare l'originale dopo un evento di perdita di dati, con garanzie di integrità e disponibilità.
Ripristino	Processo di riportare i dati dalle copie di backup sui dispositivi originali o alternativi, seguito da procedure di verifica dell'integrità.
Dati critici	Informazioni la cui perdita o indisponibilità compromette significativamente l'erogazione dei servizi sanitari o la sicurezza dei pazienti.
RTO (Recovery Time Objective)	Tempo massimo accettabile per il ripristino di un sistema o servizio dopo un'interruzione.
RPO (Recovery Point Objective)	Quantità massima accettabile di perdita di dati, espressa in termini temporali.
Disaster Recovery	Insieme di politiche e procedure per il ripristino rapido dei sistemi critici in caso di eventi catastrofici.

3. Ambito di applicazione della politica

Questa politica si applica a tutti i sistemi informativi di Ares 118, con particolare attenzione ai sistemi critici per l'erogazione dei servizi sanitari e di emergenza.

Per gli ambienti gestiti da fornitori esterni, è accettabile discostarsi da questa politica solo previo accordo formale che specifichi obiettivi di servizio equivalenti o superiori. Il team del fornitore è responsabile dell'implementazione di soluzioni adeguate conformi agli accordi definiti.

4. Classificazione e Priorità

4.1. Sistemi Critici

- Sistemi di gestione emergenze e dispatch
- Schede di soccorso e cartellini di centrale in formato elettronico
- Sistemi di comunicazione operativa

4.2. Sistemi Importanti

- Sistemi amministrativi e gestionali
- Database di configurazione
- Sistemi di monitoraggio

4.3. Sistemi Standard

- Ambienti di sviluppo e test
- Sistemi di archiviazione non critici

5. Standard minimi di implementazione

5.1. Misure di backup dei dati

1) **Pianificazione**: Per ogni ambiente deve essere creato un piano di backup, rivisto annualmente e riapprovato. Il piano deve definire obiettivi RTO e RPO per categoria di sistema.
2) **Contenuti del Piano**: Ogni politica di backup deve specificare:
    a. Programma e frequenza del backup
    b. Numero di copie da conservare (principio 3-2-1: 3 copie, 2 supporti diversi, 1 off-site)
    c. Metodi di archiviazione e crittografia
    d. Ubicazione (on-site e off-site obbligatorio per sistemi critici)
    e. Periodi di conservazione conformi alle normative;
    f. Criteri di selezione e esclusione dei file
3) **Reporting**: Il rapporto di backup deve includere:
    a. Elenco sistemi con relativa politica implementata
    b. Sistemi esclusi con motivazioni documentate
    c. Metriche di conformità agli obiettivi RTO/RPO
4) **Tipologie di backup**
    a. **Sistemi di produzione**: Backup obbligatorio con frequenze determinate dalla criticità
    a. **Ambienti di sviluppo/test**: Backup discrezionale, ma raccomandato per dati di valore
5) **Sicurezza**
    a. Crittografati secondo gli standard aziendali
    b. Conservati in ambienti sicuri
    b. Accessibili solo a personale autorizzato

5.2. Misure di test dei backup

1) **Test periodici**: Il ripristino deve essere testato secondo frequenze stabilite per categoria di sistema e obbligatoriamente dopo modifiche alle procedure
2) **Validazione**: I test devono verificare:
    a. Integrità del salvataggio
    b. Successo del ripristino (completo e parziale)
    c. Conformità agli obiettivi RTO/RPO
3) **Equivalenza operativa**: Le attività di ripristino frequenti possono sostituire i test formali se documentate e tracciate

5.3. Salvaguardia dei backup

1) **Controllo accessi**: Solo personale esplicitamente autorizzato può accedere ai backup, tipicamente limitato al team di gestione dati
2) **Gestione eccezioni**: La Direzione Strategica di Ares 118 può autorizzare accessi straordinari previo processo formale di approvazione
3) **Protezione fisica e logica**: I backup devono essere protetti da accessi non autorizzati, eventi ambientali e degrado dei supporti

5.4. Ripristino dei backup

1) **Processo formale**: Il ripristino richiede sempre richiesta documentata attraverso:
    a. Sistema di gestione richieste (basso impatto)
    b. Processo di gestione modifiche (alto impatto)
2) **Autorizzazioni**: Definizione chiara delle autorità per approvare ripristini in base all'impatto e alla criticità
3) **Procedure di emergenza**: Definizione di procedure accelerate per situazioni critiche che compromettono la sicurezza dei pazienti

6. Conformità e controllo

I backup devono essere conformi alle normative vigenti in materia di protezione dati personali e conservazione documentale sanitaria. La verifica della conformità è parte integrante dei controlli interni.

7. Controllo e revisione del documento

Questa policy è soggetta a revisione periodica per garantire la sua attualità ed efficacia. Le modifiche sostanziali richiedono l'approvazione della Direzione Aziendale.

Controllo del documento	
Autore	Team DIGIUP/Leonardo
Proprietario	
Data di creazione	1° luglio 2025
Revisione di	
Data ultima revisione	

Versione	Data di approvazione	Approvato da	Descrizione del cambiamento
Versione 1.0			Rilascio iniziale

SISTEMA SANITARIO REGIONALE
ARES 118

REGIONE LAZIO

POLITICA DI CONTROLLO DEGLI ACCESSI LOGICI

118.PO.SEC.0XX – V1.0

Contenuto

1. Policy Statement

L'accesso logico alle informazioni di Ares 118 deve essere autorizzato in base all'identificazione individuale (ID univoci basati su una convenzione di denominazione) e all'autenticazione.

I proprietari delle risorse devono mantenere un archivio di identità accurato e aggiornato per ogni sistema informativo sotto la loro responsabilità, garantendo la tracciabilità degli accessi.

L'accesso remoto alla rete Ares 118 sarà concesso solo ai collaboratori che hanno una valida esigenza aziendale per l'esecuzione di attività che richiedono l'accesso remoto. L'accesso remoto deve essere protetto utilizzando l'autenticazione multi-fattore e crittografia conforme agli standard aziendali.

Tutti i diritti di accesso logici devono essere soggetti a un ciclo di revisione periodica e documentata, con particolare attenzione agli account con privilegi elevati.

Gli accessi devono rispettare il principio del minimo privilegio necessario per l'espletamento delle funzioni assegnate.

2. Definizioni

Termine	Definizione
Meccanismi di autenticazione	I meccanismi utilizzati per stabilire la validità di un'identità dichiarata, inclusi password, codici PIN, smartcard, token di sicurezza e sistemi biometrici. La forza dell'autenticazione è determinata dal numero di fattori utilizzati.
Autenticazione multi-fattore (MFA)	Sistema di autenticazione che richiede almeno due fattori distinti tra: qualcosa che si conosce (password), qualcosa che si possiede (token) o qualcosa che si è (biometria).
Collaboratore	Personale e appaltatori di Ares 118 che lavorano per l'organizzazione, incluso tutto il personale indipendentemente dal grado, dalla funzione o dalla tipologia contrattuale.
Account predefiniti	Gli account di default sono account generici che sono presenti di default in un sistema informativo.
Account con privilegi elevati	Account con privilegi amministrativi sui sistemi informativi, soggetti a controlli rafforzati e revisioni più frequenti.
Proprietario della risorsa	Il collaboratore responsabile all'interno di Ares 118 per specifiche informazioni o sistemi, con autorità decisionale sui relativi accessi.
Account di sistema	Account utilizzati da applicazioni o servizi per operazioni automatizzate, tipicamente senza supporto per sessioni interattive.
Principio del minimo privilegio	Assegnazione dei diritti di accesso strettamente necessari per l'espletamento delle funzioni lavorative, limitando l'esposizione al rischio.
Ciclo di revisione degli accessi	Processo periodico di verifica e validazione dei diritti di accesso assegnati, con frequenza determinata dal livello di rischio.

3. Standard minimi di implementazione

3.1. Identificazione e Autenticazione

- Ogni utente deve essere univocamente identificato nel sistema
- L'autenticazione deve essere commisurata al livello di rischio delle risorse accedute
- Gli account condivisi sono vietati, salvo eccezioni documentate e approvate

3.2. Autorizzazione e Controllo degli Accessi

- L'accesso alle risorse deve essere autorizzato dal proprietario della risorsa
- I diritti devono essere assegnati secondo il principio del minimo privilegio
- Le modifiche ai diritti di accesso devono essere documentate e tracciate

3.3. Responsabilità e Governance

- Ogni risorsa deve avere un proprietario chiaramente identificato
- I proprietari sono responsabili della gestione degli accessi alle proprie risorse
- La direzione IT è responsabile dell'implementazione tecnica delle policy

3.4. Conformità e Controllo

- Tutti gli accessi devono essere conformi alle normative vigenti (ad es. GDPR, normative clinico/sanitarie, NIS 2, etc.)
- I sistemi devono garantire audit trail completi e non modificabili
- Le violazioni delle policy devono essere prontamente segnalate e gestite

4. Standard minimi di implementazione

4.1. Requisiti Generali

Applicabili a tutti i tipi di account e sistemi dell'organizzazione.

4.2. Gestione del Ciclo di Vita degli Utenti

Processo di creazione, modifica, sospensione e cancellazione di tutti i tipi di account.

4.3. Account con Privilegi Elevati

Controlli rafforzati per account amministrativi e di sistema critici.

4.4. Accesso Remoto

Requisiti specifici per l'accesso da postazioni esterne alla rete aziendale.

4.5. Gestione delle Emergenze

Procedure per garantire continuità operativa in situazioni critiche mantenendo la sicurezza.

I dettagli operativi di implementazione sono definiti nelle procedure specifiche di settore.

5. Ruoli e responsabilità

Ruolo	Responsabilità
Direzione Strategica Aziendale	Approvazione della policy e assegnazione delle risorse necessarie
Proprietario della Risorsa	Autorizzazione degli accessi e gestione dei diritti per le risorse di competenza
Direzione IT	Implementazione tecnica e mantenimento dei sistemi di controllo accessi
Responsabile Sicurezza	Monitoraggio della conformità
Audit Interno	Verifica periodica dell'efficacia dei controlli implementati

6. Controllo e revisione del documento

Questa policy è soggetta a revisione periodica per garantire la sua attualità ed efficacia. Le modifiche sostanziali richiedono l'approvazione della Direzione Aziendale.

Controllo del documento	
Autore	Team DIGIUP/Leonardo
Proprietario	
Data di creazione	1° luglio 2025
Revisione di	
Data ultima revisione	

Versione	Data di approvazione	Approvato da	Descrizione del cambiamento
Versione 1.0			Rilascio iniziale

SISTEMA SANITARIO REGIONALE
ARES
118

REGIONE
LAZIO

POLITICA DI CRITTOGRAFIA

118.PO.SEC.0XX – V1.0

Contenuto

1. Policy Statement

La crittografia deve essere utilizzata per proteggere la riservatezza, l'integrità e l'autenticità delle informazioni di Ares 118, con particolare attenzione ai dati sanitari e alle comunicazioni critiche per la gestione delle emergenze.

Devono essere utilizzati esclusivamente algoritmi crittografici approvati e conformi agli standard di settore. Le chiavi di crittografia e i certificati digitali devono essere trattati come informazioni strettamente riservate e gestiti secondo procedure formali che ne garantiscano la sicurezza durante l'intero ciclo di vita.

La scelta degli algoritmi e delle implementazioni crittografiche deve bilanciare i requisiti di sicurezza con le necessità operative, garantendo che i sistemi critici per l'emergenza sanitaria mantengano prestazioni adeguate.

2. Definizioni

Termine	Definizione
Crittografia	Uso di metodi matematici per la trasformazione dei dati al fine di proteggerne il contenuto, stabilirne l'autenticità, impedirne modifiche non rilevate e garantirne l'uso autorizzato.
Cifratura	Processo di codifica di un messaggio o informazione in modo che solo le parti autorizzate possano accedervi, utilizzando algoritmi e chiavi crittografiche.
Hashing	Funzione crittografica unidirezionale che trasforma dati di dimensioni arbitrarie in una stringa di bit di dimensioni fisse, utilizzata per verificare l'integrità dei dati.
Chiave crittografica	Valore segreto utilizzato con un algoritmo crittografico per cifrare o decifrare informazioni. La sicurezza dipende dalla segretezza della chiave e dalla sua lunghezza.
Certificato digitale	Documento elettronico che associa una chiave pubblica a un'identità, utilizzato per autenticazione e scambio sicuro di chiavi, firmato da un'autorità di certificazione fidata.
Dati sensibili	Informazioni di proprietà di Ares 118 o dati di pazienti/fornitori classificati come interni, riservati o strettamente confidenziali, inclusi tutti i dati sanitari.
PKI (Public Key Infrastructure)	Infrastruttura che gestisce chiavi pubbliche e certificati digitali, includendo autorità di certificazione, procedure di rilascio e revoca.

3. Ambito di applicazione della politica

Questa politica si applica a:

- Tutti i sistemi informativi di Ares 118
- Dati in transito su reti pubbliche o non fidate
- Dati a riposo su sistemi non fisicamente sicuri
- Comunicazioni contenenti informazioni sensibili
- Backup e archiviazione di lungo termine
- Dispositivi mobili e postazioni remote

La crittografia è obbligatoria per tutti i dati sanitari e le informazioni classificate come riservate o strettamente confidenziali.

4. Obiettivi della Crittografia

La crittografia viene utilizzata per conseguire i seguenti obiettivi di sicurezza:

4.1. Riservatezza

Protezione di informazioni sensibili attraverso tecniche di cifratura per dati in stato di riposo o in transito, impedendo l'accesso non autorizzato.

4.2. Integrità

Utilizzo di firme digitali e codici di autenticazione per verificare che le informazioni non siano state alterate, garantendo l'affidabilità dei dati sanitari.

4.3. Autenticazione

Conferma dell'identità di mittenti e destinatari nelle comunicazioni, essenziale per la tracciabilità nelle operazioni sanitarie.

4.4. Non ripudio

Utilizzo di tecniche crittografiche per ottenere prove digitali del verificarsi di eventi o azioni, fondamentale per la documentazione sanitaria.

5. Standard minimi di implementazione

5.1. Algoritmi e Standard Approvati

Cifratura simmetrica:

- AES (Advanced Encryption Standard) con chiavi minime di 256 bit
- Algoritmi legacy (DES, 3DES) sono vietati

Cifratura asimmetrica:

- RSA con chiavi minime di 2048 bit (raccomandato 3072 bit)
- Curve ellittiche (ECC) con chiavi equivalenti

Funzioni di hash:

- SHA-256 o superiori per nuove implementazioni
- SHA-1 e MD5 sono vietati per nuovi sistemi

Protocolli di comunicazione:

- TLS 1.2 come versione minima (raccomandato TLS 1.3)
- VPN con crittografia conforme agli standard sopra indicati

5.2. Gestione delle Chiavi e Certificati

Generazione delle chiavi:

- Utilizzo di generatori di numeri casuali crittograficamente sicuri
- Procedure documentate per la generazione e distribuzione

Conservazione:

- Chiavi private protette con crittografia aggiuntiva
- Accesso limitato al personale autorizzato
- Separazione dei ruoli nella gestione

Ciclo di vita:

- Procedure formali per creazione, distribuzione, aggiornamento e revoca
- Backup sicuro delle chiavi critiche
- Distruzione sicura al termine del ciclo di vita

Certificati digitali:

- Utilizzo di CA (Certificate Authority) riconosciute
- Validazione periodica e rinnovo tempestivo
- Gestione delle liste di revoca (CRL/OCSP)

5.3. Implementazione per Categorie di Dati

Dati sanitari:

- Crittografia obbligatoria in ogni stato (riposo, transito, elaborazione quando possibile)
- Chiavi dedicate per categorie di dati sensibili

Comunicazioni operative:

- Crittografia end-to-end per comunicazioni critiche
- Autenticazione forte per sistemi di dispatch

Backup e archiviazione:

- Crittografia obbligatoria per tutti i backup contenenti dati sensibili
- Chiavi di backup gestite separatamente dai dati

5.4. Dispositivi e Accesso Remoto

Dispositivi mobili:

- Crittografia completa del disco obbligatoria
- Containerizzazione per separare dati aziendali e personali

Accesso remoto:

- VPN con crittografia forte obbligatoria
- Autenticazione multi-fattore per sistemi critici

6. Responsabilità e Governance

Ufficio IT:

- Definizione degli standard crittografici
- Approvazione di nuove implementazioni
- Monitoraggio della conformità

Amministratori di sistema:

- Implementazione tecnica conforme agli standard
- Gestione operativa di chiavi e certificati
- Reporting di non conformità

Proprietari dei dati:

- Classificazione dei dati e definizione dei requisiti
- Approvazione delle eccezioni giustificate

7. Conformità e Controlli

La conformità agli standard crittografici è verificata attraverso:

- Audit periodici dei sistemi e delle implementazioni
- Test di penetrazione e vulnerability assessment
- Verifica della corretta gestione delle chiavi
- Controllo del rispetto delle normative vigenti (GDPR, normative clinico/sanitarie, NIS 2, etc.)

8. Supporto e Consulenza

Per chiarimenti sull'applicazione di questa politica o per situazioni specifiche non coperte, contattare l'Ufficio IT di Ares 118 tramite i canali ufficiali definiti nelle procedure operative.

9. Controllo e revisione del documento

Questa policy è soggetta a revisione periodica per garantire la sua attualità ed efficacia. Le modifiche sostanziali richiedono l'approvazione della Direzione Strategica Aziendale.

Controllo del documento	
Autore	Team DIGIUP/Leonardo
Proprietario	
Data di creazione	1° luglio 2025
Revisione di	
Data ultima revisione	

Versione	Data di approvazione	Approvato da	Descrizione del cambiamento
Versione 1.0			Rilascio iniziale

SISTEMA SANITARIO REGIONALE
ARES 118

REGIONE LAZIO

PROCEDURA DI GESTIONE DEL RISCHIO

118.PR.SEC.XXX – V1.0

Contenuto

1. Executive Summary - Guida Pratica al Risk Assessment

La presente procedura implementa un sistema strutturato di identificazione, valutazione e gestione dei rischi informativi, in conformità agli standard ISO/IEC 27001:2022 e ISO/IEC 27005:2022.

Obiettivi Strategici

L'implementazione di questa procedura persegue i seguenti obiettivi:

- **Standardizzazione**: Uniformare i criteri di valutazione dei rischi tra tutte le unità operative
- **Proporzionalità**: Calibrare le misure di sicurezza sulla base del rischio effettivo
- **Continuità operativa**: Garantire la disponibilità dei sistemi critici per l'assistenza sanitaria
- **Conformità normativa**: Assicurare l'aderenza ai requisiti GDPR, NIS2 e alle normative settoriali

Modello Organizzativo

La procedura adotta un modello evolutivo di responsabilità che si sviluppa per fasi:

Fase Iniziale (0-12 mesi):

- **CISO**: Coordina metodologia, consolida valutazioni e fornisce supporto diretto ai Responsabili del Rischio
- **Security Forum**: Organismo collegiale per decisioni strategiche (CISO + Direttore Generale + Direttore Amministrativo + Direttore Sanitario + Responsabile IT + DPO + Responsabile Risk Management)
- **Responsabili del Rischio**: Gestori specifici per eventi nei loro ambiti di competenza

Fase di Consolidamento (12-24 mesi):
Valutazione della necessità di supporto dedicato basata su:

- Volume di valutazioni gestite
- Complessità degli eventi identificati
- Disponibilità di risorse per funzione Security Office

Supporto Metodologico Transitorio: Durante la fase iniziale, il CISO fornisce supporto metodologico diretto coordinando con la dirigenza aziendale

- Facilitazione delle valutazioni dei Responsabili del Rischio
- Standardizzazione degli approcci
- Consolidamento dati e reporting aggregato
- Formazione e coaching operativo

Le decisioni finali rimangono sempre in capo alla dirigenza aziendale, con il CISO in ruolo di facilitatore metodologico.

Approccio Metodologico

Il sistema utilizza un metodo semi-quantitativo che combina:

- Valutazioni qualitative comprensibili agli operatori
- Calcoli quantitativi per confrontabilità e prioritizzazione
- Parametri calibrabili empiricamente sulla base dell'esperienza organizzativa
- Soglie di tolleranza differenziate per tipologia di asset

Implementazione Graduale

Riconoscendo la complessità dell'ambiente sanitario operativo 24/7, la procedura prevede:

- Fase pilota su sistemi critici identificati

- Supporto metodologico dedicato nelle valutazioni iniziali
- Formazione contestualizzata con scenari specifici del settore
- Strumenti semplificati per facilitare l'adozione iniziale

Sintesi del Processo di Risk Assessment

La presente procedura implementa un processo strutturato di gestione dei rischi per la sicurezza delle informazioni in cinque fasi:

1. **IDENTIFICARE** - Eventi che possono compromettere riservatezza, integrità, disponibilità
2. **ANALIZZARE** - Calcolare il livello di rischio (Verosimiglianza × Impatto × Asset × Controlli)
3. **CLASSIFICARE** - Verde (accettabile) / Ambra (da valutare) / Rosso (critico)
4. **TRATTARE** - Modificare, eliminare, condividere o accettare il rischio
5. **MONITORARE** - Verificare efficacia e mantenere il rischio sotto controllo

Timeline Operative Essenziali

Attività	Sistemi Critici	Altri Sistemi	Amministrativi
Rivalutazione completa	Trimestrale	Semestrale	Annuale
Trattamento eventi ROSSO	30 giorni	60 giorni	60 giorni
Fast-track emergenze	24-72 ore	-	-

Ruoli Chiave

- **Responsabile del Rischio**: Gestisce specifici eventi di rischio nel proprio ambito
- **CISO**: Coordina metodologia e consolidamento
- **Security Forum**: Decide su eventi critici e conflitti
- **DPO**: Consultazione obbligatoria per eventi che coinvolgono dati personali, con parere consultivo solo per aspetti di compliance privacy

Documenti Operativi

- **118.PR.SEC.15A**: Registro Risk Assessment (identificazione e calcolo)
- **118.PR.SEC.15B**: Piano di Trattamento (azioni e monitoraggio)
- **118.PR.SEC.16**: Procedura Incident Response (collegamento eventi)

2. Controllo e revisione del documento

Controllo del documento	
Autore	Team Leonardo
Proprietario	
Data di creazione	1° luglio 2025
Revisione di	
Data ultima revisione	

Versione	Data di approvazione	Approvato da	Descrizione del cambiamento
Versione 1.0			Rilascio iniziale

3. Nomenclatura

La presente procedura adotta il sistema di codifica documentale aziendale:

- **[ORG].[TIP].[ARE].[NUM][SUF]**

Dove:

- **ORG** = Codice organizzazione (es. 118)
- **TIP** = Tipologia documento
- **ARE** = Area funzionale
- **NUM** = Numero progressivo
- **SUF** = Suffisso (A, B, C per allegati/versioni)

Tipologie Documento (TIP)

- **PR** = Procedure operative
- **PO** = Politiche e direttive
- **TN** = Documenti tecnici/normativi
- **MO** = Moduli e template
- **RE** = Registri e log

Aree Funzionali (ARE)

- **SEC** = Security & Privacy
- **SOE** = Sistemi operativi di emergenza
- **AMM** = Amministrazione
- **QUA** = Qualità e audit
- **TEC** = Infrastrutture tecniche

- **LEG** = Legale e compliance

4. Documenti correlati

4.1.1. Documentazione interna

- 118.PR.SEC.15A - Registro Information Risk Assessment
- 118.PR.SEC.15B - Piano di trattamento del rischio
- 118.PR.SEC.16 - Procedura Incident Response
- 118.PO.SEC.01 - Politica sicurezza delle informazioni
- 118.TN.SEC.08 - Riferimenti normativi applicabili
- 118.PR.TEC.XX - Business Continuity Piattaforma GRC
- 118.MO.SEC.15C - Template Offline Risk Assessment

4.1.2. Standard e normative di riferimento

- UNI EN ISO 9001:2015 "Quality management systems - Requirements"
- ISO/IEC 27001:2022 "Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni - Requisiti"
- ISO/IEC 27005:2022 "Information security, cybersecurity and privacy protection - Information security risk management"
- UNI/PdR 174:2025 - Sistema di gestione per la cybersicurezza e la sicurezza delle informazioni armonizzato alla norma UNI CEI EN ISO/IEC 27001 e al Framework NIST CSF 2.0 - Requisiti

5. Terminologia e Definizioni

Acronimo o nozione	Definizione
Rischio	Effetto dell'incertezza sugli obiettivi (ISO 27000:2018, 3.61) Nel contesto del presente documento: possibilità che eventi compromettano la sicurezza delle informazioni sanitarie
Livello del rischio	Livello del rischio: Grandezza di un rischio espressa in termini di combinazione delle conseguenze e della loro verosimiglianza (ISO 27000:2018, 3.39) Metodo di calcolo adottato: Nel presente documento, il livello di rischio viene operativamente calcolato come: Verosimiglianza × Impatto × Fattore Asset × Fattore Controlli. Questo rappresenta l'implementazione specifica dell'organizzazione del concetto generale di livello di rischio.
Sicurezza delle informazioni (*Information Security*)	Preservazione della riservatezza, integrità e disponibilità delle informazioni *(ISO 27000:2018, 3.28)*
Riservatezza (*Confidentiality*)	Proprietà di un'informazione di non essere disponibile o rivelata a individui, entità o processi non autorizzati *(ISO 27000:2018, 3.10)*
Integrità (*Integrity*)	Proprietà di accuratezza e completezza *(ISO 27000:2018, 3.36)*

Disponibilità (*Availability*)	Proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata *(ISO 27000:2018, 3.7)*
Asset	Tutto ciò che ha valore per l'organizzazione (ISO/IEC 27000:2018, 3.6). Nel contesto sanitario include sistemi informativi, dati dei pazienti, dispositivi medici, processi assistenziali e infrastrutture tecnologiche.
Minaccia (*Threat*)	Causa potenziale di un incidente indesiderato che può risultare in danno per un sistema o un'organizzazione *(ISO 27000:2018, 3.74)*
Vulnerabilità (*Vulnerability*)	Debolezza di un asset o controllo che può essere sfruttata da una o più minacce *(ISO 27000:2018, 3.77)*
Identificazione del rischio	Processo di individuazione, riconoscimento e descrizione del rischio *(ISO 27005:2022)*
Analisi del rischio	Processo per comprendere la natura del rischio e determinare il livello del rischio *(ISO 27005:2022 – 7.3)*
Valutazione del rischio relativo alla sicurezza delle informazioni (*Information Security Risk Assessment*)	Processo complessivo di identificazione, analisi e ponderazione del rischio relativo alla sicurezza delle informazioni *(ISO 27005:2022 – 7.4)*
Ponderazione del rischio	Processo di comparazione dei risultati dell'analisi del rischio con i criteri di rischio per determinare se il rischio sia accettabile *(ISO 27005:2022)*
Trattamento del rischio	Processo per modificare il rischio *(ISO 27000:2018, 3.72)*
Opzioni di trattamento del rischio	Insieme delle possibili modalità per trattare il rischio: • **Evitare** il rischio decidendo di non iniziare o continuare l'attività • **Rimuovere** la sorgente del rischio • **Modificare** la verosimiglianza o le conseguenze • **Condividere** il rischio con altri soggetti • **Accettare** il rischio con una scelta informata *(ISO 27005:2022)*
Rischio residuo	Rischio rimanente dopo il trattamento del rischio *(ISO 27000:2018, 3.68)*
Responsabile del rischio (*Risk Owner*)	Persona o entità con la responsabilità e l'autorità per gestire un rischio *(ISO 27000:2018, 3.71)*
Controllo di sicurezza	Misura che modifica il rischio. I controlli includono qualsiasi processo, politica, dispositivo, pratica o altre azioni che modificano il rischio *(ISO 27000:2018, 3.14)*
Incidente di sicurezza delle informazioni	Singolo evento o serie di eventi di sicurezza delle informazioni indesiderati o inattesi che hanno una probabilità significativa di compromettere le operazioni aziendali e minacciare la sicurezza delle informazioni *(ISO 27000:2018, 3.31)*
Valore di tolleranza al rischio (o rischio tollerato)	Parametro utilizzato per misurare l'accettabilità di un rischio. I rischi con un livello di rischio attuale superiore a questo parametro devono considerarsi al di fuori della tolleranza dell'organizzazione al rischio

Valore di elevata tolleranza al rischio	Parametro utilizzato per misurare l'accettabilità di un rischio. I rischi con un livello di rischio attuale superiore a questo parametro devono considerarsi *significativamente* al di fuori della tolleranza dell'organizzazione al rischio
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni *(Information Security Management System) (ISO 27000:2018, 3.33)*
Monitoraggio	Determinazione dello stato di un sistema, processo o attività *(ISO 27000:2018, 3.46)*
Approccio semi-quantitativo	Metodologia che utilizza valutazioni qualitative come input e produce output numerici attraverso calcoli matematici, mantenendo la comprensibilità delle valutazioni soggettive.
Calibrazione empirica	Processo di aggiustamento dei parametri metodologici basato su dati reali dell'organizzazione, confrontando previsioni del modello con eventi effettivamente verificatisi.
Fattore di correzione	Moltiplicatore numerico che adatta il calcolo di base per riflettere caratteristiche specifiche (criticità asset, efficacia controlli). Valore iniziale basato su benchmark, soggetto a calibrazione empirica.

6. Metodologia di Misurazione

6.1. Formula di calcolo del livello di rischio

Livello di Rischio = Verosimiglianza × Impatto × Fattore Asset × Fattore Controlli

Dove:

- Verosimiglianza: Scala 1-5 secondo valutazione qualitativa
- Impatto: Scala 1-5 secondo valutazione qualitativa
- Fattore Asset: 0.8 (standard), 1.0 (importanti), 1.2 (critici)
- Fattore Controlli: 1.0 (inadeguati), 0.8 (base), 0.6 (avanzati)

Soglie di tolleranza

- Asset standard/importanti: Soglia = 6, Elevata = 12
- Asset critici: Soglia = 4, Elevata = 8

Nota metodologica: I parametri numerici sono calibrati sull'esperienza operativa e soggetti a validazione empirica continua.

Nota pratica: Per facilitare i calcoli, è disponibile un foglio Excel preconfigurato (118.MO.SEC.15C) che applica automaticamente la formula e verifica la coerenza dei parametri inseriti.

7. Scopo e campo di applicazione

7.1. Scopo

La presente procedura definisce la metodologia per l'esecuzione sistematica della valutazione e gestione dei rischi relativi alla sicurezza delle informazioni (Information Security Risk Assessment e Risk Management), in conformità ai requisiti degli standard ISO/IEC 27001:2022 e ISO/IEC 27005:2022.

La procedura ha l'obiettivo di:

- Standardizzare il processo di identificazione, analisi e valutazione dei rischi per la sicurezza delle informazioni
- Definire criteri uniformi per il trattamento e monitoraggio dei rischi
- Garantire decisioni informate e documentate sulla gestione del rischio
- Assicurare la conformità ai requisiti normativi del settore

7.2. Campo di applicazione:

La procedura si applica a:

- Tutti i sistemi informativi sanitari e amministrativi
- I processi di trattamento dei dati sanitari e personali
- Le infrastrutture IT che supportano l'erogazione dell'assistenza sanitaria
- I dispositivi medici connessi e sistemi IoMT (Internet of Medical Things)
- I processi di gestione documentale e comunicazione
- Le attività di outsourcing che coinvolgono dati personali e sanitari
- I sistemi di telemedicina e teleconsulto

Sono esclusi dal campo di applicazione i rischi puramente economici o operativi che non impattano su riservatezza, integrità o disponibilità delle informazioni.

7.3. Documenti di supporto:

- 118.PR.SEC.15A - Registro Information Risk Assessment
- 118.PR.SEC.15B - Piano di trattamento del rischio

7.4. Frequenza di applicazione

La procedura viene applicata:

- Sistematicamente per tutti i nuovi sistemi e processi
- Periodicamente secondo il calendario definito al § 8.2
- Straordinariamente in caso di incidenti o cambiamenti significativi

8. Processo

8.1. Approccio metodologico

L'attività di valutazione dei rischi relativi alla sicurezza delle informazioni (Information Security Risk Assessment, par. 6.1.2 dello standard ISO/IEC 27001:2022) è articolata in tre fasi sequenziali:

- Identificazione del rischio
- Analisi del rischio
- Ponderazione del rischio

Le fasi sopra descritte sono precedute dalla comprensione del contesto e dell'ambito in cui si valuta il rischio, e sono seguite dal trattamento del rischio (par. 6.1.3 dello standard ISO/IEC 27001:2022).

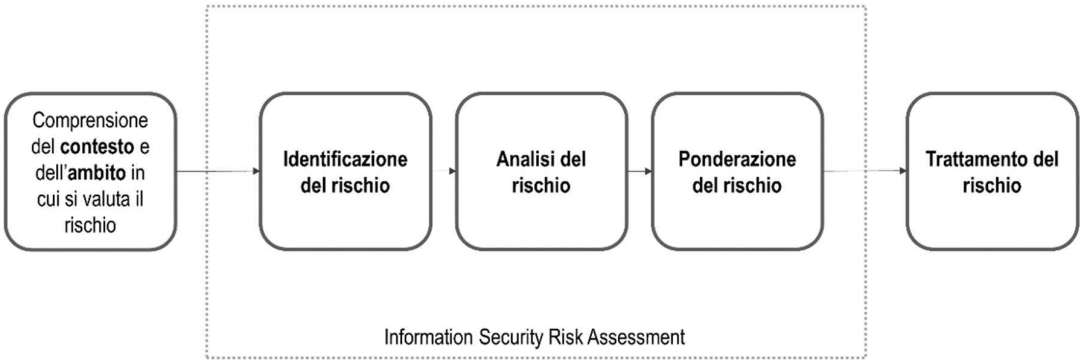

Figura 1 - Le fasi dell'Information Security Risk Assessment

8.1.1. Descrizione delle fasi

- **Comprensione del contesto**: Definizione dell'ambito di applicazione, identificazione degli asset e del contesto organizzativo e normativo.
- **Identificazione del rischio**: Individuazione sistematica dei rischi per la sicurezza delle informazioni mediante analisi di minacce, vulnerabilità e asset esposti.
- **Analisi del rischio**: Quantificazione del livello di rischio attraverso la valutazione di verosimiglianza e impatto, considerando i controlli esistenti.
- **Ponderazione del rischio**: Confronto del livello di rischio calcolato con le soglie di tolleranza per determinare la necessità di trattamento.
- **Trattamento del rischio**: Selezione e implementazione delle azioni necessarie per modificare il livello di rischio secondo le opzioni disponibili.

8.1.2. Approccio metodologico ibrido

L'organizzazione utilizza un approccio metodologico ibrido che combina:

- Identificazione basata su eventi: Scenari specifici (es. "attacco ransomware") per facilitare la comprensione operativa

- Valutazione ponderata per asset: Calcolo che considera criticità degli asset coinvolti
- Metodo qualitativo parametrizzato: Scale standardizzate con fattori numerici per confrontabilità

Questa combinazione è intenzionale e garantisce le proprietà richieste dagli standard ISO/IEC 27005:2022 (par. 6.5):

- Coerenza: Applicazione uniforme dei criteri
- Confrontabilità: Possibilità di confrontare risultati nel tempo
- Validità: Corrispondenza tra valutazione e realtà operativa
- Tracciabilità: Documentazione completa del processo decisionale

8.1.3.Affrontare le perplessità comuni

"Non abbiamo tempo per altra burocrazia"

Per questo il processo è progettato per:

- Formalizzare valutazioni che vengono effettuate mentalmente
- Fornire strumenti per comunicare meglio preoccupazioni alla Direzione
- Evitare di "reinventare la ruota" ogni volta che c'è un problema

Il tempo investito inizialmente si recupera evitando emergenze e giustificando più facilmente le risorse necessarie.

"I rischi veri non stanno in una tabella Excel"

Vero. La tabella è solo uno strumento per:

- Non dimenticarci dei rischi meno visibili ma potenzialmente gravi
- Avere un linguaggio comune tra tecnici, clinici e amministrativi
- Dimostrare che stiamo gestendo i rischi con metodo, non a sensazione

L'esperienza resta fondamentale - la procedura la struttura, non la sostituisce.

"Tanto poi nell'emergenza si fa quello che serve"

Assolutamente. Per questo esiste il fast-track. Ma proprio perché nell'emergenza si improvvisa, è cruciale:

- Ridurre le situazioni che diventano emergenze
- Avere piani pronti per gli scenari più probabili
- Documentare dopo cosa ha funzionato per la prossima volta

8.2. Frequenza delle attività di gestione dei rischi

Secondo lo standard ISO/IEC 27001:2022, par. 8.2, l'organizzazione deve effettuare le valutazioni del rischio a intervalli pianificati o quando sono proposti o si verificano cambiamenti significativi.

L'organizzazione adotta un **sistema temporale coordinato** che distingue chiaramente tra rivalutazioni complete dei rischi, implementazione delle azioni di trattamento e monitoraggio dell'avanzamento. Questa differenziazione evita sovrapposizioni operative e garantisce efficacia gestionale senza appesantire eccessivamente i processi.

Rivalutazioni complete dei rischi

Il CISO, in coordinamento con il **Security Forum** (organismo collegiale di governance della sicurezza composto dalla leadership aziendale)(§ 10.3.1), pianifica le rivalutazioni complete secondo le frequenze differenziate per tipologia di sistema. Queste rivalutazioni comportano la ripetizione dell'intero ciclo di identificazione, analisi e ponderazione per verificare l'evoluzione del profilo di rischio.

Tipologia Sistema	Frequenza	Durata Processo	Responsabilità
Sistemi informativi sanitari critici	Trimestrale	15 giorni lavorativi	CISO + Responsabili del rischio
Altri sistemi informativi	Semestrale	10 giorni lavorativi	CISO + Responsabili del rischio
Sistemi amministrativi	Annuale	5 giorni lavorativi	Responsabili del rischio

Implementazione delle azioni di trattamento

Le timeline di implementazione sono calibrate sulla criticità dell'evento e sulla tipologia di asset coinvolto, bilanciando urgenza operativa con fattibilità implementativa. Eventi che coinvolgono asset critici ricevono priorità temporale per proteggere sistemi vita-dipendenti.

Classificazione Evento	Timeline implementazione	Milestone Controllo
ROSSO + Asset Critici	30 giorni	Settimanale
ROSSO + Asset Standard/Importanti	60 giorni	Bisettimanale
AMBRA + Asset Critici	60 giorni	Mensile
AMBRA + Asset Standard/Importanti	30 giorni	Settimanale

Monitoraggio dell'avanzamento

Durante il periodo di implementazione, il responsabile del rischio verifica l'avanzamento secondo le frequenze definite nella tabella precedente. Post-implementazione, viene condotta validazione empirica dell'efficacia dei controlli nell'arco di 60-90 giorni, seguita da controllo trimestrale per il mantenimento dell'efficacia nel tempo.

Coordinamento delle attività: Il CISO supporta la dirigenza aziendale nella pianificazione integrata delle rivalutazioni periodiche con i cicli di implementazione e monitoraggio, prevedendo buffer temporali per evitare sovraccarichi operativi dei responsabili del rischio e garantire qualità delle valutazioni.

Valutazioni straordinarie vengono attivate immediatamente per:

- Cambiamenti significativi all'architettura documentale del sistema di gestione o al suo contesto
- Eventi critici per la sicurezza delle informazioni
- Incidenti che coinvolgono sistemi operativi di emergenza e dati sanitari
- Richieste specifiche della Direzione per valutazioni urgenti

Il CISO supporta la dirigenza nella valutazione della necessità e dell'ambito delle valutazioni straordinarie, coordina i responsabili del rischio competenti e definisce tempistiche accelerate quando necessario per la sicurezza dei pazienti trasportati/assistiti.

8.2.1.Collegamento con Incident Response

La gestione dei rischi è strettamente integrata con il processo di incident response definito nella procedura **118.PR.SEC.16 - Gestione degli Incidenti di Sicurezza**.

Trigger automatici da Incident a Risk Reassessment

Un incidente di sicurezza attiva automaticamente la rivalutazione del rischio quando:

- **Severità Alta/Critica** secondo classificazione incident response
- **Nuovo vettore di attacco** non precedentemente identificato
- **Controllo bypassato** che era considerato efficace
- **Impatto superiore** a quello stimato per eventi simili

Flusso di integrazione

1. **Durante l'incidente**: Il team di incident response notifica immediatamente il Responsabile del Rischio dell'area coinvolta
2. **Post-incident (entro 7 giorni)**: Analisi congiunta delle lesson learned per identificare:
    a. Nuovi eventi di rischio emersi
    b. Inefficacia di controlli esistenti
    c. Necessità di rivalutazione immediata
3. **Entro 30 giorni**: Aggiornamento formale del Risk Assessment con:
    a. Nuovo calcolo basato su dati reali dell'incidente
    b. Revisione efficacia controlli
    c. Piano di trattamento aggiornato

Ruoli durante gestione simultanea

Quando un incidente è in corso mentre si gestisce il rischio correlato:

- **Incident Commander** (da proc. 118.PR.SEC.16): Gestione operativa immediata
- **Responsabile del Rischio**: Supporto decisionale su impatti e priorità
- **CISO**: Coordinamento tra risposta tattica e revisione strategica del rischio

8.2.2.Risk Communication come Elemento Trasversale

Come evidenziato nel modello YARD (Yet Another Risk Depiction), la comunicazione del rischio rappresenta un processo che attraversa tutte le fasi del sistema di gestione. La sua efficacia determina il successo dell'intero sistema.

Principi della Risk Communication

La comunicazione del rischio deve assolvere due funzioni primarie:

1. Disseminazione delle regole organizzative e del modello operativo ERMS
2. Distribuzione tempestiva dei risultati di monitoraggio e valutazione

Strutturazione dei Flussi Informativi

Il processo richiede particolare attenzione all'efficacia della comunicazione degli obiettivi di business e dell'appetito al rischio dalla fase di Risk Context alle fasi operative successive. Questo include:

- **Flusso strategico**: Dal Risk Context verso Risk Identification, veicolando obiettivi e priorità
- **Flusso operativo**: Dal Risk Monitoring verso Risk Reporting, trasferendo evidenze e metriche
- **Flusso decisionale**: Dal Risk Reporting verso Risk Context, alimentando il ciclo successivo

Adeguamento al Contesto Sanitario

Nel contesto dell'emergenza sanitaria, la comunicazione deve considerare:

- L'operatività H24 che richiede canali sempre attivi
- La criticità temporale che impone messaggi sintetici e azionabili
- La diversità dei destinatari che necessita di linguaggi differenziati

8.3. Comprensione del contesto e dell'ambito

L'organizzazione definisce il contesto in cui opera identificando i processi critici, i servizi erogati e le condizioni che possono generare eventi di rischio per la sicurezza delle informazioni.

L'analisi del contesto esterno considera il panorama delle minacce specifiche del settore sanitario, i requisiti normativi applicabili (GDPR, normative clinico/sanitarie, NIS 2, etc.) e i fattori che possono influenzare la sicurezza delle informazioni. Particolare attenzione è rivolta all'evoluzione delle minacce cyber contro il settore sanitario e alle vulnerabilità emergenti nei dispositivi medici connessi.

Il contesto interno include l'identificazione dei processi assistenziali e amministrativi che trattano informazioni sensibili, la mappatura dei flussi informativi critici e la valutazione della cultura della sicurezza organizzativa. Vengono inoltre considerate le competenze disponibili, le risorse dedicate alla sicurezza e le caratteristiche specifiche dell'ambiente sanitario (operatività 24/7, criticità temporale degli interventi).

8.3.1.Ambito di applicazione

La valutazione considera tutti i processi che, se compromessi, potrebbero generare eventi di rischio per la sicurezza delle informazioni sanitarie, inclusi i sistemi operativi di emergenza, i processi di gestione documentale, le comunicazioni con l'esterno e le attività di outsourcing che coinvolgono dati sanitari.

8.4. Identificazione del rischio

L'identificazione del rischio è il processo sistematico di individuazione e descrizione degli eventi che potrebbero comprometterne la riservatezza, integrità o disponibilità delle informazioni sanitarie e personali. L'organizzazione adotta un approccio basato sugli eventi (ISO/IEC 27005:2022, par. 7.2.1, lett. a) che considera scenari di rischio realistici e rilevanti per il contesto sanitario.

Chiarimento metodologico

L'approccio è definito "basato su eventi" per la fase di identificazione (cosa può accadere) e utilizza "ponderazione per asset" nella fase di calcolo (quanto è critico). Questa combinazione ottimizza l'equilibrio tra comprensibilità operativa e rigore quantitativo.

Per ciascun evento identificato vengono analizzati **gli asset coinvolti, il panorama delle minacce, le vulnerabilità presenti e i controlli di sicurezza implementati**. Questo approccio consente una comprensione più intuitiva dei rischi e facilita il coinvolgimento del personale operativo (medici, infermieri, autisti-soccorritori, tecnico e amministrativo nella valutazione.

8.4.1. Tipologie di eventi considerati:

Gli eventi sono classificati in base alla loro natura e alle modalità di manifestazione. Vengono considerati eventi derivanti da attacchi informatici (ransomware, phishing, accessi non autorizzati), errori umani (configurazioni errate, perdita di dispositivi, invio di dati a destinatari sbagliati), guasti tecnici (interruzioni di sistema, corruzione dati, malfunzionamenti hardware) e cause esterne (disastri naturali, interruzioni di servizi esterni, problemi di connettività).

8.4.2. Criteri di inclusione ed esclusione:

Sono inclusi tutti gli eventi che possono compromettere la sicurezza delle informazioni sanitarie, incluse le violazioni normative quando comportano esposizione di dati sanitari o interruzione dei servizi clinici. Esempi tipici includono: attacchi ransomware che bloccano sistemi sanitari, perdita di dispositivi contenenti dati pazienti trasportati/assistiti, accessi non autorizzati a schede di soccorso, interruzioni di connettività durante attività di telemedicina.

Sono esclusi gli eventi che impattano esclusivamente gli aspetti economici o operativi senza compromettere riservatezza, integrità o disponibilità delle informazioni.

8.4.3. Gestione delle correlazioni:

Particolare attenzione è posta agli eventi che possono generare effetti a cascata su più sistemi o processi. Quando un singolo evento può impattare diversi asset o servizi, vengono considerati tutti i possibili scenari di propagazione e le relative conseguenze sull'erogazione dell'assistenza sanitaria.

8.4.4. Controlli di sicurezza esistenti:

Per ciascun evento identificato vengono inventariati i controlli di sicurezza che possono influenzarne la probabilità di accadimento o l'impatto. I controlli vengono classificati in:

- **Controlli preventivi**: impediscono il verificarsi dell'evento riducendone la probabilità
- **Controlli detective**: rilevano tempestivamente il verificarsi dell'evento riducendo il tempo di risposta
- **Controlli correttivi**: mitigano le conseguenze dell'evento riducendone l'impatto effettivo

Vengono considerati esclusivamente i controlli che hanno un effetto rilevante sulla gestione del rischio, escludendo quelli con impatto trascurabile sulla probabilità o sulle conseguenze dell'evento.

Nota per l'implementazione: Superare la "sindrome del foglio bianco"

Identificare i rischi può sembrare inizialmente overwhelming - "da dove comincio?". La risposta è: dalle preoccupazioni che già avete. Quel sistema che vi fa dormire male la notte, quella procedura che sapete essere fragile, quell'incidente che "prima o poi succederà" - sono tutti ottimi punti di partenza.

Non cercate la perfezione nella prima iterazione. È meglio identificare 10 rischi reali che cercarne 100 teorici. Il processo è iterativo: partite da quello che conoscete, poi affinerete.

8.5. Analisi del rischio

L'analisi del rischio è la fase della valutazione finalizzata a determinare il livello di rischio associato a ciascun evento identificato. Secondo lo standard ISO/IEC 27000:2018, il livello di rischio è espresso come combinazione della verosimiglianza di accadimento dell'evento e dell'impatto delle sue conseguenze.

La valutazione deve garantire proprietà di completezza, coerenza, ripetibilità e comparabilità. Una stima è completa quando considera tutti i fattori rilevanti (natura dell'evento, vulnerabilità sfruttabili, controlli esistenti, valore degli asset coinvolti); è coerente quando variazioni dei fattori producono variazioni proporzionali del risultato; è ripetibile quando conduce agli stessi risultati in condizioni invariate; è comparabile quando consente di misurare l'evoluzione del rischio nel tempo.

8.5.1.Metodologia adottata:

L'organizzazione utilizza un metodo semi-quantitativo che combina: - Valutazione qualitativa degli input (verosimiglianza e impatto tramite scale descrittive) - Calcolo quantitativo dell'output (applicazione di formula matematica ai valori qualitativi) Questo approccio ibrido mantiene la comprensibilità delle valutazioni qualitative mentre fornisce risultati numerici comparabili per le decisioni di prioritizzazione.

8.5.2.Valutazione della verosimiglianza

La verosimiglianza rappresenta la probabilità che l'evento si verifichi in un determinato periodo di tempo, considerando le caratteristiche del contesto sanitario e i controlli preventivi e detective esistenti.

Livello	Valore	Descrizione	Indicatori
Molto improbabile	**1**	Eventi eccezionali, mai verificatisi in contesti simili	Controlli robusti, vulnerabilità difficilmente sfruttabili
Improbabile	**2**	Eventi rari ma possibili in circostanze particolari	Controlli adeguati, alcune vulnerabilità note
Probabile	**3**	Eventi verificatisi in organizzazioni simili	Controlli parziali, vulnerabilità sfruttabili
Verosimile	**4**	Eventi frequenti nel settore sanitario	Controlli inadeguati, vulnerabilità note e diffuse
Molto verosimile	**5**	Eventi sistematici e ricorrenti	Controlli assenti, vulnerabilità facilmente sfruttabili

8.5.3.Valutazione dell'impatto

L'impatto misura la gravità delle conseguenze derivanti dal verificarsi dell'evento, considerando gli effetti su assistenza clinica, conformità normativa, reputazione e aspetti economici.

Livello	Valore	Impatto Clinico	Impatto Normativo	Impatto reputazionale

Molto basso	**1**	Nessun impatto su assistenza	Violazioni amministrative minori	Impatto locale limitato
Basso	**2**	Ritardi non critici	Sanzioni amministrative	Attenzione stampa locale
Medio	**3**	Attivazione procedure manuali	Procedimenti di compliance	Interesse stampa regionale
Alto	**4**	Rischio clinico, trasferimenti pazienti	Procedimenti penali	Attenzione stampa nazionale
Catastrofico	**5**	Pericolo per sicurezza pazienti	Sanzioni penali severe	Danno reputazionale critico

8.5.4.Fattori di correzione

Classificazione degli asset coinvolti:

Il calcolo del rischio viene modulato in base alla criticità degli asset coinvolti nell'evento:

- **Asset critici** (sistemi operativi di emergenza core): fattore moltiplicativo 1.2
- **Asset importanti** (sistemi di supporto clinico): fattore moltiplicativo 1.0
- **Asset standard** (sistemi amministrativi): fattore moltiplicativo 0.8

Efficacia dei controlli esistenti:

L'efficacia complessiva dei controlli (preventivi, detective, correttivi) riduce il livello di rischio:

Efficacia dei controlli (fattori iniziali soggetti a calibrazione empirica):

- **Controlli avanzati**: fattore riduttivo 0.6
  - [Basato su: implementazione completa + testing regolare + monitoraggio + incident response verificata]
- **Controlli base**: fattore riduttivo 0.8
  - [Basato su: implementazione completa + testing occasionale]
- **Controlli inadeguati**: nessuna riduzione (1.0)
  - [Controlli assenti, non funzionanti o non testati]

Nota metodologica: Questi fattori rappresentano stime iniziali derivate da benchmark di settore. Saranno calibrati empiricamente attraverso analisi retrospettiva degli incidenti verificatisi [timeline: prima revisione dopo 12 mesi di applicazione].

Processo di calibrazione: Confronto tra efficacia stimata e incidenti reali per determinare fattori ottimali specifici per l'organizzazione.

8.5.5.Formula di calcolo

Il livello di rischio viene determinato attraverso una metodologia quantitativa che combina la valutazione qualitativa della verosimiglianza e dell'impatto con fattori di correzione specifici per il contesto sanitario. La formula adottata garantisce proporzionalità dei risultati e facilità di applicazione operativa.

Formula di calcolo: Livello di Rischio = Verosimiglianza × Impatto × Fattore Asset × Fattore Controlli

Rationale metodologico della formula moltiplicativa:

La scelta moltiplicativa (anziché additiva) riflette l'interazione non-lineare tra i fattori:

- Se la verosimiglianza è zero, il rischio è zero indipendentemente dall'impatto
- Se i controlli sono perfetti (fattore 0), il rischio si annulla
- L'effetto combinato di più fattori negativi amplifica esponenzialmente il rischio

Questa formulazione è coerente con modelli consolidati di risk assessment (es. NIST SP 800-30) e sarà validata empiricamente attraverso confronto con eventi storici [§9.2- Processo di revisione].

Limitazioni riconosciute: La formula assume indipendenza tra fattori e linearità nelle scale qualitative. Questi presupposti saranno rivisti annualmente sulla base dell'esperienza operativa.

Questa metodologia moltiplicativa riflette l'interazione effettiva tra i fattori di rischio, dove l'assenza di uno qualsiasi degli elementi (ad esempio, controlli molto efficaci) può ridurre significativamente il rischio complessivo, mentre la combinazione di fattori negativi amplifica esponenzialmente la criticità.

Gestione dell'incertezza nelle valutazioni:

Riconoscendo l'incertezza intrinseca nelle valutazioni qualitative:

1. Range di confidenza: Ogni punteggio può variare di ±0.5 punti
   Esempio: Verosimiglianza 3 = effettivamente 2.5-3.5
2. Soglie con margine di sicurezza:
   - Eventi a ±1 punto dalle soglie richiedono doppia valutazione
   - In caso di dubbio, adottare approccio prudenziale (classificazione superiore)
3. Indicatori di incertezza:
   - Documentare nel registro il livello di confidenza (Alta/Media/Bassa)
   - Prioritizzare per rivalutazione eventi con confidenza Bassa
   - Richiedere evidenze aggiuntive per eventi ad alto impatto/bassa confidenza
4. Validazione incrociata:
   - Eventi ROSSO: validazione obbligatoria da secondo valutatore
   - Eventi AMBRA su asset critici: consultazione Security Forum

Range e soglie di tolleranza

Il calcolo produce valori compresi tra 0.48 (rischio minimo) e 30 (rischio massimo). Le soglie di tolleranza sono calibrate attraverso analisi empirica basata su dati storici dell'organizzazione e benchmark di settore per garantire allineamento con la percezione qualitativa del rischio.

Tipologia asset	Soglia di tolleranza	Soglia elevata	Rationale
Asset Critici	4	8	Protezione massima sistemi vita-dipendenti
Asset Importanti	6	12	Bilanciamento sicurezza-operatività
Asset Standard	6	12	Tolleranza standard per sistemi non critici

Esempi di calcolo rappresentativi

Scenario A - Ransomware su sistema di dispatch emergenze:

- Verosimiglianza: 4 (eventi frequenti nel settore sanitario)
- Impatto: 5 (blocco totale delle chiamate di emergenza - pericolo vita)
- Asset Critico: fattore 1.2 (sistema dispatch 118)
- Controlli Base: fattore 0.8
- **Calcolo: 4 × 5 × 1.2 × 0.8 = 19.2 → ROSSO**

Scenario B - Perdita dispositivo mobile equipaggio ambulanza:

- Verosimiglianza: 3 (eventi possibili durante servizio H24)
- Impatto: 2 (ritardi comunicazioni, procedure manuali disponibili)
- Asset Standard: fattore 0.8 (dispositivo comunicazione)
- Controlli Avanzati: fattore 0.6 (crittografia, remote wipe)
- **Calcolo: 3 × 2 × 0.8 × 0.6 = 2.88 → VERDE**

Scenario C - Interruzione connettività durante trasporto critico:

- Verosimiglianza: 3 (eventi verificatisi in organizzazioni simili)
- Impatto: 4 (perdita comunicazione ospedale-ambulanza, rischio clinico)
- Asset Critico: fattore 1.2 (sistema comunicazione emergenza)
- Controlli Base: fattore 0.8 (backup radio analogico)
- **Calcolo: 3 × 4 × 1.2 × 0.8 = 9.6 → ROSSO**

Nota pratica: Per facilitare i calcoli, è disponibile un foglio Excel preconfigurato (118.MO.SEC.15C) che applica automaticamente la formula e verifica la coerenza dei parametri inseriti.

Validazione della proporzionalità

Gli esempi dimostrano come la formula produca risultati proporzionali alla percezione qualitativa del rischio: l'evento ransomware su sistema clinico critico ottiene punteggio significativamente superiore rispetto alla perdita di dispositivo amministrativo, riflettendo correttamente le diverse criticità per l'organizzazione sanitaria.

Revisione periodica dei parametri: I fattori di calcolo e le soglie vengono rivisti annualmente sulla base dell'esperienza operativa acquisita, dell'analisi degli eventi effettivamente verificatisi e del confronto con l'evoluzione delle best practice di settore, garantendo mantenimento dell'accuratezza predittiva nel tempo.

8.5.6. Quando effettuare l'analisi

L'analisi viene eseguita per ogni nuovo evento identificato, quando emergono nuove vulnerabilità o controlli, dopo l'implementazione di azioni di trattamento per verificarne l'efficacia, e quando audit o verifiche evidenziano dubbi sull'effettività dei controlli esistenti.

Perché numeri e formule in un mondo di emergenze?

Può sembrare strano applicare formule matematiche a situazioni complesse come le nostre. Il motivo è semplice: ci aiutano a confrontare mele con pere. Come decidiamo se è più urgente proteggere il sistema di dispatch o quello delle schede di soccorso? Come spieghiamo alla Direzione perché servono risorse per la cybersecurity invece che per un nuovo defibrillatore?

I numeri sono un linguaggio comune che ci permette di:

- Confrontare rischi diversi con criteri oggettivi
- Tracciare se stiamo migliorando o peggiorando nel tempo
- Giustificare investimenti con dati, non solo sensazioni

La formula può sembrare complessa, ma in pratica risponde a domande semplici: Quanto è probabile? Quanto sarebbe grave? Quanto sono critici i sistemi coinvolti? Quanto ci proteggono i controlli attuali?

8.6. Ponderazione del rischio

La ponderazione del rischio è il processo di comparazione dei livelli di rischio calcolati per ciascun evento con i parametri di tolleranza definiti dall'organizzazione. Questa fase determina quali eventi richiedano un trattamento prioritario e quali possano essere accettati nel loro stato attuale.

L'organizzazione utilizza due distinte soglie di tolleranza per fornire una classificazione più articolata della criticità degli eventi e orientare le decisioni di trattamento:

- Soglia di tolleranza: al di sopra di questo valore il rischio è considerato fuori tolleranza
- Soglia di elevata tolleranza: al di sopra di questo valore il rischio è considerato significativamente critico

8.6.1. Definizione delle soglie di tolleranza

Le soglie sono calibrate sulla base della formula di calcolo che produce valori compresi tra 0.48 e 30, differenziate per tipologia di asset coinvolti negli eventi:

Per eventi che coinvolgono asset standard e importanti:

- **Soglia di tolleranza: 6**
- **Soglia di elevata tolleranza: 12**

Per eventi che coinvolgono asset critici:

- **Soglia di tolleranza: 4**
- **Soglia di elevata tolleranza: 8**

Questa differenziazione riflette la maggiore sensibilità dell'organizzazione verso eventi che potrebbero compromettere sistemi operativi di emergenza critici e la sicurezza dei pazienti trasportati/assistiti.

Metodologia di definizione delle soglie:

Le soglie rappresentano valori iniziali derivati da:

1. Analisi del range teorico della formula (0.48-30)
2. Distribuzione target: 60% eventi in area verde, 30% ambra, 10% rosso
3. Benchmark indicativi del settore sanitario

Soglie iniziali (soggette a calibrazione empirica):

- Asset critici: Soglia 4, Elevata 8
- Asset standard/importanti: Soglia 6, Elevata 12

Processo di validazione:

- Monitoraggio per 6 mesi della distribuzione effettiva degli eventi
- Analisi di corrispondenza tra classificazione e percezione dei risk owner
- Aggiustamento soglie per mantenere distribuzione target
- Approvazione modifiche da parte del Security Forum

8.6.2. Classificazione della criticità

Sulla base del confronto con le soglie, gli eventi vengono classificati secondo il seguente schema:

Classificazione	Criterio	Implicazioni
VERDE	Livello ≤ soglia di tolleranza	Rischio accettabile, trattamento opzionale
AMBRA	Soglia di tolleranza < Livello ≤ soglia elevata	Rischio fuori tolleranza, valutazione trattamento
ROSSO	Livello > soglia di elevata tolleranza	Rischio critico, trattamento obbligatorio

8.6.3. Rappresentazione grafica e monitoraggio

I risultati della ponderazione vengono rappresentati attraverso una matrice di rischio che visualizza la distribuzione degli eventi per verosimiglianza e impatto, applicando i codici colore della classificazione. Questa rappresentazione facilita la comunicazione dei risultati alla Direzione e supporta le decisioni di allocazione delle risorse.

La matrice tiene conto dei fattori di correzione (tipologia asset e efficacia controlli) per fornire una visualizzazione accurata del posizionamento di ciascun evento rispetto alle soglie di tolleranza.

8.6.4. Criteri per la determinazione delle soglie

Le soglie di tolleranza sono state definite considerando l'analisi del rischio residuo accettabile per l'organizzazione sanitaria, i benchmark di settore per organizzazioni similari, i requisiti normativi specifici del settore sanitario e la capacità operativa di gestione contemporanea dei rischi.

Le soglie vengono riviste annualmente dal CISO in collaborazione con il Security Forum[1] per assicurare l'allineamento con l'evoluzione del contesto normativo, i cambiamenti nella tipologia di minacce, le variazioni nella capacità operativa dell'organizzazione e le lezioni apprese dall'analisi degli incidenti verificatisi.

8.6.5. Considerazioni specifiche per il settore sanitario

Nel contesto sanitario, la ponderazione tiene conto di fattori aggiuntivi quali la disponibilità 24/7 richiesta per i sistemi operativi di emergenza, l'integrità critica dei dati sanitari per la continuità terapeutica, la riservatezza rafforzata richiesta per i dati personali di categorie particolari e la necessità di mantenere la continuità operativa dei sistemi critici.

[1] organismo collegiale di governance descritto al § 10.3.1, composto dalla dirigenza aziendale con potere decisionale riservato ai dipendenti dell'Azienda

Eventi che potrebbero compromettere la sicurezza dei pazienti trasportati/assistiti o l'erogazione dell'assistenza sanitaria ricevono priorità elevata indipendentemente dal loro livello di rischio calcolato, richiedendo valutazioni specifiche che considerano l'impatto sulla qualità e sicurezza delle cure.

8.7. Trattamento del rischio

Al termine della valutazione dei rischi relativi alla sicurezza delle informazioni segue la fase di trattamento del rischio (ISO/IEC 27001:2022, par. 6.1.3). Il trattamento è il processo finalizzato a modificare il livello di rischio associato agli eventi identificati, attraverso l'implementazione di controlli aggiuntivi o il miglioramento di quelli esistenti.

Ciascun responsabile del[2] rischio deve decidere, per ogni evento, se sia necessario un trattamento oppure se il livello di rischio attuale possa essere accettato. La classificazione degli eventi per grado di criticità definita nella fase di ponderazione orienta questo processo decisionale fornendo criteri oggettivi e coerenti.

8.7.1. Criteri per le decisioni di trattamento

Le decisioni di trattamento seguono un approccio strutturato basato sulla classificazione della criticità:

- Eventi VERDE (rischio accettabile): Il rischio è generalmente accettato senza ulteriori interventi, salvo valutazioni specifiche del responsabile del rischio che potrebbero richiedere comunque un trattamento per motivi strategici o di precauzione.
- Eventi AMBRA (rischio fuori tolleranza): Il responsabile del rischio valuta discrezionalmente se accettare il rischio o implementare azioni di trattamento, considerando fattori quali disponibilità di risorse, priorità organizzative e rapporto costo-beneficio degli interventi.
- Eventi ROSSO (rischio critico): Il trattamento è fortemente raccomandato. L'eventuale accettazione del rischio richiede una valutazione approfondita e l'approvazione formale di un livello gerarchico superiore, con documentazione delle motivazioni e delle misure compensative adottate.

8.7.2. Opzioni di trattamento disponibili

Per ciascun evento identificato, il responsabile del rischio può scegliere tra diverse opzioni di trattamento:

- **Modificazione del rischio**: L'opzione più comune consiste nell'implementare controlli aggiuntivi o nel migliorare quelli esistenti per ridurre la verosimiglianza dell'evento o limitarne l'impatto. Nel contesto sanitario, questo include tipicamente il rafforzamento dei sistemi di backup, l'implementazione di controlli di accesso più stringenti, la formazione del personale e il miglioramento delle procedure di incident response.

[2] Nota operativa: Per "Responsabile del Rischio" si intende la persona specificatamente assegnata alla gestione dell'evento di rischio in questione, come documentato nel Registro Information Risk Assessment.

- **Eliminazione del rischio**: Consiste nella cessazione dell'attività che genera l'evento o nella sostituzione radicale della tecnologia o del processo coinvolto. Questa opzione è applicabile quando il rischio è inaccettabile e non può essere mitigato efficacemente attraverso altri controlli.
- **Condivisione del rischio**: Il rischio viene trasferito parzialmente a terzi attraverso l'outsourcing di attività specifiche a fornitori specializzati, la stipula di polizze assicurative (cyber liability, responsabilità civile) o accordi contrattuali che redistribuiscono responsabilità e rischi.
- **Accettazione del rischio**: L'organizzazione decide consapevolmente di mantenere il rischio nel suo stato attuale. Questa scelta è appropriata quando il costo del trattamento supera il beneficio atteso, quando il rischio è già nei parametri di tolleranza, o quando non esistono soluzioni tecnicamente fattibili.

8.7.3. Definizione delle priorità di trattamento

Gli eventi vengono trattati secondo un ordine di priorità che considera primariamente il grado di criticità, poi la tipologia di asset coinvolti e infine l'impatto operativo. Per garantire adeguata protezione in contesti sanitari critici, l'organizzazione prevede un **canale fast-track** per eventi che possono compromettere immediatamente la sicurezza dei pazienti.

Classificazione delle priorità di trattamento

Priorità CRITICA - Fast-Track Emergenze Sanitarie: Eventi che comportano rischio immediato per la vita dei pazienti o compromissione di sistemi vita-dipendenti attivano automaticamente il protocollo di emergenza con implementazione immediata (entro 24-72 ore) e coinvolgimento diretto della Direzione Sanitaria.

Criteri di attivazione fast-track:

- Compromissione sistemi di centrale operativa
- Indisponibilità di dispositivi medici critici per la sicurezza dei pazienti trasportati/assistiti
- Perdita integrità dati clinici durante procedure diagnostico-terapeutiche
- Eventi che impediscono l'accesso ai sistemi di emergenza sanitaria

Priorità	Tipologia Eventi	Timeline	Governance
CRITICA	Emergenze sanitarie vita-dipendenti	24-72 ore	Direzione Sanitaria + CTO + CISO
MASSIMA	ROSSO + Asset Critici	30 giorni	Direzione + CTO + Responsabile del Rischio (supporto metodologico CISO)
ELEVATA	ROSSO + Asset Standard/Importanti + AMBRA + Asset Critici	60 giorni	Security Forum + Responsabile del Rischio (coordinamento metodologico CISO)
STANDARD	AMBRA + Asset Standard/Importanti	90 giorni	Responsabile del Rischio

Processo fast-track

L'attivazione del fast-track comporta sospensione temporanea delle procedure standard di approvazione per consentire implementazione immediata di misure di contenimento. Il CTO e il Direttore Generale con il supporto del CISO, identificano soluzioni temporanee implementabili nell'immediato, seguito da pianificazione della soluzione definitiva entro le tempistiche standard.

Esempi di attivazione fast-track:

- Ransomware che blocca sistema dispatch durante emergenza di massa
- Compromissione sistema localizzazione ambulanze durante codice rosso
- Perdita comunicazione con centrale operativa durante trasporto critico
- Corruzione dati missioni che impedisce coordinamento soccorsi

La documentazione del fast-track viene completata a posteriori mantenendo tracciabilità delle decisioni assunte in emergenza e validazione della conformità metodologica una volta risolto l'evento critico.

Coordinamento con altre procedure: Il fast-track si integra con i protocolli di emergenza sanitaria esistenti e le procedure di incident response, garantendo coerenza operativa tra sicurezza informatica e sicurezza clinica senza duplicazioni procedurali.

Esperienza sul campo: Il caso del "rischio accettato che non doveva esserlo"

In un'organizzazione di emergenza sanitaria simile alla nostra, un rischio di "perdita connettività sistema localizzazione ambulanze" era stato classificato VERDE e accettato. Sembrava ragionevole: sistema di supporto non critico, procedure radio di backup disponibili.

Poi è successo davvero, durante un'emergenza di massa di domenica sera, con personale ridotto in centrale operativa. Le procedure radio c'erano, ma la localizzazione manuale delle ambulanze sparse sul territorio ha causato ritardi significativi. Il risultato: 45 minuti per coordinare i soccorsi, difficoltà nell'invio dell'ambulanza più vicina, stress operativo per gli equipaggi.

Lezione appresa: Anche i rischi "accettabili" vanno rivalutati pensando al worst-case scenario e alle condizioni operative reali. Ora quel rischio è AMBRA con piano di formazione periodica sulle procedure di emergenza e test mensili di coordinamento senza sistema GPS.

8.7.4.Processo di selezione e implementazione

Per ciascun evento che richiede trattamento, il responsabile del rischio valuta le opzioni disponibili considerando fattibilità tecnica ed economica, tempi di implementazione, risorse necessarie ed efficacia attesa. La selezione tiene conto di vincoli organizzativi, disponibilità di competenze interne, priorità strategiche e conformità alle politiche aziendali.

L'implementazione delle azioni di trattamento viene documentata in un piano specifico che definisce responsabilità, tempistiche, risorse assegnate e criteri di verifica dell'efficacia. Il piano viene sottoposto ad approvazione formale e monitorato periodicamente per assicurare il rispetto delle scadenze e il raggiungimento degli obiettivi prefissati.

8.7.5.Calcolo del rischio residuo

Per ogni azione di trattamento implementata, viene calcolato il rischio residuo atteso utilizzando la stessa metodologia della valutazione iniziale, aggiornando i parametri di verosimiglianza, impatto e efficacia dei controlli. Il rischio residuo deve rientrare nei parametri di tolleranza definiti dall'organizzazione o essere formalmente accettato attraverso il processo di approvazione stabilito.

La valutazione del rischio residuo considera non solo l'efficacia teorica delle azioni implementate, ma anche eventuali nuove vulnerabilità o rischi introdotti dalle misure adottate, garantendo una visione completa dell'impatto complessivo sullo scenario di rischio.

Nota metodologica - Validazione empirica dei controlli:

L'aggiornamento del "Fattore Controlli" nel calcolo del rischio residuo deve basarsi sull'efficacia effettivamente osservata dei controlli implementati, non su assunzioni teoriche. È necessario un periodo di osservazione operativa (minimo 30-60 giorni per controlli IT, 90 giorni per controlli organizzativi) durante il quale vengono raccolte evidenze concrete dell'efficacia attraverso:

- Test funzionali dei controlli implementati
- Monitoraggio degli indicatori di performance
- Analisi degli eventi intercettati/mitigati
- Feedback operativo del personale coinvolto

Solo dopo questa validazione empirica si procede al ricalcolo definitivo del rischio residuo, evitando sovrastime dell'efficacia basate su valutazioni puramente teoriche.

8.8. Implementazione e controllo del trattamento

8.8.1.Piano di trattamento del rischio

L'insieme delle decisioni di trattamento definite per ciascun evento confluisce nel Piano di Trattamento del Rischio (Risk Treatment Plan), documento che costituisce la pianificazione operativa delle azioni necessarie per modificare i livelli di rischio non accettabili.

Il piano organizza le azioni per evento di rischio, definendo per ciascuna intervento le informazioni identificative (titolo, descrizione e opzione di trattamento selezionata), la pianificazione operativa (tempistiche di attuazione, responsabili dell'implementazione e modalità di esecuzione) e la valutazione delle risorse (risorse umane, tecniche ed economiche necessarie, benefici attesi e stima del rischio residuo).

Contenuto delle azioni di trattamento:

Ogni azione specificata nel piano include una stima quantitativa del rischio residuo calcolata applicando la metodologia definita al §8.5.1, aggiornando i parametri di verosimiglianza e impatto sulla base dell'efficacia attesa dei controlli implementati. Vengono inoltre documentati eventuali nuovi rischi o vulnerabilità che l'azione potrebbe introdurre, garantendo una valutazione completa dell'impatto complessivo.

Il responsabile del rischio può formulare considerazioni aggiuntive circa la fattibilità tecnica, la coerenza con altre iniziative organizzative e l'allineamento con gli obiettivi strategici dell'organizzazione, fornendo un quadro completo per le decisioni di approvazione.

Processo di approvazione:

Il piano viene sottoposto ad approvazione strutturata che include la firma dei responsabili del rischio per ciascuna azione specifica, il parere di conformità metodologica del CISO sulla proposta aziendale per la coerenza complessiva dell'approccio e l'approvazione della Direzione per l'allocazione delle risorse necessarie all'implementazione.

L'approvazione è subordinata alla verifica di completezza (tutte gli eventi identificati hanno un'opzione di trattamento definita), coerenza (le azioni sono allineate con le politiche di sicurezza), fattibilità (le risorse richieste sono disponibili o allocabili) ed efficacia (il rischio residuo stimato è accettabile per l'organizzazione).

8.8.2.Confronto con controlli ISO 27001 Appendice A

In conformità al requisito del par. 6.1.3, lett. c dello standard ISO/IEC 27001:2022, l'organizzazione confronta sistematicamente le azioni definite nel piano di trattamento con i controlli di sicurezza per verificare che non siano stati omessi controlli necessari per un trattamento efficace degli eventi di rischio.

L'organizzazione adotta un **approccio integrato** che utilizza framework complementari per garantire copertura completa e allineamento alle specificità del contesto sanitario italiano. Questo approccio riflette la necessità di bilanciare conformità normativa, best practice internazionali e requisiti specifici del settore pubblico sanitario.

Framework di riferimento e prioritizzazione

Framework primario: ISO/IEC 27001:2022 Appendice A costituisce la base obbligatoria per il mantenimento della certificazione e la conformità internazionale.

Framework integrativi: UNI/PdR 174:2025, controlli ACN e NIST SP 800-53 forniscono completamento e specificità per il contesto italiano e sanitario.

Framework	Priorità	Applicazione	Rationale
ISO 27001 Appendice A	Obbligatoria	Tutti gli eventi	Conformità certificativa
UNI/PdR 174:2025	Raccomandata	Eventi cyber-critici	Armonizzazione ISO-NIST per contesto italiano
Controlli ACN	Obbligatoria	Eventi su infrastrutture critiche	Compliance normativa nazionale
NIST SP 800-53	Complementare	Eventi tecnici complessi	Approfondimento best practice

Metodologia di confronto integrato

Il processo prevede la mappatura strutturata di ciascuna azione pianificata sui controlli dei quattro framework di riferimento, seguendo questa sequenza metodologica:

1. Mappatura primaria su controlli ISO 27001 per conformità di base
2. Verifica compliance attraverso controlli ACN per requisiti normativi nazionali
3. Armonizzazione con UNI/PdR 174:2025 per integrazione ISO-NIST ottimizzata
4. Completamento tecnico mediante controlli NIST 800-53 per approfondimenti specialistici
5. Identificazione gap trasversali e valutazione impatto omissioni

Sequenza di verifica per evento: Per ogni evento di rischio, il responsabile verifica sistematicamente la copertura attraverso i framework secondo l'ordine di priorità, documentando corrispondenze, gap identificati e decisioni di applicabilità.

Criteri di applicabilità unificati

Un controllo di qualsiasi framework è considerato applicabile quando soddisfa tutti i seguenti criteri:

- È tecnicamente implementabile nell'ambiente organizzativo specifico
- Contribuisce direttamente al trattamento di almeno uno degli eventi identificati
- Può essere realizzato con le risorse disponibili o ragionevolmente allocabili
- È richiesto da normative specifiche o rappresenta best practice consolidate per il settore

Controlli già coperti da misure equivalenti o più rigorose, non proporzionati al livello di rischio dell'organizzazione, o relativi a tecnologie non presenti nell'ambiente operativo sono considerati non applicabili con documentazione delle motivazioni.

Gestione dei controlli identificati

Per controlli applicabili non coperti dalle azioni pianificate, il responsabile del rischio segue questo processo decisionale strutturato:

- **Controlli obbligatori (ISO 27001 + ACN)**: Inclusione automatica nel piano come nuove azioni o implementazione di controlli compensativi equivalenti con efficacia dimostrabile.
- **Controlli raccomandati (UNI/PdR 174:2025)**: Valutazione specifica se l'omissione comporta gap significativo nella protezione, con decisione motivata su implementazione, controlli alternativi o accettazione del gap residuo.
- **Controlli complementari (NIST 800-53**): Analisi costo-beneficio per determinare valore aggiunto rispetto ai controlli già implementati, con preferenza per soluzioni che migliorano significativamente la postura di sicurezza.
- **Gestione delle sovrapposizioni**: Quando lo stesso controllo è presente in più framework, viene applicato il livello più rigoroso tra quelli richiesti, evitando duplicazioni implementative ma garantendo il massimo standard di protezione.

Documentazione del confronto

La verifica viene documentata attraverso una matrice integrata multi-framework che include:

- **Mappatura controlli-azioni** con indicazione del framework di origine e livello di copertura
- **Analisi gap identificati** con valutazione dell'impatto specifico e priorità di risoluzione
- **Dichiarazione di applicabilità** consolidata che documenta lo stato di tutti i controlli con relative giustificazioni per framework
- **Piano di implementazione** per controlli aggiuntivi identificati come necessari

La documentazione costituisce evidenza per audit interni ed esterni della completezza dell'approccio e viene aggiornata ad ogni revisione del piano di trattamento per mantenere allineamento con l'evoluzione dei framework di riferimento e delle esigenze organizzative.

8.8.3.Monitoraggio dell'implementazione

Il responsabile del rischio monitora periodicamente l'avanzamento delle azioni di trattamento, verificando il rispetto delle tempistiche pianificate e la qualità dell'implementazione. La frequenza del monitoraggio è calibrata sulla criticità degli eventi: settimanale per eventi ROSSO, mensile per eventi AMBRA, trimestrale per eventi VERDE.

Indicatori di monitoraggio:

Il controllo si basa su indicatori quantitativi quali percentuale di completamento, rispetto delle milestone intermedie e consumo delle risorse rispetto al pianificato, integrati da valutazioni qualitative sull'efficacia delle misure implementate e sui risultati intermedi ottenuti.

Gestione delle deviazioni:

Quando l'implementazione non procede secondo i piani, il responsabile del rischio analizza le cause del ritardo, valuta l'impatto sulla gestione complessiva del rischio e determina azioni correttive che possono includere la modifica delle tempistiche, l'allocazione di risorse aggiuntive o la ridefinizione dell'approccio di implementazione.

La cessazione di un'azione può essere decisa quando emergono evidenze che l'intervento non produrrà l'effetto atteso sul livello di rischio o quando le risorse necessarie si rivelano significativamente superiori a quelle pianificate. In tali casi, il responsabile identifica azioni alternative per raggiungere l'obiettivo di trattamento.

Storia di successo: Dall'analisi del rischio al finanziamento

Il Risk Assessment aveva identificato come ROSSO il rischio 'ransomware su sistema dispatch 118'. Il report strutturato ha permesso di ottenere un finanziamento straordinario di 50.000€ per sistema di backup isolato air-gapped, formazione anti-phishing per tutto il personale operativo e segmentazione della rete. Risultato dopo 1 anno: 3 tentativi di attacco bloccati, zero downtime del dispatch, continuità operativa garantita durante 2 emergenze di massa.

8.8.4.Approvazione del rischio residuo

Al completamento di ciascuna azione di trattamento, il responsabile del rischio rivaluta il livello di rischio effettivo dell'evento applicando la metodologia definita, considerando l'efficacia reale dei controlli implementati e gli eventuali effetti collaterali emersi durante l'implementazione.

Calcolo del rischio residuo effettivo

Il rischio residuo viene ricalcolato aggiornando i parametri di verosimiglianza e impatto sulla base dell'esperienza operativa acquisita, verificando la corrispondenza tra i benefici stimati in fase di pianificazione e quelli effettivamente ottenuti. La valutazione considera non solo l'efficacia diretta dell'azione implementata, ma anche i suoi effetti sul contesto complessivo di sicurezza e le eventuali nuove vulnerabilità introdotte.

Validazione empirica dell'efficacia dei controlli

L'aggiornamento del "Fattore Controlli" nel calcolo del rischio residuo deve basarsi sull'**efficacia effettivamente osservata** dei controlli implementati attraverso un processo di validazione strutturato che garantisce oggettività e misurabilità dei risultati.

Timeline di validazione differenziate: La durata del periodo di osservazione è calibrata sulla natura del controllo e sulla complessità del contesto sanitario per garantire raccolta di evidenze significative.

Tipologia Controllo	Periodo Osservazione	Rationale
Controlli tecnici automatizzati	60-90 giorni	Raccolta dati statistici significativi
Controlli organizzativi/formativi	90-120 giorni	Consolidamento comportamenti e competenze
Controlli di processo sanitari	120-180 giorni	Integrazione con cicli operativi sanitari
Controlli infrastrutturali	30-60 giorni	Verifica immediata funzionalità tecnica

Indicatori di efficacia misurabili

Per ciascuna tipologia di controllo vengono definiti KPI specifici che consentono valutazione oggettiva dell'efficacia raggiunta rispetto agli obiettivi prefissati.

Controlli preventivi - KPI di efficacia:

- Riduzione percentuale eventi rilevati vs baseline storica
- Tempo medio di rilevamento vulnerabilità prima dell'exploit
- Percentuale di tentativi di accesso non autorizzato bloccati
- Conformità alle policy misurata attraverso audit campionari

Controlli detective - KPI di efficacia:

- Riduzione tempo medio di detection degli incidenti (MTTD)
- Percentuale di falsi positivi su alert generati

- Copertura percentuale delle minacce rilevate vs threat intelligence
- Qualità e completezza delle evidenze raccolte per incident response

Controlli correttivi - KPI di efficacia:

- Riduzione tempo medio di recovery (MTTR) da incidenti
- Percentuale di ripristino completo entro RTO definito
- Integrità dei dati ripristinati verificata attraverso controlli automatici
- Efficacia delle procedure di comunicazione stakeholder durante recovery

Processo per inefficacia rilevata

Quando la validazione empirica dimostra che l'efficacia del controllo è significativamente inferiore alle aspettative (scostamento >30% dai KPI target), viene attivato un processo strutturato di correzione che mantiene protezione adeguata durante la fase di rimedio.

Azioni immediate (entro 7 giorni dalla rilevazione): Il responsabile del rischio identifica misure compensative temporanee per mantenere livello di protezione accettabile, analizza le cause radice dell'inefficacia attraverso root cause analysis strutturata, e comunica al CISO l'attivazione della procedura di correzione.

Piano di rimedio (entro 30 giorni): Definizione di azioni correttive specifiche che possono includere riconfigurazioni tecniche, formazione aggiuntiva del personale, modifica delle procedure operative, o sostituzione completa del controllo con soluzioni alternative. Il piano specifica timeline, risorse necessarie e nuovi KPI target per la validazione.

Rivalutazione del rischio: Durante il periodo di correzione, il rischio residuo viene temporaneamente ricalcolato considerando l'efficacia ridotta o l'assenza del controllo, permettendo valutazione realistica dell'esposizione e decisioni informate su eventuali misure aggiuntive urgenti.

Processo di approvazione del rischio residuo

Il rischio residuo validato empiricamente viene sottoposto ad approvazione formale secondo criteri predefiniti che tengono conto sia del valore calcolato che della qualità delle evidenze raccolte durante la validazione.

Livello Rischio Residuo	Autorità Approvazione	Documentazione Richiesta
VERDE (entro soglie)	Responsabile del Rischio	Report validazione KPI
AMBRA (asset critici)	Security Forum	Analisi costi-benefici aggiuntivi
ROSSO (qualsiasi asset)	Security Forum con ratifica Direzione Generale	Business case per accettazione

L'approvazione del rischio residuo comporta l'accettazione formale del livello di protezione raggiunto e la chiusura del ciclo di trattamento per l'evento specifico, fermo restando l'obbligo di monitoraggio continuo secondo le frequenze stabilite nella procedura.

8.8.5.Documentazione e reporting

L'intero processo di trattamento del rischio è supportato da un sistema documentale strutturato che assicura tracciabilità delle decisioni, verificabilità dei risultati e supporto ai processi di audit interno ed esterno.

Documentazione delle azioni:

Per ogni azione completata viene prodotta documentazione specifica che include il confronto tra rischio residuo stimato ed effettivo, l'analisi delle cause di eventuali scostamenti, la valutazione dell'efficacia dei controlli implementati e le raccomandazioni per azioni future di natura simile. Questa documentazione alimenta la base di conoscenza organizzativa per il miglioramento continuo dei processi di risk management.

Reporting periodico:

Il sistema di reporting si articola su più livelli temporali e di dettaglio. Report mensili forniscono aggiornamenti operativi sui progressi delle azioni in corso, evidenziando ritardi significativi e criticità emergenti. Report trimestrali offrono una visione consolidata dell'efficacia complessiva del piano di trattamento, includendo analisi di trend e confronti con gli obiettivi pianificati.

La Direzione riceve report annuali che sintetizzano i risultati complessivi del processo di gestione dei rischi, evidenziando l'evoluzione del profilo di rischio organizzativo, l'efficacia delle azioni implementate e le aree di miglioramento identificate per il periodo successivo.

Aggiornamento del registro dei rischi:

Il completamento di ciascuna azione comporta l'aggiornamento del registro dei rischi (118.PR.SEC.15A) con i nuovi livelli calcolati, la documentazione delle azioni implementate e la registrazione delle lezioni apprese. Il registro costituisce la fonte informativa primaria per le successive iterazioni del processo di valutazione e per la pianificazione strategica delle iniziative di sicurezza.

Condivisione delle conoscenze:

Le lezioni apprese dall'implementazione delle azioni di trattamento vengono sistematicamente condivise all'interno dell'organizzazione attraverso sessioni di knowledge sharing, aggiornamenti delle procedure operative e integrazione nei programmi di formazione del personale. Questo approccio favorisce la diffusione delle best practice e l'innalzamento complessivo della maturità organizzativa in materia di gestione dei rischi per la sicurezza delle informazioni.

L'efficacia del sistema documentale viene periodicamente verificata attraverso audit interni che ne valutano completezza, accuratezza e utilità per i processi decisionali, assicurando che risponda effettivamente alle esigenze operative e ai requisiti normativi di riferimento.

8.9. Metriche di Performance e Miglioramento Continuo

8.9.1.KPI di Sistema

L'efficacia complessiva del sistema di gestione dei rischi viene misurata attraverso indicatori chiave di performance (KPI) calcolati trimestralmente:

KPI Operativi Base (1-6 mesi):

1. **Copertura Risk Assessment**: % sistemi valutati / sistemi totali
    a. Target: 100% sistemi critici entro 6 mesi
2. **Completezza Valutazioni**: % eventi con tutti i campi compilati
    a. Target: > 95%
3. **Rispetto Timeline**: % azioni completate entro scadenza
    a. Target: > 80%

4. **Aggiornamento Registro**: % eventi rivalutati secondo frequenza
    a. Target: > 90%

KPI di Maturità del Processo:

1. **Coinvolgimento Risk Owner**: % responsabili formati e attivi
    a. Target: 100% entro 12 mesi
2. **Distribuzione Rischi**: % eventi per categoria (Verde/Ambra/Rosso
    a. Target: 70%/25%/5% (distribuzione equilibrata)
3. **Trend Rischio Residuo**: Evoluzione media livelli post-trattamento
    a. Target: Tendenza decrescente

KPI Avanzati (Solo Dopo 18+ Mesi)

Per quando il sistema è maturo:

1. **Efficacia Controlli**: % controlli che superano test periodici
    a. Target: > 85%
2. **Tempo Medio Risoluzione**: Da identificazione a chiusura evento
    a. Target: Miglioramento 10% annuo
3. **Soddisfazione Risk Owner**: Survey annuale sull'utilità del processo
    a. Target: > 4/5

Nota implementativa: KPI aggiuntivi saranno considerati progressivamente in base alla maturità del sistema e alla disponibilità di dati significativi.

8.9.2.Dashboard e Reporting

Il Security Office mantiene una **Risk Management Dashboard** con visualizzazione di:

- **Profilo di Rischio Organizzativo**: Distribuzione eventi per criticità e trend temporale
- **Stato Trattamenti**: Avanzamento azioni per priorità con alerting ritardi
- **Performance KPI**: Gauge e trend dei principali indicatori
- **Heatmap Rischi**: Matrice dinamica verosimiglianza/impatto per area

La dashboard è accessibile a:

- **Direzione**: Vista executive con sintesi e trend
- **Security Forum**: Vista completa per decisioni strategiche
- **Responsabile del Rischio**: Vista filtrata sui propri eventi
- **Auditor**: Vista read-only per verifiche

8.9.3.Processo di Miglioramento

Trimestralmente, il CISO supporta l'analisi dei KPI per identificare:

- Aree con performance sotto target
- Trend negativi da invertire

- Best practice da replicare
- Necessità di revisione metodologica

Le azioni di miglioramento vengono tracciate nel sistema di gestione qualità aziendale.

8.9.4. Tipologie di Indicatori e Loro Correlazione

Il sistema di monitoraggio si basa su tre categorie di indicatori complementari, come definito nelle best practice internazionali:

Key Control Indicators (KCI)

Forniscono una misura dell'efficacia dei controlli dal punto di vista del rischio. Esempi specifici per il contesto sanitario:

- Percentuale di sistemi critici con backup verificato nelle ultime 24h
- Copertura della formazione sulla sicurezza per il personale clinico
- Tempo medio di applicazione delle patch di sicurezza sui dispositivi medicali

Key Risk Indicators (KRI)

Offrono segnali precoci dell'aumento dell'esposizione al rischio. Nel nostro contesto:

- Incremento anomalo dei tentativi di accesso ai sistemi operativi di emergenza
- Variazione nel volume di e-mail sospette segnalate
- Numero di near-miss relativi alla sicurezza delle informazioni

Key Performance Indicators (KPI)

I KPI già definiti in §7.9.1 rappresentano misure aggregate della performance nel tempo.

Correlazione tra Indicatori

La sequenza KCI degradati → KRI in aumento → KPI in peggioramento permette un approccio predittivo alla gestione del rischio, consentendo interventi preventivi prima della materializzazione degli eventi

8.10. Strumenti di Supporto e Automazione

8.10.1. Strumenti Operativi

L'organizzazione implementa il sistema di gestione dei rischi utilizzando strumenti già disponibili, privilegiando soluzioni operative immediate e affidabili. Il sistema si basa principalmente su template Excel standardizzati (118.MO.SEC.15C) che automatizzano il calcolo dei livelli di rischio tramite formule preimpostate, validano i parametri di input controllando i range ammessi e generano automaticamente la classificazione Verde/Ambra/Rosso basata sulle soglie definite.

La documentazione viene gestita attraverso il sistema documentale aziendale, che garantisce l'archiviazione del Registro Risk Assessment (118.PR.SEC.15A) secondo la procedura 118.PR.QUA.02, mantiene il controllo versioni centralizzato con gestione accessi differenziati per ruolo e assicura backup automatici secondo le policy aziendali. Il coordinamento operativo si realizza attraverso:

- Calendario condiviso per pianificazione scadenze e milestone
- Sistema e-mail per notifiche e comunicazioni operative
- Piattaforma riunioni per Security Forum e coordinamento CISO
- Sistema ticketing esistente per tracking azioni di trattamento

8.10.2. Automazioni Implementate

Gli strumenti attuali forniscono un livello base di automazione che supporta efficacemente le attività operative quotidiane. I controlli automatici includono la validazione di coerenza degli input tramite formule condizionali, alert visivi per il superamento delle soglie di tolleranza ed evidenziazione automatica di eventi scaduti o in ritardo. Il sistema genera inoltre consolidamenti automatici dei dati provenienti da fogli multipli e produce grafici di distribuzione dei rischi per area.

Il tracking delle attività si basa su notifiche calendario per le scadenze periodiche e checklist automatiche per verificare la completezza della documentazione richiesta.

8.10.3. Evoluzione verso Piattaforma GRC

L'organizzazione valuterà l'adozione di una piattaforma GRC dedicata quando il volume operativo e la complessità del sistema raggiungeranno soglie che giustifichino l'investimento tecnologico. I criteri di valutazione includono il raggiungimento di 50+ eventi di rischio attivi simultaneamente, il coinvolgimento di 10+ Risk Owner in modo continuativo e una complessità gestionale non più sostenibile con gli strumenti attuali.

Requisiti funzionali minimi per la piattaforma:

- Gestione centralizzata del Registro Risk Assessment con accesso web
- Workflow automatizzati per le approvazioni del Security Forum
- Calcolo automatico dei livelli di rischio con validazione avanzata
- Dashboard real-time e generazione automatica di report periodici
- Integrazione con sistemi di ticketing per le azioni di trattamento
- Conformità ISO 27001 e audit trail completo per verifiche

8.10.4. Continuità Operativa

Le procedure di business continuity garantiscono la continuità del sistema di gestione dei rischi anche in caso di indisponibilità degli strumenti informatici. Ogni Risk Owner mantiene template Excel offline aggiornati, mentre la documentazione viene sottoposta a backup mensili per garantire la disponibilità locale delle informazioni critiche. Il sistema prevede inoltre procedure per l'esecuzione di calcoli manuali senza supporto informatico e canali di comunicazione alternativi per le escalation urgenti.

In caso di futura implementazione di piattaforma GRC, sarà sviluppata una procedura di business continuity specifica (118.PR.TEC.XX) che includerà export periodici automatici, procedure di import massivo per il ripristino e meccanismi di sincronizzazione differita per l'allineamento dei dati post-interruzione.

8.10.5. Pianificazione Evolutiva

L'evoluzione tecnologica segue un approccio graduale basato su evidenze operative concrete. La fase di consolidamento (primi 12 mesi) si concentra sull'ottimizzazione degli strumenti attuali e sulla standardizzazione dei processi, misurando il ROI del sistema base. La fase di preparazione (mesi 13-18) prevede lo sviluppo del business case per la piattaforma GRC, l'analisi dei fornitori disponibili e la definizione dei requisiti tecnici dettagliati.

L'eventuale fase di implementazione (mesi 19-24) includerà la selezione e il deployment della piattaforma, la migrazione dei dati esistenti e il training degli utenti, con un go-live graduale per minimizzare i rischi operativi. La fase di maturità successiva si focalizzerà sull'implementazione di automazioni avanzate e sull'integrazione con l'ecosistema IT aziendale, mantenendo un approccio di evoluzione continua basata sul feedback operativo e sulla sostenibilità economica.

8.11. Valutazione e Miglioramento della Cultura del Rischio

8.11.1. Premessa

La cultura del rischio rappresenta il sistema di valori, convinzioni e comportamenti che caratterizzano l'approccio dell'organizzazione alla gestione del rischio. Come evidenziato dalla letteratura, essa influenza direttamente l'efficacia del sistema di gestione del rischio, condizionando le decisioni con scelte potenzialmente non basate sull'evidenza oggettiva del livello di rischio.

8.11.2. Modello di Maturità della Cultura del Rischio

L'organizzazione adotta un modello di maturità a cinque livelli per valutare sistematicamente l'evoluzione della propria cultura del rischio:

Livello 1 - Vulnerable

- Assenza di attenzione verso le tematiche di gestione del rischio
- Tendenza ad accettare gli incidenti piuttosto che prevenirli
- Mancanza di pianificazione strutturata

Livello 2 - Reactive

- Limitata attenzione alla prevenzione
- Decisioni guidate da logiche di costo minimo
- Focus sulla ricerca dei responsabili piuttosto che delle cause sistemiche

Livello 3 - Compliant

- Approccio formale guidato principalmente dalla conformità normativa
- Prevenzione motivata dal timore delle sanzioni
- Attenzione focalizzata sulla compliance

Livello 4 - Proactive

- Consapevolezza dell'importanza della gestione del rischio
- Visione olistica dei processi interni
- Pianificazione basata sull'analisi del rischio

Livello 5 - Resilient

- Piena integrazione del rischio nei processi decisionali
- Trasparenza e condivisione delle informazioni nell'ecosistema
- Miglioramento continuo basato sulle lezioni apprese

8.11.3. Aree di Valutazione

La valutazione della cultura viene condotta su sei aree comportamentali critiche:

1. **Comunicazione**
   - Capacità di condividere informazioni rilevanti per il rischio con tempestività e completezza. Una comunicazione efficace garantisce che le vulnerabilità siano note a tutti gli stakeholder interessati.
2. **Formazione**
   - Continuità nell'aggiornamento delle competenze necessarie alla gestione del rischio. Include la valutazione dell'effettivo apprendimento e il monitoraggio dei risultati formativi.
3. **Gestione degli Incidenti**
   - Capacità di risposta strutturata basata su pianificazione e verifica dell'efficacia. Comprende l'analisi delle cause radice e la condivisione delle lezioni apprese.

4. **Investimenti**
   - Allocazione di risorse coerente con le necessità identificate nel piano di trattamento del rischio, superando logiche di puro contenimento dei costi.
5. **Responsabilità**
   - Chiarezza nell'attribuzione di ruoli e responsabilità, con monitoraggio sistematico dell'efficacia operativa.
6. **Etica e Trasparenza**
   - Capacità di agire nell'interesse comune dell'organizzazione e dell'ecosistema, condividendo informazioni rilevanti anche con stakeholder esterni.

8.11.4. Metodologia di Valutazione

Per ciascuna area e livello di maturità viene definito un obiettivo specifico. La valutazione procede assegnando un grado percentuale di raggiungimento dell'obiettivo, permettendo di tracciare l'evoluzione nel tempo.

Il risultato aggregato fornisce il **Cultural Maturity Index (CMI)**, un nuovo KPI del sistema che si integra con le metriche definite in §8.9.

8.12. Implementazione graduale (Risk Assessment Light)

Per facilitare l'adozione iniziale, è disponibile un approccio semplificato:

Fase 1 - Quick Assessment (primi 3 mesi):

- Utilizzare solo 3 livelli di valutazione (Basso-Medio-Alto)
- Applicare fattori asset fissi: Critici 1.5, Standard 1.0
- Utilizzare fattori controlli semplificati: Buoni 0.7, Scarsi 1.0
- Focus sui rischi più evidenti (top 10 per area)

Fase 2 - Assessment completo (dopo 3 mesi):

- Transizione graduale alla metodologia completa
- Validazione dei risultati Quick Assessment
- Calibrazione parametri basata su esperienza Fase 1

Criteri di transizione:

- Completamento assessment di almeno 20 eventi in Fase 1
- Formazione completata per tutti i risk owner
- Disponibilità di supporto tecnico per calcoli complessi

9. Modalità di Revisione

Il coordinamento metodologico della manutenzione della presente procedura è affidato al **CISO**, con approvazione delle modifiche da parte del Security Forum, assicurando il suo allineamento con l'evoluzione della normativa interna ed esterna e con gli aggiornamenti degli standard internazionali di riferimento.

9.1. Frequenza di revisione

Revisione ordinaria:

La procedura è sottoposta a revisione completa con frequenza annuale, includendo la verifica della metodologia di valutazione, l'aggiornamento dei parametri di calcolo e la validazione delle soglie di tolleranza sulla base dei dati storici raccolti.

Con frequenza semestrale viene condotta una verifica mirata delle soglie di tolleranza e dei fattori di correzione utilizzati nel calcolo del rischio, per assicurare che rimangano allineati con l'evoluzione del contesto operativo e delle minacce.

Revisione straordinaria:

Revisioni straordinarie vengono attivate in presenza di aggiornamenti significativi degli standard ISO/IEC 27001 e 27005, modifiche sostanziali della normativa sanitaria o di protezione dei dati personali, cambiamenti organizzativi che impattino sui processi di risk management, o incidenti di sicurezza che evidenzino lacune metodologiche nella valutazione dei rischi.

9.2. Processo di revisione

Il processo di revisione include l'analisi dell'efficacia della metodologia applicata attraverso la verifica della corrispondenza tra valutazioni previsionali e rischi effettivamente manifestatisi. Viene condotta una validazione delle soglie di tolleranza confrontando i risultati ottenuti con benchmark di settore e best practice internazionali.

Le scale di valutazione di verosimiglianza e impatto vengono aggiornate quando necessario per riflettere l'evoluzione del panorama delle minacce specifiche del settore delle emergenze sanitarie. Particolare attenzione è posta all'integrazione delle lezioni apprese dall'applicazione pratica della procedura e dalla gestione degli incidenti verificatisi.

La revisione considera inoltre la coerenza della presente procedura con altre procedure di sicurezza dell'organizzazione, assicurando l'allineamento metodologico e terminologico con il sistema di gestione complessivo.

9.3. Approvazione e comunicazione degli aggiornamenti

Le modifiche alla procedura vengono sottoposte ad approvazione formale del **Security Forum** e della **Direzione** prima della loro implementazione. Gli aggiornamenti significativi vengono comunicati a tutti i Responsabili del Rischio attraverso sessioni di formazione specifiche che illustrano le modifiche metodologiche e i loro impatti operativi.

La documentazione delle modifiche include la motivazione degli aggiornamenti, l'analisi dell'impatto sui processi esistenti e le indicazioni per l'implementazione delle nuove disposizioni. Viene inoltre aggiornata la formazione del personale coinvolto nei processi di risk assessment per assicurare la corretta applicazione della metodologia rivista.

10. Responsabilità

10.1. Responsabili dei rischi relativi alla sicurezza delle informazioni

10.1.1. Modello organizzativo distribuito

L'organizzazione adotta un modello distribuito di gestione dei rischi, dove le responsabilità sono assegnate in base alla competenza specifica e alla conoscenza approfondita dei processi coinvolti negli eventi di rischio.

10.1.2. Criteri di assegnazione

Per ciascun evento di rischio identificato viene nominato uno specifico Responsabile del Rischio (Responsabile del Rischio), selezionato tra i dipendenti che possiedono:

- **Conoscenza approfondita** dei processi e sistemi coinvolti nell'evento
- **Autorità decisionale** per le opzioni di trattamento e allocazione risorse
- **Competenze tecniche** per valutare efficacia dei controlli esistenti e proposti

Tipologie di assegnazione:

- **Responsabili di processo** per eventi che impattano workflow operativi specifici
- **Responsabili di sistema** per eventi tecnologici su piattaforme dedicate
- **Responsabili funzionali** per eventi trasversali a più processi/sistemi

10.1.3. Compiti del Responsabile del Rischio

Ogni Responsabile del Rischio, **per gli eventi di sua competenza**:

- Conduce l'identificazione sistematica degli eventi nel proprio ambito
- Esegue l'analisi quantitativa applicando la metodologia definita
- Decide sulle opzioni di trattamento considerando fattibilità, costi e benefici
- Pianifica e supervisiona l'implementazione delle azioni di trattamento
- Monitora l'efficacia dei controlli implementati
- Mantiene aggiornata la documentazione nel registro dei rischi

10.1.4. Gestione delle sovrapposizioni

La stessa persona può essere **Responsabile del Rischio per eventi multipli** quando ha competenza trasversale, autorità decisionale sull'ambito e disponibilità operativa per gestire il carico di lavoro.

10.1.5. Documentazione delle assegnazioni

Nel **Registro Information Risk Assessment** (118.PR.SEC.15A), per ogni evento viene specificato:

- Nome, ruolo e contatti del Responsabile del Rischio assegnato
- Ambito di competenza (processi/sistemi di riferimento)
- Eventuali Responsabili secondari per eventi complessi

Esempi di assegnazione:

- Ransomware su sistema dispatch 118 → Responsabile: Direttore Operativo ARES
- Accesso non autorizzato database missioni → Responsabile: Coordinatore Centrale Operativa
- Perdita dispositivo equipaggio con dati pazienti trasportati/assistiti → Responsabile: Coordinatore Territoriale

10.2. Ruoli specifici per il contesto sanitario

I seguenti ruoli ricoprono **funzioni specialistiche** nel processo di gestione dei rischi e possono essere nominati **Responsabili del Rischio** per eventi specifici della loro competenza o fornire **supporto specialistico** ad altri Responsabili del Rischio.

Direttore Sanitario - Potenziale Responsabile del Rischio per eventi clinici**:**

- **Assegnazione diretta** per eventi che impattano sistemi operativi di emergenza critici o sicurezza pazienti trasportati/assistiti
- **Validazione specialistica** per eventi gestiti da altri Responsabile del Rischio ma con impatto clinico
- **Definizione priorità** per eventi multipli che coinvolgono assistenza sanitaria

Responsabile della Protezione dei Dati (DPO) - Supporto specialistico obbligatorio:

Il DPO mantiene piena autonomia e indipendenza funzionale nel processo di risk management:

Per eventi che coinvolgono dati personali:

- **Consultazione obbligatoria** entro 5 giorni dalla valutazione
- **Parere scritto** su conformità GDPR delle misure proposte
- **Diritto di richiedere rivalutazione** se rileva sottovalutazione rischi privacy
- **Documentazione motivata** in caso di disaccordo con il Risk Owner

Salvaguardie di indipendenza:

- **Non assume mai ruolo di Risk Owner** per preservare indipendenza
- **Fornisce pareri consultivi** vincolanti solo per conformità normativa
- **Può richiedere escalation** al Titolare per criticità privacy sottovalutate
- **Partecipazione non permanente** al Security Forum per tematiche specifiche

Responsabile dei Sistemi Informativi - Potenziale Responsabile del Rischio per eventi IT:

- **Assegnazione preferenziale** per eventi tecnico-informatici
- **Assessment tecnico** di fattibilità per azioni di trattamento tecnologiche
- **Coordinamento implementazione** controlli tecnologici trasversali

10.3. Coordinamento e governance del modello distribuito

10.3.1. Security Forum

Il Security Forum costituisce l'organismo collegiale di governance per le decisioni strategiche relative alla sicurezza delle informazioni.

Composizione permanente:

- **Presidente**: Direttore Generale
- **Direttore Amministrativo** (governance economico-finanziaria)
- **Direttore Sanitario** (competenza clinica e operativa)
- **Direttore UOC ICT** (competenza tecnico-informatica)
- **Referente Privacy interno** (compliance normativa)

Partecipanti non permanenti:

- **CISO** (supporto metodologico, senza diritto di voto)
- **DPO** (per eventi che coinvolgono dati personali)

Competenze del Security Forum:

- Approvazione delle strategie generali di gestione dei rischi
- Decisioni definitive su eventi ROSSO e conflitti tra Risk Owner
- Definizione delle soglie di tolleranza organizzative
- Approvazione modifiche metodologiche della procedura

Convocazione: Su iniziativa del Presidente o di due membri permanenti

10.3.2. Chief Information Security Officer (CISO) - Supporto metodologico:

Il CISO fornisce supporto specialistico al sistema di gestione dei rischi, operando in coordinamento con la dirigenza aziendale:

- **Facilitazione metodologica** delle valutazioni condotte dai Risk Owner
- **Supporto nella risoluzione di divergenze** tecniche tra Risk Owner
- **Consolidamento del reporting** per supportare le decisioni della Direzione
- **Pareri di conformità** metodologica per eventi complessi
- **Formazione e coaching** dei Risk Owner sui processi e strumenti

Limitazioni operative:

- **Non assume responsabilità decisionali** in sostituzione della governance aziendale
- **Fornisce supporto consultivo** senza autorità decisionale diretta
- **Opera sotto la supervisione** del Security Forum per aspetti strategici

10.3.3. Responsabili di Unità Operative, Funzioni, Servizi e Uffici - - Pool di potenziali Responsabile del Rischio

- **Candidati primari** per assegnazione come Responsabili del Rischio per eventi nei loro ambiti
- **Supporto operativo** per implementazione azioni quando non sono Responsabile del Rischio diretti
- **Escalation** al CISO per eventi che superano le loro competenze

10.3.4. "CISO - Supporto metodologico e coordinamento operativo

- Facilitazione diretta del lavoro dei Responsabili del Rischi
- Standardizzazione degli approcci metodologici
- Consolidamento dati da multiple valutazioni per analisi aggregate
- Valutazione periodica della necessità di struttura dedicata"

10.4. Documentazione e gestione delle assegnazioni

10.4.1. Calibrazione e Consistenza delle Valutazioni

Per garantire uniformità nelle valutazioni condotte dai diversi Responsabile del Rischio, l'organizzazione implementa:

Calibrazione Periodica Semestrale

- **Workshop di allineamento** con tutti i Responsabile del Rischio per:
  - Revisione criteri di valutazione con esempi pratici
  - Analisi casi di studio per allineamento interpretativo
  - Discussione valutazioni divergenti su eventi simili

Peer Review per Eventi Critici

- Eventi classificati ROSSO vengono sottoposti a **doppia valutazione indipendente**
- In caso di divergenza > 20% nel punteggio, viene attivata escalation al Security Forum per mediazione, con supporto metodologico del CISO se richiesto
- Documentazione delle motivazioni per divergenze accettate

Audit di Consistenza Trimestrale

- Campionamento 10% delle valutazioni per verifica:
  - Corretta applicazione della metodologia
  - Coerenza con valutazioni precedenti simili

  - Completezza documentazione supporto
- Report al Security Forum con azioni correttive se necessario

Libreria di Riferimento Il Security Office mantiene una **Knowledge Base** con:

- Catalogo eventi tipo con valutazioni di riferimento
- Esempi di calcolo per scenari comuni
- FAQ su interpretazione criteri
- Lesson learned da valutazioni precedenti

10.4.2. Tracciabilità delle responsabilità

L'assegnazione specifica del Responsabile del Rischio per ciascun evento è documentata nel **Registro Information Risk Assessment** (118.PR.SEC.15A) con:

- **Identificazione nominativa** del Responsabile del Rischio principale
- **Ruoli di supporto** (DPO, specialisti clinici, tecnici)
- **Ambito di competenza** dettagliato per l'evento specifico
- **Criteri di assegnazione** utilizzati per la nomina

10.4.3. Gestione dei cambiamenti

Revisione annuale delle assegnazioni nell'ambito della revisionedel sistema di gestione della sicurezza delle informazioni dell'organizzazione per verificare:

- Allineamento competenze-responsabilità per eventi evoluti
- Disponibilità operativa dei Responsabili del Rischio
- Necessità di riassegnazioni per cambiamenti organizzativi

Aggiornamenti straordinari per:

- Cambiamenti organizzativi che modificano competenze/autorità
- Nuovi eventi che richiedono assegnazione di responsabilità
- Sovraccarichi operativi che necessitano redistribuzione

10.4.4. Validazione competenze

Il CISO conduce **assessment periodico** delle competenze dei Responsabili del Rischio verificando:

- Adeguatezza delle conoscenze tecniche per gli eventi assegnati
- Efficacia delle decisioni di trattamento adottate
- Qualità della documentazione e del reporting prodotti
- Necessità di formazione specifica per nuove tipologie di eventi

11. Allegati

La presente procedura è supportata da documenti operativi che ne facilitano l'applicazione pratica e garantiscono la tracciabilità completa del processo di gestione dei rischi per la sicurezza delle informazioni.

11.1. Registro Information Risk Assessment (118.PR.SEC.15A)

Il Registro Information Risk Assessment costituisce il documento operativo centrale per l'applicazione della metodologia definita nella presente procedura, strutturato per supportare il **modello distribuito di gestione dei rischi** e garantire la tracciabilità completa delle decisioni adottate.

Contenuto del registro:

Il documento include fogli di lavoro per:

- **Identificazione degli eventi** con descrizione dettagliata degli scenari e classificazione per tipologia
- **Mappatura delle minacce e vulnerabilità** associate agli eventi identificati
- **Inventario degli asset coinvolti** con classificazione della criticità (standard/importanti/critici)
- **Assegnazione specifica dei Responsabili del Rischio** per ciascun evento, inclusi ruoli di supporto e criteri di nomina
- **Documentazione dei controlli esistenti** con valutazione empirica dell'efficacia e classificazione (preventivi/detective/correttivi)
- **Calcolo strutturato dei livelli di rischio** applicando la metodologia qualitativa con fattori di correzione
- **Tracking della validazione empirica** dei controlli implementati e dell'efficacia effettiva osservata

Utilizzo operativo nel modello distribuito:

Il registro viene utilizzato dai singoli Responsabili del Rischio per gli eventi di loro competenza, dal CISO per il coordinamento metodologico e il consolidamento del profilo di rischio organizzativo, e dai revisori per verificare l'applicazione corretta della metodologia distribuita.

11.2. Piano di trattamento del rischio (118.PR.SEC.15B)

Il Piano di trattamento del rischio documenta le decisioni operative per la gestione degli eventi che richiedono interventi specifici, integrando le valutazioni dei diversi Responsabili del Rischio in un documento consolidato.

Struttura del piano:

Per ciascun evento che richiede trattamento, il piano documenta:

- **Responsabile del Rischio assegnato** e ruoli di supporto coinvolti
- **Opzione di trattamento selezionata** con motivazione tecnico-economica
- **Azioni specifiche** con responsabilità, tempistiche e modalità di implementazione
- **Stima delle risorse** e valutazione del rischio residuo atteso
- **Matrice di confronto multi-framework** (ISO 27001, UNI/PdR 174:2025, ACN, NIST 800-53)
- **Criteri di validazione empirica** dell'efficacia e timeline per la verifica post-implementazione

Gestione e aggiornamento:

Il piano è soggetto ad approvazione formale secondo il processo definito al §7.8.1 e viene aggiornato periodicamente per riflettere l'avanzamento delle azioni, i risultati della validazione empirica e l'emergere di nuovi eventi di rischio sotto la responsabilità dei diversi Responsabile del Rischio.

11.3. Utilizzo e manutenzione degli allegati

I documenti allegati sono parte integrante del sistema di gestione distribuito per la sicurezza delle informazioni e sono soggetti al controllo delle versioni secondo le procedure organizzative standard.

Gestione delle responsabilità:

- **Responsabili del Rischio individuali**: Mantengono aggiornate le sezioni relative agli eventi di loro competenza
- **CISO**: Coordina la coerenza metodologica e il consolidamento delle informazioni
- **CISO**: Fornisce supporto tecnico per l'utilizzo corretto dei template e la risoluzione di questioni interpretative

Formazione e supporto distribuito:

L'utilizzo efficace degli allegati nel modello distribuito è supportato da:

- **Formazione specifica** per ogni Responsabile del Rischio sui template e metodologie
- **Linee guida operative** per la gestione delle interfacce tra diversi Responsabile del Rischio
- **Supporto metodologico** centralizzato per garantire uniformità nell'applicazione dell'approccio multi-framework

Evoluzione continua:

Gli allegati vengono aggiornati per riflettere i risultati della **validazione empirica continua** dei parametri metodologici e l'evoluzione delle best practice nel confronto multi-framework dei controlli di sicurezza.

12. Conclusione: un Percorso di Miglioramento Continuo

Implementare un sistema strutturato di Risk Assessment in una realtà operativa come la nostra non è semplice. Richiede tempo, pazienza e la collaborazione di tutti. Ma ricordiamoci perché lo facciamo:

- Ogni rischio che preveniamo è un'emergenza che non dovremo gestire
- Ogni vulnerabilità che identifichiamo è un potenziale incidente evitato
- Ogni controllo che implementiamo è maggiore serenità operativa

Non puntiamo alla perfezione immediata. Puntiamo a essere un po' più preparati ogni giorno, a imparare dai quasi-incidenti, a costruire una cultura della sicurezza che diventi naturale come indossare i guanti prima di un intervento.

Segnalate dubbi, proponete miglioramenti, condividete preoccupazioni. Insieme possiamo costruire un sistema che non sia solo conforme agli standard, ma che davvero protegga la nostra capacità di salvare vite.

Il rischio zero non esiste, ma ogni rischio gestito è una vittoria.

12.1. Il Percorso verso la Resilienza

La maturità ultima non è solo gestire i rischi ma diventare un'organizzazione resiliente, capace di:

- Assorbire shock senza compromettere i servizi critici

- Apprendere rapidamente dagli eventi
- Evolvere proattivamente anticipando i cambiamenti
- Condividere conoscenza nell'ecosistema sanitario

Questo richiede un'evoluzione culturale che va oltre la conformità, verso una mentalità dove il rischio è opportunità di miglioramento, non solo minaccia da contenere.

13. Appendici

13.1. Appendice A - Checklist per Responsabile del Rischio

B.1 Checklist Identificazione Rischio

□ Ho considerato tutte le tipologie di minacce (cyber, fisiche, organizzative)?
□ Ho mappato tutti gli asset coinvolti nell'evento?
□ Ho verificato vulnerabilità note per tecnologie coinvolte?
□ Ho considerato effetti domino su altri sistemi/processi?
□ Ho inventariato controlli esistenti (preventivi, detective, correttivi)?
□ Ho consultato il DPO se coinvolti dati personali/sanitari?

B.2 Checklist Analisi e Calcolo

□ Verosimiglianza basata su evidenze oggettive (non percezioni)?
□ Impatto considera tutti gli aspetti (sanitario, normativo, reputazionale)?
□ Classificazione asset verificata e aggiornata?
□ Efficacia controlli basata su test/evidenze non teorica?
□ Calcolo matematico verificato (formula applicata correttamente)?
□ Documentazione completa nel registro 118.PR.SEC.15A?

B.3 Checklist Trattamento

□ Opzione di trattamento proporzionata al livello di rischio?
□ Risorse necessarie disponibili/ottenibili?
□ Timeline rispetta priorità definite da procedura?
□ Rischio residuo stimato accettabile?
□ Piano include milestones verificabili?
□ KPI per validazione empirica definiti?

B.4 Checklist Monitoraggio

□ Verifiche programmate secondo frequenza richiesta?
□ Evidenze raccolte per validazione empirica?
□ Scostamenti da piano documentati e gestiti?
□ Rischio residuo ricalcolato con dati reali?
□ Lesson learned documentate per future valutazioni?
□ Aggiornamenti comunicati a stakeholder rilevanti?

13.2. Appendice B - Domande Frequenti

Q: Devo essere un esperto di sicurezza informatica per essere Responsabile del Rischio?
A: No. Devi essere esperto del TUO ambito. Il CISO ti supporta sulla parte tecnica di sicurezza.

Q: Cosa succede se sbaglio una valutazione?
A: Le valutazioni si affinano nel tempo. L'importante è documentare il ragionamento. Gli "errori" sono opportunità di apprendimento, non colpe.

Q: E se identifico un rischio ma non ho budget per risolverlo?
A: Documentalo comunque. Un rischio documentato e accettato formalmente è meglio di uno ignorato. Inoltre, avere l'analisi pronta può sbloccare fondi quando disponibili.

Q: Quanto tempo ci vuole per una valutazione completa?
A: Prima valutazione: 4-6 ore con supporto. Successivi aggiornamenti: 30-60 minuti. Il tempo si riduce con l'esperienza.

Q: Come faccio a sapere se un controllo è "base" o "avanzato"?
A: Controlli avanzati sono implementati, testati regolarmente e con efficacia dimostrata. Se hai dubbi, parti da "base" e migliora con l'evidenza.

Q: Posso modificare una valutazione già approvata?
A: Certamente, anzi è raccomandato quando emergono nuove informazioni. Documenta cosa è cambiato e perché.

Q: Il fast-track bypassa tutti i controlli?
A: No, bypassa solo l'iter autorizzativo standard. I controlli di sicurezza devono comunque essere implementati, solo con massima urgenza.

Q: Chi decide se sono il Responsabile del Rischio giusto per un evento?
A: Il CISO in base a competenza e autorità decisionale. Se non ti senti adeguato, parlane subito per identificare il owner corretto.

"**Q: Come viene garantito il supporto metodologico senza un Security Office dedicato?** A: Nella fase iniziale, il CISO fornisce supporto diretto. La creazione di una struttura dedicata sarà valutata in base al volume operativo e alla crescita del sistema.

ISMS-ORG-PRC-xxx Procedura di Valutazione della Sicurezza per le Terze Parti

1. Scopo e campo di applicazione

La presente procedura definisce il processo di valutazione della sicurezza delle terze parti che hanno o avranno un rapporto contrattuale diretto con Ares 118.

2. Processo di valutazione (Panoramica)

Questa sezione fornisce una visione d'insieme del processo di valutazione della sicurezza delle terze parti, illustrando le fasi principali e il flusso logico dell'intero ciclo di vita della gestione del rischio. La comprensione della sequenza e delle interdipendenze tra le diverse fasi è fondamentale per garantire un'implementazione efficace della procedura. Questo approccio assicura che tutte le parti coinvolte abbiano una chiara comprensione delle attività, delle tempistiche e delle responsabilità, facilitando il coordinamento tra le diverse funzioni aziendali coinvolte nel processo. La panoramica qui presentata costituisce la base concettuale per i capitoli successivi, che esploreranno in dettaglio ciascuna componente del processo.

Diagramma di flusso del processo:

Fase iniziale:

- Input: Nuovo fornitore o revisione periodica
- Pre-valutazione e classificazione del rischio
- Determinazione del Tier applicabile (1-4)

Fase di valutazione:

- Applicazione dei requisiti specifici per il Tier
- Per Tier 1-2: invio e analisi del questionario di self-assessment
- Calcolo del punteggio di conformità

Fase decisionale:

- Approvazione diretta, condizionata o rifiuto
- Gestione delle eccezioni (per Tier 1)
- Definizione delle azioni correttive se necessarie

Fase di monitoraggio:

- Calendario delle revisioni periodiche
- Gestione degli incidenti
- Rivalutazione in caso di cambiamenti
- Transizione tra livelli di rischio

3. Pre-valutazione del rischio

Questa sezione descrive il processo preliminare di identificazione e classificazione del rischio associato alle terze parti, elemento fondamentale per l'applicazione proporzionata ed efficiente dei controlli di sicurezza. La prevalutazione consente di determinare in modo oggettivo e ripetibile la categoria di rischio di ciascun fornitore (Tier 1-4), assicurando

che le risorse di sicurezza siano allocate in modo coerente con il livello di rischio effettivo. Attraverso una serie di criteri strutturati e fattori modificatori, il processo di prevalutazione permette di ridurre la soggettività intrinseca alla valutazione del rischio, fornendo un metodo standardizzato utilizzabile da tutti i responsabili aziendali. I risultati di questa fase determinano l'intensità e la profondità del processo di valutazione successivo, garantendo un approccio calibrato per ciascun fornitore.

3.1 Schema di Prevalutazione del Rischio per Terze Parti

Schema per la valutazione preliminare del rischio dei fornitori, da utilizzare prima dell'applicazione della procedura completa.

3.1.1 Criteri di valutazione inziale (Parte A)

Questa sezione definisce i parametri fondamentali per una valutazione oggettiva e strutturata del rischio potenziale di ciascun fornitore. I criteri sono organizzati in tre macroaree (natura del servizio, profilo del fornitore, modalità operativa) che coprono gli aspetti essenziali della relazione con la terza parte. Ogni criterio viene valutato su una scala da 0 (rischio minimo) a 4 (rischio massimo), consentendo una classificazione iniziale sistematica e coerente. Questi elementi rappresentano la base oggettiva della valutazione e devono essere applicati a tutti i fornitori indipendentemente dal contesto specifico.

1. Natura del servizio/relazione

Criterio	Punteggio
Tipologia di accesso ai dati	
Nessun accesso a dati aziendali	0
Accesso a dati non sensibili/pubblici	1
Accesso a dati confidenziali aziendali	2
Accesso a dati personali (GDPR)	3
Accesso a dati sensibili/strategici	4
Integrazione con sistemi IT[1]	
Nessuna integrazione	0
Accesso a sistemi isolati/non critici	1
Integrazione con sistemi secondari	2
Integrazione con sistemi importanti	3
Integrazione con sistemi critici/core	4
Criticità per il business	
Servizio non essenziale	0
Servizio utile ma facilmente sostituibile	1
Servizio importante con alternative disponibili	2
Servizio significativo con poche alternative	3
Servizio critico/infrastrutturale	4

2. Profilo del fornitore

Criterio	Punteggio
Dimensione[2]	
Fornitore strategico mission-critical (grande azienda: ≥ 250 dipendenti, > €50 milioni o bilancio > €43 milioni)	0
Fornitore core business (grande azienda: ≥ 250 dipendenti, > €50 milioni o bilancio > €43 milioni)	1

[1] Per la classificazione dei sistemi IT secondo questa scala, fare riferimento all'Appendice A: Criteri di Classificazione dei Sistemi IT

[2] RACCOMANDAZIONE DELLA COMMISSIONE del 6 maggio 2003 relativa alla definizione delle microimprese, piccole e medie imprese - https://eur-lex.europa.eu/eli/reco/2003/361/oj

Criterio	Punteggio
Fornitore rilevante (media impresa < 250 dipendenti, ≤ €50 milioni o bilancio ≤ €43 milioni)	2
Fornitore rilevante (piccola impresa < 50 dipendenti, ≤ €10 milioni)	3
Fornitore marginale (microimpresa < 10 dipendenti, ≤ €2 milioni)	4
Localizzazione geografica	
Italia	0
UE/SEE/UK	1
Paesi con adeguatezza privacy (Svizzera, ecc.)	2
USA o altri paesi con accordi di privacy	3
Paesi senza accordi di privacy adeguati	4
Certezza legale e conformità	
Certificazioni multiple (ISO 27001, 9001, ecc.)	0
Almeno una certificazione rilevante	1
Adozione di standard senza certificazione	2
Conformità dichiarata senza evidenze	3
Nessuna informazione sulla conformità	4

3. Modalità operativa

Criterio	Punteggio
Accesso fisico alle strutture[3]	
Nessun accesso fisico	0
Accesso occasionale ad aree non sensibili	1
Accesso regolare ad aree non sensibili	2
Accesso occasionale ad aree sensibili	3
Accesso regolare ad aree sensibili/critiche	4
Livello di autonomia	
Operatività completamente supervisionata	0
Operatività con approvazioni per azioni chiave	1
Operatività con monitoraggio regolare	2
Operatività con verifiche periodiche	3
Operatività autonoma con minima supervisione	4
Visibilità esterna	
Nessuna visibilità esterna della collaborazione	0
Visibilità limitata a stakeholder specifici	1
Visibilità interna all'azienda	2
Visibilità ai clienti/partner	3
Visibilità pubblica/rappresenta il brand	4

3.1.2 Fattori aggravanti/mitiganti (Parte B)

Questa sezione integra la valutazione base con elementi specifici che possono influenzare significativamente il profilo di rischio del fornitore. I fattori aggravanti (+2 ciascuno) identificano circostanze che aumentano potenzialmente l'esposizione al rischio, mentre i fattori mitiganti (-2 ciascuno) riconoscono elementi che rafforzano il profilo di sicurezza del fornitore. Questi modificatori permettono di contestualizzare la valutazione e di adattarla alle specificità di ciascuna relazione, garantendo una classificazione finale più accurata e rappresentativa del rischio effettivo. L'applicazione di questi fattori deve essere documentata con evidenze oggettive.

1. **Fattori aggravanti (+2 ciascuno)**

[3] Vedi Nota Esplicativa "Classificazione delle Aree Fisiche" in appendice B

La presenza di uno o più dei seguenti elementi può contribuire ad aumentare il livello di rischio complessivo attribuito alla terza parte, comportando un aggravio nella valutazione del profilo di sicurezza.

- Utilizzo di subappaltatori/subfornitori non controllati da Ares118
- Storia di incidenti di sicurezza/privacy negli ultimi tre anni
- Gestione di processi di pagamento/finanziari (emissione o ricezione fatture, gestione transazioni, trattamento IBAN, ecc.)
- Operatività in settori altamente regolamentati (medicale, finanziario, produttivo)
- Assenza di un referente per la sicurezza o la compliance nel fornitore
- Presenza di account privilegiati o accesso remoto ai sistemi Ares118

2. **Fattori mitiganti (-2 ciascuno)**

La presenza di uno o più dei seguenti elementi può contribuire a mitigare il livello di rischio complessivo attribuito alla terza parte:

- Rapporto consolidato con Ares118 da almeno 3 anni, senza segnalazioni o evidenze di incidenti rilevanti in materia di sicurezza delle informazioni o protezione dei dati personali.
- Certificazione SOC 2 Tipo II attiva e riferita al servizio fornito:
  - –2 punti per fornitori non classificati come *Tier 1*;
  - –1 punto per fornitori *Tier 1*, in quanto tale certificazione rappresenta un requisito di base atteso.
- Certificazione ISO/IEC 27001 in corso di validità e riferita al perimetro rilevante:
  - –2 punti per fornitori non *Tier 1*;
  - –1 punto per fornitori *Tier 1* (ove già richiesto nei requisiti contrattuali minimi).
- Polizza assicurativa cyber liability attiva, con:
  - massimale adeguato rispetto alla dimensione del fornitore e alla criticità del servizio;
  - copertura esplicita per data breach, incident response e responsabilità verso terzi.
- Programma di "security by design" formalmente documentato, con evidenza della sua applicazione nei processi di sviluppo, progettazione o erogazione del servizio fornito ad Ares118.
- Penetration test indipendente superato negli ultimi 12 mesi, condotto da soggetto qualificato e riferito al perimetro tecnologico utilizzato per i servizi forniti ad Ares118.
  - È richiesto che eventuali vulnerabilità di severità *alta* o *critica* siano state risolte o poste sotto controllo con misure tecniche adeguate.

3.1.3 Calcolo del punteggio e classificazione (Parte C)

Questa sezione definisce il metodo di quantificazione e interpretazione finale del rischio, trasformando i punteggi assegnati nelle sezioni precedenti in una classificazione operativa. Il processo di calcolo assicura che la valutazione sia metodica e riproducibile, mentre le soglie predefinite garantiscono coerenza nell'assegnazione dei livelli di rischio (Tier). La classificazione risultante determina direttamente il regime di controlli da applicare al fornitore, ed è quindi fondamentale per calibrare correttamente l'impegno di risorse nella gestione della relazione. Il risultato di questa fase rappresenta l'input essenziale per tutte le fasi successive del processo di gestione del rischio.

1. Sommare i punteggi della Parte A (min 0, max 36)
2. Applicare modificatori della Parte B
3. Se dopo l'applicazione dei fattori aggravanti/mitiganti il punteggio totale è superiore a 40, considerarlo comunque come 40 (limite massimo della scala)
4. Classificare secondo la seguente scala:

Punteggio Totale	Classificazione preliminare	Tier
0-8	Rischio Basso	4
9-18	Rischio Medio	3
19-28	Rischio Alto	2
29-40	Rischio Critico	1

3.1.4 Regole di escalation automatica (Parte D)

Questa sezione stabilisce principi di sicurezza non negoziabili che prevalgono sul calcolo numerico del punteggio. Queste regole rappresentano "guardrail" di sicurezza che assicurano che determinate categorie di rischio, particolarmente significative per la protezione dei dati e la conformità normativa, siano sempre adeguatamente classificate indipendentemente dagli altri fattori. L'applicazione di queste regole è obbligatoria e non discrezionale, garantendo che i fornitori che gestiscono dati particolarmente sensibili o che hanno accessi privilegiati siano sempre sottoposti al regime di controllo appropriato, a tutela dell'organizzazione e degli interessati.

Indipendentemente dal punteggio totale, classificare automaticamente come:

- **Rischio Alto (minimo)**: Fornitori che gestiscono dati personali di grandi volumi
- **Rischio Critico (sempre)**: Fornitori che gestiscono dati sanitari/biometrici/giudiziari o con accesso privilegiato ai sistemi core

3.1.5 Istruzioni operative (Parte E)

Questa sezione traduce i principi valutativi in azioni concrete, definendo il flusso di lavoro pratico per l'implementazione dello schema. Le istruzioni delineano responsabilità, sequenza delle attività e requisiti di documentazione, assicurando uniformità nell'esecuzione del processo. Questi passaggi operativi garantiscono che la valutazione non rimanga un esercizio teorico ma si trasformi in un processo aziendale strutturato e tracciabile. L'aderenza rigorosa a queste istruzioni è essenziale per garantire la validità legale e organizzativa dell'intero processo di gestione del rischio dei fornitori.

1. La valutazione preliminare deve essere completata dal Responsabile del Rapporto
2. In caso di dubbi sulla classificazione, consultare il CISO
3. Documentare brevemente le motivazioni dei punteggi assegnati
4. Procedere con la valutazione completa secondo il Tier identificato
5. Alla conclusione della valutazione completa, confermare o rivedere la classificazione

3.2 Integrazione con il Processo di Procurement[4]

L'integrazione della valutazione di sicurezza delle terze parti nel ciclo di procurement è essenziale per identificare e mitigare i rischi prima che divengano operativi. Questo approccio "security by design" garantisce che la sicurezza sia un criterio decisionale formale in ogni fase del rapporto con il fornitore, non un'attività successiva o separata.

Il processo si articola come segue:

Fase di selezione iniziale:

- Completamento della prevalutazione prima della short-list dei fornitori
- Inclusione dei requisiti di sicurezza nei documenti di gara/richiesta di offerta (RFI/RFP)

Fase di valutazione delle offerte:

- La prevalutazione deve essere completata prima della valutazione tecnica/economica
- I requisiti di sicurezza sono inclusi nei criteri di selezione con peso proporzionale al Tier identificato:
  - Tier 1: 25-30% del punteggio complessivo
  - Tier 2: 15-20% del punteggio complessivo
  - Tier 3: 10% del punteggio complessivo
  - Tier 4: criterio pass/fail senza punteggio specifico

L'applicazione del limite superiore o inferiore del range di peso avviene in base ai seguenti criteri:

[4] Vedi Appendice B: Guida Pratica all'Integrazione della Sicurezza nel Procurement

- Utilizzo del limite superiore (es. 30% per Tier 1): quando il servizio/prodotto ha un forte impatto sulla sicurezza delle informazioni o involve dati sensibili o critici, o quando esiste un rischio normativo significativo.
- Utilizzo del limite inferiore (es. 25% per Tier 1): quando, pur rientrando nella categoria di rischio, il servizio/prodotto ha minori impatti o esistono efficaci controlli compensativi già implementati.

La decisione sul peso specifico deve essere documentata e approvata dal CISO.

Fase di contrattualizzazione:

- Nessun contratto può essere firmato senza completamento della valutazione di sicurezza
- I requisiti di sicurezza identificati devono essere inclusi come allegato contrattuale
- Per i Tier 1-2, i contratti devono includere KPI di sicurezza con verifiche periodiche

Rinnovi contrattuali:

- Ogni rinnovo richiede una nuova valutazione di sicurezza o conferma della precedente
- Aggiornamento dei requisiti in base a eventuali modifiche normative o tecnologiche

4. Requisiti in base al livello di rischio

Questa sezione definisce i controlli di sicurezza da implementare per ciascun livello di rischio, secondo un approccio progressivo e proporzionato. I requisiti sono cumulativi, nel senso che ogni livello incorpora tutti i requisiti dei livelli inferiori, aggiungendo ulteriori misure commisurate all'aumentare del rischio. Questo approccio graduale consente di ottimizzare le risorse, concentrando gli sforzi di valutazione e controllo dove il rischio è maggiore, senza imporre oneri ingiustificati ai fornitori con profilo di rischio contenuto. La conformità a questi requisiti deve essere verificata e documentata formalmente prima di stabilire o continuare la relazione commerciale.

4.1 Rischio basso (Tier 4)

- Accordo di non divulgazione (NDA) firmato prima dell'accesso alle informazioni

4.2 Rischio medio (Tier 3)

- Accordo formale nel contratto che include:
  - Conformità alle politiche di sicurezza di Ares 118
  - Clausola di riservatezza
  - Nomina di un responsabile per la sicurezza delle informazioni
  - Diritto di audit da parte di Ares118
  - Conseguenze in caso di non conformità

4.3 Rischio alto (Tier 2)

- Tutto quanto previsto per i livelli precedenti
- Compilazione del questionario di self-assessment sulla sicurezza
- Valutazione dei controlli di sicurezza interni
- Definizione di eventuali controlli correttivi
- Calcolo del punteggio di conformità sulla base del questionario (vedi §5.2)
- Attribuzione di un rating di sicurezza da 1 a 5

4.4 Rischio critico (Tier 1)

- Tutto quanto previsto per i livelli precedenti
- Presentazione di documentazione aggiuntiva:
  - Rapporto SOC 2 di tipo II in corso di validità

- Certificazioni di sicurezza riconosciute (es. ISO 27001)
- Risultati di Penetration test recenti
- Altre evidenze richieste nella valutazione

- Il punteggio ottenuto nel questionario di autovalutazione deve essere ≥ 4.00 per l'approvazione diretta
- In caso di punteggio 3.00-3.99, attivazione approvazione condizionata e controllo rafforzato (vedi §5.3)
- Con punteggio < 3.00: approvazione subordinata all'autorizzazione eccezionale (vedi §5.3)

5. Processo operativo di valutazione

Questa sezione descrive la metodologia di valutazione approfondita che segue la classificazione preliminare del rischio. Mentre la prevalutazione iniziale stabilisce il livello di rischio teorico, il processo operativo qui delineato verifica l'effettiva maturità dei controlli di sicurezza implementati dal fornitore, con particolare attenzione ai fornitori classificati come rischio alto o critico (Tier 1 e 2). Attraverso questionari strutturati, analisi quantitativa delle risposte e verifica delle evidenze, questo processo fornisce una valutazione oggettiva e difendibile della postura di sicurezza del fornitore. Il sistema di scoring ponderato consente di tradurre le evidenze qualitative in metriche quantitative, facilitando decisioni basate su dati e garantendo coerenza di valutazione anche tra fornitori diversi. L'esito di questa fase determina l'approvazione, l'approvazione condizionata o il rifiuto del fornitore, nonché la definizione di eventuali misure correttive o compensative necessarie per mitigare i rischi identificati.

5.1 Invio del questionario di self-assessment

Per i fornitori classificati come rischio alto o critico:

- La Direzione Strategica, il Responsabile IT o funzioni paritarie, supportata dal CISO, invia il questionario di self-assessment
- Il questionario copre 11 domini di controllo allineati con gli standard di sicurezza
- Viene stabilita una scadenza per la compilazione

5.2 Analisi delle risposte

- Verifica della completezza delle informazioni
- Analisi dei controlli dichiarati per ciascun dominio (11 domini + sottocategorie)
- Il questionario include anche controlli legati alla protezione dei dati personali in conformità al GDPR

Il punteggio complessivo è calcolato utilizzando i pesi assegnati a ciascun dominio, come indicato nella tabella seguente:

Dominio	**Peso (%)**
A. Security Policy	5%
B. Organisation of Information Security	10%
C. Asset Management	10%
D. Human Resources Security	5%
E. Physical and Environmental Security	10%
F. Communications and Operations Management	15%
G. Access Control	15%
H. Systems Acquisition, Development and Maintenance	10%
I. Information Security Incident Management	10%
J. Business Continuity Management	5%
K. Compliance	5%
Totale	**100%**

La formula per il calcolo del punteggio totale è:

$$\text{Punteggio totale} = (\Sigma\ (\text{Punteggio dominio} \times \text{Peso dominio})) \ / \ (\Sigma\ \text{Pesi})$$

Dove:

- Punteggio dominio è il punteggio ottenuto nel dominio
- Peso dominio è il peso assegnato al dominio

Il punteggio totale fornisce una misura complessiva della conformità del fornitore ai requisiti di sicurezza.

- Il punteggio è espresso su scala 1-5
- Classificazione finale:
  - **5.00 – Eccellente**
  - **4.00 – 4.99 – Adeguato**
  - **3.00 – 3.99 – Da migliorare**
  - **< 3.00 – Inadeguato**

5.3 Gestione degli esiti

Questa fase rappresenta il momento decisionale del processo di valutazione, in cui i risultati dell'analisi vengono tradotti in una determinazione formale sullo stato di conformità del fornitore. Basandosi sui dati oggettivi raccolti attraverso il questionario di self-assessment e la documentazione di supporto, viene assegnata una delle possibili categorie di esito (approvazione, approvazione condizionata, rifiuto), seguendo un approccio strutturato e documentato. Ogni categoria di esito comporta conseguenze operative e contrattuali specifiche, che devono essere comunicate chiaramente al fornitore e alle funzioni aziendali coinvolte. La gestione degli esiti richiede un equilibrio tra rigore metodologico e pragmatismo operativo, per garantire che i controlli di sicurezza siano proporzionati al rischio effettivo e sostenibili nel tempo. Il processo decisionale viene documentato formalmente, consentendo la ricostruzione del percorso logico seguito e garantendo la coerenza delle valutazioni nel tempo.

Approvazione

- Il fornitore soddisfa i requisiti minimi per il suo livello di rischio, ovvero:
  - Tier 4: NDA firmato
  - Tier 3: Tutte le clausole contrattuali richieste presenti e accettate
  - Tier 2: Punteggio complessivo nel questionario ≥ 4.00 e nessuna criticità nei domini ad alto impatto
  - Tier 1: Documentazione aggiuntiva completa, punteggio ≥ 4.00 e nessuna criticità nei domini ad alto impatto
- Documentazione dell'esito positivo della valutazione
- Punteggio ≥ 4.00
- Nessuna criticità nei domini ad alto impatto

Approvazione condizionata

- Identificazione delle non conformità significative
- Definizione di un piano di rimedio con tempistiche
- Implementazione di controlli compensativi temporanei
- Monitoraggio dell'implementazione delle azioni correttive
- Punteggio tra 3.00 e 3.99
- Richiesto piano correttivo e approvazione CISO

Rifiuto

Il rifiuto di un fornitore avviene quando:

- Criteri oggettivi:
  - Punteggio complessivo < 3.00 nel questionario di self-assessment
  - Mancanza di documentazione essenziale richiesta per il Tier di appartenenza

- Impossibilità di implementare i controlli minimi richiesti entro tempistiche accettabili

- Criteri specifici per Tier:
  - Tier 1: Rifiuto di fornire documentazione critica (es. SOC 2, ISO 27001) o punteggio < 3.00, o score inferiore a 2.50 in domini critici (Access Control, Communications Management, Incident Management)
  - Tier 2: Punteggio < 3.00 o rifiuto di completare il questionario di self-assessment
  - Tier 3: Rifiuto di accettare una o più clausole contrattuali obbligatorie
  - Tier 4: Rifiuto di firmare l'NDA

- Linee rosse (cause di rifiuto automatico indipendentemente dal Tier e dal punteggio):
  - Storia documentata di incidenti di sicurezza gravi con gestione inadeguata negli ultimi 12 mesi
  - Violazioni normative in ambito sicurezza o privacy negli ultimi 24 mesi
  - Evidenti falsificazioni nelle risposte al questionario o nella documentazione fornita
  - Subappalto a terze parti non approvate per attività critiche, senza possibilità di controllo
  - Rifiuto di implementare controlli compensativi temporanei quando necessari

La decisione di rifiuto richiede:

- Documentazione formale delle motivazioni con evidenze oggettive
- Approvazione del CISO
- Per fornitori strategici (indipendentemente dal Tier), informativa al CTO

Dopo un rifiuto:

- Il fornitore può richiedere una nuova valutazione non prima di sei mesi, dimostrando i miglioramenti implementati
- Viene mantenuto un registro dei fornitori rifiutati con le relative motivazioni
- Nel caso di fornitore esistente, viene definito un piano di migrazione verso soluzioni alternative

Gestione delle eccezioni (solo Tier 1)

Se un fornitore Tier 1 non raggiunge il livello 5 (eccellente):

- Documentazione formale delle carenze
- Definizione di controlli compensativi specifici
- Inserimento del rischio nel Registro dei rischi
- Approvazione formale dell'eccezione da parte del CTO

6. Monitoraggio continuo

La gestione del rischio delle terze parti non si esaurisce con la valutazione iniziale, ma richiede un processo di supervisione continua per tutta la durata della relazione commerciale. Questa sezione definisce le modalità di monitoraggio periodico, la gestione delle scadenze e i trigger per le rivalutazioni non programmate. Il monitoraggio continuo riconosce la natura dinamica delle minacce alla sicurezza e l'evoluzione dei servizi forniti, garantendo che la postura di sicurezza del fornitore rimanga allineata ai requisiti di Ares 118 nel tempo. La frequenza e l'intensità dei controlli sono calibrate in base al livello di rischio, applicando maggiori risorse di supervisione dove il rischio è più elevato. Questo approccio proattivo permette di identificare tempestivamente nuovi rischi o deterioramenti nei controlli di sicurezza, consentendo interventi tempestivi prima che eventuali vulnerabilità possano trasformarsi in incidenti. Il monitoraggio continuo chiude il ciclo della gestione del rischio, trasformandolo da evento isolato a processo integrato nel ciclo di vita della relazione con il fornitore.

6.1 Revisioni programmate

- **Tier 1 (Rischio critico)**: revisione annuale obbligatoria
- **Tier 2 (Rischio alto)**: revisione ogni 18-24 mesi
- **Tier 3-4**: revisione alla scadenza del contratto o in caso di modifiche significative

6.2 Gestione delle scadenze

- Promemoria automatici per certificazioni e rapporti di audit: 2 mesi prima della scadenza
- Richiesta di certificati aggiornati alla scadenza

6.3 Rivalutazione del rischio

- In caso di incidenti di sicurezza che coinvolgono il fornitore
- In caso di modifiche sostanziali nel rapporto contrattuale
- In caso di cambiamenti dei servizi o dei dati trattati

6.3.1 Gestione della Transizione tra Livelli di Rischio

Quando un fornitore viene riclassificato a un livello di rischio superiore:

Notifica e giustificazione: Comunicazione formale al fornitore della nuova classificazione con motivazioni

Piano di adeguamento:

- Da Tier 4 a Tier 3: 30 giorni per conformarsi ai requisiti aggiuntivi
- Da Tier 3 a Tier 2: 60 giorni per completare il questionario e implementare i controlli richiesti
- Da Tier 2 a Tier 1: 90 giorni per fornire la documentazione aggiuntiva

Periodo di transizione: Durante il periodo di adeguamento:

- Monitoraggio rafforzato delle attività del fornitore
- Revisione addizionale a metà del periodo di adeguamento
- Possibile implementazione di controlli compensativi temporanei

Verifica finale: Al termine del periodo di adeguamento, verifica della conformità ai requisiti del nuovo livello

6.4 Gestione degli Incidenti con Fornitori

Un processo strutturato di gestione degli incidenti che coinvolgono i fornitori è essenziale per garantire una risposta rapida ed efficace alle violazioni di sicurezza. Questa sezione definisce le modalità di classificazione, notifica, valutazione e remediation degli incidenti, stabilendo chiare linee di responsabilità e tempistiche di intervento. La formalizzazione di questo processo assicura che le conseguenze degli incidenti siano minimizzate attraverso azioni tempestive e coordinate, e che le lezioni apprese vengano documentate per prevenire futuri eventi simili. L'approccio graduato alla gestione degli incidenti permette di calibrare la risposta in base alla gravità dell'evento, ottimizzando l'utilizzo delle risorse di sicurezza.

6.4.1 Classificazione degli Incidenti

Gli incidenti che coinvolgono fornitori sono classificati in base a criteri di impatto, durata, propagazione e natura dei servizi coinvolti, in coerenza con quanto previsto dalla Direttiva (UE) 2022/2555 (NIS2) e dalle linee guida dell'Agenzia per la Cybersicurezza Nazionale (ACN). Tale classificazione consente di calibrare le azioni di risposta e le eventuali notifiche alle autorità competenti.

Livello	Descrizione	Criteri principali	Azioni richieste
0 – Evento minore	Evento registrato che non ha prodotto impatti né sulla sicurezza né sulla continuità.	Nessun dato o sistema impattato. Nessuna interruzione o anomalia operativa.	Documentazione interna. Nessuna azione urgente.
1 – Incidente minore	Evento che ha causato un impatto limitato, senza coinvolgimento di dati sensibili o sistemi critici.	Effetti contenuti, durata < 4h, nessuna propagazione.	Contenimento interno. Notifica opzionale.
2 – Incidente rilevante	Evento con impatto su servizi non critici o dati non sensibili. Richiede azioni strutturate di contenimento o ripristino.	Durata > 4h, coinvolgimento di sistemi secondari, possibile propagazione.	Attivazione della gestione incidenti. Notifica interna obbligatoria.
3 – Incidente significativo	Evento che ha causato o è idoneo a causare grave perturbazione o perdite materiali/immateriali significative, in linea con l'art. 23 NIS2.	Coinvolgimento di dati sensibili o sistemi critici. Impatto su terzi. Durata > 12h.	Valutazione per notifica obbligatoria ad ACN. Escalation interna.
4 – Incidente critico	Evento con impatto grave e diffuso sulla continuità dei servizi essenziali o con compromissione di dati personali/sanitari.	Violazione grave, ampia propagazione, impatto sistemico o reputazionale.	Notifica immediata ad ACN, DPO, autorità competenti. Attivazione piano di risposta.

Nota: la presenza di incidenti classificati ai livelli 3 o 4 comporta l'obbligo di valutazione immediata in merito alla notifica all'ACN ai sensi della normativa vigente. La valutazione deve essere condotta in coordinamento con il Referente Sicurezza, il DPO e, ove previsto, il fornitore coinvolto.

6.4.2 Processo di Risposta agli Incidenti

Notifica iniziale:

Il fornitore deve notificare Ares 118 al verificarsi di un incidente secondo la seguente tempistica, in coerenza con la classificazione NIS2/ACN:

- ***Incidenti Gravi (Grado 4):** entro **4 ore***
- ***Incidenti Significativi (Grado 3):** entro **12 ore***
- ***Incidenti Minori (Grado 2):** entro **24 ore***
- ***Altri eventi di sicurezza (Grado 1):** entro **72 ore***

Valutazione dell'incidente:

Il CISO di Ares 118 supporta nella valutazione la segnalazione ricevuta e determina:

- *la gravità effettiva dell'incidente,*
- *l'impatto sui servizi e dati,*
- *la necessità di attivazione del piano di escalation.*

Azioni correttive:

- ***Per incidenti Grado 3 e 4:** può essere disposta la sospensione temporanea della relazione contrattuale, in attesa della verifica delle misure correttive.*
- ***Per tutti i gradi:** è richiesto al fornitore un **piano di remediation** con azioni concrete e scadenze temporali definite.*

Follow-up e verifica:

Ares 118 verifica l'implementazione delle azioni correttive e, in caso di difformità o ritardo, si riserva di attivare le clausole contrattuali di penalità o revisione dell'accordo.

Rapporto post-incidente:

Il fornitore deve fornire, entro 7 giorni dalla risoluzione dell'incidente, un report contenente almeno:

- *le cause dell'incidente (root cause analysis),*
- *l'impatto effettivo sui dati, processi e servizi,*
- *le misure correttive adottate,*
- *le misure preventive implementate per evitare recidive.*

6.4.3 Conformità alla Direttiva NIS2

In linea con la Direttiva (UE) 2022/2555 (NIS2), Ares 118 impone requisiti specifici per i fornitori che accedono a sistemi e dati critici o che operano come parte della supply chain dei servizi essenziali:

Obblighi di notifica rafforzati (Grado 3 e 4):

- **Notifica iniziale**: secondo le tempistiche già definite (4/12 ore)
- **Rapporto preliminare**: entro **12 ore**, con:
  - valutazione dell'impatto
  - misure di contenimento adottate
- **Aggiornamenti**: ogni **24 ore** fino alla completa risoluzione
- **Rapporto finale**: entro **6 giorni** dalla risoluzione

Contenuto minimo delle notifiche:

- Identificazione univoca del fornitore coinvolto
- Descrizione della natura e della tipologia dell'incidente
- Data e ora della rilevazione
- Sistemi e dati potenzialmente impattati
- Impatto geografico (eventuale coinvolgimento transfrontaliero)
- Misure tecniche attuate tempestivamente

Obblighi per fornitori Tier 1 e Tier 2:

- Simulazioni e test documentati di incident response almeno **una volta l'anno**
- Analisi congiunta dei rischi sulla catena di fornitura

- Procedure di escalation chiare e documentate
- Collaborazione con Ares 118 nella notifica all'**ACN** (Agenzia per la Cybersicurezza Nazionale), ove necessario

Conseguenze in caso di mancata conformità:

- La **mancata o ritardata notifica** costituisce **violazione contrattuale grave**
- Può comportare:
  - sospensione temporanea dei privilegi di accesso,
  - revisione del livello di fiducia assegnato al fornitore,
  - esclusione da future forniture.

Nota: Per fornitori di infrastrutture critiche o servizi essenziali, Ares118 potrà stabilire requisiti aggiuntivi in accordo con le disposizioni dell'ACN e la classificazione dell'entità secondo la NIS2.

7. Ruoli e responsabilità

L'efficacia di questa procedura dipende da una chiara attribuzione di ruoli e responsabilità all'interno di Ares 118. Questa sezione definisce il modello di governance del processo di valutazione, assicurando che ogni fase abbia un chiaro "owner" e che le necessarie separazioni di responsabilità siano rispettate. La gestione del rischio delle terze parti richiede un approccio cross-funzionale, con il coinvolgimento di diverse competenze e prospettive. La matrice RACI qui delineata stabilisce chi è Responsabile, chi Approva, chi deve essere Consultato e chi deve essere Informato per ciascuna attività chiave, eliminando ambiguità e sovrapposizioni. Questa chiara attribuzione di responsabilità garantisce accountability in ogni fase del processo, facilita la scalabilità della procedura e assicura continuità anche in caso di avvicendamento del personale coinvolto.

7.1 Matrice RACI

Attività	DG	DA	DS	DEC	RUP	REFERENTE PRIVACY	DIRETTORE ICT	RESPONSABILE CYBERSICUREZZA	CISO	DPO	RESPONSABILE RAPPORTO	SECURITY OFFICE
Prevalutazione iniziale												
Classificazione del rischio												
Invio questionario (Tier 1-2)												
Valutazione risposte questionario												
Definizione controlli correttivi												
Approvazione diretta												
Approvazione condizionata												
Approvazione con eccezioni (Tier 1)												
Rifiuto												
Monitoraggio periodico												
Gestione incidenti fornitori												
Revisione annuale procedura												

7.2 Processo di Escalation Interna

In caso di disaccordo sulla classificazione del rischio o sulle azioni da intraprendere:

- **Primo livello**: Confronto diretto tra Responsabile del rapporto e Security Office
- **Secondo livello**: Escalation al Responsabile per la Cybersicurezza che valuta la situazione e consultazione del CISO per ottenere parere
- **Terzo livello**: Per casi irrisolti o di particolare importanza strategica, escalation alla *Governance* per decisione finale

Le decisioni di escalation devono essere documentate, con motivazioni e firma dei responsabili coinvolti.

8. Documenti correlati

ISMS-ORG-MOD-01: Modulo di autovalutazione della sicurezza e della privacy

9. Dettagli sulla versione del documento

Data	Autore	Revisione	Descrizione
01-07-2025	TEAM DIGIUP/Leonardo	1.0	

10. Approvazioni

Nome	Ruolo	Data di approvazione	Firma

Appendice A: Criteri di Classificazione dei Sistemi IT

Criteri per la Classificazione dei Sistemi IT

Per rendere più oggettiva e coerente la valutazione dei sistemi IT nella scala di punteggio da 1 a 4, si faccia riferimento ai seguenti criteri:

1. Sistemi isolati/non critici (Punteggio 1)

Definizione: Sistemi con impatto operativo limitato e minima interconnessione con altri asset.

Criteri di identificazione:

- **Impatto operativo:** L'indisponibilità del sistema causa al massimo disagi minori e non blocca processi aziendali
- **Dati gestiti:** Non contiene dati confidenziali o sensibili
- **Integrazione:** Funziona autonomamente senza dipendenze da altri sistemi
- **RTO (Recovery Time Objective):** Superiore a 72 ore (può rimanere non disponibile per 3+ giorni senza impatti significativi)
- **Utenti:** Utilizzato da un numero limitato di utenti o per funzioni occasionali
- **Esempi:** Sistemi di test/staging, siti web informativi interni, sistemi di knowledge base non critici

2. Sistemi secondari (Punteggio 2)

Definizione: Sistemi che supportano processi aziendali ma non sono essenziali per le attività primarie.

Criteri di identificazione:

- **Impatto operativo:** L'indisponibilità causa inefficienze operative ma non blocca le funzioni core business
- **Dati gestiti:** Contiene dati confidenziali ma non critici
- **Integrazione:** Si interfaccia con altri sistemi ma con accoppiamento debole
- **RTO:** Tra 24 e 72 ore
- **Utenti:** Utilizzato regolarmente da più dipartimenti per attività di supporto
- **Esempi:** Sistemi di reporting, strumenti di collaborazione interna, sistemi di gestione documentale, portali intranet

3. Sistemi importanti (Punteggio 3)

Definizione: Sistemi che supportano processi aziendali significativi e la cui indisponibilità impatta la capacità operativa.

Criteri di identificazione:

- **Impatto operativo:** L'indisponibilità compromette significativamente l'efficienza aziendale, causando potenziali perdite economiche
- **Dati gestiti:** Contiene dati critici per il business o dati personali in volumi significativi
- **Integrazione:** Fortemente integrato con altri sistemi aziendali, con dipendenze bidirezionali
- **RTO:** Tra 4 e 24 ore
- **Utenti:** Utilizzato quotidianamente da gran parte dell'organizzazione
- **Regolamentazione:** Soggetto a requisiti di compliance specifici
- **Esempi:** CRM, sistemi HR, sistemi di pianificazione della produzione, portali clienti/fornitori

4. Sistemi critici/core (Punteggio 4)

Definizione: Sistemi essenziali per la continuità operativa dell'azienda e la cui indisponibilità ha impatto immediato sul core business.

Criteri di identificazione:

- **Impatto operativo:** L'indisponibilità causa interruzione immediata di processi critici con gravi perdite economiche o danni reputazionali
- **Dati gestiti:** Contiene dati altamente sensibili, strategici o soggetti a severe normative di protezione
- **Integrazione:** Costituisce il nucleo dell'infrastruttura IT con cui si interfacciano la maggior parte degli altri sistemi
- **RTO:** Inferiore a 4 ore, spesso con requisiti di alta disponibilità (99.9%+)
- **Utenti:** Impatta direttamente clienti, fornitori o la maggior parte delle operazioni interne
- **Regolamentazione:** Soggetto a severi requisiti normativi (es. GDPR, NIS2)
- **Esempi:** ERP, sistemi di produzione, sistemi di controllo industriale (SCADA), sistemi di pagamento, infrastrutture cloud principali, sistemi di sicurezza fisica

Appendice B: Classificazione delle Aree Fisiche

Definizione di Area Sensibile/Critica

Nota sulla Classificazione delle Aree Fisiche:

Ai fini di questa procedura, le aree fisiche sono classificate come segue:

Aree Sensibili/Critiche

Spazi fisici la cui compromissione potrebbe causare:

- Impatti significativi sulla continuità operativa
- Accesso non autorizzato a informazioni riservate
- Danni a infrastrutture critiche
- Violazioni normative rilevanti
- Rischi per la sicurezza delle persone

Esempi di aree sensibili/critiche:

- Data center e locali server
- Sale di controllo operativo
- Archivi di documentazione riservata (fisica o digitale)
- Laboratori R&D e aree di test
- Aree di produzione ad alta sicurezza
- Uffici della direzione con accesso a informazioni strategiche
- Locali tecnici con sistemi di supporto critici (es. alimentazione, condizionamento)

Aree Non Sensibili

Spazi fisici la cui compromissione avrebbe impatti contenuti e gestibili.

Esempi di aree non sensibili:

- Uffici amministrativi generici
- Sale riunioni standard
- Aree comuni (mensa, corridoi, reception)
- Aree di produzione standard (non contenenti processi o informazioni critiche)
- Nel contesto sanitario: aree amministrative, sale d'attesa, corridoi pubblici

Frequenza di Accesso

- **Occasionale**: accesso sporadico, tipicamente meno di una volta al mese
- **Regolare**: accesso frequente, settimanale o quotidiano

La classificazione delle aree deve essere documentata formalmente nel piano di sicurezza fisica aziendale e rivista periodicamente (almeno annualmente) o in seguito a modifiche significative nell'organizzazione degli spazi.

Appendice C: Guida Pratica all'Integrazione della Sicurezza nel Procurement

C.1 Introduzione e scopo

Questa appendice fornisce esempi pratici, casi d'uso e strumenti implementativi per integrare efficacemente le valutazioni di sicurezza delle terze parti nel ciclo di procurement di Ares 118. Lo scopo è tradurre i requisiti formali della procedura in azioni concrete che possano essere facilmente implementate dai team di procurement, sicurezza e dalle business unit.

C.2 Esempi di Applicazione per Fase

C.2.1 Fase di selezione iniziale

Esempio 1: Fornitore di servizi cloud (Tier 1)

Scenario: Ares 118 necessita di un nuovo fornitore di servizi cloud per ospitare applicazioni che gestiscono dati di produzione e informazioni sensibili.

Azioni di sicurezza:

- Il Responsabile IT completa la prevalutazione utilizzando lo schema in sezione 3.1, ottenendo un punteggio di 32 (Tier 1) considerando:
  - Accesso a dati sensibili/strategici (+4)
  - Integrazione con sistemi critici/core (+4)
  - Criticità elevata per il business (+4)
- Nel documento RFP vengono inseriti i seguenti requisiti di sicurezza obbligatori:
  - Certificazione ISO 27001 in corso di validità
  - Certificazione SOC 2 Tipo II degli ultimi 6 mesi
  - Capacità di crittografia dei dati a riposo e in transito
  - Controlli di accesso con autenticazione multifattore
  - Separazione fisica e logica dell'infrastruttura (multi-tenancy sicura)
  - SLA di notifica incidenti entro quattro ore
  - Possibilità di eseguire penetration test con approvazione

Documentazione prodotta:

- Scheda di prevalutazione del rischio completata
- Sezione di sicurezza all'interno della RFP con requisiti dettagliati
- Questionario preliminare di sicurezza da compilare con la risposta alla RFP

Esempio 2: Fornitore di servizi di formazione (Tier 3)

Scenario: Ares118 ricerca un provider di servizi di formazione per il personale di produzione.

Azioni di sicurezza:

- La prevalutazione assegna un punteggio di 12 (Tier 3) considerando:
  - Accesso occasionale a dati aziendali non sensibili
  - Nessuna integrazione con sistemi IT critici
  - Servizio importante ma con alternative disponibili

- Il documento RFI (Request for Information) include:
  - Requisito di conformità alle politiche di sicurezza di Ares118
  - Clausola di riservatezza per materiali formativi proprietari
  - Richiesta di un referente per la sicurezza

Documentazione prodotta:

- Scheda di prevalutazione del rischio semplificata
- Sezione minimale sulla sicurezza all'interno del documento RFI

C.2.2 Fase di valutazione delle offerte

Esempio 1: Sistema di tracciabilità della filiera alimentare (Tier 1)

Scenario: Valutazione di fornitori per un sistema di tracciabilità completa della filiera, cruciale per la sicurezza alimentare e conformità normativa.

Processo di valutazione:

- Il criterio "sicurezza" pesa il 30% del punteggio complessivo
- La valutazione di sicurezza considera:
  - Completezza delle certificazioni (40%)
  - Risposta al questionario di sicurezza (30%)
  - Demo delle funzionalità di sicurezza e tracciabilità (20%)
  - Referenze di sicurezza verificabili nel settore alimentare (10%)

Confronto fornitori (esempio):

Criterio	**Peso**	**Fornitore A**	**Fornitore B**
Prezzo	40%	90/100 (miglior prezzo)	75/100 (15% più costoso)
Funzionalità	30%	80/100	85/100
Sicurezza	30%	65/100 (mancano controlli di integrità dei dati)	95/100 (eccellente con blockchain)
Punteggio finale	100%	**79/100**	**84/100**

Risultato: Viene selezionato il Fornitore B nonostante il costo maggiore, data la criticità del sistema per la sicurezza alimentare e la conformità alle normative di tracciabilità.

Esempio 2: Fornitore di dispositivi IoT per monitoraggio temperatura (Tier 2)

Scenario: Valutazione di fornitori di sensori IoT per il monitoraggio della temperatura nelle celle frigorifere.

Processo di valutazione:

- La sicurezza pesa il 20% del punteggio complessivo
- Aspetti di sicurezza valutati:
  - Sicurezza delle comunicazioni wireless (crittografia)
  - Protezione dei dati raccolti
  - Gestione aggiornamenti firmware e patch di sicurezza
  - Protezione dell'interfaccia di gestione

Confronto fornitori (esempio):

Criterio	Peso	Fornitore X	Fornitore Y
Prezzo/prestazioni	50%	85/100	80/100
Durabilità/affidabilità	30%	75/100	90/100
Sicurezza	20%	60/100 (firmware non aggiornabile)	85/100 (crittografia avanzata, aggiornamenti OTA)
Punteggio finale	100%	**77/100**	**84/100**

Risultato: Fornitore Y selezionato grazie alla maggiore durabilità e funzionalità di sicurezza, nonostante il costo leggermente superiore. Il sistema di monitoraggio temperatura è considerato critico per la sicurezza alimentare.

C.2.3 Fase di contrattualizzazione

Esempio 1: Software ERP (Tier 1)

Elementi di sicurezza nel contratto:

- Allegato dedicato alle misure di sicurezza (10 pagine) che include:
  - Requisiti di autenticazione avanzata (MFA) per tutti gli accessi amministrativi
  - Crittografia completa del database e dei backup
  - Segregazione degli ambienti (sviluppo, test, produzione)
  - Procedure di gestione dei cambiamenti con approvazione formale
  - Requisiti di protezione API e integrazione sicura con altri sistemi
- KPI specifici per la sicurezza:
  - Tempo di implementazione patch critiche: max 7 giorni
  - Tempo di risposta a incidenti critici: max 30 minuti
  - Disponibilità del sistema: 99.95% in orario operativo
  - Frequenza penetration test: semestrale
- Penali finanziarie per violazioni della sicurezza:
  - 5% del valore mensile per ogni giorno di ritardo nell'applicazione di patch critiche
  - 10% del valore annuale per violazioni di dati dovute a vulnerabilità note e non corrette
- Piano di exit strategy con procedure di migrazione dati e know-how

Esempio 2: Sistema di controllo qualità e sicurezza alimentare (Tier 1)

Elementi di sicurezza nel contratto:

- Allegato dedicato alle misure di sicurezza (8 pagine) che include:
  - Requisiti di integrità dei dati per test di qualità e sicurezza alimentare
  - Procedure di autenticazione e gestione accessi al sistema HACCP
  - Requisiti di logging e audit trail per dimostrare conformità alle autorità
  - Procedure di backup e disaster recovery per dati sensibili di produzione
- KPI specifici per la sicurezza:
  - Tempo di risposta a incidenti critici: max 30 minuti
  - Tempo di notifica per problemi di integrità dati: max 4 ore
  - Disponibilità del sistema di monitoraggio: 99.99%
  - Frequenza test di ripristino dati: mensile
- Penali finanziarie per violazioni della sicurezza:
  - 5% del valore mensile per ogni ora di indisponibilità durante la produzione
  - 10% del valore annuale per perdita di dati di tracciabilità non recuperabili

- Diritto di audit con 24 ore di preavviso
- Piano di exit strategy con procedure sicure di migrazione dati di tracciabilità

C.2.4 Rinnovi contrattuali

Esempio 1: Aggiornamento infrastructure-as-code (Tier 1)

Scenario: Un fornitore di servizi di automazione dell'infrastruttura cloud in uso da 2 anni deve rinnovare il contratto. Nel frattempo, Ares 118 ha implementato nuovi controlli di sicurezza DevSecOps.

Azioni:

- Esecuzione di una nuova valutazione di rischio completa
- Identificazione gap rispetto ai nuovi requisiti:
  - Necessità di scanning automatico di vulnerabilità in pipeline CI/CD
  - Scansione delle immagini container prima del deployment
  - Implementazione di controlli per prevenire modifiche non autorizzate all'infrastruttura
  - Logging centralizzato di tutte le modifiche all'infrastruttura
- Negoziazione di un addendum al contratto con i nuovi requisiti
- Piano di implementazione con milestone vincolanti entro 60 giorni dal rinnovo

Esempio 2: Software di etichettatura prodotti (Tier 2)

Scenario: Un fornitore di software per etichettatura prodotti in uso da 3 anni deve rinnovare il contratto. Nel frattempo, sono entrate in vigore nuove normative sulla tracciabilità e dichiarazione allergeni.

Azioni:

- Esecuzione di una nuova valutazione di rischio completa
- Identificazione gap rispetto ai nuovi requisiti:
  - Necessità di integrazione con database allergeni centrale
  - Requisiti di audit trail completo per modifiche alle etichette
  - Verifica automatica di conformità normativa
- Negoziazione di un addendum al contratto con i nuovi requisiti
- Piano di implementazione con milestone vincolanti entro 90 giorni dal rinnovo

C.3 Template e Checklist

C.3.1 Checklist per la Fase di Selezione Iniziale

Checklist pre-RFP/RFI per terze parti:

- Completata prevalutazione del rischio (Sezione 3.1)
- Identificato il Tier di rischio (1-4)
- Consultato Security Office per fornitore Tier 1-2
- Documentate motivazioni dei punteggi assegnati
- Identificati requisiti di sicurezza da includere in RFP/RFI
- Preparato questionario di sicurezza preliminare (se necessario)
- Verificata l'assenza del fornitore da blacklist di sicurezza
- Identificate certificazioni di sicurezza richieste

C.3.2 Checklist per la Valutazione delle Offerte

Criteri di sicurezza da valutare:

- Completezza e qualità delle risposte al questionario di sicurezza
- Validità e ambito delle certificazioni presentate
- Adeguatezza delle politiche di sicurezza del fornitore
- Qualità del processo di gestione incidenti
- Risultati di eventuali audit/penetration test
- Controlli di background su incidenti di sicurezza pregressi
- Presenza e qualità di un SOC (Security Operation Center)
- Capacità di garantire continuità operativa
- Conformità normativa specifica del settore
- Processo di gestione degli accessi e identity management

C.3.3 Template di Sezione di Sicurezza per Contratti

Template per Fornitore Tier 1 (Rischio Critico)

ALLEGATO X - REQUISITI DI SICUREZZA

1. DEFINIZIONI
   [Definire termini chiave: Incidente di Sicurezza, Dati Confidenziali, ecc.]
2. REQUISITI GENERALI DI SICUREZZA
   2.1 Il Fornitore si impegna a mantenere attive e valide per l'intera durata del contratto le seguenti certificazioni:
   - ISO 27001:2013 o successiva
   - SOC 2 Tipo II
   [Altre certificazioni specifiche]
   2.2 Il Fornitore si impegna a implementare e mantenere un sistema di gestione della sicurezza delle informazioni conforme alle best practice del settore.
3. CONTROLLI DI SICUREZZA SPECIFICI
   3.1 Controllo Accessi
   [Dettagli sui requisiti di autenticazione, MFA, privileged access, ecc.]
   3.2 Crittografia
   [Standard di crittografia richiesti per dati a riposo e in transito]
   3.3 Sicurezza Fisica
   [Requisiti per l'accesso ai data center e altre strutture sensibili]
   3.4 Business Continuity
   [RTO, RPO, requisiti di disaster recovery, test periodici]
   3.5 Gestione Vulnerabilità
   [Requisiti di patching, scanning, penetration test]
4. NOTIFICA INCIDENTI
   4.1 Il Fornitore notificherà ad Ares118 qualsiasi Incidente di Sicurezza entro [X] ore dalla scoperta.
   4.2 Processo dettagliato di gestione incidenti... [dettagli]
5. AUDIT E VERIFICHE
   5.1 Ares118 si riserva il diritto di condurre audit di sicurezza con preavviso di [X] giorni.
   5.2 Il Fornitore fornirà report di sicurezza mensili contenenti... [dettagli]
6. SUBRESPONSABILI
   [Requisiti per approvazione e controllosubresponsabili)
7. LIVELLI DI SERVIZIO (SLA) RELATIVI ALLA SICUREZZA
   [Tabella di SLA con metriche, target e penali]
8. GESTIONE DEL FINE RAPPORTO
   [Procedure sicure di restituzione o cancellazione dati]

B.3.4 Template di Report di Valutazione Sicurezza

REPORT DI VALUTAZIONE SICUREZZA FORNITORE

Fornitore: [Nome Fornitore]
Data valutazione: [Data]
Valutatore: [Nome]
Tier di rischio: [1-4]
1. RISULTATI PRE-VALUTAZIONE

Punteggio totale: [XX/40]
Fattori determinanti: [Elenco dei principali fattori che hanno influenzato la classificazione]
2. QUESTIONARIO SELF-ASSESSMENT
Punteggio complessivo: [X.XX/5.00]
Punti di forza: [Elenco]
Aree di miglioramento: [Elenco]
Punteggi per dominio:
- Security Policy: [X.XX/5.00]
- Organisation of Information Security: [X.XX/5.00]
- [Continuare per tutti i domini]
3. VERIFICA CERTIFICAZIONI
[Elenco certificazioni verificate con date di validità]
4. AZIONI RICHIESTE
[Elenco di controlli correttivi richiesti con tempistiche]
5. RACCOMANDAZIONE FINALE
[ ] Approvazione
[ ] Approvazione condizionata
[ ] Rifiuto
Motivazione: [Dettagli sulla decisione]
6. APPROVAZIONI
Figura interna: [Nome, Data]

C.4 Considerazioni speciali per fornitori tecnologici

C.4.1 Criticità dei fornitori tecnologici

I fornitori di tecnologia meritano un'attenzione particolare nel processo di valutazione della sicurezza poiché:

1. **Accesso privilegiato:** Spesso richiedono accessi con elevati privilegi ai sistemi Ares 118
2. **Integrazioni profonde:** Si interfacciano con molteplici sistemi critici contemporaneamente
3. **Distanza dal core business:** Il personale IT potrebbe non rilevare anomalie funzionali come invece farebbero gli esperti di produzione alimentare
4. **Aggiornamenti e patch:** Richiedono procedure specifiche per gestire gli aggiornamenti senza compromettere la sicurezza

C.4.2 Valutazioni aggiuntive per fornitori tecnologici

Per i fornitori di servizi tecnologici, oltre alla valutazione standard, verificare:

- **Processo di Secure Development:** Pratiche di sicurezza nel ciclo di sviluppo del software
- **Gestione delle vulnerabilità:** Tempi di risposta a CVE critiche e processo di patch management
- **Crittografia e gestione chiavi:** Metodi di crittografia e gestione sicura delle chiavi
- **Controllo degli accessi privilegiati:** Meccanismi di protezione degli account amministrativi
- **Procedure di backup e disaster recovery:** Frequenza, test di ripristino, conservazione offsite

C.5 Gestione dei Casi Particolari

C.5.1 Fornitori Esistenti (Retroattività)

Processo di adeguamento:

1. **Pianificazione:** Creare un inventario dei fornitori esistenti e classificarli per priorità in base a:
   - Criticità per il business
   - Tipologia di dati gestiti
   - Scadenza contrattuale
2. **Comunicazione:** Informare i fornitori esistenti del nuovo processo con:

- Lettera formale che spiega i nuovi requisiti
- Timeline di implementazione (tipicamente 6-12 mesi)
- Conseguenze del mancato adeguamento

3. **Valutazione graduale:**
   - Iniziare con i fornitori più critici (Tier 1)
   - Procedere con un'implementazione a fasi (3-6-9-12 mesi)
   - Prevedere sessioni di supporto per i fornitori con difficoltà di adeguamento
4. **Gestione delle non conformità:**
   - Per fornitori critici non conformi: sviluppare piani di rimedio con milestone vincolanti
   - Per fornitori non critici: valutare la sostituzione alla scadenza contrattuale
   - Per casi intermedi: implementare controlli compensativi temporanei

C.5.2 Acquisizioni e Fusioni

Quando Ares 118 acquisisce una nuova azienda o si fonde con essa, è necessario:

1. **Due diligence di sicurezza preacquisizione:**
   - Valutare i fornitori della società target come parte del processo di due diligence
   - Identificare rischi critici di sicurezza legati ai fornitori esistenti
2. **Fase di integrazione:**
   - Creare un inventario completo dei fornitori della società acquisita
   - Applicare la prevalutazione a tutti i fornitori
   - Pianificare la valutazione completa dei fornitori Tier 1 e 2 entro 90 giorni
   - Armonizzare contratti e requisiti di sicurezza
3. **Possibili approcci:**
   - **Fast-track**: Mantenimento dei fornitori esistenti con adeguamento accelerato
   - **Phased**: Adeguamento graduale basato su priorità e scadenze contrattuali
   - **Consolidation**: Sostituzione dei fornitori duplicati con quelli già approvati

C.5.3 Gestione delle Emergenze

In situazioni di emergenza dove è necessario ingaggiare rapidamente un fornitore:

1. **Processo accelerato:**
   - Completare sempre lo schema di pre-valutazione del rischio come descritto nella sezione 3.1 (tempo stimato: 1-2 ore) per determinare il Tier di rischio
   - Per fornitori Tier 3-4: procedere con approvazione temporanea (max 30 giorni)
   - Per fornitori Tier 1-2: implementare controlli compensativi immediati, tra cui:
     - Accesso limitato e supervisionato
     - Monitoraggio rafforzato
     - Segregazione dai sistemi critici quando possibile
     - NDA rafforzato con clausole penali
2. **Regolarizzazione post-emergenza:**
   - Completare la valutazione completa entro 30 giorni dall'ingaggio
   - Implementare tutti i controlli richiesti o terminare la relazione
3. **Approvazione:**
   - L'approvazione di emergenza richiede firma Direttore Generale per Tier 3-4
   - L'approvazione di emergenza richiede firma Direttore Sanitario o Direttore Amministrativo per Tier 1-2
   - Tutte le approvazioni di emergenza devono essere registrate e motivate

C.6 Indicatori di Successo e KPI

Per valutare l'efficacia dell'integrazione della sicurezza nel procurement, si suggerisce di monitorare i seguenti indicatori:

C.6.1 KPI di Processo

- % di nuovi fornitori sottoposti a prevalutazione prima della contrattualizzazione (target: 100%)
- Tempo medio di completamento della valutazione di sicurezza (target: Tier 1: 15 giorni, Tier 2: 10 giorni, Tier 3-4: 5 giorni)
- % di fornitori Tier 1-2 con questionario di self-assessment aggiornato (target: 100%)
- % di contratti con clausole di sicurezza appropriate al Tier (target: 100%)

C.6.2 KPI di Efficacia

- Numero di incidenti di sicurezza originati da terze parti (target: riduzione annua del 20%)
- % di fornitori che soddisfano tutti i requisiti di sicurezza senza eccezioni (target: >90%)
- Tempo medio di risoluzione delle non conformità di sicurezza (target: <60 giorni)
- % di rinnovi contrattuali preceduti da rivalutazione della sicurezza (target: 100%)

C.6.3 Dashboard di Monitoraggio

Dashboard di monitoraggio:

- Status di sicurezza di tutti i fornitori Tier 1-2 (codice colore: verde, giallo, rosso)
- Scadenze imminenti (certificazioni, audit, revisioni)
- Non conformità aperte con stato di avanzamento
- Trend degli incidenti di sicurezza per fornitore
- Statistiche comparative tra diversi dipartimenti/business unit

SISTEMA SANITARIO REGIONALE
ARES 118

REGIONE LAZIO

ATTESTATO DI PUBBLICAZIONE

Deliberazione N° **1212** del **30/12/2025**

Si dichiara che, ai sensi dell'art. 31 L. R. Lazio 45/1996 e del combinato disposto degli artt. 32 L. 69/2009 e 12 L. R. Lazio 1/2011, la presente deliberazione è pubblicata in data ***30/12/2025*** *sull'Albo pretorio, consultabile sul sito web istituzionale www.ares118.it, per rimanervi affissa 15 giorni consecutivi e contestualmente resa disponibile al Collegio Sindacale.*

Il direttore UOC Affari Generali (o suo sostituto)
Fulvia Casati
(Firmato digitalmente)