Repertorio: **Decreti del Commissario Straordinario** classif.: I/3

rep. / data: *vedi segnatura.xml* allegati: 1

Oggetto: Sistema di gestione della sicurezza delle informazioni (ISO/IEC 27001:2022). Adozione del documento "D1 - Contesto e Governo" - anno 2025

Note per la trasparenza

Struttura competente:	Direzione - Ufficio Supporto Giuridico alla Direzione e gestione documentale
Contenuto del provvedimento:	Il provvedimento dispone l'adozione del documento denominato “D1 - Contesto e Governo” per l'anno 2025 che definisce l'ambito del Sistema di gestione della sicurezza delle informazioni (SGSI), la politica e l'individuazione di ruoli e responsabilità, secondo la norma ISO/IEC 27001:2022

La sicurezza dei sistemi d'informazione è uno dei requisiti previsti dai regolamenti dell'Unione Europea che definiscono i criteri per il riconoscimento degli organismi pagatori istituiti dagli Stati membri.

A partire dal 16 ottobre 2016 tale requisito è obbligatorio per tutti gli organismi pagatori che non abbiano già provveduto ad adeguare i propri sistemi d'informazione alla norma internazionale di riferimento (ISO/IEC 27001).

Lo standard ISO/IEC 27001 è una norma internazionale che definisce i requisiti e le regole per impostare e gestire un Sistema di gestione della sicurezza delle informazioni (SGSI o ISMS dall'inglese Information security management system). La norma ha quindi l'obiettivo di garantire la sicurezza delle informazioni, intesa come la difesa delle caratteristiche di disponibilità, riservatezza e integrità delle stesse, nonché dei documenti che le contengono.

Secondo quanto disposto dal punto 5 della norma ISO/IEC 27001:2022, relativo alla Leadership, l'alta Direzione stabilisce una politica per la sicurezza delle informazioni che deve comprendere in particolare gli obiettivi aziendali e un impegno a soddisfare i requisiti richiesti in materia di sicurezza delle informazioni e il documento “D1 - Contesto e Governo”, aggiornato annualmente, costituisce un punto cardine della politica della sicurezza dell’Agenzia.

Tutto ciò premesso e considerato,

IL COMMISSARIO STRAORDINARIO

RICHIAMATA la legge regionale 9 novembre 2001, n. 31 “Istituzione dell'Agenzia veneta per i pagamenti” (AVEPA) così come da ultimo modificata dalla legge regionale del 4 luglio 2023, n. 14;

DATO ATTO che con deliberazione n. 370 del 4 aprile 2024 la Giunta regionale del Veneto ha conferito a Fabrizio Stella l'incarico di Commissario Straordinario dell'AVEPA, con decorrenza 16 aprile 2024, prorogato con DGR n. 1169 del 15 ottobre 2024;

VISTO il regolamento delegato (UE) n. 907/2014 della Commissione dell'11 marzo 2014, il quale stabilisce all'Allegato I, articolo 1, paragrafo 3, lettera b) che la sicurezza dei sistemi d'informazione è certificata in conformità con l'Organizzazione internazionale per la standardizzazione 27001: Sistemi di gestione della sicurezza delle informazioni - Requisiti (ISO). Tale previsione non si applica agli organismi pagatori responsabili della gestione e del controllo di una spesa annuale non superiore a 400 milioni di euro;

PRESO ATTO che il 1° ottobre 2013 è stata pubblicata la norma ISO/IEC 27001:2013, la quale sostituisce la norma ISO/IEC 27001:2005; il 25 ottobre 2022 è stata poi pubblicata la ISO/IEC 27001:2022, recepita in Europa come EN ISO/IEC 27001:2023 (pubblicata il 26 luglio 2023). In Italia l'edizione 2022 è stata recepita come UNI CEI EN ISO/IEC 27001:2024 (pubblicata il 20 febbraio 2024, in vigore dal 25 gennaio 2024);

ACCERTATO l'avvenuto regolare svolgimento dell'istruttoria relativa alla formazione del presente decreto e la sua conformità alla normativa vigente;

DATO ATTO che il presente provvedimento non comporta alcun impegno di spesa;

DECRETA

1. di adottare, per le motivazioni esposte in premessa, il documento “D1 - Contesto e Governo” anno 2025 (**allegato A**);

2. di pubblicare nel sito SharePoint, Portale per la sicurezza delle informazioni di AVEPA, il documento “D1 - Contesto e Governo” anno 2025.

Il Commissario Straordinario
Fabrizio Stella
(sottoscritto con firma digitale)

D1

CONTESTO E GOVERNO

Contesto in cui opera AVEPA, ambito di applicazione, politica di sicurezza, ruoli e responsabilità

DESCRIZIONE DOCUMENTO	
AUTORE	Giacomo Odoni
VERSIONE	6.0.01
DATA ULTIMA REVISIONE	2024.12.16
STATO DOCUMENTO	APPROVATO
APPROVAZIONE	Direzione
CLASSIFICAZIONE	PUBBLICO
DIVULGAZIONE	Pubblicazione SharePoint aziendale e comunicazione alle parti interessate

INDICE

1. TRATTAMENTO DEL DOCUMENTO

1.1 Distribuzione del documento

Il presente documento (rif. art. 5.2 ISO 27001:2022) deve:

- essere diffuso all'interno dell'AVEPA (di seguito anche “Agenzia”), portandone a conoscenza tutti i dipendenti attraverso la pubblicazione nel sito SharePoint aziendale;
- essere reso disponibile per le eventuali altre parti interessate, limitatamente agli argomenti di loro interesse.

1.2 Approvazione ed archiviazione del documento

La versione definitiva del Documento è approvata e adottata con decreto del Commissario Straordinario dell'AVEPA, registrato all’interno del sistema di gestione documentale dell’Agenzia (Docway) nel repertorio “Decreti del Commissario”, accessibile a tutti i dipendenti.

1.3 Data di inizio validità

La data di inizio validità coincide con la data di approvazione del decreto di adozione da parte del Commissario Straordinario dell'AVEPA.

1.4 Scopo del documento

Con il presente documento si vuole presentare il contesto in cui opera l'AVEPA (rif. art. 4 ISO 27001:2022), definire l'impegno della Direzione attraverso una politica per la sicurezza delle informazioni, stabilire i ruoli e le responsabilità (rif. art. 5 ISO 27001:2022). Per raggiungere tale obiettivo questo documento si propone di:

- presentare un quadro strutturale per la collocazione degli obiettivi relativi alla sicurezza delle informazioni (rif. art. 4 norma ISO 27001:2022);
- formalizzare l'impegno della Direzione a soddisfare i requisiti relativi alla sicurezza delle informazioni;
- definire l'ambito di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI);
- identificare i ruoli e le responsabilità per l'implementazione e la manutenzione di un appropriato SGSI continuamente migliorato (rif. art. 5 norma ISO 27001:2022).

1.5 Versioni

- 2024.12.16 – Giacomo Odoni: aggiornamento contenuti, revisione finale.
- 2024.11.20 – Giacomo Odoni: prima stesura.

1.6 Abbreviazioni e termini utilizzati

- AVEPA = Agenzia veneta per i pagamenti
- SUA = Sportello unico agricolo
- AGEA = Agenzia per le erogazioni in agricoltura
- AAC = AVEPA, Area amministrazione e contabilità
- ACS = AVEPA, Area controllo strategico, contabilizzazione e recupero crediti
- AIT = AVEPA, Area integrazione territoriale e supporto alla Direzione
- ATC = AVEPA, Area tecnica competitività imprese
- ATP = AVEPA, Area tecnica pagamenti diretti
- DIR = AVEPA, Direzione
- SIT = AVEPA, Area servizi IT
- SGSI = Sistema di Gestione per la Sicurezza delle Informazioni

2. AVEPA E IL CONTESTO IN CUI OPERA

2.1 Presentazione dell'Agenzia

L'Agenzia Veneta per i Pagamenti (AVEPA) è un ente strumentale istituito dalla Regione del Veneto per svolgere inizialmente funzioni di organismo pagatore regionale (OPR) degli aiuti, dei premi e dei contributi nel settore agricolo. Negli anni le competenze dell'ente sono cresciute e si sono diversificate, assorbendo una serie di deleghe regionali, tra cui la funzione di organismo intermedio per la gestione di parte del Programma Operativo Regionale (POR) FESR 2014-2020 della Regione del Veneto e, da ultimo, la gestione degli strumenti finanziari regionali per la concessione di finanziamenti a sostegno delle imprese.

L'AVEPA è un ente di diritto pubblico dotato di autonomia amministrativa, organizzativa, contabile e patrimoniale nei limiti previsti dalla legge istitutiva (legge regionale 9 novembre 2001, n. 31) in quanto tale, l'Agenzia è soggetta ai poteri di indirizzo e controllo spettanti alla Giunta regionale, nel rispetto delle forme di autonomia di cui gode.

L'Agenzia ha iniziato la propria attività nel 2002 e nello stesso anno ha ottenuto il primo riconoscimento ad operare in qualità organismo pagatore da parte dell'allora Ministero delle politiche agricole (ora Ministero dell'agricoltura, della sovranità alimentare e delle foreste); in seguito, nel 2003 e nel 2004, il riconoscimento ministeriale è stato esteso ad ulteriori settori di intervento.

Dal 2011 l'Agenzia ha incorporato le strutture e le funzioni degli ex Ispettorati regionali dell'agricoltura, divenendo il punto di riferimento a livello regionale per l'erogazione di servizi pubblici dedicati al mondo agricolo.

Dal 2017 l'Agenzia svolge le funzioni di organismo intermedio, ai sensi dell'art. 123 par. 7 del Regolamento (UE) n. 1303/2013, per la gestione di parte del Programma Operativo Regionale (POR) FESR 2014-2020 della Regione del Veneto.

L'AVEPA è strutturata nel territorio con una sede centrale a Padova e una sede periferica per ogni capoluogo di provincia del Veneto (denominata Sportello unico agricolo - SUA).

Ulteriori informazioni relative all'Agenzia e alle sue attività sono consultabili nella sezione “Agenzia” del sito web istituzionale *www.avepa.it*.

2.2 Soggetti interni ed esterni

L'Agenzia nello svolgimento della propria attività entra in contatto con numerosi soggetti interni ed esterni. La definizione dei “Ruoli e Responsabilità” interne è presente nel capitolo dedicato in questo stesso documento. Le principali parti interessate sono rappresentate da:

- la Direzione dell'AVEPA, organo di vertice dell'Agenzia rappresentato dal Commissario, nominato direttamente dal Presidente della Giunta regionale;
- i Dirigenti di Area, di Settore e degli Sportelli Unici dell'Agenzia, i quali partecipano alla sicurezza attraverso coinvolgimento specifico durante le riunioni;
- il personale dell'AVEPA, tutto il personale dipendente che concorre alla mission aziendale con le proprie competenze; tra questi si segnalano le “Elevate qualificazioni” che supportano il management nel raggiungimento degli obiettivi aziendali;
- i beneficiari dell'AVEPA, ovvero tutti i soggetti che usufruiscono dei vari servizi offerti dall'Agenzia;
- i soggetti che collaborano con l'AVEPA, ovvero tutti i soggetti esterni che concorrono con l'AVEPA, attraverso convenzioni, per il raggiungimento degli obiettivi aziendali attraverso competenze precise; in ambito agricolo i più rilevanti sono i Centri di assistenza agricola (CAA) ed i liberi professionisti accreditati, che gestiscono il fascicolo aziendale;
- i fornitori/outsourcer, soggetti terzi con cui l'AVEPA stipula contratti o sottoscrive Accordi Quadro o aderisce a Concessioni che contribuiscono in qualità di partner agli obiettivi dell'Agenzia;
- i soggetti istituzionali, quali la Regione del Veneto, la Commissione Europea, il Ministero dell’Agricoltura, della Sovranità Alimentare e delle Foreste (Masaf), ecc.;
- i certificatori dei conti, individuati dalla Commissione europea per verificare la correttezza dell'operato dell'Agenzia;
- le forze di polizia e l'autorità giudiziaria, con cui l'AVEPA intrattiene comunicazioni per controlli di varia natura.

L'Agenzia è inoltre soggetta ad attività di vigilanza e controllo da parte di alcuni soggetti istituzionali quali:

- Regione del Veneto: il Consiglio regionale definisce gli indirizzi per l'attività dell'Agenzia e ne controlla l'attuazione attraverso la competente Commissione Consiliare; la Giunta Regionale esercita funzioni di vigilanza e controllo definendo gli indirizzi in materia di organizzazione, funzionamento, dotazione organica e risorse finanziarie dell'Agenzia;
- Ministero dell’agricoltura, della sovranità alimentare e delle foreste (Masaf): esercita una costante supervisione sull'AVEPA e gli altri organismi pagatori regionali in relazione al mantenimento dei criteri di riconoscimento previsti dall’allegato I del Reg. (UE) 907/2014 ora sostituito dall’allegato I del Regolamento Delegato (UE) 2022/127 della Commissione del 7 dicembre 2021;
- Agenzia per le erogazioni in agricoltura (AGEA): funge da organismo di coordinamento

degli organismi pagatori;

- Commissione Europea: effettua varie attività di controllo di natura contabile e amministrativa sui contenuti dei conti annuali e delle rendicontazioni periodiche ai fini della liquidazione dei conti degli organismi pagatori. Sulla base di specifiche analisi dei rischi effettua attività di audit relative alle attività degli organismi pagatori, verificandone il rispetto dei criteri di riconoscimento;
- Corte dei Conti Europea: svolge attività di controllo sull'utilizzo dei fondi dell'Unione europea;
- Organismi di certificazione: sono i soggetti esterni indipendenti che esaminano i conti, il sistema di controllo e la compliance normativa dell'AVEPA.

2.3 Riferimenti normativi

Nella sezione “Amministrazione trasparente” del sito dell’Agenzia, al link di seguito riportato, è possibile consultare un elenco delle norme e dei regolamenti che disciplinano l’organizzazione e l’attività dell’Agenzia: https://www.avepa.it/riferimenti-normativi

2.4 L'adozione dello standard ISO 27001

Il percorso che l'Agenzia ha intrapreso per adottare lo standard ISO 27001 è iniziato nel 2005 quando, secondo quanto disposto dall'allegato I al regolamento (CE) n. 885/2006, abrogato dal regolamento delegato (UE) n. 907/2014 a sua volta sostituito dall’allegato I del Regolamento Delegato (UE) 2022/127 della Commissione del 7 dicembre 2021, ha scelto tale standard per garantire la sicurezza del proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e ha comunicato la propria decisione all'AGEA Coordinamento con nota prot. 1671400 del 16.12.2005.

L'Agenzia ha certificato il proprio SGSI alla norma ISO 27001:2005, ottenendo la certificazione nel corso del 2008, successivamente rinnovata senza soluzione di continuità che ha sostituito la versione del 2005. Nel 2024 AVEPA ha iniziato il percorso per la ricertificazione secondo la norma ISO27001:2022, in applicazione della quale viene redatto il presente documento.

3. AMBITO DI APPLICAZIONE E PERIMETRO

L'ambito di applicazione comprende le attività, i processi, i servizi e le applicazioni che sono oggetto di certificazione e ai quali si applicano le regole in materia di sicurezza, così come previsto dalla norma: “L'organizzazione deve determinare i confini e l'applicabilità del Sistema di Gestione per la Sicurezza delle Informazioni per stabilirne il campo di applicazione” (rif. art. 4.3 ISO 27001:2022).

Il perimetro definisce l'ampiezza del Sistema di Gestione per la Sicurezza delle Informazioni e quindi individua i siti, le infrastrutture, ma anche determinati aspetti fisici e logici, nei confronti dei quali valgono le regole del SGSI.

L'Agenzia ha definito il **campo di applicazione** del proprio SGSI come sottoindicato:

Gestione dei servizi informativi a supporto dell'autorizzazione, dell'esecuzione e della contabilizzazione dei pagamenti alle imprese agricole.

Il **perimetro** del Sistema di Gestione per la Sicurezza delle Informazioni era rappresentato in prima battuta dalla sede centrale dell'Agenzia; nell'anno 2019, a seguito dello studio di fattibilità svolto nel 2018, il perimetro di applicazione della ISO27001:2013 è stato allargato in modo da includere, oltre che la sede centrale anche le strutture periferiche (SUA).

La società affidataria del servizio di audit per la certificazione ISO27001: 2013 ha provveduto, nel corso delle proprie verifiche, a valutare l'idoneità degli Sportelli Unici Agricoli ed ha certificato la conformità anche delle strutture periferiche dell'Agenzia alla norma ISO 27001:2013.

4. POLITICA DEL SGSI

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni dell'AVEPA consiste nel garantire un adeguato livello di sicurezza dei dati e delle informazioni, nell'ambito della gestione dei servizi informativi a supporto dell'autorizzazione, dell'esecuzione e della contabilizzazione dei pagamenti alle imprese agricole, attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali le informazioni sono soggette.

Con la presente politica, l'AVEPA intende formalizzare i seguenti obiettivi misurabili nell'ambito della sicurezza delle informazioni:

- proteggere le risorse informative dalle minacce, siano esse interne o esterne, di tipo organizzativo o tecnologico, accidentali o intenzionali, assicurando:
  - la riservatezza: proprietà per cui l'informazione non è resa disponibile o comunicata a soggetti non autorizzati;
  - l'integrità: proprietà di tutelare l'accuratezza e la completezza delle informazioni a cui l'Agenzia attribuisce un valore;
  - la disponibilità: proprietà per cui l'informazione deve essere accessibile ed utilizzabile previa richiesta da parte di un'entità autorizzata;
- promuovere la cultura della sicurezza delle informazioni, aumentando la sensibilità delle persone che prestano la loro attività in Agenzia dell'importanza del loro contributo nell'efficacia del Sistema di Gestione della Sicurezza delle Informazioni attraverso attività di formazione, costituzione di gruppi di lavoro, ecc.;
- sostenere e affiancare le indicazioni previste dalla normativa vigente in materia di privacy e tutela dei dati;
- preservare l'immagine dell'Agenzia dando garanzia ai soggetti esterni preposti al controllo sulla sua organizzazione e sul suo operato di efficienza, competenza e affidabilità e della corretta gestione dei rischi;
- integrare il Sistema di Gestione per la Sicurezza delle Informazioni nei processi dell'organizzazione e nella sua struttura generale di gestione;
- individuare i rischi e i responsabili del trattamento e gestione degli stessi;
- garantire la continuità operativa dell'Agenzia;
- attuare le opportune azioni per fronteggiare le violazioni della sicurezza ed effettuare una corretta rilevazione ed indagine;
- aumentare la collaborazione con la Regione Veneto e con le Agenzie Nazionali (ACN) per la riduzione del rischio cyber delle informazioni sui confini regionali e nazionali, anche partecipando a progetti Regionali o Nazionali orientati al rilievo e gestione delle emergenze cyber;
- portare standard elevati di gestione dei dati, anche attraverso adesione a Concessioni

Nazionali o Regionali per la migrazione a Cloud della PA Certificati o Accreditati;

- garantire la sovranità del dato;
- mantenere tutti i sistemi aggiornati con specifici piani di patching;
- eseguire una volta all’anno il Penetration Test;
- tracciare gli incident;
- fare una review annuale degli incident;
- erogare “security awareness” almeno ogni due anni;
- avere un uptime della infrastruttura di produzione almeno del 99%;
- sensibilizzazione del management e migrazione alla nuova norma ISO27001:2022.

4.1 Impegno della Direzione

Il presente documento vuole esprimere in un testo unico l'importanza che la sicurezza delle informazioni riveste per la Direzione e concretizza l'organizzazione necessaria per tutelare la confidenzialità, l'integrità e la disponibilità dei dati.

La Direzione si impegna a sviluppare, mantenere, controllare e migliorare in modo costante la sicurezza delle informazioni in conformità alla norma ISO 27001:2022 ed è consapevole che la sicurezza è un processo culturale complesso e prolungato che deve progressivamente coinvolgere tutte le risorse umane ed organizzative.

Per queste ragioni la Direzione si impegna a fornire le risorse necessarie e adeguate al Sistema di Gestione per la Sicurezza delle Informazioni, in modo che lo stesso consegua gli esiti previsti.

Al fine di coordinare le molteplici attività relative alla sicurezza delle informazioni che interessano trasversalmente tutte le unità organizzative dell'Agenzia la Dirigenza, durante le riunioni periodiche, tratta gli ambiti specifici della sicurezza, informando tutti i componenti, presenti e assenti all'incontro.

5. DEFINIZIONE GENERALE DI RUOLI E RESPONSABILITÀ

Secondo quanto disposto dall'art. 5.3 della norma ISO 27001:2022 in materia di ruoli, responsabilità e autorità all'interno dell'organizzazione, l'AVEPA individua i principali soggetti coinvolti ed i loro ruoli al fine di:

- assicurare che il SGSI sia conforme alla norma ISO 27001:2022;
- garantire che il SGSI sia efficace nel conseguire gli obiettivi;
- gestire il SGSI garantendo un miglioramento continuo dello stesso, attraverso opportune azioni di controllo e correttive;
- individuare i responsabili dei rischi relativi alla sicurezza delle informazioni;
- riferire alla Direzione in merito alle prestazioni del SGSI.

L'Agenzia deve garantire che i soggetti che svolgono attività che ricadono nell'ambito del proprio Sistema di Gestione per la Sicurezza delle Informazioni siano competenti, mettendo in atto azioni rivolte a far acquisire o incrementare la loro competenza, quali ad esempio, la formazione in materia di sicurezza, l'addestramento, l'affiancamento, la loro riallocazione, ecc.

L'art. 7.3 della norma prevede che le persone che svolgono attività che influenzano le prestazioni dell'Agenzia in materia di sicurezza delle informazioni siano consapevoli del loro contributo nel conseguire gli obiettivi stabiliti e, per contro, delle conseguenze derivanti dal non essere conformi ai requisiti del Sistema di Gestione per la Sicurezza delle Informazioni.

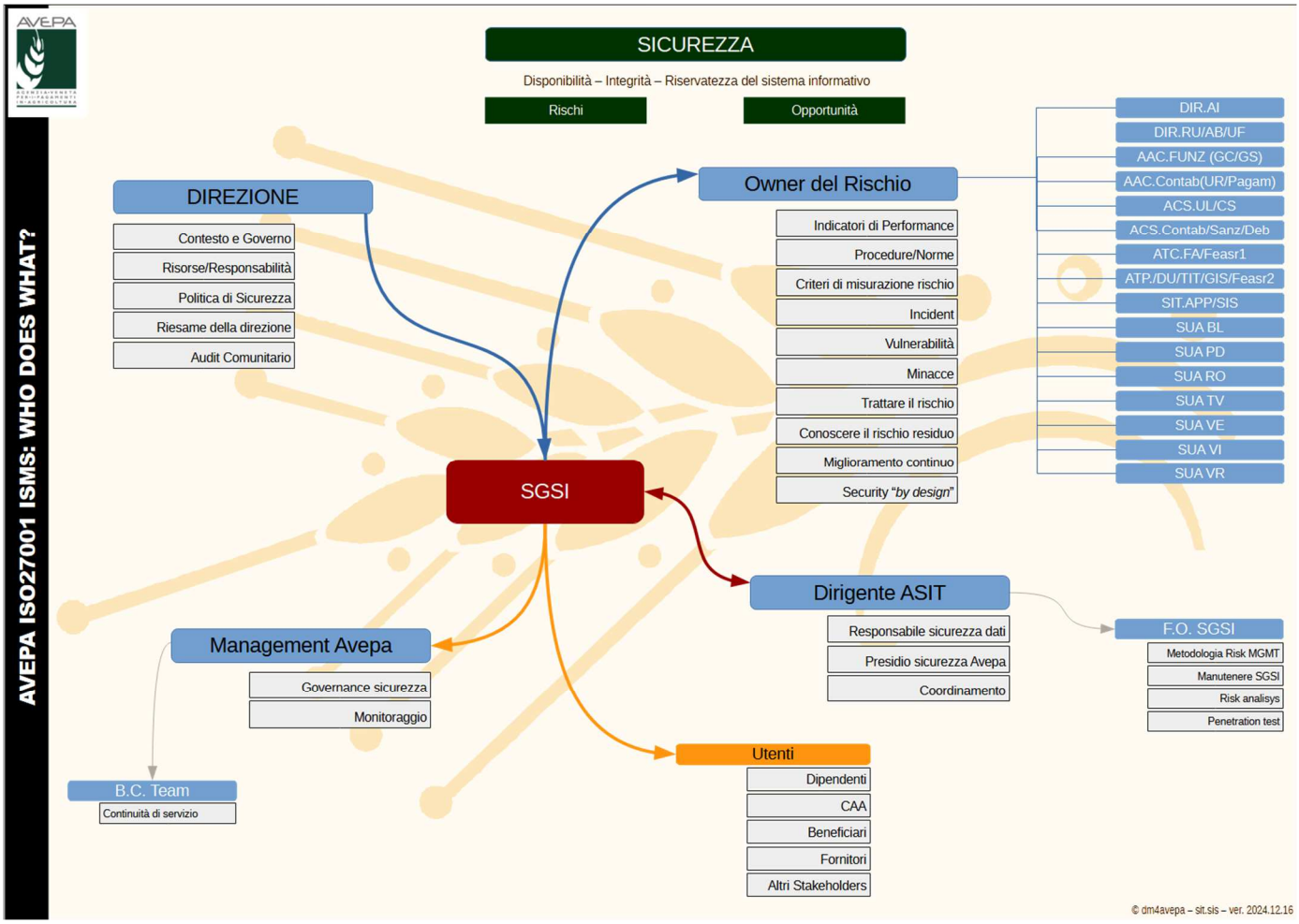

Illustrazione 1: Flusso delle responsabilità per il SGSI

5.1 La Direzione

La Direzione si impegna nello sviluppo, nella verifica dell'efficacia e nel miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni.

La Direzione è responsabile:

- del rilascio del documento contenente la politica relativa al SGSI e la definizione e dimensionamento formale dei ruoli e delle responsabilità nell'ambito del SGSI, contenuti nel documento *D1 - Contesto e Governo*;
- della definizione del "Riesame della Direzione", documento *D3 - Riesame della Direzione*;
- di fornire le risorse necessarie ed adeguate al Sistema di Gestione per la Sicurezza delle Informazioni.

5.1.1 Riesame della Direzione

Il Riesame della Direzione consiste nell'attività di verifica del SGSI al fine di assicurare l'idoneità alla norma, l'adeguatezza e l'efficacia dello stesso. Il Riesame, che deve essere eseguito almeno una volta l'anno, è disciplinato dall'art. 9.3 della norma ISO 27001:2022 il quale prevede che lo stesso debba includere considerazioni su:

- lo stato delle azioni derivanti dai precedenti riesami della Direzione;
- i cambiamenti dei fattori esterni e interni che possono avere attinenza con il Sistema di Gestione per la Sicurezza delle Informazioni;
- le informazioni di ritorno sulle prestazioni relative alla sicurezza delle informazioni, compresi:
    - le non conformità e azioni correttive;
    - i risultati del monitoraggio e della misurazione (indicatori di performance su SGSI);
    - i risultati degli audit (interni ed esterni);
    - il raggiungimento degli obiettivi per la sicurezza delle informazioni;
    - le informazioni di ritorno dalle parti interessate;
    - i risultati della valutazione del rischio e lo stato del piano di trattamento del rischio;
    - le opportunità per il miglioramento continuo.

Gli elementi in uscita dal riesame della Direzione devono comprendere le decisioni relative alle opportunità per il miglioramento continuo e ogni necessità di modifiche al Sistema di Gestione per la Sicurezza delle Informazioni.

Il Riesame della Direzione è approvato dal legale rappresentante dell'AVEPA e presentato alla Dirigenza.

5.2 Gestione del SGSI

Il raggruppamento di risorse omogenee definito come “Area” nell'AVEPA costituisce la macrostruttura di massimo livello ed è posta a governo dei settori e delle elevate qualificazioni.

Le Aree sono individuate in base a grandi tipologie di intervento che si distinguono nell'ambito dell'azione istituzionale dell'Agenzia. Ogni Area dispone di un elevato grado di autonomia progettuale ed operativa nell'ambito degli indirizzi impartiti dalla Direzione. Le Aree sono affidate alla responsabilità di un Dirigente, il quale ha il compito di pianificare e coordinare le attività operative della propria area.

In posizione gerarchicamente subordinata rispetto all’Area si situa il “Settore”, nel cui ambito ogni dirigente è dotato di autonomia e programma le attività di competenza gestendo le risorse umane, i procedimenti ed ogni altra azione delle strutture organizzative cui sono preposti.

Al fine di coordinare le molteplici attività relative alla sicurezza delle informazioni che interessano trasversalmente tutte le unità organizzative dell'Agenzia la Dirigenza, in sede di riunione periodica convocata per attività istituzionali, pone all’ordine del giorno anche temi di sicurezza in relazione ai quali:

- ratifica gli obiettivi di controllo applicati al SGSI;

- riesamina il SGSI al fine di verificare la sua adeguatezza ed efficacia, nonché le possibilità di miglioramento e implementazione;
- definisce i criteri per l'accettazione dei rischi e i livelli di rischio accettabili;
- supporta fattivamente la Direzione nella stesura del Riesame della Direzione;
- è informata sui risultati del Vulnerability Assessment compiuto;
- monitora l'applicazione del piano di trattamento dei rischi;
- armonizza le differenti azioni in ambito di sicurezza.

Ogni dirigente, per l'ambito di cui è responsabile:

- promuove la cultura della sicurezza delle informazioni nei confronti dei propri collaboratori;
- vigila sul rispetto delle norme e delle procedure stabilite a tale fine;
- assicura l'integrazione dei requisiti del SGSI nei propri processi interni;
- comunica alla Direzione obiettivi e priorità di sicurezza per la propria Area;
- promuove il miglioramento continuo del SGSI attraverso azioni di controllo e correttive.

Alcuni **Dirigenti (sia della sede centrale che delle strutture periferiche) sono *owner* dei rischi** relativi alla sicurezza delle informazioni per i contenitori loro assegnati dalla Direzione. Per il proprio contenitore ogni owner:

- raccoglie i suggerimenti provenienti dal Responsabile per la Sicurezza delle Informazioni;
- compila la matrice di rischio e la invia al RSI accettando i rischi residui;
- definisce e presidia l'applicazione del proprio piano di trattamento dei rischi, comunicandone lo stato al RSI;
- stabilisce e monitora gli indicatori di performance per la valutazione dell'efficacia del SGSI;
- definisce e divulga norme e procedure utili alla mitigazione del rischio;
- monitora e valuta gli incident di sicurezza;
- applica il principio “security by design” ai propri progetti ed attività;
- consulta il Responsabile per la Sicurezza delle Informazioni ad ogni cambiamento significativo, o per l’introduzione di nuove prassi che impattano sulla sicurezza delle informazioni;
- promuove e favorisce la formazione dei propri dipendenti, in particolare quella rivota all’uso dei gestionali e alla loro sicurezza.

5.2.1 Business Continuity Team

Al fine di garantire la continuità operativa in caso di evento dannoso che comprometta l'operatività dell'Agenzia è stato costituito un Business Continuity Team composto da alcuni dirigenti dell'AVEPA, le cui competenze sono elencate nel documento relativo alla continuità operativa ed al quale si rimanda per approfondimenti.

5.3 Dirigenti Area Servizi Information technology

5.3.1 Dirigente Area Servizi IT

Il **Dirigente dell'Area Servizi IT** è titolare, tra le altre, della funzione di responsabile per la sicurezza delle informazioni. Si tratta della figura di riferimento per il mantenimento e l'implementazione di un elevato livello di sicurezza delle informazioni, in particolare attraverso la verifica della corretta implementazione della politica e delle procedure relative alla sicurezza dei dati e la prevenzione di possibili incidenti al sistema informatico/informativo dell'Agenzia.

La responsabilità può essere delegata dal Dirigente ad altra persona ritenuta idonea attraverso opportuna formalizzazione e comunicazione.

5.3.2 Dirigente del Settore sistemi e sicurezza IT

Al **Dirigente del Settore sistemi e sicurezza IT**, in capo al quale è stata posta la Funzione operativa Sistema di Gestione per la Sicurezza delle Informazioni, è attribuita la responsabilità di coordinare le azioni relative alla gestione del SGSI in attuazione degli obiettivi e piani definiti dall'ente. Tra i compiti di questo Dirigente vi sono quelli relativi all'adozione della documentazione del SGSI, ad eccezione di quanto di competenza della Direzione. Il dirigente è anche il Responsabile per la sicurezza delle informazioni.

5.3.3 Funzione operativa SGSI

La **Funzione operativa Sistema di Gestione per la Sicurezza delle Informazioni** è composta da referenti tecnici a supporto del "Responsabile per la Sicurezza delle Informazioni". I referenti della funzione devono risultare competenti ed affidabili nel presidio della sicurezza dei dati.

La FO SGSI:

- coordina ed armonizza le attività necessarie per il mantenimento della certificazione del Sistema di Gestione per la Sicurezza delle Informazioni alla norma ISO 27001:2022;
- collabora con l'Organismo di certificazione durante gli audit periodici di rinnovo e sorveglianza;
- suggerisce miglioramenti pratici per ridurre il rischio collegato alla sicurezza dei dati, verifica le vulnerabilità dell'AVEPA, analizza il rischio e lo comunica al Responsabile per la sicurezza delle informazioni e/o agli owner responsabili;
- costituisce un punto di supporto per la corretta comprensione degli strumenti di misurazione dei rischi, verifica la corretta compilazione della documentazione in tema di sicurezza redatta dagli Owner dei rischi, promuove la diffusione delle migliori pratiche da applicare;
- favorisce la conoscenza dei principi di base e delle disposizioni da osservare raccoglie le informazioni provenienti da Vulnerability Assessment;
- mantiene elevata la sensibilità nei temi di sicurezza.

5.4 Contenitori, requisiti di sicurezza, owner del rischio

La norma ISO 27001 prevede l'individuazione dei risk owner: persone o entità che hanno la responsabilità e l'autorità per gestire i rischi. Le Aree, così come definite, possono contenere al loro interno diversi contenitori rilevanti che fanno capo ad un medesimo owner. Per consentire una più coerente gestione all'interno della stessa Area, ogni owner del rischio individua un unico referente di Area con il compito di coordinare le attività relative alla gestione della sicurezza delle informazioni e di rapportarsi con l'Area servizi IT per gli adempimenti di competenza.

Per la gestione puntuale della sicurezza si individuano i seguenti contenitori rilevanti nel sistema informativo dell'Agenzia.

5.4.1 Direzione

Presidia la documentazione (materiale o immateriale), la comunicazione, le pubblicazioni all'albo on line e gli affari istituzionali.

- Owner: Dirigente Settore Affari istituzionali (Marco Passadore).
- Comprende: Docway, Sportello Automatico, Bridge, intranet, AVEPA on line.
- Descrizione: questo contenitore include le applicazioni web per la gestione del protocollo informatico (incluso lo Sportello Automatico e Bridge), del portale web istituzionale dell'AVEPA, il controllo sulle credenziali di accesso alla rete rilasciate agli esterni, la intranet aziendale (in dismissione) e il sito SharePoint AVEPA on line. Gestisce anche il ciclo di vita della documentazione.

5.4.2 AAC.RU/AB/UF

È un contenitore collocato nell'Area Amministrazione e contabilità (AAC) che presidia la gestione delle Risorse Umane (RU), le Abilitazioni Badge (AB) e l'Ufficio Formazione (UF).

- Owner: Dirigente Settore Sviluppo risorse umane (Chiara Contin).
- Comprende: gestione del personale, abilitazioni badge, portale H3, dati dei cronotimbratori, sicurezza fisica e formazione.
- Descrizione: questo contenitore include tutti gli strumenti per la gestione del personale, comprende anche la gestione dell'accesso fisico alle sedi e la gestione della sicurezza fisica (safety). Il Settore, gestisce le attività di smart working, "lavoro agile", e si occupa della definizione del Piano organizzativo del lavoro agile (POLA), un piano che individua le modalità attuative del lavoro agile per le attività che possono essere svolte in tale modalità e definisce le misure organizzative, i requisiti tecnologici, i percorsi formativi del personale, anche dirigenziale, e gli strumenti di rilevazione e di verifica periodica dei risultati conseguiti, anche in termini di miglioramento dell'efficacia e dell'efficienza dell'azione amministrativa, della digitalizzazione dei processi, nonché della qualità dei servizi erogati. Il contenitore include, inoltre, le attività di formazione del personale e di alcuni stakeholder (CAA).

5.4.3 AAC.Funzionamento (GC/GS)

È un contenitore collocato nell'Area amministrazione e contabilità (AAC) che presidia l'ufficio Gare e Contratti (GC) e l'ufficio Gestione Sedi (GS).

- Owner: Dirigente Settore funzionamento (Chiara Contin).

- Comprende: Ragioneria Generale, le sedi dell'Agenzia e le attrezzature, la gestione dei contratti che l'AVEPA stipula (comprendendo anche Office365), la definizione delle politiche di accesso fisico.
- Descrizione: contiene tutti gli strumenti materiali ed immateriali inventariati e/o acquistati dall'Agenzia, comprendendo anche le risorse necessarie per la gestione dell'intero ciclo di vita di tali beni. Sono qui compresi: contratti con i fornitori, sedi, manutenzioni sedi, hardware e software acquisti (esclusi i software di core).

5.4.4 AAC.Contab (UR/Pagam)

È un contenitore collocato nell'Area amministrazione e contabilità (AAC) che presidia la ragioneria generale (Ragioneria) e i Pagamenti (Pagamenti OP).

- Owner: Dirigente Settore contabilità (Chiara Contin).
- Comprende: Ragioneria generale e pagamenti dell'AVEPA.
- Descrizione: questo contenitore gestisce la ragioneria generale dell'ente e i servizi di pagamento e incassi dell'OP.

5.4.5 ACS.UL.CS

È un contenitore collocato nell'Area controllo strategico, contabilizzazione e recupero crediti (ACS) che assicura supporto all'assistenza legale dell'Agenzia (Ufficio supporto giuridico UL) e il controllo strategico dell'ente (CS).

- Owner: Dirigente Area controllo strategico, contabilizzazione e recupero crediti (Marco Passadore).
- Comprende: assistenza legale (l'applicativo ufficio legale) e controllo strategico (estrazione dati e impostazione materie applicativo H3).
- Descrizione: questo contenitore include l'attività stragiudiziale e preparazione delle pratiche di contenzioso, supporto giuridico attraverso la formulazione di pareri, rapporti con gli organi inquirenti. Include altresì il controllo strategico dell'ente, ossia le attività inerenti all'integrità dell'AVEPA (trasparenza, antifrode, anticorruzione e antiriciclaggio), il controllo di gestione (piano della performance e valutazione del personale), le procedure relative all'irrogazione delle sanzioni.

5.4.6 ACS.ContabOP/Sanz/DebOP

È un contenitore collocato nell'Area controllo strategico, contabilizzazione e recupero crediti (ACS) che presidia la contabilità (contabOP), le Sanzioni (Sanzioni) e i Debiti dell'organismo pagatore (DebOP).

- Owner: Dirigente Area controllo strategico, contabilizzazione e recupero crediti (Marco Passadore).
- Comprende: registrazione e rendicontazione delle operazioni contabili dell'OP, irrogazione sanzioni, irregolarità e recupero crediti OP.
- Descrizione: questo contenitore include tutti gli strumenti per la gestione della contabilità dell'OP, sanzioni dell'OP e il registro debitori dell'OP.

5.4.7 ATC.FA/FEASRnoSIGC

È un contenitore collocato nell'Area tecnica competitività imprese (ATC) che presidia il Fascicolo Aziendale (FA), le domande di aiuto e di pagamento delle misure del PSR non connesse alle superfici né agli animali (FEASR no SIGC) e le attività delegate.

- Owner: Dirigente Area tecnica competitività imprese (Luca Furegon).
- Comprende: fascicolo, calamità naturali (Calnat), rapporti con i CAA, patentino Agricoltore (IAP), Banca della terra, AvepaMobile, Webservices verso l'esterno, domande di aiuto e di pagamento delle misure del PSR non connesse alle superfici né agli animali.
- Descrizione: questo contenitore raccoglie le informazioni sullo stato delle aziende dei beneficiari (anagrafiche, camerali, territoriali), le domande di aiuto e di pagamento delle misure del PSR non connesse alle superfici né agli animali, le domande relative ad attività delegate dalla Regione del Veneto.

5.4.8 ATP.FEASR SIGC/DU/TIT/GIS

È un contenitore collocato nell'Area tecnica pagamenti diretti (ATP) che presidia le domande di aiuto e di pagamento delle misure del PSR connesse alle superfici e agli animali (FEASR SIGC), le domande uniche (DU), la gestione dei titoli, il GIS aziendale (GIS).

- Owner: Dirigente Area tecnica pagamenti diretti (Alessandro Rama).
- Comprende: GIS aziendale, domanda unica, App condizionalità, AvepaImage, gestione titoli, domande di aiuto e di pagamento delle misure del PSR connesse alle superfici e agli animali.
- Descrizione: questo contenitore raccoglie le informazioni necessarie per le domande di aiuto e/o di pagamento delle misure del PSR connesse alle superfici e agli animali, per le domande uniche, per la gestione dei titoli, per la condizionalità e per il regime di produzione biologica.

5.4.9 SIT.APP.SIS

È un contenitore collocato nell'Area servizi IT (SIT) che presidia lo sviluppo applicativo (APP) e i sistemi e la sicurezza IT (SIS).

- Owner: Dirigente Area servizi IT (Fabio Binotto).
- Comprende: sviluppo applicativo, applicazioni Mission Critical, Back office applications: Gestione richieste, sviluppo app mobile; Identity / Rule Management: GUARD, SSO, CAS, WSO2; governance sistemi, datacenter, connettività, datawarehowse, ftp, cartelle condivise locali, Postazioni di Lavoro.
- Descrizione: questo contenitore gestisce l'autenticazione e profilazione agli applicativi mission critical dell'Agenzia, le applicazioni necessarie per le attività di change management, le estrazioni di dati, le applicazioni di business, lo sviluppo applicativo. Include inoltre i sistemi e la loro governance, le applicazioni, i tool per il datawarehouse, la connettività, le configurazioni delle postazioni di lavoro, ovvero il patching, protezione, amministrazione remota, software installabile.

5.4.10 AIT.CT

È un contenitore collocato nell'Area Integrazione territoriale e supporto alla Direzione (AIT) che presidia il coordinamento in materia di procedure di controllo su tematiche amministrative comuni ai diversi settori di intervento dell'Agenzia (es. Appalti, Aiuti di Stato, Antimafia, etc.).

- Owner: Dirigente Area Integrazione territoriale (Gianluca Bevilacqua).
- Comprende: controlli sul casellario giudiziale, procedure e controlli sugli appalti, sugli aiuti di stato, sulle verifiche antimafia.
- Descrizione: questo contenitore assicura l'aggiornamento delle procedure, dei Manuali e dei flussi operativi riguardanti le materie di competenza, il coordinamento delle strutture tecniche dell'Agenzia in materia di procedure di controllo su tematiche amministrative comuni ai diversi settori di intervento dell'Agenzia (es. Appalti, Aiuti di Stato, Antimafia, etc.) e il relativo aggiornamento normativo. Predisporne ed aggiorna la manualistica, le procedure e la documentazione di controllo su tali tematiche provvedendo anche alla relativa diffusione e alla formazione del personale addetto.

5.5 Ufficio Audit comunitario

L'Agenzia si è dotata di un servizio di controllo interno, denominato ufficio Audit comunitario, che si trova in una posizione indipendente rispetto alle altre strutture dell'Agenzia in quanto incardinato all'interno della Direzione, cui è tenuto a riferire l'esito dei controlli svolti. Secondo quanto previsto dalla norma ISO 27001:2022, l'ufficio Audit comunitario conduce ad intervalli regolari degli audit interni relativamente al Sistema di Gestione per la Sicurezza delle Informazioni, al fine di verificare se questo sia:

- conforme ai requisiti della norma ISO 27001:2022 e alle leggi e regolamenti in materia di sicurezza dei dati;
- conforme ai requisiti identificati per la sicurezza delle informazioni;
- efficacemente realizzato, mantenuto e aggiornato;
- efficace nel conseguire gli obiettivi.

L'art. 9.2 della norma ISO 27001:2022 stabilisce, inoltre, che l'organizzazione deve:

- pianificare, stabilire, attuare e mantenere uno o più programmi di audit, comprensivi di frequenze, metodi, responsabilità, requisiti di pianificazione e reporting. I programmi di audit devono prendere in considerazione l'importanza dei processi coinvolti e i risultati di audit precedenti;
- definire i criteri di audit e il campo di applicazione per ciascun audit;
- selezionare gli auditor e condurre gli audit in modo da assicurare l'obiettività e l'imparzialità del processo di audit;
- assicurare che i risultati degli audit siano riportati ai pertinenti responsabili;
- conservare informazioni documentate quale evidenza dell'attuazione del programma di audit e dei risultati di audit.

La realizzazione degli audit viene pianificata all'interno del Piano di audit quinquennale e del Piano delle attività, che prevedono l'attuazione di almeno un intervento di audit sul Sistema di Gestione per la Sicurezza delle Informazioni nell'arco dell'anno. Le attività di audit seguono quanto prescritto dal “Manuale delle attività di audit” relativamente alla conduzione degli interventi di audit ed in particolare per gli interventi di audit IT, esplicitata in una sezione dedicata. L'attività si svolge conformemente ai criteri accettati a livello internazionale e viene registrata in documenti di lavoro.

5.6 Responsabilità degli utenti

Gli utenti, cioè il personale dell'AVEPA che quotidianamente accede al sistema informatico e gli utenti esterni che si collegano ai sistemi dell'Agenzia, sono tenuti a:

- consultare, conoscere e rispettare le indicazioni contenute nella documentazione presente nella sezione dedicata al SGSI nella Intranet aziendale, in particolare il documento "N1 Norme utilizzo strumenti informatici", il quale, oltre a contenere i principi per l'idoneo utilizzo delle risorse informatiche e telematiche dell'Agenzia, descrive compiutamente i corretti comportamenti per ottemperare alle disposizioni sulla qualità e sicurezza;
- consultare, conoscere e rispettare le prescrizioni sull’utilizzo delle risorse informatiche contenute nel codice di comportamento adottato dall’AVEPA;
- seguire le indicazioni periodiche sulle buone pratiche come comunicate dal responsabile della sicurezza delle informazioni (o suoi collaboratori) o ricevute dai corsi di formazione e riportate dai dirigenti responsabili dei singoli uffici ai propri collaboratori;
- segnalare al proprio Dirigente, al Dirigente dell'Area servizi IT o al Responsabile della sicurezza informatica (anche tramite il Form disponibile in intranet nella sezione SGSI), ogni violazione delle misure di sicurezza di cui vengano a conoscenza;
- partecipare ai corsi di formazione e sensibilizzazione e attivamente al presidio della sicurezza sulla propria Postazione di Lavoro.

6. POLITICHE PER LA MISURAZIONE DEI RISCHI

Il Responsabile per la sicurezza delle informazioni e la Funzione operativa SGSI hanno adottato una metodologia di analisi del rischio che ha portato alla definizione, nel 2018, di uno strumento per la pesatura del rischio, formalizzato e presentato agli owners, e provvedono a mantenerlo costantemente aggiornato.

7. REVISIONI

Il presente documento è soggetto a revisione in occasione di significative modifiche organizzative e tecnologiche rilevanti per la gestione delle informazioni. Il capitolo relativo a ruoli e responsabilità deve essere esaminato ad ogni rilevante cambiamento avvenuto nell'organizzazione dell'Agenzia.